Dr. Sayid Muhammad Rifqi Noval, S.H., M.H.
Soecipto, S.T., M.H.
Ahmad Jamaludin, S.H., M.H.

PERLINDUNGAN HAK DIGITAL

Ancaman Privasi di Tengah Serangan *Social Engineering*

PERLINDUNGAN HAK DIGITAL

Ancaman Privasi di Tengah Serangan *Social Engineering*

PERLINDUNGAN HAK DIGITAL

Ancaman Privasi di Tengah Serangan *Social Engineering*

Dr. Sayid Muhammad Rifqi Noval, S.H., M.H.
Soecipto, S.T., M.H.
Ahmad Jamaludin, S.H., M.H.

RAJAWALI PERS
Divisi Buku Perguruan Tinggi
PT RajaGrafindo Persada
D E P O K

Perpustakaan Nasional: Katalog dalam terbitan (KDT)

Sayid Muhammad Rifqi Noval, Soecipto, dan Ahmad Jamaludin.

Perlindungan Hak Digital: Ancaman Privasi di Tengah Serangan *Social Engineering*/
Sayid Muhammad Rifqi Noval, Soecipto, dan Ahmad Jamaludin
—Ed. 1—Cet. 1.—Depok: Rajawali Pers, 2022.
xx, 232 hlm., 23 cm
Bibliografi: hlm. 191
ISBN 978-623-372-593-4

2022.3628 RAJ
Dr. Sayid Muhammad Rifqi Noval, S.H., M.H.
Soecipto, S.T., M.H.
Ahmad Jamaludin, S.H., M.H.
PERLINDUNGAN HAK DIGITAL
Ancaman Privasi di Tengah Serangan Social Engineering

Cetakan ke-1, September 2022

Hak penerbitan pada PT RajaGrafindo Persada, Depok

Editor : Indi Vidyafi
Setter : Jaenudin
Desain Cover : Tim Kreatif RGP

Dicetak di Rajawali Printing

PT RAJAGRAFINDO PERSADA

Anggota IKAPI

Kantor Pusat:
Jl. Raya Leuwinanggung, No.112, Kel. Leuwinanggung, Kec. Tapos, Kota Depok 16456
Telepon : (021) 84311162
E-mail : rajapers@rajagrafindo.co.id http: //www.rajagrafindo.co.id

Perwakilan:

Jakarta-16456 Jl. Raya Leuwinanggung No. 112, Kel. Leuwinanggung, Kec. Tapos, Depok, Telp. (021) 84311162. **Bandung**-40243, Jl. H. Kurdi Timur No. 8 Komplek Kurdi, Telp. 022-5206202. **Yogyakarta**-Perum. Pondok Soragan Indah Blok A1, Jl. Soragan, Ngestiharjo, Kasihan, Bantul, Telp. 0274-625093. **Surabaya**-60118, Jl. Rungkut Harapan Blok A No. 09, Telp. 031-8700819. **Palembang**-30137, Jl. Macan Kumbang III No. 10/4459 RT 78 Kel. Demang Lebar Daun, Telp. 0711-445062. **Pekanbaru**-28294, Perum De' Diandra Land Blok C 1 No. 1, Jl. Kartama Marpoyan Damai, Telp. 0761-65807. **Medan**-20144, Jl. Eka Rasmi Gg. Eka Rossa No. 3A Blok A Komplek Johor Residence Kec. Medan Johor, Telp. 061-7871546. **Makassar**-90221, Jl. Sultan Alauddin Komp. Bumi Permata Hijau Bumi 14 Blok A14 No. 3, Telp. 0411-861618. **Banjarmasin**-70114, Jl. Bali No. 31 Rt 05, Telp. 0511-3352060. **Bali**, Jl. Imam Bonjol Gg 100/V No. 2, Denpasar Telp. (0361) 8607995. **Bandar Lampung**-35115, Perum. Bilabong Jaya Block B8 No. 3 Susunan Baru, Langkapura, Hp. 081299047094.

PRAKATA

Alhamdulillah. Tiada kata yang patut terucap selain ungkapan puji dan syukur kehadirat Allah Swt., karena dengan hidayah dan kuasa-Nya mengizinkan tim penulis untuk menyelesaikan buku ini dalam keadaan sehat walafiat. Buku ini merupakan salah satu luaran penelitian Hibah Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi, Direktorat Jenderal Pendidikan Tinggi, Riset, dan Teknologi dalam skema Penelitian Dasar Perguruan Tinggi (PDUPT) pada tahun 2022 dengan judul *Model Perlindungan Hukum Korban Kebocoran Data Pribadi Melalui Serangan Social Engineering di Era Digital Ekonomi*.

Tim penulis diketuai oleh Dr. Sayid Muhammad Rifqi Noval, S.H., M.H. dengan anggota Ir. Soecipto, M.H. dan Ahmad Jamaludin, S.H., M.H. Buku ini menjadi seri kedua buku ketua tim penulis yang membahas mengenai hak-hak digital, setelah sebelumnya mengulas perihal *right on online safety* dengan titik fokus *cyberbullying* dan diterbitkan pada tahun 2021. Dalam buku ini tim penulis akan melakukan pembahasan terkait dengan hak privasi dan memfokuskan kajian terhadap pelanggaran data yang terjadi melalui serangan *social engineering*.

Tim penulis menyadari bahwa dalam proses penyelesaian buku ini, tentu tidak terlepas dari segala bantuan, dukungan, dan bimbingan dari berbagai pihak yang terlibat. Untuk itu, dengan segala kerendahan hati, tim penulis menghaturkan ucapan terima kasih. Kepada yang terhormat:

1. Pimpinan Universitas Islam Nusantara;
2. Pimpinan Fakultas Hukum dan Teknik Universitas Islam Nusantara;
3. Kepala Lembaga Penelitian dan Pengabdian Kepada Masyarakat Universitas Islam Nusantara;
4. Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi;
5. Direktorat Jenderal Pendidikan Tinggi, Riset, dan Teknologi;
6. Yayasan Assalaam Bandung;
7. Penerbit RajaGrafindo Persada;
8. Keluarga Besar Tim Penulis.

Bagi para pembaca, saran dan kritik yang membangun selalu tim penulis harapkan untuk perbaikan berikutnya karena kehadiran buku ini masih jauh dari harapan dan kesempurnaan. Akhirnya, hanya kepada Allah jualah kita berserah diri yang disertai doa, semoga Allah Swt. selalu menyertai dalam setiap derap langkah kita. *Aamiin*.

Bandung, 2022

Tim Penulis

SAMBUTAN

Puji dan syukur kami panjatkan kehadirat Allah Swt., karena atas berkat, rahmat, dan karunia-Nya, buku *Perlindungan Hak Digital: Ancaman Privasi di Tengah Serangan Social Engineering* dapat diterbitkan. Buku ini disusun untuk luaran penelitian hibah Kementerian Pendidikan, Kebudayaan, Riset dan Teknologi dengan fokus kajian terkait hak privasi dan pelanggaran data yang terjadi melalui serangan *social engineering*.

Di era digital ini, tidak dapat dipungkiri bahwa manusia tidak dapat menjalani hidup tanpa pemanfaatan dari teknologi informasi yang sudah semakin canggih. Teknologi informasi telah mengubah pola hidup masyarakat dan menyebabkan perubahan sosial budaya, ekonomi, dan kerangka hukum yang berlangsung dengan signifikan. Banyak pula kemudahan yang turut dirasakan dengan hadirnya teknologi informasi, termasuk kemudahan dalam mengakses data. Namun, dari berbagai kemudahan yang dirasakan, tersisip pula ancaman *social engineering* yang turut mengancam hak privasi setiap penggunanya.

Melalui buku ini, Anda dapat mengetahui tentang pemanfaatan teknologi digital dan serangan siber yang perlu diwaspadai. Buku ini dikemas secara apik dan padat agar dapat menuntun masyarakat

untuk lebih terbuka dan waspada dalam pemanfaatan teknologi digital.

Akhir kata tetaplah menjadi penerang dalam pengetahuan. Tetaplah menjadi katalisator dalam mengembangkan dan mentransformasi ilmu pengetahuan.

Dr. M. Samsuri, S.Pd., M.T.

Kepala LLDIKTI Wilayah IV Jawa Barat-Banten

[Halaman ini sengaja dikosongkan]

DAFTAR ISI

DAFTAR TABEL

[Halaman ini sengaja dikosongkan]

DAFTAR GAMBAR

DAFTAR SINGKATAN

1.	2FA	: *2 (Two) Factor Authentication*
2.	ACT	: *Association for Competitive Technology*
3.	AFF	: *Advance Fee Fraud*
4.	AI	: *Artificial Intelligence*
5.	AOL	: *America Online*
6.	AP	: *Access Point*
7.	APWG	: *Anti Phishing Working Group*
8.	ATM	: Anjungan Tunai Mandiri
9.	BBB	: *Better Business Bureau*
10.	BCA	: Bank Central Asia
11.	BCI	: *Brain Computers Interface*
12.	BEC	: *Business Email Compromise*
13.	BHO	: *Browse Helper Object*
14.	BitB	: *Browser-in-the-Browser*
15.	BOA	: *Bank of America*
16.	BPD	: Bank Pembangunan Daerah
17.	BRI	: Bank Rakyat Indonesia
18.	BNI	: Bank Negara Indonesia

19. BSSN : Badan Siber dan Sandi Negara
20. CAC : *Cyberspace Administration of China*
21. CC : *Cloud Computing*
22. CCTV : *Closed Circuit Television*
23. CEO : *Chief Executive Officer*
24. CFO : *Chief Financial Officer*
25. CIA : *Central Intelligence Agency*
26. CISA : *Cybersecurity & Infrastructure Security Agency*
27. CPI : *Corruption Perception Index*
28. CS : *Customer Service*
29. CSS : *Cascading Style Sheets*
30. DBIR : *Data Breach Investigation Report*
31. DOI : *Digital Object Identifier*
32. DoS : *Denial of Service*
33. DDos : *Distributed Denial of Service*
34. DFA : *Department of Foreign Affairs*
35. DRM : *Digital Right Management*
36. DM : *Direct Message*
37. DNS : *Domain Name System*
38. EAC : *Email Account Compromise*
39. EFCC : *Economic and Financial Crimes Commission*
40. ENISA : *European Union Agency for Cybersecurity*
41. EU : *European Union*
42. FACT : *Federation Against Copyright Theft*
43. FBI : *Federal Bureau of Investigation*
44. FDIC : *Federal Deposit Insurance Corporation*
45. FTC : *Federal Trade Commission*
46. GB : *Giga Byte*
47. GDPR : *General Data Protection Regulation*
48. GM : *General Motors*
49. HAM : Hak Asasi Manusia

50. HTML : *Hyper Text Markup Language*
51. HRE : *Human Rights Education*
52. ICPC : *Independent Corrupt Practices and Other Related Offences Commission*
53. IGI : *Investigative Group International*
54. IP Address : *Internet Protocol Address*
55. ISTR : *Internet Security Threat Report*
56. KK : Kartu Keluarga
57. KPAI : Komisi Perlindungan Anak Indonesia
58. KPU : Komisi Pemilihan Umum
59. KTP : Kartu Tanda Penduduk
60. KUHP : Kitab Undang-Undang Hukum Pidana
61. ML : *Machine Learning*
62. NFT : *Non Fungible Token*
63. NIK : Nomor Induk Kependudukan
64. NPWP : Nomor Pokok Wajib Pajak
65. OTP : *One Time Password*
66. OS : *Operating System*
67. OSINT : *Open Source Intelligence*
68. PBB : Perserikatan Bangsa-Bangsa
69. PC : *Personal Computer*
70. PDF : *Portable Document Format*
71. PIN : *Personal Identification Number*
72. PPATK : Pusat Pelaporan dan Analisis Transaksi Keuangan
73. RAR : *Roshal Archive*
74. RAT : *Routine Activity Theory*
75. RDP : *Remote Desktop Protocol*
76. RUU : Rancangan Undang-Undang
77. SARS : *Special Anti-Robbery Squads*
78. SE : *Social Engineering*
79. SIM : Surat Ijin Mengemudi

80. SIM Card : *Subscriber Identity Module Card*
81. SIR : *Security Intelligence Report*
82. SKCK : Surat Keterangan Catatan Kepolisian
83. SSL : *Secure Sockets Layer*
84. SM : Sebelum Masehi
85. SMS : *Short Message Service*
86. SMSC : *Short Message Service Center*
87. Spam : *Sending and Posting Advertisement in Mass*
88. SSO : *Single Sign On*
89. SQL : *Structured Query Language*
90. TLD : *Top Level Domain*
91. UE : Uni Eropa
92. UKM : Usaha Kecil dan Menengah
93. UN : *United Nations*
94. URL : *Uniform Resource Locators*
95. USB : *Universal Serial Bus*
96. US-CERT : *United States Computer Emergency Readiness Team*
97. UU ITE : Undang-Undang Informasi dan Transaksi Elektronik
98. *QR Code* : Quick Response Code
99. VNC : *Virtual Network Computing*
100. VoIP : *Voice Over Internet Protocol*
101. VP : *Vice President*
102. VPN : *Virtual Private Network*
103. WA : *WhatsApp*
104. WHO : *World Health Organization*

PETUNJUK PENGGUNAAN *QR CODE*

Kode QR memberikan akses cepat menuju situs web tanpa perlu mengetik atau mengingat alamat web. Terdapat beberapa *QR code* guna melengkapi dan menunjang kelengkapan informasi dalam buku ini.

Pengguna Apple

Anda dapat menggunakan aplikasi kamera di iPhone, iPad, untuk memindai kode QR. Cara memindai kode QR:

1. Buka aplikasi kamera dari layar utama, pusat kontrol, atau layar terkunci.
2. Pilih kamera belakang. Pegang perangkat sehingga kode QR muncul di jendela bidik dalam aplikasi kamera. Perangkat Anda akan mengenali kode QR dan menampilkan pemberitahuan.
3. Ketuk pemberitahuan untuk membuka tautan yang terhubung dengan kode QR tersebut.

Pengguna Android

1. Buka aplikasi *browser* di *smartphone* Anda, kemudian buka situs web QR (https://webqr.com/). Kemudian aktifkan fitur kamera dengan ketuk *allow*.
2. Lalu Anda dapat arahkan kamera pada situs web QR kepada *barcode* atau *QR code* yang hendak Anda pindai.

[Halaman ini sengaja dikosongkan]

BAB 1
PENDAHULUAN

Sukar rasanya bila saat ini, kita memutuskan untuk dapat menjalani hidup dengan tanpa memanfaatkan teknologi internet. Pencarian informasi melalui ponsel, menikmati tayangan Netflix ataupun YouTube, hingga pemesanan makanan melalui aplikasi Gojek seolah menjadi salah satu rutinitas sebagian masyarakat saat ini. Manfaat internet pada akhirnya telah mulai dirasakan, tetapi tentu turut tersisip ancaman yang sesungguhnya membayangi setiap penggunaannya. Tingginya pemanfaatan teknologi dalam transaksi ekonomi masyarakat saat ini, yang dapat terlihat dari 25,8% populasi dunia telah menggunakan *internet banking* dalam bertransaksi,[1] sebaiknya diiringi dengan instrumen hukum yang memberikan rasa aman dalam setiap aktivitasnya, terutama dari besarnya ancaman serangan siber yang mungkin terjadi. Diketahui bila saat ini, serangan siber kian meningkat dan menunjukkan urgensi hadirnya kajian yang dapat membantu meminimalkan risiko yang dapat dihadapi oleh siapa pun. Studi yang dilakukan oleh University of Maryland mendapatkan bahwa serangan siber saat ini rata-rata terjadi sebanyak 2.244 kali dalam sehari atau setiap 39 detik terjadi sebuah serangan siber.[2] Bahkan serangan siber melalui spam, bertumbuh mencapai 72%

[1]Victoria Wang, *et.al.,* "Internet Banking in Nigeria : Cybersecurity Breaches, Practice and Capability", *International Journal of Law*, Vol. 62, September 2020, hlm. 1.

[2]Michel Cukier, "Study: Hackers Attack Every 39 Seconds", *University of Maryland*, 9 Februari 2007, https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds (diakses pada 5 Mei 2022).

dari semua surel di seluruh dunia, yang mengakibatkan kerugian finansial besar dan berdampak semakin terancamnya keamanan siber, khususnya terhadap potensi kebocoran data pribadi.[3]

Studi lainnya yang dilakukan oleh IT Chronicles mengungkapkan bahwa serangan *ransomware* meningkat 400% setiap tahunnya, bahkan untuk setiap harinya 300.000 *malware* baru diproduksi, 23.000 serangan *denial of service* (DoS atau DdoS) terjadi dan 30.000 *website* diretas.[4] Data tersebut tentu mengungkapkan semakin rentannya perlindungan keamanan siber saat ini, khususnya terhadap potensi kebocoran data pribadi, termasuk di Indonesia yang 210 juta penduduknya telah aktif memanfaatkan internet saat ini.[5] Terjadinya kebocoran data 274 juta Kartu Tanda Penduduk (KTP) warga Indonesia, data nasabah Bank Rakyat Indonesia (BRI) dan Bank Indonesia, konsumen Tokopedia hingga kebocoran data yang menimpa Badan Siber dan Sandi Negara (BSSN), menjadi contoh rentannya keamanan data pribadi di Indonesia saat ini. Ketika negara-negara lain, telah mengatur secara khusus keamanan siber hingga rinci pada bentuk serangan tertentu, seperti *antispam laws,*[6] ataupun regulasi khusus terkait kebocoran data seperti *data breach notification law* di Hongkong,[7] Australia,[8; 9] dan negara EU.[10] Indonesia masih memiliki

---

[3]Alex Kigerl, "Routine Activity Theory and Malware, Fraud, and Spam at The National Level", *Crime, Law and Social Change*, Vol. 76, Issue 2, September 2021, hlm. 110.

[4]William Goddard, "Cyber Security Statistics 2020", *IT Chronicles*, 27 Mei 2021, https://itchronicles.com/information-security/cyber-security-statistics-2020/ (diakses pada 6 Mei 2022).

[5]Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), *Profil Internet Indonesia 2022*, Juni 2022, hlm. 9.

[6]Elinor Camri, "Regulating Behaviours on the European Union Internet, the Case of Spam Versus Cookies", *International Review of Law, Computers & Technology*, Vol. 31, Issue 3, 2017, hlm. 290.

[7]Rebecca Ong dan Sandy Sabapathy, "Hong Kong's Data Breach Notification Scheme: From the Stakeholder Perspective", *Computer Law and Security Review*, Vol. 42, September 2021, hlm. 1-16.

[8]Dennis Gibson dan Clive Harfield, "Contradictions and Inconsistencies in Australia's Mandatory Data Breach Notification Laws", *Computer Law and Security Review*, Vol. 42, September 2021, hlm. 1-11.

[9]Angela Daly, "The Introduction of Data Breach Notification Legislation in Australia: A Comparative View", *Computer Law and Security Review*, Vol. 34, Issue 3, June 2018, hlm. 477-495.

[10]Rogers Alunge, "Breach of Security vs Personal data Breach: Effect on EU data Subject Notification Requirements", *International Data Privacy Law*, Vol. 11, Issue 2, April 2021, hlm. 163-181.

pekerjaan rumah untuk memiliki payung hukum utamanya. Tertundanya RUU Perlindungan Data Pribadi serta RUU Keamanan Siber, yang sejatinya diharapkan dapat menjadi solusi peristiwa kebocoran data, pada akhirnya perlu disikapi dengan menghadirkan kebijakan dini yang memberikan perlindungan hukum bagi korban kebocoran data maupun instrumen pencegahan guna menghindari seseorang menjadi korban.

Selain itu, diperlukan sebuah upaya pelurusan, terhadap pandangan umum yang menilai jika serangan siber yang menjadi penyebab kebocoran data hanya dapat dilakukan oleh seseorang dengan latar belakang kemampuan Informasi dan Teknologi (IT) serta dukungan peralatan mutakhir. Faktanya, serangan tersebut dapat dilakukan oleh kalangan umum, bahkan tanpa membutuhkan dukungan peralatan khusus yang dikenal dengan istilah *social engineering attack*.

Serangan siber sendiri didefinisikan sebagai *a hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions*.[11] Definisi lainnya menjelaskan bahwa serangan siber merupakan serangan dalam dunia maya, baik yang ditujukan untuk menyerang ataupun bertahan yang diharapkan dapat sebagai penyebab kematian seseorang atau kerusakan suatu objek yang dituju,[12] sementara definisi yang diberikan oleh Hathaway diuraikan dengan menunjukkan perbedaan antara *cyber-attack, cyber-crime,* dan *cyber-warfare*, yang menjelaskan bila *cyber-attack* merusak fungsi jaringan komputer untuk **tujuan politik atau keamanan nasional.**[13] Lebih lengkap perbedaan menurut Hathway ditunjukkan dalam tabel berikut.

[11]Nick Ebner, "Cyber Space, Cyber Attack and Cyber Weapons : A Contribution to the Terminology", *Institute for Peace Research and Security Policy*, University of Hamburg, October 2015, hlm. 4.

[12]Kartini Eliva Angel Tampubolon, "Perbedaan Cyber Attack, Cybercrime, dan Cyber Warfare", *Jurist-Diction*, Vol. 2, No. 2, Maret 2019, hlm. 542.

[13]Oona A. Hathaway, *et.al.*, "The Law of Cyber-Attack", *California Law Review*, Vol. 100, 2012, hlm. 826.

Tabel 1. Karakteristik Utama dari Berbagai Tindakan Siber[14]

	Type of cyber-action		
	Cyber-attack	*Cyber-crime*	*Cyber-warfare*
Involves only non–state actors		√	
Must be violation of criminal law, committed by means of a computer system		√	
Objective must be to undermine the function of a computer network	√		√
Must have a political or national security purpose	√		√
Effects must be equivalent to an "armed attack," or activity must occur in the context of armed conflict			√

Sementara definisi yang diberikan Duncan Hodges dan Sadie Creese dapat menjadi rujukan yang sesuai dengan maksud tujuan buku ini, yakni:[15]

> *"An electronic attack to a system, enterprise or individual that intends to disrupt, steal or corrupt assets where those assets might be digital (such as data or information or a user account), digital services (such as communications) or a physical asset with a cyber component (such as the process control system found in a building, air craft or nuclear refinement facility). Typically such attacks seek to compromise the confidentiality, integrity or availability of digital assets, and so cyber security controls seek to preserve these properties in some way."*

Masalah utama dalam serangan siber, sesungguhnya adalah sifat spekulatif dari serangan tersebut. Mengingat jangkauan ancaman yang umum terjadi cukup luas, baik terhadap pemerintah, bisnis, maupun individu. Beberapa kemungkinan yang terjadi meliputi:[16]

1. *attacks interfering with internet related networks, installations, server parks, major firms;*
2. *attacks on financial industries such as banking and securities trading;*
3. *attacks denying access to defense ministry computer networks including email and other sensitive systems;*

---

[14]*Ibid.,* hlm. 833.

[15]Duncan Hodges dan Sadie Creese, "Understanding Cyber-attacks", dalam James A. Green (ed), *Cyber Warfare: A Multidisciplinary Analysis* (New York: Routledge, 2015), hlm. 34.

[16]Nick Myers, *Cyber Security: Cyber Crime, Attacks and Terrorism* (Old Dominion University UN Day 2020 Issue Brief, GA First Committee (DISC), 2020), hlm. 2-3.

4. *energy industries, electricity generation and distribution, including oil refineries and oil and gas pipelines;*
5. *interference with critical infrastructure such as emergency service, hospitals, energy generation, and distribution, or transportation.*
6. *attacks on government systems by criminal, terrorist, or revolutionary organizations seeking information;*
7. *violation of commercial and individual privacy.*

Di Indonesia pada paruh pertama 2021, Badan Siber dan Sandi Negara (BSSN) melaporkan jumlah serangan siber yang mencapai hingga 741.441.648, meningkat dari tahun sebelumnya sebanyak 495.000.000.[17] Bahkan pada bulan Oktober 2021, Pusat *Malware* Nasional milik BSSN mengalami serangan siber berupa *web defacement attack*. Situs web (pusmanas.bssn.go.id) yang berisi basis data perangkat lunak jahat (*malware)* yang dianalisis oleh BSSN tersebut diubah tampilannya,[18] sementara itu Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia mendapatkan serangan siber 385.980 sepanjang bulan Januari-Juni 2022, atau rata-rata 2.150 serangan setiap harinya. Serangan siber menyasar *website* Kemenkumham, aplikasi persuratan internal serta aplikasi kepegawaian. Khusus web Kemenkumham, berbarengan dengan serangan yang terjadi di antaranya berupa *malicious session* (71%), *server side code injection* (21%), dan *malicious scan* (6%).[19]

---

[17]Andi Nugroho, "Paruh Pertama 2021, Jumlah Serangan Siber di Indonesia Capai 741,44 Juta, Melebihi Total Serangan Tahun Lalu", *Cyberthreat*, 24 Agustus 2021, https://cyberthreat.id/read/12306/Paruh-Pertama-2021-Jumlah-Serangan-Siber-di-Indonesia-Capai-74144-Juta-Melebihi-Total-Serangan-Tahun-Lalu (diakses pada 7 Mei 2022).

[18]Andi Nugroho, "Pusat Malware Nasional BSSN Terkena Deface, Hacker Brasil: Ini Serangan Balasan", 25 Oktober 2021, *Cyberthreat.id,* https://cyberthreat.id/read/12634/Pusat-Malware-Nasional-BSSN-Terkena-Deface-Hacker-Brasil-Ini-Serangan-Balasan (diakses pada 8 Mei 2022).

[19]Rhazes Putra, "Kemenkumham Terima Serangan Siber 385.980 Kali, Terbanyak dari AS", *Detik News*, 14 Juni 2022, https://news.detik.com/berita/d-6126722/kemenkumham-terima-serangan-siber-385980-kali-terbanyak-dari-as (diakses pada 20 Juni 2022).

APA ITU WEB *DEFACEMENT ATTACK?*[20]

Web defacement attack merupakan cara peretas untuk mengejek administrator sistem karena protokol keamanan yang buruk, dan sebagai cara untuk menunjukkan reputasi sebagai peretas yang terampil.[21] Peretas mengubah tampilan visual situs web, dan mengakibatkan reputasi organisasi terkait dapat rusak, karena tidak dapat melindungi dirinya sendiri dari serangan siber. Setelah perusakan, pengguna internet mungkin akan mempertanyakan apakah akan memercayakan informasi pribadi kepada perusahaan tersebut atau memberikan data sensitifnya.[22]

Diketahui, setidaknya terdapat sebuah pola umum pada setiap serangan siber yang dilakukan dalam empat tahap, yakni *survey, delivery, breach,* dan *affect*. Pada tahap ***survey***, penyerang (*attackers)* akan memanfaatkan segala cara yang tersedia untuk menemukan kerentanan teknis, prosedural hingga fisik yang dapat dieksploitasi. Penyerangan akan menggunakan sumber informasi terbuka seperti LinkedIn dan Facebook, layanan manajamen/pencarian nama domain serta media sosial serta menggunakan alat pemindaian jaringan untuk mengumpulkan dan menilai informasi apa pun tentang komputer sistem keamanan. Tahap ***delivery***, penyerang akan mencari celah untuk masuk dalam posisi yang memungkinkan untuk dapat mengeksploitasi kerentanan yang berpotensi atau telah diidentifikasi sebelumnya, seperti mengirimkan surel yang berisi tautan kepada situs web berbahaya atau lampiran yang berisi kode berbahaya, memberikan *flashdisk* yang telah terinfeksi pada sebuah pameran, atau membuat situs web palsu yang berharap untuk dikunjungi oleh target.[23]

Dalam tahap ***breach***, diketahui bahwa kerugian bisnis target akan bergantung pada skala kerentanan dan metode eksploitasi, karena memungkinkan mereka untuk membuat perubahan yang memengaruhi sistem, mendapatkan akses pada akun *online,* atau mendapatkan kendali

[20]Konark Truptiben Dave, "Brute-force Attack "Seeking but Distressing"", *International Journal of Innovations in Engineering and Technology*, Vol. 2, Issue 3, Juni 2013, pp. 75-78, hlm. 75-76.

[21]C. Jordan Howell, *et.al.,* "Website Defacement and Routine Activities: Considering the Important oh Hackers' Valuations of Potential Targets", *Journal of Crime and Justice*, Vol. 42, Issue 5, 2019, pp. 536-550, https://doi.org/10.1080/0735648X.2019.1691859, hlm. 537.

[22]George W. Burruss, *et.al.,* "Website Defacer Classification: A Finite Mixture Model Approach", *Social Science Computer Review*, 2021, pp. 1-13, DOI: https://doi.org/10.1177/0894439321994232, hlm. 1.

[23]National Cyber Security Centre, "Common Cyber Attacks: Reducing the Impact", *Cyber Attacks White Paper,* Januari 2016, hlm. 7.

penuh atas komputer, tablet hingga *smartphone* korban. Setelah melakukan ini, penyerang dapat berpura-pura menjadi korban dan menggunakan hak akses sah untuk mendapatkan akses ke sistem dan informasi lain. Tahap ***affect,*** penyerang mungkin memiliki motivasi agar dapat menjelajahi sistem milik korban, memperluas akses, dan membangun kehadiran yang terus-menerus. Mengambil alih akun pengguna umumnya menjamin kehadiran terus-menerus. Apabila penyerang dapat mengambil alih akun administrator, maka dimungkinkan untuk dapat mengendalikan lebih banyak sistem. Saat melakukan ini, penyerang akan sangat berhati-hati untuk tidak memicu proses pemantauan sistem. Setelah mencapai tujuannya, penyerang akan lebih mudah untuk keluar dan dengan hati-hati akan menghilangkan bukti kehadirannya. Tindakan lainnya umumnya adalah dengan membuat rute akses untuk penerobosan berikutnya oleh penyerang atau bagi orang lain yang sebelumnya telah dijual aksesnya.[24] Sementara itu, pandangan lainnya menguraikan dalam tujuh tahapan, yakni *reconnaissance, weaponization, delivery, exploitation, installation, command, and control, action on objective*.[25]

Berdasarkan sifatnya, serangan siber terbagi atas serangan teknis dan serangan sosial (*social engineering)*. Serangan teknis lebih ditujukan menyerang jaringan logika melalui berbagai metode untuk mendapatkan akses ilegal, mencuri informasi, atau memasukkan *malware* yang bisa merusak jaringan fisik dan persona siber (pengguna internet), sedangkan *social engineering* ditujukan untuk memengaruhi manusia pada dan melalui ruang siber yang cenderung berkaitan erat dengan perang politik, perang informasi, perang psikologi, propaganda[26] yang bertanggung jawab atas 98% insiden serangan siber pada tahun 2021.[27] Secara global, bahkan terjadi peningkatan serangan siber pada masa pandemi, sebagaimana yang ditunjukkan dalam gambar berikut.

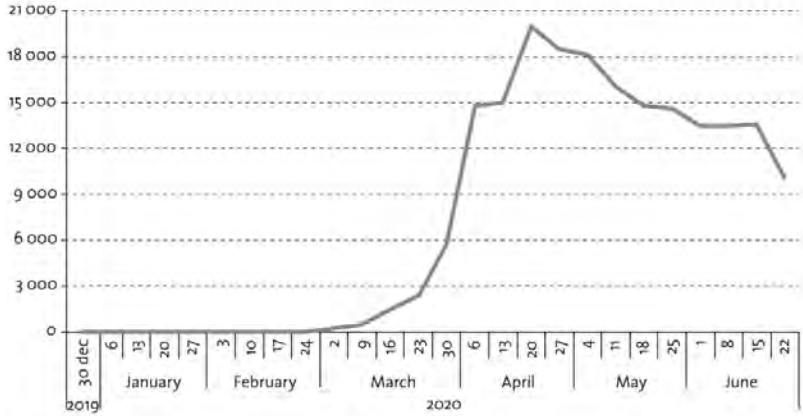
---

[24]*Ibid*.

[25]Craig Reeds, "The Seven Phases of a Cyber Attack", *DNV*, https://www.dnv.com/article/the-seven-phases-of-a-cyber-attack-118270 (diakses pada 8 Mei 2022).

[26]Hinsa Siburian (Kepala Badan Siber dan Sandi Negara) dalam Tenri Gobel dan Paramitha Sandy, "Pakai Internet Tanpa Budaya Keamanan Siber, Kita Akan Hancur", *Cyberthreat*, 9 Desember 2021, https://cyberthreat.id/insightdetil/9548/Menyoroti-Budaya-Keamanan-Siber (diakses pada 9 Mei 2022).

[27]Purple Sec, "2021 Cyber Security Statistic: The Ultimate List of Stats, Data & Thrends", *Purple Sec*, https://purplesec.us/resources/cyber-security-statistics/#SocialEngineering (diakses pada 9 Mei 2022).



Gambar 1. Serangan Siber Sejak Pandemi Covid-19[28]

Sebagaimana diketahui bersama, saat ini kebocoran data pribadi semakin marak terjadi bahkan pada 12 Mei 2021 diketahui 279 juta data warga Indonesia bocor dan diiklankan oleh akun Kotz di Raidforums.com. Data yang dijual berupa NIK, KTP, telepon, *email,* nama, alamat hingga gaji. Akun tersebut menyebutkan telah menyediakan 1 juta data contoh secara gratis untuk dicoba.[29] Tidak hanya itu, bahkan data penduduk Pemerintah Kabupaten Magelang berupa NIK dan KK diunggah tanpa enkripsi pada *portal open data* (opendata.magelangkab.go.id) saat bulan Juni 2021, yang diketahui dilakukan oleh kantor desa wilayah setempat.[30] Data lainnya dilaporkan oleh Cisco yang menunjukkan bahwa sebanyak 60% pelaku usaha kecil dan menengah (UKM) di Indonesia mengalami pencurian informasi pelanggan oleh pelaku kejahatan. Hampir 29% UKM Indonesia yang mengalami serangan siber melihat bahwa alasan utama adalah karena solusi

[28]Rodrigo Mariano Diaz, "Cybersecurity in the Time of Covid-19 and the Transition to Cyberimmunity", *Bulletin FAL: Facilitation of Transport and Trade in Latin America and the Caribbean,* Bulletin 382, Number 6, 2020, hlm. 10.

[29]Reska K. Nistanto, "Data 279 Juta Penduduk yang Bocor Identik dengan Milik BPJS, Kominfo Panggil Direksi", *Kompas*, 21 Mei 2021, https://tekno.kompas.com/read/2021/05/21/14351007/data-279-juta-penduduk-yang-bocor-identik-dengan-milik-bpjs-kominfo-panggil?page=all (diakses pada 9 Mei 2022).

[30]Nanda Sagita Ginting, "Diskominfo Kabupaten Magelang Masih Lakukan Penyelidikan Terkait Kebocoran Data Penduduknya", *Tribun Jogja,* 7 Juni 2015, https://jogja.tribunnews.com/2021/06/07/diskominfo-kabupaten-magelang-masih-lakukan-penyelidikan-terkait-kebocoran-data-penduduknya (diakses pada 9 Mei 2022).

keamanan siber yang dianggap tidak memadai untuk mendeteksi atau mencegah serangan. Sementara itu, 21% menyebutkan bahwa alasan utama terjadinya serangan adalah tidak adanya solusi keamanan siber. Selain kehilangan data pelanggan, UKM di Indonesia yang mengalami insiden serangan siber juga kehilangan data karyawan (63%), surel internal (62%), informasi bisnis yang sensitif (60%), informasi keuangan (54%), dan kekayaan intelektual (54%).[31]

Peristiwa kebocoran data yang marak saat ini sangat mengancam privasi dan erat kaitannya dengan studi keamanan siber. Kebocoran data adalah mendapatkan akses data penting seseorang atau organisasi oleh pengguna yang tidak sah. Data penting organisasi dapat berupa informasi pelanggan, rencana bisnis, kondisi keuangan, informasi pasien, data kartu kredit, dan lainnya.[32] Berdasarkan penelitian yang dilakukan oleh **HFS Research** perihal kebocoran data pada perusahaan, diketahui bahwa 69% mengalami kebocoran karena faktor internal (*insider leaks)* dan 57% mengalami kebocoran karena faktor eksternal (*outsider leaks)*. Salah satu contohnya terjadi pada kasus proyek kendaraan otonom Google Waymo, yang setelah pekerja utama proyek tersebut meninggalkan perusahaan, ternyata mendirikan perusahaan rintisan dan menjual rahasia dagang perusahaan kepada perusahaan lain.[33]

Diketahui bahwa 90% penyebab terjadinya kebocoran data disebabkan oleh serangan *social engineering*.[34] Subdit Direktorat Kriminal Umum Polda Metro Jaya mencatat, sepanjang 2019 terdapat 2.300 pengaduan kasus *social engineering* yang diterima oleh Subdit *Cyber Crime* Polda Metro Jaya. Kepala Divisi Humas Mabes Polri Irjen Argo mengungkapkan salah satu pelaku yang menggunakan teknik *social*

---

[31]Erwin Prima, "Studi Cisco: 60 Persen UKM Indonesia Alami Pencurian Informasi", 24 Oktober 2021, https://tekno.tempo.co/read/1520571/studi-cisco-60-persen-ukm-indonesia-alami-pencurian-informasi/full&view=ok (diakses pada 10 Mei 2022).

[32]K.S. Wagh, "A Survey: Data Leakage Detection Techniques", *International Journal of Electrical and Computer Engineering*", Vol. 8, No. 4, Agustus 2018, pp-2247-2253, DOI: 10.11591/ijece.v8i4.pp2247-2253, hlm. 2247.

[33]Jawon Kim, *et.al.,* "Research on Behavior-Based Data Leakage Incidents for the Sustainable Growth of an Organization", *Journal Sustainability*, Vol. 12, No. 15, 2020, DOI: https://doi.org/10.3390/su12156217, hlm. 1.

[34]Mitnick Security, "6 Types of Social Engineering Attacks", *Mitnick Security*, 5 April 2021, https://www.mitnicksecurity.com/blog/6-types-of-social-engineering-attacks (diakses pada 10 Mei 2022).

engineering dengan modus meminta nomor OTP (*One-Time Password)*, berhasil mendapatkan kode OTP dan membobol setidaknya 3.070 akun nasabah bank dan aplikasi transportasi *online* sejak 2017 lalu. Total yang didapat sekitar Rp19 miliar dari bank dan sisanya didapat dari pembobolan akun ojek *online* sehingga totalnya Rp21 miliar.[35] Apabila selama ini kajian *social engineering* umum dilakukan oleh para penstudi keamanan siber, maka buku ini akan melakukan pengkajiannya dengan menggunakan optik hukum. Dalam lingkup wilayah hukum, *social engineering* bukanlah istilah baru. Roscoe Pound dengan teori pragmatisme hukum dan Mochtar Kusumaatmadja dengan teori hukum pembangunan turut menggunakan istilah *social engineering* dalam konsepnya. Namun, dalam tulisan ini, *social engineering* yang dimaksud memiliki perbedaan makna. Maka untuk memperjelasnya akan diuraikan perbedaan makna dari istilah *social engineering* tersebut.

Dalam sebuah literatur disebutkan bahwa *social engineering* sebenarnya adalah cabang studi dalam psikologi dan sosiologi yang meneliti sifat dan perilaku manusia dari perspektif persuasi dan pengaruh. *Social engineering* telah lama digunakan dalam praktik sebagai metode yang efektif untuk memanipulasi individu manusia untuk melakukan suatu tindakan atau mengungkapkan informasi yang diinginkan, baik dengan membangun hubungan dan kepercayaan palsu dengan orang tersebut, atau dengan mengeksploitasi kelemahan orang tersebut. *Social engineering* bukanlah teknik tunggal, melainkan kumpulan teknik. Teknik-teknik ini sengaja dibuat untuk memanfaatkan sifat-sifat tertentu yang melekat pada sifat manusia, misalnya keinginan untuk membantu, kecenderungan untuk memercayai orang, takut mendapat masalah, dan keinginan untuk mengambil jalan pintas.[36]

Literatur lainnya menjelaskan bahwa istilah *social engineering* turut digunakan dalam dua konteks keamanan informasi dan ilmu politik. Dalam konteks keamanan informasi, *social engineering* menggambarkan

---

[35]Yuswardi A. Suud, "Tangkal Rekayasa Sosial di Platform Digital, Gojek Tempuh Jalan Apa?", *Cyberthreat,* 26 Oktober 2020, https://cyberthreat.id/insightdetil/8973/Tangkal-Rekayasa-Sosial-Gojek-Tempuh-Jalan-Apa (diakses pada 10 Mei 2022).

[36]Van Nguyen, *Attribution of Spear Phishing Attacks: A Literature Survey*, (Australian Government, Department of Defence, Cyber and Electronic Warfare Division, Defense Science and Technology Organisation, South Australia: DSTOP Defence Science and Technology Organisation, 2013), hlm. 3.

fenomena ketika seseorang dipengaruhi untuk mengambil tindakan tertentu, yang mungkin (dan kerap) bertentangan dengan kepentingan dirinya sendiri. Dalam ranah ilmu politik, istilah tersebut memiliki arti yang sedikit serupa, namun dalam skala yang lebih besar — memengaruhi sejumlah besar ("massa") orang. Definisi *social engineering* yang paling populer nampaknya adalah yang diberikan oleh Harl dalam konferensi *Access All Areas III* pada tahun 1997, yakni seni dan ilmu untuk membuat korban menuruti keinginan dari pelaku. Teknik tersebut tidak serupa dengan mengendalikan pikiran, karena tidak memungkinkan pelaku untuk membuat korban melakukan perintah secara liar di luar perilaku normalnya. Hadnagy menawarkan beberapa pandangan lebih lanjut terkait istilah *social engineering* dengan mencatat bahwa teknik *social engineering* kerap digunakan dalam kehidupan sehari-hari oleh orang-orang yang umumnya memiliki niat baik — misalnya dokter yang memengaruhi perilaku pasien dengan tujuan akhir meningkatkan kesehatan mereka. Dalam hal ini, Hadnagy menyarankan pentingnya untuk membedakan antara alat — *social engineering* — dan niat — yang sering kali berbahaya.[37]

Mudahnya untuk membujuk seseorang dapat diketahui dari analisis yang dilakukan oleh Microsoft ketika mengungkapkan bahwa 48% orang akan menukar kata sandi dengan sepotong cokelat. Hal tersebut dapat terjadi karena mudahnya seseorang untuk mengatakan "ya". Sebagai makhluk sosial, pengambilan keputusan seseorang kerap dipengaruhi oleh orang lain. Sehingga para pelaku kejahatan kerap memanfaatkan keadaan tersebut untuk mengambil kesempatan dalam memperoleh informasi dari seseorang. Cialdini menjelaskan bahwa terdapat enam prinsip persuasi yang membuat seseorang terdorong mengikuti permintaan orang lain, yaitu: (1) *reciprocity;* (2) *scarcity;* (3) *authority;* (4) *consistency;* (5) *liking;* (6) *consensus*.[38]

Cialdini menjelaskan perihal ***reciprocity*** (timbal balik) dengan mengungkapkan bahwa seseorang cenderung untuk bersikap adil.

---

[37]Yavor Papazov, "Social Engineering", *Educational Notes Paper*, North Atlantic Treaty Organization (NATO) dan Science and Technology Organization, 2016, pp. 1-18, DOI: 10.14339/STO-EN-IST-143-08-PDF, hlm. 2.

[38]Diana Kelley, "The Pschology of Social Engineering-the "Soft" Side of Cybercrime", *Microsoft*, 30 Juni 2020, https://www.microsoft.com/security/blog/2020/06/30/psychology-social-engineering-soft-side-cybercrime/ (diakses pada 10 Mei 2022).

Faktanya, menerima hadiah memicu respons neurologis pada area otak yang terkait dengan pengambilan keputusan. Apabila suatu hari seorang teman membelikan sebuah makan siang, maka muncul perasaan wajib untuk mengganti kembali membelikannya makan pada kesempatan lain ketika beraktivitas bersama. *Social psychologists* mengungkapkan bahwa apabila seseorang menerima kartu liburan dari orang asing, 20% akan mengirimkannya kembali dan memberikan *mint* pada akhir makan dapat meningkatkan pemberian tip sebesar 18%-21%. Dalam serangan siber seperti *phishing,* prinsip timbal balik dapat terlihat ketika seseorang menerima *email* berisi kupon gratis atau hadiah lainnya yang mewajibkan penerima untuk mendaftarkan akunnya. Prinsip ***scarcity*** (kelangkaan) dijelaskan dengan memberikan gambaran maraknya situs web perjalanan yang memberikan informasi ketika terdapat beberapa penerbangan atau kamar yang tersedia. Telah menjadi sifat manusia untuk menempatkan nilai yang lebih tinggi pada sesuatu yang persediaannya terbatas. Dalam suatu studi terhadap para mahasiswa, diketahui bahwa kue akan terasa lebih menarik bila jumlahnya lebih sedikit pada sebuah toples. Dalam serangan *phishing*, penyerang memanfaatkan keinginan seseorang bagi hal-hal yang tampaknya langka dengan memberikan batas waktu pada penawaran dalam surel, atau pada taktik lainnya, penyerang memberitahukan bahwa akun mereka akan dinonaktifkan dalam waktu 24 jam apabila target tidak mengeklik tautan untuk menyelesaikannya.[39]

Prinsip ***authority*** (otoritas) menunjukkan bahwa seseorang cenderung mengikuti instruksi/jejak para ahli yang kredibel, seperti dokter, guru, atasan, dan pemimpin politik yang memiliki pengaruh besar atas tindakan dan perilaku seseorang. Studi Milgram mengungkapkan bahwa seorang peneliti berhasil meyakinkan para sukarelawan untuk memberikan kejutan listrik yang tinggi terhadap "peserta" yang tidak dapat menjawab pertanyaan dengan benar — sebetulnya peserta adalah aktor yang berpura-pura merasakan sakit, dan tidak ada kejutan listrik yang diberikan. Dalam *phishing* prinsip otoritas sangat umum dan efektif digunakan untuk mengelabui seseorang. Penyerang menipu *Chief Executive Officer* (CEO) untuk menuntut agar *Chief Financial Officer (*CFO) mengirimkan uang dengan cepat dengan teknik *spear phishing*.

[39]*Ibid.*

Ketika dikombinasikan dengan urgensi, seseorang kerap takut untuk mengatakan tidak kepada atasannya. Prinsip ***consistency*** (konsistensi) memanfaatkan sifat manusia yang menghargai integritas. Umumnya manusia mengagumi kejujuran dan keandalan seseorang, sehingga jika terdapat orang yang menyatakan mencintai lingkungan maka dirinya akan berusaha untuk tidak diketahui bila telah membuang sampah di taman. Sebuah studi mengungkapkan bila meminta seseorang untuk berkomitmen terhadap lingkungan ketika menginap di sebuah hotel, 25% dimungkinkan untuk menggunakan kembali handuk yang telah ada. Dalam *phishing* prinsip konsisten digunakan oleh penyerang dengan memanfaatkan keinginan seseorang untuk konsisten dengan meminta sesuatu yang "kecil" pada sebuah surel hingga kemudian meminta lebih banyak kembali pada suatu saat nanti.[40]

Prinsip ***liking*** (menyukai) memanfaatkan sifat manusia yang lebih cenderung mengatakan "ya" kepada seseorang yang disukainya. Apabila seorang teman meminta bantuan, akan lebih mudah untuk mengatakan "ya" dibandingkan bantuan yang diminta oleh orang asing. Walaupun terhadap orang asing dapat sangat persuasif jika dinilai baik. Dalam sebuah eksperimen undian, seseorang lebih cenderung membeli tiket undian apabila yang menjual tiket membawakan soda, dan lebih kecil kemungkinannya jika seseorang tersebut hanya membeli soda untuk dirinya sendiri. Dalam *phishing* prinsip *liking* dilakukan oleh penyerang berpura-pura menjadi teman yang dikenalnya dan berharap penerima tidak meneliti konten surel tersebut. Prinsip terakhir yakni ***consensus,*** memanfaatkan kondisi ketidakyakinan seseorang yang kemudian mencari orang lainnya untuk membantu menentukan pendapatnya, bahkan ketika seseorang telah yakin, pendapat *consensus* dapat sangat dipertimbangkan. Dalam *phishing* prinsip *consensus* digunakan dengan mengeksploitasi tren budaya, seperti ketika terjadi bencana alam, penyerang kerap menyamar menjadi organisasi badan amal untuk mengumpulkan sumbangan.[41]

[40]*Ibid.*
[41]*Ibid.*

1. Peristiwa Pencurian Berlian Bank ABN Amro

Peristiwa Pencurian Berlian Bank ABN Amro

Pada awal Maret 2007, seseorang telah mencuri berlian dari brankas penyimpanan pada Bank ABN Amro seberat 120.000 karat yang bernilai $28 juta. Pelaku telah menjadi nasabah tetap pada bank tersebut selama setahun terakhir, dengan nama Carlos Hector Flomenbaum dari Argentina, yang dikenal sebagai pedagang berlian yang terpercaya dan mendapatkan akses kepada brankas bank. Diketahui bahwa selama ini, pelaku menggunakan identitas palsu karena paspor yang digunakannya dilaporkan telah hilang dicuri pada beberapa tahun sebelumnya di Israel.

Yang menarik pada kasus pencurian ini, bahwa pelaku mendapatkan berlian tersebut dengan bersenjatakan "pesona pribadi". Selama satu tahun, pelaku rutin mengunjungi bank, berteman dengan staf dan secara bertahap mendapatkan kepercayaan dari pekerja bank. Pelaku bahkan membawakan pekerja bank cokelat hingga akhirnya mendapatkan kunci asli untuk dibuatkan salinan, serta mendapatkan informasi di mana berlian tersebut berada. Sebagai informasi, *Diamond High Council* di Antwerp menyatakan bahwa daerah tersebut telah dilengkapi dengan keamanan yang menelan biaya lebih dari €1 juta. Lebih dari separuh berlian dunia diperdagangkan di distrik permata Antwerpen. Labirin jalan-jalan di sekitar stasiun pusat kota menghasilkan omset £12 miliar setahun. Untuk melayani perdagangan yang menguntungkan ini, bank harus mengakomodasi klien yang ingin menyimpan berlian semalaman, tetapi mengambil kembali besok hari. Sehingga, beberapa pelanggan tertentu mendapatkan akses khusus ke dalam brankas.

Untuk informasi lebih lanjut terkait **Peristiwa Pencurian Berlian Bank ABN Amro,** Anda dapat *scan QR code* di samping.[42]

[42]Stephen Castle, "Thief Woos Bank Staff Which Chocolates- Then Steals Diamonds Worth £14m", *Independent*, 18 Maret 2007, https://www.independent.co.uk/news/world/europe/thief-woos-bank-staff-chocolates-then-steals-diamonds-worth-163-14m-5332414.html (diakses pada 11 Mei 2022).

2. Kasus Carbanak

Kasus Carbanak

Salah satu kasus *social engineering* lainnya yang ramai diperbincangkan adalah kasus **Carbanak**. Pada tahun 2018 tiga anggota kelompok kejahatan siber internasional telah ditangkap dan diadili pada pengadilan distrik AS di Seattle. Ketiga warga Negara Ukraina bernama Dmytro Fedorov, Feir Hladyr, dan Andrii Kopakov merupakan anggota peretas yang dikenal dengan sebagai kelompok Carbanak (juga dikenal FIN7 dan *Navigator Group*). Sejak 2015 kelompok Carbanak terlibat dalam kegiatan penyerangan *malware* yang menargetkan lebih dari 100 perusahaan AS, terutama di industri restoran, *game*, dan perhotelan. Kelompok ini telah meretas ribuan sistem komputer dan mencuri jutaan nomor kartu kredit serta debit pelanggan yang digunakan maupun dijual untuk mendapatkan keuntungan.

Tercatat untuk Amerika saja, Carbanak berhasil menembus jaringan komputer perusahaan di 47 negara bagian dan mencuri 15 juta catatan kartu pelanggan dari lebih 6.500 di 3.600 lokasi penjualan. Intrusi turut terjadi di Inggris, Australia serta Prancis. Perusahaan yang secara terbuka mengungkapkan menjadi korban peretasan adalah Chipotle Mexican Grill, Chilis's, Arby's, dan Jason's Deli. Selain itu, di Washington Barat, Carbanak menargetkan Kasino Emerald Queen dan bisnis lokal lainnya.

Langkah penyerangan Carbanak pada umumnya dilakukan dengan mengirim *email phishing* kepada karyawan perusahaan. Setiap *email* menyertakan file terlampir yang kerap dalam bentuk dokumen Microsoft Word. Pesan di dalam *email* berisikan informasi bisnis yang mengarahkan korban untuk membuka lampiran dan tanpa disadari mengaktifkan *malware* yang akan menginfeksi komputer. Misalnya saat pelaku menargetkan jaringan hotel, pelaku akan mengirim *email* yang berisikan keinginan untuk reservasi hotel dengan detail informasi dalam lampiran.

Untuk informasi lebih lanjut terkait **Kasus Carbanak,** Anda dapat *scan QR code* di samping.[43]

Keamanan siber merupakan tindakan yang diambil untuk melindungi komputer atau jaringan dari akses yang tidak sah guna menjaga keamanan dan integritas informasi yang tersimpan di dalamnya. Keamanan siber melibatkan intervensi teknis yang melindungi data, informasi

[43]FBI, "How Cyber Crime Group FIN7 Attacked and Stole Data form Hundreds of U.S. Companies", *FBI*, 1 Agustus 2018, https://www.fbi.gov/contact-us/field-offices/seattle/news/stories/how-cyber-crime-group-fin7-attacked-and-stole-data-from-hundreds-of-us-companies (diakses pada 10 Mei 2022).

identitas, dan perangkat keras dari akses atau ancaman yang tidak sah termasuk keamanan aset di dunia maya. *Routine Activity Theory* (RAT) mengungkapkan bila terdapat tiga kondisi yang mengakibatkan terjadinya kejahatan bila seluruhnya bertemu. Tiga kondisi tersebut adalah pelaku yang termotivasi, target yang sesuai, dan tidak adanya perlindungan yang cakap.[44] Craigen lebih lanjut menjelaskan bahwa keamanan siber sebagai organisasi dan kumpulan sumber daya, proses, dan struktur yang digunakan untuk melindungi aset tertentu di dunia maya dan sistem yang mendukung dari peristiwa yang bertentangan dengan hukum.[45]

Meningkatnya pemanfaatan teknologi informasi saat ini semakin meningkatkan potensi terjadinya serangan siber. Laporan yang dirilis oleh Symantec pada tahun 2012 menyatakan bahwa serangan siber telah mengakibatkan kerugian hingga 114 miliar USD, dan bila ditotalkan dengan langkah pemulihan sebesar 385 miliar USD dan diperkirakan akan menelan biaya sebesar 10,5 triliun USD per tahun pada tahun 2025.[46] Korban serangan siber turut mengalami peningkatan secara signifikan. Survei yang dirilis oleh Symantec terhadap 20.000 orang di 24 negara, menunjukkan bahwa 69% telah menjadi korban serangan siber, dan 14 orang dewasa menjadi korban serangan siber setiap detiknya atau lebih dari 1 juta serangan setiap hari.[47] Laporan lainnya yang dirilis oleh ISACA's *State of Cybersecurity* mengungkapkan bahwa *social engineering* dialami oleh 85% organisasi pada tahun 2018, meningkat 16% selama satu tahun. Biaya tahunan rata-rata serangan *social engineering* untuk organisasi pada tahun 2018 telah melebihi $1,4 juta, meningkat 8% dibandingkan tahun sebelumnya.[48]

Digital menjadi suatu istilah yang lazim digaungkan oleh sebagian besar organisasi saat ini. Upaya memastikan langkah ke depan yang selaras dengan

---

[44]Alex Kigerl, *Op. Cit.*, hlm. 112.

[45]Michael D. Richardson, *et.al.*, "Planning for Cyber Security in Schools: The Human Factor", *Education Planning Journal*, Vol. 27, No. 3, 2020, pp. 23-29, hlm. 24.

[46]Devin Partida, "Social Engineering Cyberattacks and How They're Impacting Business", *Security Infowatch*, 21 Desember 2020, https://www.securityinfowatch.com/cybersecurity/article/21203580/social-engineering-cyberattacks-and-how-theyre-impacting-businesses (diakses pada 10 Mei 2022).

[47]Julian Jang-Jaccard dan Surya Nepal, "A Survey of Emerging Threats in Cybersecurity", *Journal of Computer and System Sciences*, Vol. 80, Issue 5, August 2014, pp. 973-993, DOI: https://doi.org/10.1016/j.jcss.2014.02.005. hlm. 973.

[48]ISACA's State of Cybersecurity dalam Zuoguang Wang, *et.al.*, "Defining Social Engineering in Cybersecurity", *IEEE Access*, Volume 8, 2020, pp. 85094-85115, DOI: 10.1109/ACCESS.2020.2992807, hlm. 85094.

perkembangan teknologi telah mengubah tatanan organisasi yang selama ini telah dibangun. Konsekuensi digitalisasi organisasi pada sebagian besar aspek melahirkan ancaman keamanan siber yang kian hari meningkat terjadi. Sebagian besar teknik kejahatan dunia maya berkisar pada menemukan dan mengeksploitasi titik lemah dalam infrastruktur digital perusahaan. *Social engineering* berbeda karena menargetkan manusia bukan jaringan itu sendiri. Manusia merupakan mata rantai terlemah dalam arsitektur keamanan siber. Salah satu alasan sederhananya karena manusia mudah dimanipulasi. Manusia tunduk pada emosi yang kerap mengesampingkan sebuah komitmen terhadap sebuah logika. Manusia memiliki dimensi psikologis yang tidak dimiliki oleh komputer, yang didasarkan pada logika murni dan logis. Kelemahan dan kebutuhan psikologis manusia, ingatan yang terbatas membuat seseorang rentan terhadap penipuan dan manipulasi emosional.[49] Kecenderungan ini yang mendukung laporan bahwa 95% dari semua insiden siber disebabkan oleh faktor manusia.[50]

Upaya untuk meningkatkan keamanan jaringan melalui solusi teknologi seperti *firewall*, deteksi intrusi, dan perangkat biometrik memberikan perlindungan yang sah terhadap berbagai ragam ancaman. Namun, langkah-langkah tersebut beranjak dari asumsi bila semua ancaman terhadap keamanan organisasi berasal dari sumber atau penyerang eksternal. Sehingga diperlukan pemahaman yang baik jika elemen manusia di dalam organisasi perlu mendapatkan perhatian yang serius.[51]

Social engineering menjadi sangat efektif dan telah menjadi tren pelaku saat ini. Menurut Departemen Kehakiman AS, serangan *social engineering* adalah salah satu ancaman paling berbahaya di dunia. Pada tahun 2016, perusahaan analis keamanan siber Cyence menyatakan bahwa Amerika Serikat adalah negara yang menjadi sasaran utama serangan *social engineering* dan memiliki biaya serangan tertinggi diikuti oleh Jerman dan Jepang. Perkiraan biaya serangan tersebut di AS adalah $121,22 miliar. Secara khusus, perusahaan AS sangat ditargetkan dan dipengaruhi oleh penjahat dunia maya dan peretas dari mana saja di dunia. Perusahaan-

---

[49]Nabie Y. Conteh dan Malcolm D. Royer, "The Rise in Cybercrime and the Dynamincs of Exploiting the Human Vulnerabilty Factor", *International Journal of Computer (IJC)*, Vol. 20, No. 1, 2016, pp. 1-12, hlm. 3.

[50]Michael D. Richardson, *Op. Cit.*, hlm. 23.

[51]Lee Hadlington, "The "Human Factor" in Cybersecurity: Exploring the Accidental Insider" dalam John. McAlaney, *et.al.* (Eds), *Psychological and Behavioral Examinations in Cyber Security*, (Hersey: IGI Global, 2018), DOI: http://doi.org/10.4018/978-1-5225-4053-3.ch003, hlm. 47.

perusahaan ini menangani data berharga internasional yang signifikan dan ketika perusahaan-perusahaan ini diretas, itu sangat berdampak pada ekonomi dan privasi di seluruh dunia. Salah satunya adalah perusahaan Equifax yang diretas selama beberapa bulan dan data pelanggan sensitif dicuri pada tahun 2018. Equifax adalah agen pelaporan dan pemantauan kredit konsumen yang mengumpulkan data individu serta konsumen bisnis untuk memantau riwayat kredit mereka dan mencegah penipuan. Akibat pencurian data tersebut, penyerang mengakses informasi pribadi 145,5 juta konsumen Amerika. Data tersebut meliputi nama lengkap konsumen, tanggal lahir, nomor jaminan sosial (SSN), nomor SIM, alamat, nomor telepon, informasi kartu kredit, dan nilai kredit. Pelanggaran ini merupakan hasil dari serangan *phishing* yang dilakukan dengan mengirimkan ribuan *email* yang berpura-pura dari lembaga keuangan atau bank besar seperti *Bank of America*.[52]

Secara historis, konsep *social engineering* sebagai prinsip-prinsip psikologi yang disalahgunakan untuk memanipulasi manusia telah dikenal selama ratusan tahun. Diketahui dalam peristiwa perang Troya pada tahun 1184 SM. Dalam novel *The Odyssey* dikisahkan peristiwa perang panjang antara Troya dan Yunani. Setelah pengepungan selama 10 tahun, orang-orang Yunani akhirnya membangun kuda kayu raksasa dan menyembunyikan beberapa tentara di dalamnya. Troya akhirnya terkena tipuan, dengan membawa masuk kuda tersebut melewati penjagaan yang selama ini melindunginya untuk dipajangkan sebagai tanda kemenangannya. Setelah matahari terbenam dan Troya beristirahat, tentara Yunani yang telah menunggu di dalam kuda mulai menyelinap keluar dan membuka gerbang di sekitar kota. Tentara Yunani kemudian menyerang Troy dari dalam wilayahnya sehingga berhasil menghancurkannya. Ribuan tahun setelahnya, beberapa orang mulai memberi nama pada jenis penipuan seperti ini. Peretas bernama Kevin Mitnick membantu memopulerkan istilah *social engineering* dalam dunia keamanan siber pada tahun 1990-an, sebagai seorang aktor jahat yang merekayasa situasi sosial untuk mengelabui seseorang untuk mengambil tindakan tertentu.[53]

---

[52]Fatima Salahdine dan Naima Kaabouch, "Social Engineering Attacks: A Survey", *Future Internet,* Vol. 11, No. 89, 2019, pp. 1-17, DOI : 10.3390/fi11040089, hlm. 1-2.

[53]Kevin Mitnik dan The Global Ghost Team, *The History of : Social Engineering & How to Stay Safe* (Las Vegas: Mitnick Security Consulting, 2020), hlm. 5.

3. Kisah Kevin Mitnick dan Motorola

Kasus Serangan Kevin Mitnick dan Motorola

Di tengah pengejaran oleh FBI, Kevin bekerja pada sebuah firma hukum besar di Denver. Suatu ketika, Kevin membaca majalah yang mencantumkan produsen *handset* selular terbaik seperti Nokia, Ericsson, Fujitsu, NEC serta Motorola. Ketertarikannya, membuat Kevin terpacu untuk mengejar *source code* masing-masing produk. Dengan harapan dapat berkomunikasi secara pribadi dan menghindari penangkapan, Kevin memulai langkahnya untuk memanipulasi teknologi dalam ponsel MicroTAC Ultra Lite yang dikembangkan oleh Motorola. Agar dapat berjalan tanpa terdeteksi dan terlacak, Kevin memutuskan untuk mencari *source code firmware* telepon. Sebagai target awal, upaya berkomunikasi dengan manajer proyek MicroTAC Ultra Lite dilakukan dan tersambung pada resepsionis yang meneruskannya berkali-kali kepada pihak lain, hingga berakhir pada VP untuk semua Motorola Mobility.

Ketika menerima pengalihan telepon berulang kali, Kevin mendapatkan beragam informasi menarik, salah satunya adalah fakta bahwa Motorola memiliki pusat penelitian yang berlokasi di Arlington Heights. Dengan berpura-pura sebagai pegawai karyawan dari cabang Arlington, Kevin meminta untuk dapat menghubungi Manajer Proyek Ultra Lite dan mendapatkan informasi tambahan kembali bila manajer, Pam tengah berlibur. Pada pesan suaranya, manajer meninggalkan nomor kontak untuk menghubungi orang lain ketika dirinya tidak ada. Kevin menelepon kontak tersebut, Alicia, dan bertanya apakah Pam pergi berlibur? – agar menciptakan ilusi bahwa Kevin dan Pam telah terhubung sebelumnya dan membuat ceritanya semakin dapat dipercaya. Kevin kemudian memberi tahu Alicia bahwa Pam berjanji kepadanya bahwa akan mengiriminya *source code* Ultra Lite, namun mengatakan bahwa Pam terkendala mengirimkannya, dan Alicia dapat mengirimkannya.

Kevin kemudian menginstruksikan kepada Alicia tentang cara *zip file*, karena ada ratusan file. Tetapi ketika Kevin mencoba menginstruksikan tentang cara mentransfer zip ke FTP anonimnya, koneksi gagal dan Alicia memintanya untuk menunggu, sementara beranjak pergi untuk memanggil manajer keamanannya agar dapat membantu.

Di sinilah Kevin panik, menyadari jika petugas keamanan terlibat, maka akan mencurigai adanya kecurangan. Tetapi yang mengejutkan, Alicia kembali dengan nama pengguna dan kata sandi pribadi petugas keamanan ke server proxy untuk mengunggah file.

Narasi cerdas ini membantu Kevin menyelesaikan misinya dan pergi dengan *source code*. Meskipun pada akhirnya Kevin tidak melakukan apa pun dengan kode tersebut, jenis informasi yang sangat sensitif ini dapat dengan mudah dijual untuk keuntungan tinggi, atau digunakan sebagai pemerasan terhadap Motorola untuk pembayaran yang besar jika berada di tangan penjahat dunia maya.

Untuk informasi lebih lanjut terkait **Serangan Kevin Mitnick dan Motorola**, Anda dapat melihat video dengan *scan QR code* di samping.

A. Hak-hak Digital

Memahami hak asasi manusia dan perkembangannya menuntut pemahaman utuh dari makna suci keberadaannya hingga diskursus terhadapnya, yang tidak jarang melahirkan pertentangan ataupun perbedaan pandangan dalam melihatnya. Salah satu perdebatannya adalah penggunaan istilah *new human rights* dan *digital rights*. Buku ini akan lebih fokus untuk membahas perihal *digital rights,* namun guna memperjelas, akan sedikit diuraikan perihal istilah *new human rights* yang lekat hubungannya dengan kebaruan atau *novelty*. Mart Susi menjelaskan bahwa unsur kebaruan dalam *new human rights* memiliki dua aspek utama, yakni epistemik dan ontik. Aspek epistemik dipengaruhi oleh waktu dan mengacu pada proses pengembangan pengetahuan dan praktik diskursif dari pengenalan gagasan klaim *new human rights*, umumnya mencerminkan nilai sosial yang penting secara fundamental, hingga beberapa saat setelah pengakuan regional atau universal, baik dalam *human rights positive* atau *soft law*, ataupun sebaliknya, penolakannya. Klaim 'kebaruan' dimulai sebelum dan berakhir setelah pengakuan *new human rights* dalam keluarga yang disebut hak asasi manusia yang berdiri sendiri. Sementara aspek ontik kebaruan mengacu pada konseptualisasi *new human rights* dalam lingkaran hak asasi manusia yang telah mapan. Aspek ontik adalah tentang isi klaim *new human rights vis-à vis* hak asasi manusia yang telah ditetapkan, yang terakhir dipahami sebagai hak asasi manusia di mana tidak ada kontestasi tentang keberadaan mereka pada prinsipnya dan pengakuan keberlakuannya.[54]

Oleh karena kompleksitas konsep hak asasi manusia modern, *new human rights* turut dapat tetap dalam keadaan kontestasi yang berkelanjutan, yang dapat menyebabkan fragmentasi internasional tentang perlunya hak ini atau penolakan hak di masa depan. Bahkan bila *new human rights* diperkenalkan dan kemudian diterima melalui kondisi ideal diskursif, *new human rights* dapat mengklaim kebaruan setidaknya untuk beberapa waktu setelahnya. Kontestasi klaim *new human rights* turut dapat menyebabkan *new human rights* ini secara

[54]Mart Susi, "Novelty in New Human Rights: The Decrease in Universality and Absractness Thesis", dalam Andreas Von Arnauld (ed), *The Cambridge Handbook of New Human Rights: Recognition, Novelty, Rhetoric* (UK: Cambridge University Press, 2020), hlm. 21-22.

meyakinkan dipandang sebagai bagian dari hak yang ada, dalam hal ini istilah "*novelty*" membawa bobot retoris yang dominan.[55]

Penjelasan Mart Susi di atas tidak serta dapat mengenyampingkan pandangan penstudi lain, yang menilai bila pengkajian hak asasi manusia belum selesai dan paripurna, sehingga beragam upaya telah dilahirkan guna mengenalkan lebih jauh hingga menyelami hak asasi manusia, seperti *Human Rights Education* (HRE) yang merupakan konsep pendidikan dan pelatihan dengan tujuan guna berkontribusi aktif dalam pembangunan budaya universal hak asasi manusia melalui pengajaran tentang hak asasi manusia dan kebebasan dasar.[56] Pada wilayah lain, perlu diakui bila pengkajian terhadap hak asasi manusia kian tumbuh dan berkembang dalam ruang akademik, salah satunya terkait perkembangan teknologi informasi yang bagi sebagian penstudi dinilai telah mengubah arsitektur dasar hak asasi manusia. Teknologi dalam lingkup HAM digambarkan sebagai pedang bermata dua, yang dapat berakibat baik maupun buruk. Teknologi telah menghadirkan peluang baru bagi kemajuan hak asasi manusia. Seperti media sosial dan aplikasi perpesanan layaknya WhatsApp yang telah digunakan guna memobilisasi orang dalam membela hak dan kepentingannya. Tidak hanya itu, internet telah memainkan peran penting dalam membantu organisasi hak asasi manusia guna mengumpulkan dan menyebarkan informasi tentang hak asasi manusia kepada masyarakat umum, serta sistem penyimpanan informasi yang dapat memudahkan penyimpanan dan penggunaan informasi, bahkan ponsel pintar yang dapat menjadi alat ampuh untuk merekam dan mendokumentasikan pelanggaran HAM.[57]

Pada sisi lain, perkembangan teknologi telah melahirkannya konsep baru terkait pengawasan masyarakat. *Dataveillance,* CCTV di tempat umum, petugas polisi yang dilengkapi dengan kamera video telah menjadi bagian integral dari kehidupan masyarakat saat ini,

---

[55]*Ibid*.

[56]Alison E. C. Struthers, "Human Rights: A Topic Too Controversial for Mainstream Education?", *Human Rights Law Review*, Vol. 16, Issue 1, 2016, hlm. 131-132.

[57]Mark Anthony V Ambay III, *et.al.,* "Dystopia is Now: Digital Authoritarianism and Human Rights in Asia", *Global Campus Human Rights Journal*, Vol. 3, No. 2, 2019, hlm. 271.

hingga pemerintah dan berbagai perusahaan yang telah mengumpulkan sejumlah besar informasi pribadi sampai batas tertentu yang bahkan dapat mengenal seseorang lebih baik dibandingkan teman maupun keluarganya.[58]

Pada tahun 2012, Vinton Cerf yang dikenal sebagai salah satu bapak internet berpendapat bahwa tidak terdapat hak asasi manusia atas internet, yang kemudian secara tegas ditolak oleh Kay Mathieses dengan mengatakan bahwa Cerf gagal melihat perbedaan antara hak asasi manusia dasar dan hak asasi manusia turunan. Memahami hak yang terkait dengan teknologi informasi dan komunikasi (TIK) seperti internet sebagai hak turunan adalah kunci untuk memahami hak asasi manusia di era digital. Pandangan Cerf memperjelas bahwa diperlukan pertimbangan yang lebih cermat terhadap hak asasi manusia dan TIK. Untuk itu Mathieses menyarankan kerangka berpikir melalui relevansi hak asasi manusia dengan konteks digital dan relevansi teknologi digital dengan hak asasi manusia.[59]

Keterkaitan antara digitalisasi, teknologi informasi dan hak asasi manusia umumnya dikaji dari optik ancaman yang dihadirkan oleh teknologi terhadap hak asasi manusia. Beragam contoh pelanggaran hak asasi manusia yang diakibatkan oleh penyalahgunaan teknologi digital umumnya hadir pada bidang pengawasan digital, privasi, keamanan dalam beraktivitas di dunia maya, ketidakmampuan orang untuk mengakses internet hingga menghadirkan respons terhadapnya berupa konsep integritas digital[60] hingga hak-hak digital.

Menurut tipologinya, terdapat tiga generasi hak asasi manusia digital atau hak-hak digital. Generasi pertama melibatkan proses penyesuaian hak asasi manusia *offline* yang luas pada dunia *online*. Generasi kedua menggambarkan kemunculan hak digital baru, yaitu hak yang melindungi aktivitas *online* yang tidak memiliki kedekatan secara paralel di dunia *offline*. Meskipun hak digital generasi kedua dapat ditelusuri kembali dalam hak asasi manusia *offline* yang telah ada, namun perkembangannya

---

[58]Roman V. Prudentov, "Private Life and Surveillance in a Digital Era: Human Rights in European Perspective", *Digital Law Journal*, Vol. 1, No. 2, 2020, hlm. 43.

[59]Kay Mathiesen, "Human Rights for the Digital Age", *Journal of Mass Media Ethics*, Vol. 29, Issue 1, 2014, hlm. 2.

[60]Johan Rochel, "Connecting the Dots: Digital Integrity as a Human Right", *Human Rights Law Review*, Vol. 21, Issue 2, 2021, hlm. 358.

yang baru tidak sepenuhnya dapat dimasukkan dalam hak-hak asalnya dan akan sulit untuk sepenuhnya menangkap kepentingan dan kebutuhan yang akan dilindungi jika tidak dilindungi dan diakui sebagai hak yang berdiri sendiri. Sementara itu, generasi ketiga terdiri dari hak milik persona *online* baru, yaitu representasi digital atau virtual dari orang atau badan hukum yang dapat eksis dan menggunakan hak secara terpisah dari manusia atau badan hukum yang menciptakannya. Pada saat yang sama, generasi ketiga hak asasi manusia digital juga diharapkan untuk fokus pada tugas perusahaan internet dan entitas lain yang menjalankan kekuasaan tata kelola *de facto* dari pemegang hak.[61]

Tahun 2014, *United Nations Human Rights Office of the High Commissioner* mempublikasikan laporan berjudul *the charter of human rights and principles for the internet* yang bertujuan untuk memastikan semua aktor, baik publik maupun swasta, menghormati dan melindungi hak asasi manusia di internet. Oleh karena itu, dilakukan sebuah perumusan berupa *10 Internet Rights & Principles,* yakni sebagai berikut.[62]

1. *Universality and Equality*

   Semua manusia dilahirkan bebas dan setara dalam martabat dan hak, yang harus dihormati, dilindungi, dan dipenuhi dalam lingkungan *online*.

2. *Rights and Social Justice*

   Internet adalah ruang untuk pemajuan, perlindungan serta pemenuhan hak asasi manusia dan pemajuan keadilan sosial. Setiap orang memiliki kewajiban untuk menghormati hak asasi orang lain di lingkungan *online*.

3. *Accessibility*

   Setiap orang memiliki hak yang sama untuk mengakses dan menggunakan internet yang aman dan terbuka.

4. *Expression and Association*

   Setiap orang berhak untuk mencari, menerima, dan memberikan informasi secara bebas di internet tanpa sensor atau campur tangan

[61]Dafna Dror-Shpoliansky dan Yuval Shany, "It's The End of The (Offline) World as We Know it: From Human Rights to Digital Human Rights – a Proposed Typology", *Hebrew University of Jerusalem Legal Research Paper,* No. 20-36, 2020, (hlm. 25).

[62]Marianne Fraklin, *et.al.,* "The Charter of Human Rights and Principles for the Internet", *Internet Governance Forum dan United Nation*, August 2014, hlm. 7.

lainnya. Setiap orang juga berhak untuk berserikat secara bebas melalui dan di internet, untuk tujuan sosial, politik, budaya atau lainnya.

5. *Privacy and Data Protection*

   Setiap orang berhak atas privasi *online*. Ini termasuk kebebasan dari pengawasan, hak untuk menggunakan enkripsi, dan hak untuk anonimitas *online*. Setiap orang juga berhak atas perlindungan data, termasuk kontrol atas pengumpulan, penyimpanan, pemrosesan, pembuangan, dan pengungkapan data pribadi.

   Konsep anonimitas *online* ini dikenal sebagai *the right to a name*. Sekalipun menjadi perdebatan, Ulbashev menjelaskan pandangannya dengan memberikan penjelasan bahwa saat seseorang menggunakan nama panggilan di internet, seseorang tidak kehilangan *the right to a name*. Sebaliknya, mereka menggunakan hak ini. Selain itu, mengakui bahwa internet adalah bagian dari kehidupan pribadi, negara harus memperlakukannya dengan sangat hormat.

   Penggunaan nama panggilan tidak mengandung sesuatu yang ilegal. Ini dapat dibandingkan dengan mengenakan burqa. Meskipun nama samaran "menutupi kepribadian", itu tidak menggantikan nama (seperti kerudung, menyembunyikan wajah seorang wanita, tidak benar-benar menghilangkan kepribadiannya). Nama samaran, seperti halnya mengenakan burqa, adalah pilihan bebas oleh orang yang bebas.[63]

6. *Life, Liberty, and Security*

   Hak untuk hidup, kebebasan, dan keamanan harus dihormati, dilindungi, dan dipenuhi secara *online*. Hak-hak ini tidak boleh dilanggar, atau digunakan untuk melanggar hak-hak lain, di lingkungan *online*.

7. *Diversity*

   Keragaman budaya dan bahasa di internet harus dipromosikan, termasuk inovasi teknis serta kebijakannya harus didorong untuk memfasilitasi pluralitas ekspresi.

---

[63]Alim K. Ulbashev, "The Right to a Name: Back to the Future", *Digital Law Journal*, Vol. 1, No. 3, 2020, hlm. 44.

8. *Network Equality*

   Setiap orang harus memiliki akses universal dan terbuka kepada konten internet, bebas dari prioritas diskriminatif, penyaringan atau kontrol lalu lintas atas dasar komersial, politik atau alasan lainnya.

9. *Standards and Regulation*

   Arsitektur internet, sistem komunikasi, serta format dokumen dan data harus didasarkan pada standar terbuka yang memastikan interoperabilitas, penyertaan, dan kesempatan yang sama bagi semua.

10. *Governance*

    Hak asasi manusia dan keadilan sosial harus membentuk landasan hukum dan normatif di mana internet beroperasi dan diatur. Ini akan terjadi secara transparan dan multilateral, berdasarkan prinsip keterbukaan, partisipasi inklusif dan akuntabilitas.

Pada tahun 2016, sebuah tambahan diberikan dalam Pasal 19 Deklarasi Universal Hak Asasi Manusia yang mendeklarasikan akses kepada internet sebagai hak asasi manusia yang mendasar,[64] setelah sebelumnya pada tahun 2015, Dewan Hak Asasi Manusia PBB telah terlebih dahulu mengadopsi resolusi penting yang mengakui hak privasi di era digital dengan menegaskan bahwa "*the same rights that people have offline must also be protected online, including the right to privacy*",[65] maka menjadi sebuah pemahaman bersama jika terjadi proses evolusi pada konsep hak asasi manusia yang telah ada, dan lazim saat ini dikenal dengan istilah hak digital.

Beberapa pengertian dari hak digital, di antaranya sebagai berikut.

1. *Digital rights are recognized as a type of property rights. They will be able to certify the rights to all objects of civil rights (except for intangible benefits) to participate in civil legal relations, as objects of civil circulation.*[66]

---

[64]Cynthia K. Sanders dan Edward Scanlon, "The Digital Divide Is a Human Right Issue: Advancing Social Incluision Through Social Work Advocacy", *Journal of Human Rights and Social Work*, Vol. 6, Issue 2, 2021, hlm. 135.

[65]Yohannes Eneyew Ayalew, "Untrodden Paths Towards the Right to Privacy in The Digital Era Under African Human Right Law", *International Data Privacy Law*, Vol. 12, Issue 1, February 2022, hlm. 22.

[66]A. A. Kartskia dalam Kambariddin M. Mehmonov dan Elbek T. Musaev, "Legal Regime of Digital Rights", *Elementary Education Online*, Vol. 21, Issue 2, 2022, hlm. 1684.

2. *Digital rights are human and legal rights that allow individual to access, use, create, and publish digital content on devices such as computers and mobile phone, as well as in virtual spaces and communities.*[67]
3. *The totality of electronic data (digital code or designation) existing in a decentralized information system, information technology and technical means of which provide a person with unique access to this digital code or designation, as well as the opportunity to familiarize with the description of the corresponding object of civil rights at any time.*[68]
4. *Digital rights are considered the same basic human rights that exist in the offline world, but only in the online world.*[69]
5. *Human rights as applicable in the digital sphere. That is human rights in both physically constructed spaces, such as infrastructure and devices, and in spaces that are virtually constructed, like our online identities and communities.*[70]
6. *The extension of fundamental human rights protections for digital data tied to a person's identity and behavior in the physical or virtual realms.*[71]

Pada 22 Januari 2022, Komisi Eropa (*European Commission)* mengusulkan kepada Parlemen dan Dewan Eropa untuk menandatangani deklarasi hak dan prinsip yang akan memandu transformasi digital di Uni Eropa. Draf deklarasi tentang *digital rights and principles* bertujuan guna memberikan semua orang titik referensi yang jelas tentang jenis transformasi digital yang dipromosikan dan dipertahankan di Eropa. Draf ini akan pula memberikan panduan bagi pembuat kebijakan dan perusahaan ketika berhadapan dengan teknologi baru. Deklarasi

---

[67]Reventlow dalam Luci Pangrazio dan Julian Sefton Green, "Digital Rights, Digital Citizenship and Digital Literacy: What's the Difference?", *Journal of New Approaches in Educational Research*, Vol. 10, No. 1, 2021, hlm. 19.

[68]Draft Federal Law N 424632-7 "On Amandemeny to Parts One, Two and Article 1124 of Part Three of the Civil Code of the Russian Federation" dalam Korobeinikova TS, "Digital Rights as an Object of Civil Rights", *Prosiding Advances in Economic, Business and Management Research*, Vol. 138, 2nd International Scientific and Practical Conference "Modern Management Trends and the Digital Economy: From Regional Development to Global Economic Growth (MTDE 2020)", hlm. 231.

[69]Timofey Grigorievich Makarov dan Elena Vassilievna Kobchikova, "Digital Rights", *Utopia y Praxis Latinoamericana*, Vol. 25, No. 12, 2020, hlm. 203.

[70]Institute for Internet & the Just Society, "Digital Human Rights", https://www.internetjustsociety.org/digital-human-rights (diakses pada 2 Juli 2022).

[71]Rebekah Dowd, *The Birth of Digital Human Rights: Digitized Data Governance as a Human Rights Issue in the EU* (Cham: Palgrave Macmillan, Springer, 2022), hlm. 249.

tersebut juga akan menentukan pendekatan terhadap transformasi digital yang akan dipromosikan oleh UE di seluruh dunia. Draf tersebut mencakup hak-hak dan prinsip-prinsip utama dalam transformasi digital, seperti menempatkan orang dan hak-hak individu sebagai pusatnya, mendukung solidaritas dan inklusi, memastikan kebebasan memilih secara *online*, mendorong partisipasi dalam ruang publik digital, meningkatkan keselamatan, keamanan, dan pemberdayaan individu serta mempromosikan keberlanjutan masa depan digital.[72]

Setelah serangkaian diskusi panjang perihal kehadiran hak-hak digital, pada awal tahun 2022, Profesor Hukum dari Universitas Leiden, Bart Custers kembali mendiskusikan perihal hak-hak digital dengan tajuk ***'New Digital Rights'.*** Pembahasan ini diawali Custers dengan mencermati kondisi persoalan hukum yang berkaitan dengan hak-hak warga negara dengan melakukan kategorisasi pada tiga jenis problematika, yakni: (1) pelanggaran hak akibat (penggunaan) teknologi baru; (2) hak yang saling bertentangan akibat (penggunaan) teknologi baru; (3) masalah baru yang dihasilkan dari (penggunaan) teknologi baru, yang belum terdapat haknya.[73] Dalam tulisannya tersebut, Custers kembali menawarkan sepuluh *new digital rights,* yakni:[74] *(1) the right to be offline; (2) the right to internet access; (3) the right not to know; (4) the right to change your mind; (5) the right to start over with a clean (digital) slate; (6) the right to expiry dates for data; (7) the right to know the value of your data; (8) the right to a clean digital environment; (9) the right to a safe digital environment;* dan *(10) the right to digital education.*

Dalam pembahasannya perihal *the right to be offline,* Custers menjelaskan perihal kehadiran *right to disconnect* yang diperkenalkan oleh Prancis pada tahun 2017. Namun, pada satu sisi, hak ini memiliki irisan dengan hak lainnya yang menjadi bagian kajian hak-hak digital, seperti *right to internet access* di India yang sejak 2019 telah dinyatakan sebagai hak fundamental oleh Mahkamah Agung, dan menjadi bagian dari

---

[72]European Commission, "Commission Puts Forward Declaration on Digital Rights and Principles for Everyone in the EU", *Press Release*, 22 Januari 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_452 (diakses pada 27 Juni 2022).

[73]Bart Custers, "New Digital Rights: Imagining Additional Fundamental Rights for the Digital Era", *Computer Law & Security Review*, Vol. 44, 2022, pp. 1-13, DOI: https://doi.org/10.1016/j.clsr.2021.105636, hlm. 1.

[74]*Ibid.*, hlm. 6-12.

hak atas pendidikan serta hak privasi sebagaimana yang diamanatkan dalam Pasal 21 Konstitusi India. Berkaca pada kasus *"Faheema Shirin vs State of Kerela 2019",* terkait seorang mahasiswi berusia 19 tahun di Kerala yang dikeluarkan dari asramanya karena menolak menyerahkan ponselnya antara pukul 6 sore hingga 10 malam. Mahasiswi tersebut memperjuangkan jalannya secara hukum melawan aturan asrama, dan berpendapat bahwa aturan asrama melanggar hak fundamentalnya atas kebebasan berekspresi, hak atas privasi dan hak atas pendidikan. Oleh karena *handphone* tidak hanya digunakan untuk hiburan, tetapi juga digunakan untuk keperluan akademik seperti persiapan tugas kuliah atau bahkan makalah penelitian.[75]

Berdasarkan sifatnya, terdapat lima fitur khusus *digital rights,* yakni: (1) harus diabadikan dalam undang-undang; (2) pelepasan haknya dapat dilakukan murni dalam kerangka sistem informasi yang relevan; (3) pemilik hak digital adalah subjek yang dapat melepaskan hak ini, kecuali ditentukan lain oleh hukum; (4) persetujuan debitur untuk pengalihan hak digital berdasarkan transaksi tidak diperlukan; dan (5) undang-undang menetapkan hak-hak digital yang dapat dinegosiasikan.[76]

Sementara itu, *digital rights* sendiri begitu erat kaitannya dengan hak atas privasi, bahkan privasi umumnya menjadi tema utama yang muncul ketika pengkajian dilakukan terhadap *digital rights*. Saat ini, privasi memiliki makna dan pengertian yang luas. Beberapa penstudi berupaya untuk mendefinisikannya sebagai *demands respect for a broad range of loosely allied personal interests: physical or bodily integrity; personal identity and lifestyle (at least to some respects), including sexuality and sexual orientation; reputation; family life; the home and home environment, includes reference to the types of information available about an individual, whether they are primary or derived from analysis. These types of information include behavioral, financial, medical, biometric, consumer, and biographical*.[77]

---

[75]Mehak Ahuja dan Anshdha Sharma, "Right to Internet: Fundamental Right", *IOSR Journal of Humanities and Social Science*, Vol. 25, Issue 12, Series 8, 2020, pp. 1-12, DOI: 10.9790/0837-2512080112, hlm. 1.

[76]Timofey Grigorievich Makarov, *Loc. Cit*.

[77]Juliane Damen, *et.al.,* "The Human Right of Privacy in the Digital Age", *Staat, Recht und Politik- Forschungs- und Diskussionpapiere*, Working Paper, Universitatsverlag Potsdam, 2017, hlm. 2-3.

B. Definisi *Social Engineering*

1. *Social Engineering* Menurut Roscoe Pound

Bagi para penstudi hukum di Indonesia, kata *social engineering* mengandung relasi yang kuat dengan dua teori besar hukum yang dikenalkan oleh Roscoe Pound serta Mochtar Kusumaatmadja. Roscoe Pound mengenalkan konsep *law as a tool of social engineering*.[78] Bahkan Munir Fuady dalam bukunya membuat bab khusus dengan judul *Teori Hukum yang Merekayasa Masyarakat*. Konsep *law as a tool of social engineering* yang dirilis oleh Roscoe Pound bertentangan dengan pandangan yang umumnya dianut saat itu, bahwa bukan perubahan hukum yang memengaruhi perkembangan masyarakat, tetapi justru perubahan dalam masyarakat yang memengaruhi perkembangan hukum.[79]

Fokus utama Pound dengan konsep *law as a tool of social engineering* adalah *interest balancing*, dan karenanya yang terpenting adalah tujuan akhir dari hukum yang diaplikasikan dan mengarahkan masyarakat ke arah yang lebih maju. Bagi Pound, antara hukum dan masyarakat terdapat hubungan yang fungsional. Dan karena kehidupan hukum terletak pada karya yang dihasilkannya bagi dunia sosial, maka tujuan utama dalam *social engineering* adalah mengarahkan kehidupan sosial itu ke arah yang lebih maju. Menurutnya, hukum tidaklah menciptakan kepuasan, tetapi hanya memberikan legitimasi atas kepentingan manusia untuk mencapai kepuasan tersebut dalam keseimbangan. Hukum sebagai sarana *social engineering*, bermakna penggunaan hukum secara sadar untuk mencapai tertib atau keadaan masyarakat sebagaimana dicita-citakan, atau untuk melakukan perubahan yang diinginkan. Hukum tidak lagi dilihat sekadar sebagai tatanan penjaga *status quo*, tetapi juga diyakini sebagai sistem pengaturan untuk mencapai tujuan-tujuan tertentu secara terencana. Sifat hukum sebagai produk *by design* intelektual ilmiah dalam konsep *social engineering*, terlihat jelas dalam rincian persoalan yang menurut Pound wajib dilakukan oleh seorang ahli hukum sosiologis agar hukum dapat benar-benar efektif sebagai alat perubahan sosial. Secara sistematis

[78]Roscoe Pond, *Contemporarty Juristic Theory* (Claremont CA: Pamona College, 1940), hlm. 80.

[79]Munir Fuady, *Teori-Teori Besar (Grand Theory) dalam Hukum* (Jakarta: Kencana, 2013), hlm. 251.

Pound mengemukakan enam langkah yang harus dilakukan dalam mewujudkan hukum sebagai sarana perubahan sosial, yaitu:[80]

a. mempelajari efek sosial yang nyata dari lembaga-lembaga serta ajaran-ajaran hukum;
b. melakukan studi sosiologis dalam rangka mempersiapkan perundang-undangan untuk mempelajari pelaksanaannya dalam masyarakat serta efek yang ditimbulkan, untuk kemudian dijalankan;
c. melakukan studi tentang bagaimana peraturan hukum menjadi efektif;
d. memperhatikan sejarah hukum, artinya mempelajari efek sosial yang ditimbulkan oleh ajaran-ajaran hukum pada masa yang lalu dan bagaimana cara menimbulkannya. Studi ini dimaksudkan untuk menunjukkan bagaimana hukum pada masa yang lalu itu tumbuh dari kondisi sosial, ekonomi, dan psikologis, bagaimana ia menyesuaikan diri pada kesemuanya itu, dan seberapa jauh kita dapat mendasarkan atau mengabaikan hukum itu guna mencapai hasil yang kita inginkan;
e. pentingnya melakukan penyelesaian individual berdasarkan nalar, bukan berdasarkan peraturan hukum semata. Artinya, hakim diberi keleluasaan untuk memutuskan perkara berdasarkan nalar yang umum untuk memenuhi tuntutan keadilan dari pihak-pihak yang bersengketa;
f. mengusahakan secara lebih efektif agar tujuan-tujuan hukum dapat tercapai.

Social engineering merupakan konsep sentral dan dominan dari keseluruhan bangunan pemikiran hukum Roscoe Pound. Hal ini merupakan konsekuensi logis dari akal pemikiran Pound yang berbasis kepada sosiologi. Pound menjadikan sosiologi sebagai fondasi utama dalam menciptakan teori hukumnya, dengan ide utama untuk mentransformasikan hukum dalam tataran ide menjadi hukum dalam tataran realitas (*to bring the law in books into direct contact with the law in action)*. Hukum tidak boleh diisolasi dan terisolasi dari realitas sosial yang dinamis.[81]

---

[80]Bernard L. Tanya, *et.al., Teori Hukum: Strategi Tertib Manusia Lintas Ruang dan Generasi* (Yogyakarta: Genta Publishing, 2013), hlm. 145-147.

[81]Atip Latipulhayat, "Khazanah: Roscoe Pound"*, Padjajaran Jurnal Ilmu Hukum,* Vol. 1, No. 2, 2014, hlm. 417.

Istilah *social engineering* digunakan oleh Pound ketika menjelaskan mengenai fungsi dan peran hukum dan ahli hukum (*lawyers)*. Menurut Pound ahli hukum itu harus berperan seperti seorang insinyur (*engineer)* ketika yang bersangkutan akan mendirikan sebuah bangunan, jembatan, dan sebagainya. Dalam hal ini seorang insinyur akan membuat dan menyiapkan sebuah perencanaan (*planning)* yang kemudian akan diikuti dengan pengumpulan material-material yang diperlukan. Selanjutnya sang insinyur akan membuat sejumlah penyesuaian antara material yang terkumpul dengan perencanaan yang dibuat agar sesuai dengan kebutuhan. Dalam konteks ini Pound kemudian menganalogikan seorang ahli hukum dengan seorang insinyur ketika yang bersangkutan akan membuat hukum. Ahli hukum harus memiliki perencanaan yang matang, mampu menginventarisasi kebutuhan-kebutuhan masyarakat dan selanjutnya ahli hukum tersebut harus mampu melakukan penyesuaian-penyesuaian dan keseimbangan dari berbagai kepentingan tersebut sehingga tercipta bangunan hukum yang kokoh dan fungsional.[82]

Dua kata yang digunakan dalam teori *"social engineering"* adalah pertama, kata *"social"* yang merujuk kepada kelompok individu yang membentuk suatu masyarakat, dan kedua adalah kata *"engineering",* yang berarti ilmu terapan yang digunakan oleh seorang insinyur untuk menghasilkan produk akhir yang diperlukan oleh masyarakat yang diperlukan untuk memenuhi kebutuhan masyarakat tersebut. Dengan mengombinasikan kedua kata tersebut, Pound berbicara mengenai fungsi dan peran seorang insinyur. Menurut Pound, sebagaimana halnya seorang insinyur, hakim dan ahli hukum harus menerapkan hukum di ruang pengadilan yang memungkinkan aspirasi masyarakat dapat dipenuhi dan dilaksanakan. Oleh karenanya Pound kemudian menyebut hukum sebagai *a tool of social engineering*.[83]

2. *Social Engineering* Menurut Mochtar Kusumaatmadja

Di Indonesia, *social engineering* kerap identik dengan pemikiran Mochtar Kusumaatmadja, setelah mengintrodusir sebuah teori hukum pembangunan yang dibangun di atas teori kebudayaan dari Norhrop,

[82]*Ibid.*, hlm. 418.
[83]*Ibid.*, hlm. 419.

teori orientasi kebijaksanaan (*policy-oriented)* dari Mc. Dougal dan Laswell, serta teori pragmatis dari Roscoe Pound. Teori hukum pembangunan Mochtar merupakan transformasi dari teori hukumnya sendiri, dengan penambahan transformasi dari teori hukum Roscoe Pound. Namun, Mochtar dengan sangat ketat menyatakan bahwa ia menolak konsepsi mekanis dan konsepsi *'law as a tool of social engineering'*, dan karenanya menggantikan istilah 'alat' (*a tool)* itu dengan istilah sarana.[84]

Terdapat tiga hal baru yang dikembangkan oleh Mochtar Kusumaatmadja dalam dunia hukum, yaitu: konsep hukum baru, hukum sebagai sarana pembaharuan masyarakat, dan hukum ada yang bersifat netral dan tidak netral.[85] Gagasan utama Mochtar Kusumaatmadja adalah "hukum sebagai sarana pembaharuan masyarakat", yang kemudian dikenal dengan nama "teori hukum pembangunan". Teori ini mengatakan, bahwa hukum merupakan sarana pembaharuan masyarakat yang didasarkan atas anggapan bahwa adanya keteraturan atau ketertiban dalam usaha pembangunan atau pembaharuan itu merupakan sesuatu yang diinginkan atau bahkan dipandang (mutlak) perlu. Anggapan lain yang terkandung di dalam konsepsi tersebut menurut Mochtar adalah bahwa hukum dalam arti kaidah atau peraturan hukum dapat berfungsi sebagai alat (pengatur) atau sarana pembangunan dalam arti penyalur arah kegiatan manusia ke arah yang dikehendaki oleh pembangunan atau pembaharuan.[86]

Dalam tulisannya, Atip memberikan perhatian dengan penggunaan kata pembaharuan masyarakat oleh Mochtar Kusumaatmadja. Menurutnya istilah ini kemungkinan besar adalah terjemahan dari kata *"social engineering"* yang kemudian menjadi kontroversial ketika diterjemahkan lagi (oleh beberapa kalangan) menjadi rekayasa masyarakat (sosial). Titik kontroversinya adalah pada kata "rekayasa" yang maknanya antara lain adalah penerapan kaidah-kaidah ilmu hukum dalam pelaksanaan (aplikasi ilmu), misalnya perancangan, konstruksi, dan sebagainya. Makna kata rekayasa ini sangat dekat dengan sesuatu

---

[84]Lili Rasjidi dan I.B Wyasa Putra, *Hukum Sebagai Suatu Sistem* (Bandung: Mandar Maju, 2003), hlm. 182-183.

[85]Lili Rasjidi dalam kata pengantar pada Romli Atmasasmita, *Teori Hukum Intergratif: Rekonstruksi terhadap Teori Hukum Pembangunan dan Teori Hukum Progresif* (Yogyakarta: Genta Publishing, 2012), hlm. V.

[86]Mochtar Kusumaatmadja, *Konsep-Konsep Hukum dalam Pembangunan* (Bandung: Alumni, 2006), hlm. 88.

yang bersifat mekanistik, sehingga ketika digandengkan dengan kata "*social*" (masyarakat) akan cenderung bermakna negatif, karena akan dipahami sebagai mengelabui masyarakat. Persepsi ini akan mendapat pembenaran ketika rekayasa juga dapat dimaknai sebagai rencana jahat atau persengkokolan untuk merugikan pihak lain.[87]

3. Rekaya Sosial Menurut Jalaluddin Rakhmat

Pada tahun 1999, Jalaluddin Rakhmat menerbitkan buku dengan judul *Rekayasa Sosial: Reformasi, Revolusi, atau Manusia Besar?*. Jalaluddin Rakhmat menguraikan bila perubahan sosial yang direncanakan kerap diistilahkan dengan *social engineering* yang diartikan sebagai rekayasa sosial.[88] Istilah *social engineering* yang dimaksud dalam buku ini berbeda dengan makna yang dimaksud sebelumnya, baik oleh Roscoe Pound dan Mochtar Kusumaatmadja. Makna yang diperuntukkan dalam tulisan Jalaluddin Rakhmat dimaksudkan dalam pembahasan perubahan sosial.

Alasan yang diutarakan mengapa menggunakan rekayasa sosial, karena untuk mengubah masyarakat dibutuhkan perencanaan sosial, manajemen perubahan ataupun rekayasa sosial. Bila dibandingkan dengan istilah perencanaan, rekayasa memiliki jangkauan makna yang lebih luas atau lebih pragmatis. Suatu rekayasa pasti mengandung perencanaan, tetapi tidak seluruh perencanaan diimplementasikan hingga teraktualisasi di alam nyata. Dibandingkan dengan istilah manajemen perubahan, istilah rekayasa sosial juga lebih memiliki makna yang pasti. Objek dari rekayasa sosial sudah pasti, yaitu perubahan sosial menuju suatu tatanan dan sistem baru dengan yang dikehendaki sang perekayasa (*the social engineer*).[89]

4. *Social Engineering* dalam Studi Keamanan Siber

Dalam konteks keamanan siber, *social engineering* menggambarkan jenis serangan yang bertujuan mengeksploitasi kerentanan manusia (dengan cara memengaruhi, persuasi, penipuan, manipulasi, dan membujuk) guna

---

[87]Atip Latipulhayat, "Khazanah: Mochtar Kusumaatmadja", *Padjajaran Jurnal Ilmu Hukum*, Vol. 1, No. 3, 2014, pp. 626-642, hlm. 631.

[88]Jalaluddin Rakhmat, *Rekayasa Sosial: Reformasi, Revolusi, atau Manusia Besar?* (Bandung: Rosdakarya, 1999), hlm. 46.

[89]*Ibid.*, hlm. vi.

melanggar tujuan keamanan (seperti kerahasiaan, integritas, ketersediaan, pengendalian, kemampuan audit) dunia maya (seperti infrastruktur, data, sumber daya, pengguna, dan operasi). Dapat disimpulkan bila *social engineering* adalah jenis serangan dengan tujuan mengeksploitasi kerentanan manusia melalui interaksi sosial untuk melanggar keamanan dunia maya.[90]

Pirnau mengungkapkan beberapa faktor kelemahan manusia yang berkontribusi pada keberhasilan serangan *social engineering* yaitu sebagai berikut.[91]

a. *Greed*

   Bentuk paling umum *social engineering* diwakili oleh pesan-pesan di mana penyerang mencoba mengambil keuntungan dari korban yang menjadi sasaran serakah. "Hei, saya punya banyak uang dan saya berjanji akan memberi Anda setengahnya jika Anda menawarkan saya beberapa informasi tentang diri Anda".

b. *Fear*

   Penyerang dapat menakut-nakuti korban sehingga korban harus bertindak berbeda dari biasanya. Dalam kasus ini, penyerang mengandalkan ketakutan korban, memerasnya, mengklaim bahwa ia memiliki informasi sensitif tentang korban dan jika korban tidak membayar sejumlah uang yang diminta, informasi tersebut akan dipublikasikan melalui internet.

c. *The Feeling of Urgency*

   Penyerang (biasanya melalui kampanye pemasaran) membujuk korban atas tawaran yang menguntungkan.

d. *Curiosity*

   Terungkap dalam berbagai artikel, gambar, dan film yang mengandung kata dan frasa seperti: "mengejutkan", "Anda tidak akan percaya", "sensasional", dan sebagainya dengan maksud untuk membuat orang ingin mengetahuinya dan mengeklik pesan tersebut. Dengan demikian, rasa ingin tahu menantang orang untuk bereaksi berbeda dari biasanya.

---

[90]Zuoguang Wang, *et.al.*, "Social in Cybersecurity: A Domain Ontology and Knowledge Graph Applicatioan Examples", *Journal Cybersecurity*, Vol. 4, Issue 31, 2001, pp. 1-21, DOI: https://doi.org/10.1186/s42400-021-00094-6, hlm. 1.

[91]Mironela Pirnau, "Considerations on Preventing Social Engineering Over the Internet", *Memoirs of the Scientific Sections of The Romanian Academy*, 2017, hlm. 86-87.

e. *Sympathy*

Menggunakan metode penipuan, penyerang menceritakan kisah tentang topik yang paling tidak menyenangkan, dengan konten sensitif, untuk mendapatkan simpati korban: "Kami diserang di hotel tempat kami menginap", dan sejumlah uang diminta, uang yang dijanjikan penjahat untuk kembali — yang tidak pernah terjadi.

f. *Respect Towards Authorities*

Korban mengira bahwa mereka berkomunikasi dengan manajer perusahaan tempat mereka bekerja, dengan atasan mereka atau dengan salah satu pejabat. Namun, jika korban yang ditargetkan telah mengeklik salah satu tautan, komputer akan terinfeksi *ransomware*.

g. *Trust in a Certain Person*

Korban menerima pesan yang tampaknya disampaikan oleh orang yang dapat dipercaya, guru, mentor, dan lainnya. Sebenarnya, tautan yang disertakan dalam pesan tersebut mungkin berbahaya. Tautan harus dianalisis dengan cermat sebelum diakses, meskipun tampaknya dikirim oleh orang yang dapat dipercaya.

Selanjutnya, terdapat fitur khas yang menjadikan *social engineering* menjadi serangan yang populer dilakukan oleh peretas serta menjadi ancaman yang serius, universal, dan *persistent* dalam keamanan siber, yakni: (1) apabila dibandingkan dengan serangan klasik seperti peretasan kata sandi yang menggunakan *brute force* serta eksploitasi kerentanan *software*, *social engineering* justru mengeksploitasi kerentanan manusia untuk melewati atau menerobos pagar keamanan, tanpa harus bertarung dengan *firewall* atau antivirus; (2) dalam beberapa skenario serangan, *social engineering* dapat dilakukan dengan sederhana seperti melakukan panggilan telepon dan menyamar sebagai orang dalam untuk mendapatkan informasi rahasia; (3) dalam beberapa dekade terakhir, ketika upaya pertahanan berfokus pada wilayah digital, ternyata kerap mengabaikan faktor manusia dalam keamanannya. Seiring perkembangan teknologi keamanan, serangan klasik menjadi semakin sulit dan membuat para penyerang beralih ke *social engineering*; (4) kerentanan manusia tampaknya tak terhindarkan, mengingat tidak ada sistem siber yang tidak bergantung pada manusia atau melibatkan faktor manusia.[92]

[92] *Ibid.*

Kompleksitas yang dimiliki oleh *social engineering* itu sendiri, mengakibatkan sukarnya mendapatkan definisi tunggal terhadapnya. Setidaknya terdapat beberapa definisi *social engineering* yaitu sebagai berikut.

a. *The act of manipulating a person to take an action that may or may not be in the target's best interest.*[93]
b. *The act of manipulating human beings, most often with the use of psychological persuasion, to gain access to systems containing data, documents, and information that the social engineer should not have access to obtain.*[94]
c. *A psychological exploitation which scammers use to skillfully manipulate human weaknesses and carry out emotional attacks on innocent people.*[95]
d. *The practice of fooling someone into giving up something they wouldn't otherwise surrender through the use of psychological tricks.*[96]
e. *The casual or calculated manipulation of people to influence them to do things they would not ordinary do.*[97]
f. *The malicious intent of people who are trying to gain access to sensitive data and information through illegal means.*[98]
g. *Phenomenon where people are influenced into taking a particular action, which may (and often is be against their own best interest).*[99]
h. *The art and science of getting people to comply to your wishes. It is not a way of mind control, it will not allow you to get people to perform tasks wildly outside of their normal behavior and it is far from foolproof.*[100]

---

[93]Christopher Hadnagy, *Social Engineering: The Art of Human Hacking* (Indianapolis: Wiley Publishing, 2011), hlm. 37.

[94]Amy Hetro Washo, "An Interdisciplinary View of Social Engineering: A Call to Action for Research", *Computers in Human Behavior Reports*, Vol. 4, 2021, hlm. 2.

[95]Brandon Atkins dan Wilson Huang, "A Study of Social Engineering in Online Frauds", *Open Journal of Social Science*, Vol. 1, No. 3, 2013, pp. 23-32, DOI: I:10.4236/jss.2013.13004, hlm. 2.

[96]Curry dalam Nabie Y. Conteh dan Malcolm D. Royer, *Op. Cit.,* hlm. 2.

[97]Kevin Mitnick dalam *Ibid*.

[98]M. Neela Malar, "Impact of Cyber Crimes on Social Networking Pattern of Girls", *International Journal of Internet of Things*, Vol. 1, No. 1, 2012, pp. 9-15, DOI: 10.5923/j.ijit.20120101.02, hlm. 11.

[99]Yavor Papazov, "Social Engineering, Science and Technology Organization", *Educational Notes Paper,* North Atlantic Treaty Organization, 2016, hlm. 2.

[100]*Ibid.*

i. *The process of utilizing human behavior to breach security without the victim being aware they have been manipulated.*[101]

j. *It is an attempt to trick someone into providing confidential information to attack a system or network.*[102]

Setelah memahami definisi *social engineering* yang memberikan penekanan pada seni menggerakkan orang lain untuk melakukan sesuatu serta faktor kebiasaan manusia yang rentan untuk dipengaruhi selanjutnya dapat diketahui beberapa jenis keterampilan pelaku dalam mengeksploitasi korban agar dapat masuk pada sistem yang ditargetkan, di antaranya sebagai berikut.[103]

a. *Impersonating Staff*

Ini adalah seni menemukan situasi dalam meyakinkan target yang dapat berupa seseorang atau komputer guna membagikan informasi atau melakukan suatu tindakan. Hal ini dilakukan sebagian besar melalui telepon atau *email*. Hoaks yang paling berpengaruh dan berbahaya untuk pencapaian akses fisik ke sistem apa pun adalah berpura-pura menjadi seseorang dari dalam korporasi. Beberapa pengguna mungkin memberikan kata sandinya kepada orang yang tidak dikenal pada panggilan telepon, berpikir bahwa mereka adalah anggota staf IT. Umumnya penelepon menunjukkan bahwa akun mereka mungkin dibatasi/dinonaktifkan dan tidak dapat untuk mengakses *email* penting atau mengakses berbagai jaringan yang diperlukan jika target tidak bekerja sama. Ini adalah serangan yang paling memakan waktu karena memerlukan penyelidikan dan penelitian untuk mendapatkan data dan informasi mengenai target untuk menetapkan legalitas di benak target.

b. *Intimidation Strategies*

Dalam hal ini, penyerang mencoba berpura-pura sebagai seseorang yang penting seperti bos besar dari kantor pusat, seorang inspektur dari pemerintah, klien utama perusahaan, atau orang lain yang

---

[101]Lindiwe T. Hove, "Strategies Used to Mitigate Social Engineering Attacks", *Dissertations*, College of Management and Technology, Walden University, 2020, hlm. 6.

[102]*Ibid.*

[103]Neetu Bansla, *et.al.*, "Social Engineering: A Technique for Managing Human Behavior", *Journal of Information Technology and Science*, Vol. 5, Issue 1, 2019, hlm. 20.

dapat menyerang rasa takut ke dalam hati karyawan. Umumnya pelaku akan datang dengan cara mendesak, memanggil korban, berteriak, marah ataupun kesal. Pelaku juga dapat mengancam karyawan untuk memecat jika mereka tidak mendapatkan informasi yang mereka butuhkan.

c. *Hoaxing*

Hoaks adalah upaya untuk mengelabui dan berpura-pura agar seseorang menjadi percaya akan sesuatu yang "palsu" adalah sebuah kenyataan. Ini juga dapat menyebabkan diambilnya keputusan yang karena takut akan insiden yang tidak diinginkan.

d. *Playing on User's Sympathy*

Pelaku mungkin berpura-pura menjadi karyawan dari luar, mungkin dari perusahaan telepon atau penyedia layanan ISP. Sifat manusia adalah membantu orang yang sedang kesusahan.

e. *Creating Confusion*

Trik lainnya adalah dengan didahului upaya menciptakan sebuah masalah dan kemudian mengambil keuntungan dari keadaan itu. Ini dapat sesederhana menyalakan alarm kebakaran sehingga semua orang akan meninggalkan area dengan cepat, tanpa mengunci komputernya. Pelaku kemudian dapat menggunakan *logged-on session* untuk melakukan pekerjaan kotor mereka.

f. *Reverse Social Engineering*

Praktik serangan *social engineering* yang lebih rumit terjadi ketika pelaku mendapatkan dan membuat orang lain mengajukan pertanyaan kepadanya alih-alih menanyai mereka. Pelaku biasanya harus melakukan banyak perencanaan, persiapan, penjadwalan, peramalan, penelitian, dan investigasi untuk melakukannya, menempatkan diri mereka pada posisi otoritas atau keahlian.

Dalam perkembangannya, perlu diketahui karakter khusus dari pelaku *social engineering*, yang tujuan dan pendekatan aksi penyerangan *social engineering* di dunia maya serupa dengan pelaku di dunia fisik. Namun, terdapat perbedaan yang signifikan. *Pertama*, dunia maya menyediakan penyerang lebih banyak sumber daya untuk mempersonalisasi serangan, dan memberikan mekanisme perlindungan identitas yang lebih baik. *Kedua*, kemungkinan anonimitas saluran

digital memungkinkan penyerang untuk melindungi identitasnya ketika berpotensi beroperasi pada yurisdiksi yang berbeda sehingga membantu dalam menghindari sanksi hukum.

Saluran digital juga memungkinkan penyerang mendekati banyak korban secara bersamaan, menurunkan biaya serangan dan meningkatkan kemungkinan menemukan korban. Akibatnya, serangan *social engineering* dengan tingkat respons rendah masih menguntungkan. *Ketiga,* lebih mudah untuk memproyeksikan kredibilitas (untuk menciptakan kepercayaan) di dunia maya dibandingkan di dunia fisik karena umumnya individu mengandalkan heuristik dasar untuk menilai kredibilitas. Sebagian besar individu mengasosiasikan kredibilitas di dunia maya dengan atribut yang dangkal, seperti tampilan profesional dari sebuah situs web, atau keberadaan konten yang kaya dan berkualitas tinggi.[104]

Perlu diperhatikan, bahwa kredibilitas mengurangi kecurigaan, meningkatkan persuasi pesan, dan meningkatkan kerentanan korban terhadap serangan *social engineering*. Kredibilitas penyerang dicirikan oleh atribut, di antaranya kesamaan, reputasi, dan kepercayaan. Kesamaan dapat dengan mudah dibangun secara *online* karena penyerang dapat menggunakan informasi di media sosial dan situs web untuk membangun kesamaan dengan korban. Informasi seperti keyakinan, norma, dan dialek komunitas berguna bagi penyerang. Dengan menggunakan informasi semacam ini, penyerang dapat menyamar sebagai anggota komunitas atau kenalan pada forum *online* atau grup media sosial.

Reputasi kerap kali didasarkan pada jaringan rekanan seseorang. Salah satu metode untuk meningkatkan persepsi orang lain tentang reputasi penyerang di dunia maya adalah dengan meningkatkan koneksi media sosial penyerang dengan individu yang memiliki reputasi baik. Seorang penyerang dapat membangun kesamaan yang dirasakan untuk menarik individu yang memiliki reputasi baik untuk menerima undangan untuk terhubung. Daya tarik lain untuk menarik individu terkemuka di media sosial adalah ukuran jejaring sosial yang dimaksud. Seorang penyerang dapat memproyeksikan jaringan sosial yang luas melalui penggunaan bot dan persona palsu.

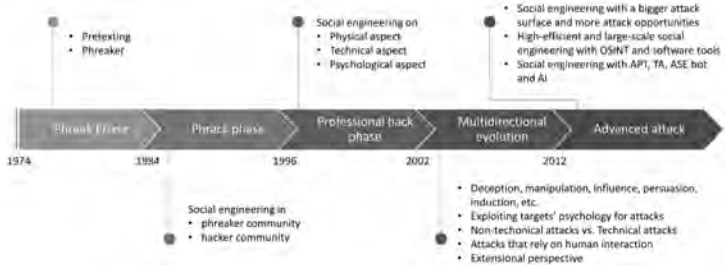
---

[104]Rosana Montanez Rodriguez, *et.al., Cybersecurity and Cognitive Science, Chapter 1 - Social Engineering Attacks and Defense in the Physical World vs. Cyberspace: A Contrast Study* (UK: Academic Press, 2022), hlm. 7-8.

Kepercayaan adalah persepsi bahwa pihak lain bertindak dengan iktikad baik. Untuk memproyeksikan kepercayaan, penyerang dapat memasukkan artefak (misalnya tautan, gambar, grafik) dalam pesan. Misalnya, indikator keamanan seperti gembok *Secure Sockets Layer* (SSL) atau gambar organisasi yang menjamin kepercayaan individu, seperti logo *Better Business Bureau* (BBB) atau *Federal Deposit Insurance Corporation* (FDIC). Penyerang juga dapat menyertakan URL yang tampaknya berasal dari situs terpercaya yang diketahui. Penyerang dapat menggunakan URL yang menyerupai URL yang sah dan terkenal (misalnya www.paypa1.com, di mana huruf "l" diganti dengan angka "1"). Pendekatan lain adalah membuat URL jahat yang tampak tidak berbahaya, seperti URL panjang yang ketika dipersingkat oleh *browser*, tampak tidak berbahaya. Misalnya, penyerang dapat menggunakan https://myaccount.google.com-securitysettingpage.tk. Terakhir, penyerang dapat mengeksploitasi kepercayaan korban pada pihak ketiga, yang mungkin merupakan layanan atau entitas yang dipercaya oleh korban dan dapat menyediakan saluran komunikasi antara korban dan penyerang (misalnya, situs kencan atau pekerjaan).

C. Fase dan Pola Umum *Social Engineering*

Dalam tulisannya, Zuoguang Wang menguraikan evolusi konseptual *social engineering* pada studi keamanan siber dalam lima fase, yaitu: (1) *phreak phase;* (2) *phrack phase;* (3) *professional hack phase;* (4) *multidirectional evolution;* dan (5) *advanced attack,* seperti yang diilustrasikan pada Gambar 2. Periodisasi ini dilakukan berdasarkan penelusuran literatur-literatur yang menggunakan istilah *social engineering*.



Gambar 2. Evolusi Konsep *Social Engineering* dalam Studi Keamanan Siber[105]

[105]Zuoguang Wang, *et.al., Defining Social Engineering in Cybersecurity, Op. Cit.,* hlm. 85096.

Pada fase pertama, ***phreak phase,*** diketahui bila *social engineering* pertama kali digunakan pada artikel dengan tajuk *more on trashing* pada September 1984 yang diterbitkan oleh *The Hacker's Quarterly*. Dalam tulisannya disebutkan bila sampah perusahaan Telco mengandung banyak informasi berharga serta membahas metode khusus guna mengumpulkan informasi pada sampah yang telah dibuang. Pada artikel lainnya di tahun yang sama, yakni *Switching Center and Operators* turut membahas *social engineering* terkait upaya membujuk operator agar memberikan informasi serta berpura-pura menjadi karyawan perusahaan telekomunikasi untuk mendapatkan informasi sehingga pada fase ini konsep *social engineering* terutama mengacu pada proses menggunakan dalih untuk membujuk target guna memberikan informasi lebih lanjut.[106]

Dalam analisis literatur yang dilakukan, asal-usul konsep *social engineering* diduga muncul sebelum tahun 1984 (penyebaran istilah). Pernyataan tersebut didasarkan atas pernyataan John Draper yang memperkenalkan istilah tersebut pada pertengahan 1970-an sebagai serangan peniruan identitas. Selanjutnya turut diketahui bila istilah *social engineering* telah menjadi tren pada pertengahan 1980-an, atau bahkan tahun 1974 yang digunakan sebagai istilah bagi dalih memanggil seseorang untuk mendapatkan informasi atau meyakinkan mereka untuk melakukan sesuatu untuk orang lain sehingga dapat disimpulkan bila istilah *social engineering* pada *phreak phase* digambarkan sebagai pendekatan untuk memperoleh informasi atau bantuan dari operator perusahaan telepon dengan menggunakan "dalih", persuasi, dan peniruan.[107]

Fase selanjutnya, yakni ***phrack phase.*** Pada fase ini istilah *social engineering* termanifestasikan dalam makna *phrack* yang merupakan gabungan dari konsep *phreack* dan *hack*. Pada satu sisi, *social engineering* kerap berperan sebagai konsep pada komunitas *phreaker* telepon, yang lekat dengan makna peniruan, dalih, dan persuasi dan saat ini turut termanifestasi pada lingkup baru yakni penipuan. Pada fase ini *social engineering* dianggap sebagai *bullshitting, trickery,* dan *deceit* untuk mendapatkan informasi. *Social engineering* diasosiasikan oleh komunitas peretas dengan proses penggunaan

[106]*Ibid.*
[107]*Ibid.,* hlm. 85096-85097.

interaksi sosial dalam memperoleh informasi mengenai sistem komputer korban, yang memberikan peretas jalan pintas yang efisien dan dalam banyak kasus memfasilitasi serangan yang tidak mungkin dilakukan melalui cara lain. Pada fase ini, teknik *dumpster diving* dinilai berguna dalam menemukan informasi berharga yang menjadikan pertahanan pertama dari serangan adalah sampah perusahaan. Pada era 1984-1955, konotasi *hack* terlihat dari aktivitas penipuan, memanipulasi dialog, *reverse social engineering*, serta *dumpster diving*.[108]

Fase ketiga yang terjadi pada 1996-2001 dikenal sebagai ***professional hack phase***. Pada fase ini, *social engineering* termanifestasi dalam tiga aspek berikut.[109]

1. Pendekatan yang Lebih Beragam dalam Tingkat Fisik

   Untuk serangan rekayasa sosial di tingkat fisik, peretas dapat berpura-pura menjadi pekerja pemeliharaan atau konsultan yang memiliki akses ke organisasi dan berjalan di tempat kerja untuk melakukan perusakan kantor, menemukan kata sandi yang tergeletak di sekitar, atau berdiri dan melihat karyawan yang tidak sadar memasukkan kata sandinya (*shoulder surfing*).

2. Teknik *Email Phishing* dan *Trojan* Secara Bertahap Muncul

   Serangan *phishing* pertama terjadi pada tahun 1996 dan dirancang untuk mencuri *username*, *password*, nomor kartu kredit dan informasi pribadi lainnya dari *America Online* (AOL). Penyerang mengirim *email* palsu dan pesan instan yang tampaknya berasal dari dukungan AOL. Laporan Verizon pada tahun 2020 menunjukkan bahwa *phishing* yang merupakan bagian dari *social engineering* bertanggung jawab atas 25% pelanggaran data pada tahun 2019 dan 2020.[110]

3. Aspek Psikologi dalam *Social Engineering*

   Pengaruh sosial, persuasi, dan manipulasi kepercayaan mulai dibahas. Secara signifikan disadari secara bertahap bahwa manusia sebagai mata rantai terlemah dari rantai keamanan secara bertahap.

Fase selanjutnya adalah *multidirectional evolution,* yang berlangsung sepanjang 2002 hingga 2012 dengan hadirnya perhatian publik yang

[108]*Ibid.,* hlm. 85097.
[109]*Ibid.,* hlm. 85098.
[110]Devin Partida, *Ibid*.

tinggi terhadap ancaman dari serangan *social engineering*. Pada satu sisi, keadaan tersebut melahirkan diskursus *social engineering* yang terkadang bertentangan secara konseptual. *Shoulder surfing* dan *dumpster diving* dianggap sebagai metode serangan *social engineering*, namun literatur lainnya mengecualikannya dari taksonomi *social engineering* secara eksplisit. Fenomena ini menyebabkan timbulnya beragam problematika, di antaranya batas konseptual yang tidak jelas, penyalahgunaan terminologi, serta diferensiasi dan dekomposisi konseptual yang disebabkan oleh ketegangan struktural yang dihasilkan oleh evolusi konseptual terarah yang berbeda. Setidaknya terdapat lima hal yang menjadi pembahasan utama pada fase ini, yakni: *(1) social engineering concepts that emphasize deception and manipulation; (2) social engineering concepts that emphasize psychological exploitation; (3) technical features of social engineering; (4) social engineering concepts that emphasize social interaction; and (5) social engineering concepts from external perspective.*[111]

Meskipun serangan *social engineering* berbeda satu sama lain, terdapat pola umum dengan fase yang serupa. Pola umum tersebut melibatkan empat tahap, yakni: (1) mengumpulkan informasi tentang target; (2) menjalin komunikasi dengan target; (3) memanfaatkan informasi yang tersedia serta melakukan serangan; dan (4) pergi tanpa jejak. Gambar 3 merupakan ilustrasi tahapan dari serangan *social engineering*.[112]

Gambar 3. Pola Umum *Social Engineering*

[111]Zuoguang Wang, *et.al., Defining Social Engineering in Cybersecurity, Op. Cit.,* hlm. 85098-85100.

[112]Fatima Salahdine dan Naima Kaabouch, *Op. Cit.,* hlm. 2.

Dalam fase penelitian atau disebut pengumpulan informasi, penyerang memilih korban berdasarkan beberapa persyaratan. Pada fase menjaring, penyerang mulai mendapatkan kepercayaan dari korban melalui kontak langsung atau komunikasi *email*. Pada fase bermain, penyerang memengaruhi korban secara emosional untuk memberikan informasi sensitif atau melakukan kesalahan keamanan. Pada fase keluar, penyerang berhenti tanpa meninggalkan bukti apa pun.[113]

D. Data dan Dampak *Social Engineering*

Sukar untuk mendapatkan angka akurat yang merinci peningkatan kejahatan dunia maya di seluruh dunia, mengingat data tersebut dibangun berdasarkan jumlah serangan, pelanggaran, dan peristiwa keamanan lainnya yang dilaporkan. Namun, beberapa data menunjukkan beberapa data pelanggaran yang terjadi, yakni sebagai berikut.

1. Laporan yang dirilis oleh Ponemon Institute menjelaskan bahwa 45% orang dewasa di Amerika Serikat telah mengungkapkan informasi pribadi, dengan 110 juta pelanggaran yang terjadi selama periode 2013-2014.[114]
2. Laporan Statista pada tahun 2015 menjelaskan bahwa dua perusahaan besar Adobe dan eBay telah mengalami pelanggaran data, dengan 145 juta data dari 152 juta data yang dicuri pada Agustus 2015.[115]
3. 5.000 warga menjadi korban *web phishing* dengan total kerugian 100 juta hryvnia atau sekitar $3.360.000. Serangan tersebut dilakukan oleh sebuah geng berjumlah 9 orang yang mengoperasikan 400 situs *web phishing*. Para pelaku telah ditangkap oleh Kepolisian Siber Ukraina pada Juni 2022.[116]

---

[113]*Ibid.*

[114]Ponemon Institute dalam Nabie Y. Conteh dan Malcolm D. Royer, *Op. Cit.*, hlm. 4.

[115]Statista dalam *Ibid*.

[116]Bill Toulas, "Ukraine Arrest Cybercrime Gang Operating Over 400 Phishing Sites", *Bleeping Computer*, 29 Juni 2022, https://www.bleepingcomputer.com/news/security/ukraine-arrests-cybercrime-gang-operating-over-400-phishing-sites/ (diakses pada 7 Juli 2022).

Indonesia memiliki catatan tersendiri terkait kejahatan dengan modus *social engineering*. Kepolisian Indonesia, menyatakan terdapat 2.300 laporan pada tahun 2019.[117] Keadaan ini juga yang menjadikan Indonesia sebagai negara dengan jumlah *spam calls* tertinggi di Asia. Laporan tersebut berdasarkan studi yang dilakukan oleh perusahaan teknologi Truecaller, yang telah membantu upaya untuk memblokir dan mengidentifikasi 31,3 miliar *spam calls*, yang meningkat 18% dari tahun 2019. Dalam laporannya Truecaller merilis 20 negara teratas yang terkena *spam calls* pada tahun 2020, yaitu sebagai berikut.[118]

Tabel 2. 20 Negara Teratas yang Terkena *Spam Calls* pada Tahun 2020[119]

No.	Negara	Rata-rata *Spam Call* Pengguna/ Bulan
1.	Brasil	49,9
2.	Amerika Serikat	28,4
3.	Hungaria	28,3
4.	Polandia	20,4
5.	Spanyol	18,3
6.	Indonesia	18,3
7.	Inggris	17,4
8.	Ukraina	17,1
9.	India	16,8
10.	Cile	16,8
11.	Meksiko	15,5
12.	Vietnam	14,7
13.	Russia	14,3
14.	Peru	12,8
15.	Jerman	12,6
16.	Romania	11,9
17.	Afrika Selatan	11,3
18.	Yunani	9,0
19.	Belgia	8,5
20.	Colombia	8,0

[117]CNN Indonesia, "Penipuan Online, Kejahatan Paling Banyak di 2019", *CNN Indonesia*, 23 Januari 2020, https://www.cnnindonesia.com/teknologi/20200123164303-185-468075/penipuan-online-kejahatan-paling-banyak-di-2019 (diakses pada 13 Mei 2022).

[118]Kim Fai Kok, "Truecaller Insight: Top 20 Countries Affected By Spam Calls in 2020", *Truecaller*, 8 Desember 2020, https://truecaller.blog/2020/12/08/truecaller-insights-top-20-countries-affected-by-spam-calls-in-2020-2/ (diakses pada 13 Mei 2022).

[119]*Ibid.*

Penelusuran yang dilakukan oleh Ismail Fahmi selama 2 bulan dan dipublikasikan pada 14 Maret 2021, menemukan setidaknya terdapat 331 akun penipu yang mencantut HaloBCA, serta 113 akun penipu yang mengaku *customer care* BNI. Lebih lanjut Ismail menjelaskan, modus yang dilakukan oleh pelaku adalah dengan menggunakan ***bot*** untuk mengirim pesan kepada para nasabah yang sedang panik karena mengalami kendala urusan perbankan. Penipu memiliki *bot* yang memonitor percakapan yang mengandung kata, misalnya HaloBCA, BNI, dan lainnya. Pelaku kemudian menghubungi korban yang panik dengan mengirimi DM atau membalas pesannya, dan tidak jarang menambahkan nomor WhatsApp (WA) atau nomor yang dapat dihubungi beserta tautan yang mengarahkan nasabah kepada percakapan pribadi. Pelaku kerap menindaklanjuti dengan menelepon maupun *video call* dan tidak jarang menggunakan *background* seolah tengah berada di kantor dengan logo palsu untuk menipu nasabah. Pelaku kemudian akan meminta beberapa data seperti nomor rekening, nomor kartu ATM, nama lengkap bahkan *One-Time Password* (OTP). Beberapa nasabah telah menjadi korban dengan nominal yang beragam, seperti Rp1 juta hingga Rp16 juta.[120]

Beragam dampak pelanggaran *social engineering* tentu dialami oleh institusi. Nabie menjelaskan dampak yang terjadi, yakni: (1) kerugian finansial; (2) reputasi; dan (3) waktu pemulihan.[121] Seperti yang dialami oleh Twitter karena kelalaian karyawannya yang mengakibatkan akun Twitter Bill Gates, Barack Obama, Jeff Bezos, dan Joe Biden pada Juli 2020 diretas. Peretas memanfaatkan akun Bill Gates untuk menuliskan tawaran menggandakan bitcoin yang merupakan penipuan.[122] Beberapa peristiwa kebocoran, **dugaan kebocoran data,** dan pengumpulan data pribadi secara ilegal lainnya yang terjadi, di antaranya sebagai berikut.

---

[120]Ismail dalam Inggried Dwi Wedhaswary, "Banyak Nasabah "Terjebak" Akun Bodong Bank di Twitter, Simak Analisis Drone Emprit", *Kompas*, 14 Maret 2021, https://www.kompas.com/tren/read/2021/03/14/145600565/banyak-nasabah-terjebak-akun-bodong-bank-di-twitter-simak-analisis-drone?page=all (diakses pada 18 Juli 2021).

[121]Nabie Y. Conteh dan Malcolm D. Royer, *Op. Cit.*, hlm. 5-6.

[122]Roy Franedya, "Twitter Ungkap Sebab Akun Bill Gates Hingga Obama Bisa Diretas", *CNBC Indonesia*, 16 Juli 2020, https://www.cnbcindonesia.com/tech/20200716124829-37-173232/twitter-ungkap-sebab-akun-bill-gates-hingga-obama-bisa-dihack (diakses pada 13 Mei 2022).

No.	Tahun	Instansi	Uraian
1.	2022	Mangatoon	Mangatoon merupakan aplikasi iOS dan Android yang marak digunakan oleh pengguna guna membaca komik manga secara *online*. Pada bulan Mei 2022, Mangatoon mengalami pelanggaran data yang mengekspos data dari 23 juta akun penggunanya. Pelanggaran data ini terjadi, setelah peretas mencurinya dari basis data *Elasticsearh* yang menggunakan kredensial lemah.[123]
2.	2022	Open Sea	Pasar NFT terbesar, OpenSea mengungkapkan bila telah mengalami serangan *phishing*. Sebagai perusahaan dengan lebih dari 600.000 pengguna dan volume transaksi melampaui $20 miliar, OpenSea mengungkapkan bila penyerangan telah mencuri alamat *email* pengguna dan membagikan alamat *email* tersebut kepada pihak yang tidak berwenang.[124]
3.	2022	Chicago Public Schools (Amerika Serikat)	Pada akhir Desember 2021, Chicago Public Schools mengalami pelanggaran data yang mengekspos 500.000 data siswa dan 60.000 karyawan setelah salah satu vendor, Battelle for Kids, mengalami serangan *ransomware*.[125]

[123]Lawrence Abrams, "Mangatoon Data Breach Exposes Data form 23 Million Accounts", *Bleeping Computer*, 9 Juli 2022, https://www.bleepingcomputer.com/news/security/mangatoon-data-breach-exposes-data-from-23-million-accounts/ (diakses pada 15 Juli 2022).

[124]Sergiu Gatlan, "OpeanSea Discloses Data Breah, Warn Users of Phising Attacks", *Bleeping Computers*, 30 Juni 2022, https://www.bleepingcomputer.com/news/security/opensea-discloses-data-breach-warns-users-of-phishing-attacks/ (diakses pada 7 Juli 2022).

[125]Lawrence Abrams, "Ransomware Attack Exposes Data of 500,000 Chicago Students", *Bleeping Computers*, 21 Mei 2022, https://www.bleepingcomputer.com/news/security/ransomware-attack-exposes-data-of-500-000-chicago-students/ (diakses pada 9 Juni 2022).

4.	2022	General Motors	Pada April 2022, General Motors (GM) mendeteksi aktivitas *login* yang mencurigakan. General Motors akhirnya mengumumkan bila telah terkena serangan dengan metode menebak isian kredensial (*credential stuffing*) yang mengungkap informasi pelanggan dan memungkinkan peretas untuk menukarkan poin hadiah dengan kartu hadiah. GM mengoperasikan *platform* daring yang membantu pemilik kendaraan Chevrolet, Buick, GMC, dan Cadillac mengelola tagihan dan menukarkan poin hadiah.[126]
5.	2022	Bank Indonesia	Pada awal tahun 2022, data internal Bank Indonesia dipublikasikan di *dark web* hingga mencapai 74,8 GB. Pelaku peretasan, geng Conti diduga pertama kali menyerang kantor perwakilan Bank Indonesia Provinsi Bengkulu, dan menyebabkan 200 komputer terserang *ransomware.*[127]

[126]Benjamin David, "US Car Giant General Motors Hit by Cyber-Attack Exposing Car Owners' Personal Info", *Info Security Magazine*, 24 Mei 2022, https://www.infosecurity-magazine.com/news/general-motors-hit-by-cyber-attack/ (diakses pada 9 Juni 2022).

[127]Agustin Setyo Wardani, "Makin Parah, Serangan Ransomeware BI Ternyata Hantam 200 Komputer di 20 Cabang", *Liputan 6,* 24 Januari 2021, https://www.liputan6.com/tekno/read/4867855/makin-parah-serangan-ransomware-bi-ternyata-hantam-200-komputer-di-20-cabang (diakses pada 14 Mei 2022).

6.	2021	PT Pertamina PTC	Pada Oktober 2021, data pribadi pelamar PT Pertamina PTC diketahui telah bocor. Pertamina PTC ialah anak perusahaan minyak negara, Pertamina, yang bergerak di bidang pengembangan sumber daya manusia melalui pelatihan, konsultasi, dan manajemen. Pembocor data tersebut ialah akun "Astarte", yang akhirnya mengunggah data pelamar kerja tersebut dengan judul "163k Indonesian documents KYC" pada 8 Januari 2021 pada sebuah forum jual beli data. Ukuran datanya mencapai 60 GB. Astarte mengklaim bahwa isi data tersebut mencapai 163.181 file. Diketahui bahwa data pelamar yang dibocorkan tersebut mencakup, antara lain: (1) KTP; (2) KK; (3) SIM; (4) NPWP; (5) SKCK; (6) Foto Diri; (7) Akta Kelahiran; (8) Ijazah Sekolah; (9) Transkrip Nilai; (10) *Curriculum Vitae;* (11) Kartu BPJS Kesehatan; dan lainnya.[128]
7.	2021	Kepolisian Republik Indonesia	Pertengahan bulan November, peretas Brasil membocorkan basis data Kepolisian Republik Indonesia secara gratis yang diambil dari subdomain server web https://e-rehab.propam.polri.go.id/. Peretas tersebut membagikan dua tautan yang berisi basis data Polri yaitu "polrileak.txt" berukuran 10,27 megabit dan "polri.sql". Tidak hanya itu, peretas mengklaim memiliki 28 ribu kredensial *login* dan informasi pribadi.[129]

[128]Oktarina Paramitha Sandy, "Data Pelamar Pertamina PTC Bocor, ELSAM Soroti Notifikasi Pemilih Data hingga Posko Pengaduan", 19 Januari 2022, https://cyberthreat.id/read/13341/Data-Pelamar-Pertamina-PTC-Bocor-ELSAM-Soroti-Notifikasi-Pemilik-Data-hingga-Posko-Pengaduan (diakses pada 15 Mei 2022).

[129]Andi Nugroho, "Peretas Brasil 'son1x' Serang Subdomain Propam Polri, Satu Server Web Ditanam Backdoor", *Cyberthrat*, 19 November 2021, https://cyberthreat.id/read/12886/Peretas-Brasil-son1x-Serang-Subdomain-Propam-Polri-Satu-Server-Web-Ditanam-Backdoor (diakses pada 15 Mei 2022).

8.	2021	Costco Wholesale Corporation	Pada 5 November, perusahaan grosir Costco telah menginformasikan bila informasi kartu pembayaran (kartu dan debit) konsumen diduga telah dicuri ketika berbelanja di salah satu tokonya. Costco mengoperasikan rantai besar toko ritel khusus keanggotaan dan memiliki 737 gudang di seluruh dunia. Costco memastikan pelanggaran setelah menemukan perangkat *skimming* kartu pembayaran di salah satu gerainya selama pemeriksaan rutin yang dilakukan oleh perusahaan.[130]
9.	2021	Departemen Luar Negeri (DFA) Filipina	Pada pertengahan tahun, DFA Filipina mengumumkan telah mematikan (*take down)* layanan *online passport tracker,* aplikasi untuk memantau status pengajuan paspor. Diketahui bahwa ditemukan informasi pribadi pemohon paspor telah terekspos setelah data pelacak *online* muncul di pencarian Google. Masalah privasi data pada pelacak paspor DFA berasal dari informasi pribadi pelamar yang "dikodekan" dalam sumber atau program pelacak, yang dapat diakses secara *online*. Informasi seperti surel, tanggal lahir, dan nomor kontak termasuk di antara data yang dapat diakses.[131]
10.	2021	FBI	13 November 2021, peretas membobol sistem surel Biro Investigasi Federal Amerika Serikat. Peretas mengirimkan puluhan ribu pesan surel peringatan terkait kemungkinan serangan siber. FBI menyatakan bahwa surel spam peringatan tersebut palsu dan berasal dari sebuah alamat surel resmi yang berakhir @ic.fbi.gov.[132]

[130]Sergiu Gatlan, "Costco Disclose Data Breach After Finding Credit Card Skimmer", *Bleeping Computer*, 12 November 2021, https://www.bleepingcomputer.com/news/security/costco-discloses-data-breach-after-finding-credit-card-skimmer/ (diakses pada 15 Mei 2022).

[131]Sofia Tomacruz, "DFA Takes Down Online Passport Tracker After Data Exposure Flagged", *Rappler*, 10 November 2021, https://www.rappler.com/nation/dfa-takes-down-passport-tracker-after-data-exposure-flagged (diakses pada 17 Mei 2022).

[132]Reuters, "Hackers Compromise FBI Email System, Send Thousands of Messages", *Reuters*, 14 November 2021, https://www.reuters.com/world/us/hackers-compromise-fbis-external-email-system-bloomberg-news-2021-11-13/ (diakses pada 17 Mei 2022).

11.	2021	Robinhood	Pada November 2021, 7 juta data pelanggan Robinhood dijual pada forum dan pasar peretas. Robinhood merupakan aplikasi perdagangan gratis yang populer bagi investor. Data yang dicuri diketahui berupa alamat surel 5 juta pelanggan, nama lengkap 2 juta pelanggan. Seorang aktor ancaman bernama Pompurin menyatakan menjual informasi tersebut dengan penawaran 10 ribu USD.[133]
12.	2021	Komisi Perlindungan Anak Indonesia	Pada Oktober 2021, dua kumpulan basis data yang diklaim milik KPAI ditawarkan di forum jual beli data, Raid Forum. Basis data tersebut diunggah oleh akun C77 pada 13 Oktober 2021 dengan tajuk "*Leaked Database* KPAI" (kpai.go.id). C77 memberikan sampel data yang disusun dalam bentuk *table* dan berisi identitas, nama, nomor KTP, telepon, pekerjaan, alamat, *email*, tempat tanggal lahir, kota. Lebih lanjut diketahui bahwa basis data yang bocor diduga berasal dari layanan pengaduan *online* situs web KPAI.[134]
13.	2021	Twitch	Pada Oktober 2021, platform *live streaming* video Twitch mengalami pelanggaran data. Dalam sebuah unggahan pada 4chan. sebuah akun anonim membagikan tautan torrent yang mengarah kepada arsip data berukuran 125 GB yang berisikan sekitar 6.000 repositori internal Twitch Git.[135]

[133]Laweence Abrams, "Robinhood Discloses Data Breach Impacting 7 Million Customers", *Bleeping Computer*, 8 November 2021, https://www.bleepingcomputer.com/news/security/robinhood-discloses-data-breach-impacting-7-million-customers/ (diakses pada 17 Mei 2022).

[134]Andi Nugroho, "Basis Data Pengaduan KPAI Dijual di Internet, BSSN: Ada Kebocoran Akun Server", 22 Oktober 2021, https://cyberthreat.id/read/12625/Basis-Data-Pengaduan-KPAI-Dijual-di-Internet-BSSN-Ada-Kebocoran-Akun-Server (diakses pada 17 Mei 2022).

[135]Nivedita Balu, "Amazon's Twitch Hit by Data Breach", *Reuters*, 7 Oktober 2021, https://www.reuters.com/technology/amazons-twitch-hit-by-data-breach-2021-10-06/ (diakses pada 18 Mei 2022).

14.	2021	Bangkok Airways	Diketahui pada 23 Agustus 2021, maskapai penerbangan Bangkok Airways menjadi korban serangan siber. Peretas dimungkinkan telah mengakses data pribadi penumpang berupa nama lengkap, kewarganegaraan, jenis kelamin, nomor telepon, *email,* alamat fisik, informasi paspor, riwayat perjalanan, informasi kartu kredit. Serangan tersebut dilakukan oleh kelompok *ransomware* LockBit, yang mengklaim telah mencuri data sebesar 200 GB.[136]
15.	2021	T-Mobile	Pada 16 Agustus 2021, operator seluler di Amerika Serikat T-Mobile mengungkapkan bahwa terdapat peretas yang melakukan akses ilegal pada server internalnya. Seorang peretas mengklaim telah memperoleh data lebih dari **100 juta** orang. Data tersebut termasuk informasi nomor jaminan sosial, nomor telepon, nama, alamat serta informasi SIM.[137]

[136]Iounut Ilascu, "Lockbit Gang Leaks Bangkok Airways Data, Hits Accenture Customers", *Bleeping Computer*, 1 September 2021, https://www.bleepingcomputer.com/news/security/lockbit-gang-leaks-bangkok-airways-data-hits-accenture-customers/ (diakses pada 18 Mei 2022).

[137]Lawrance Abrams, "Hacker Claims to Steal Data of 100 Million T-Mobile Customers", *Bleeping Computer*, 15 Agustus 2021, https://www.bleepingcomputer.com/news/security/hacker-claims-to-steal-data-of-100-million-t-mobile-customers/ (diakses pada 18 Mei 2022).

16.	2021	BRI Life	Pada 27 Juli 2021, akun bernama "reckt" pada sebuah forum jual beli data menawarkan basis data nasabah PT Asuransi BRI Life. Akun ini mengklaim memiliki basis data 2 juta nasabah BRI Life dengan ukuran 410 MB dan dokumen-dokumen yang dipindai sebanyak 463.000 berkas dengan ukuran 252 GB. Dokumen ini mencakup KTP, KK, NPWP, foto buku rekening, akta kelahiran, akta kematian, surat perjanjian bukti transfer, bukti keuangan, bukti surat kesehatan, lengkap dengan polis asuransi jiwa. Sebagai bukti sampel data, akun ini memberikan file berukuran 2,5 GB berikut lampiran video yang menunjukkan isi data sampel. Seluruh data tersebut ditawarkan dengan harganya US$7.000 dalam bentuk bitcoin. Pihak BRI memberikan keterangan bila pelaku kejahatan siber melakukan intrusi ke dalam sistem BRI Life Syariah yang merupakan *stand alone system* dan terpisah dari *core system* BRI Life. Dalam sistem tersebut, terdapat tidak lebih dari **25.000** pemegang polis syariah individu.[138]
17.	2021	Aplikasi Transportasi *Online* Didi	Otoritas keamanan siber Cina, *Cyberspace Administration of China* (CAC) meminta aplikasi Didi dikeluarkan dari *App Store China* dengan tuduhan telah mengumpulkan data pribadi pengguna secara ilegal. Didirikan pada 2012, Didi menguasai 94,6% pasar transportasi *online* di China dengan mitra pengemudi mencapai **21 juta** orang. Melalui data yang dihimpun, pada 2015 diketahui Didi telah mem-*profiling* pegawai-pegawai dari kementerian di Vina.[139]

[138]Andi Nugroho, "Yang Perlu Diketahui Seputar Peretasan Sistem BRI Life", *Cyberthreat*, 29 Juli 2021, https://cyberthreat.id/read/12171/Yang-Perlu-Diketahui-Seputar-Peretasan-Sistem-BRI-Life (diakses pada 18 Mei 2022).

[139]Yingzhi Yang, *et.al.*, "Chinese Regulators Send Teams to Didi for Cybersecurity Review", *Reuters*, 16 Juli 2021, https://www.reuters.com/technology/chinese-regulators-send-on-site-teams-conduct-cybersecurity-review-didi-2021-07-16/ (diakses pada 18 Mei 2022).

18.	2021	Air India	Pada Februari 2021, maskapai penerbangan Air India mengalami kebocoran data informasi pribadi penumpang. Diduga sebanyak **4,5 juta** penumpang terkena dampak. Data yang bocor, antara lain nama, tanggal lahir, kontak, paspor, tiket, serta data kartu kredit.[140]
19.	2021	Volkswagen	Produsen mobil Volkswagen mengatakan lebih dari **3,3 juta** informasi pelanggannya terekspos karena salah satu vendor meninggalkan *cache* data pelanggan tidak aman di internet. Volkswagen mendapat peringatan adanya kebocoran data pada 10 Maret 2021. Data yang terekspos mencakup informasi pribadi pelanggan dan calon pembeli, termasuk nama, alamat surat, *email,* dan nomor telepon, kendaraan yang dibeli, disewa, info kelayakan untuk pembelian atau pinjaman, nomor SIM, tanggal lahir, nomor jaminan sosial, asuransi sosial, nomor rekening, nomor identifikasi pajak.[141]
20.	2021	LinkedIn	Basis data **700 juta** pengguna LinkedIn ditawarkan secara *online* pada forum jual beli data, *RaidForums.* Sebuah akun bernama TomLiner mengklaim memiliki basis data tersebut berisi alamat *email,* nama lengkap, nomor telepon, alamat rumah, catatan geolokasi, jenis kelamin, nama pengguna dan URL profil LinkedIn akun media sosial dan lainnya. TomLiner telah mengungkap sampel data 1 juta pengguna pada 22 Juni 2021 dan menawarkan seluruh data LinkedIn tersebut senilai US$5.000.[142]

[140]Sergiu Gatlan, "Air India Data Breach Impacts 4.5 Million Costumers", *Bleeping Computer*, 21 Mei 2021, https://www.bleepingcomputer.com/news/security/air-india-data-breach-impacts-45-million-customers/ (diakses pada 19 Mei 2022).

[141]Zack Whittaker, "Volkswagen Says a Vendor's Security Lapse Exposed 3,3 Milion Drivers's Details", *Tech Crunch*, 1 Juni 2021, https://techcrunch.com/2021/06/11/volkswagen-says-a-vendors-security-lapse-exposed-3-3-million-drivers-details/ (diakses pada 19 Mei 2022).

[142]Sven Taylor, "New LinkedIn Data Leak Leaves 700 Milion Users Exposed", *Restore Privacy*, 27 Juni 2021, https://restoreprivacy.com/linkedin-data-leak-700-million-users/ (diakses pada 19 Mei 2022).

21.	2021	Mercedes Benz AS	Mercedes Benz Amerika Serikat pada 24 Juni 2021 mengungkapkan mengalami kebocoran data perihal **1.000** data pelanggan dan calon pembeli yang telah mendaftar. Data-data tersebut termasuk nama pelanggan, alamat, *email,* nomot telepon, informasi kartu kredit, nomor jaminan sosial, dan nomor SIM.[143]
22.	2021	Alibaba	Celah keamanan pada situs belanja Taobao yang merupakan bagian dari Alibaba Group membuat seorang pengembang perangkat lunak Tiongkok selama delapan bulan berhasil mengumpulkan lebih dari **1 miliar** informasi pengguna. Pengembang tersebut menggunakan *web crawler* yang dirancang di situs Taobao mulai tahun 2019. Informasi yang dikumpulkan termasuk ID pengguna, nomor ponsel, komentar pelanggan, serta nomor telepon.[144]
23.	2021	Carter	Jaringan ritel pakaian bayi Carter secara tidak sengaja mengekspos data pribadi dari ratusan ribu pelanggannya. Masalah tersebut terjadi pada Linc, vendor yang digunakan perusahaan untuk mengotomatiskan pembelian *online*. Diketahui bahwa lebih dari 410.000 file dan ratusan ribu data pelanggan terungkap.[145]

[143]Mercedes-Benz, "Mercedes-Benz USA Announce Initial Findings of Dara Investigation Affecting Customers and Interested Buyers", 24 Juni 2021, https://media.mbusa.com/releases/release-ee5a810c1007117e79e1c871352a4afa-mercedes-benz-usa-announces-initial-findings-of-data-investigation-affecting-customers-and-interested-buyers (diakses pada 20 Mei 2022).

[144]Yang Jie dan Liza Lin, "Alibaba Falls Victim to Chinese Web Crawler in Large Data Leak", *The Wall Street Journal*, 15 Juni 2021, https://www.wsj.com/articles/alibaba-falls-victim-to-chinese-web-crawler-in-large-data-leak-11623774850 (diakses pada 21 Mei 2022).

[145]Becky Bracken, "Baby Clothes Giant Carter's Leaks 410K Customer Records", *Threat Post*, 11 Juni 2021, https://threatpost.com/baby-clothes-carters-leaks-customer-records/166866/ (diakses pada 21 Mei 2022).

24.	2020	Canada Post	Pada bulan Desember 2020, Canada Post mendapat serangan *ransomware* dan memengaruhi 44 pelanggan besar komersial dan **950.000** pelanggan penerima.[146]
25.	2018	British Airways	**420.000** data staf dan pelanggan British Airways mengalami kebocoran data yang terjadi pada 22 Juni 2018. Pada Oktober 2020, Kantor Komisi Informasi Inggris mengeluarkan denda kepada British Airways sebesar US$27,7 juta.[147]
26.	2016	Booking	Peretas yang diduga bekerja untuk badan intelijen Amerika Serikat telah membobol server Booking.com pada 2016. Dalam serangan tersebut, data pengguna terkait dengan Timur Tengah dicuri. Informasi tersebut terungkap dalam buku berjudul *De Machine: In de ban van Booking.com.* Dalam buku yang ditulis oleh tiga jurnalis dari surat kabar nasional Belanda NRC, pelanggaran data itu disebut dengan *"PIN-leak".* Dalam buku tersebut diketahui bahwa para peretas mengakses ribuan reservasi hotel terkait dengan negara-negara Timur Tengah, termasuk Arab Saudi, Qatar, dan Uni Emirat Arab.[148]

[146]Lawrence Abrams, "Canada Post Hit by Data Breach After Supplier Ransomeware Attack", *Bleeping Computer*, 27 Mei 2021, https://www.bleepingcomputer.com/news/security/canada-post-hit-by-data-breach-after-supplier-ransomware-attack/ (diakses pada 21 Mei 2022).

[147]Yadarisa Shabong, "British Airways Settles with 2018 Breach Victims", *Reuters*, 7 Juli 2021, https://www.reuters.com/business/aerospace-defense/british-airways-reaches-settlement-with-customers-over-2018-data-breach-2021-07-06/ (diakses pada 21 Mei 2022).

[148]Dan Goodin, "Booking.com was Reportedly Hacked by a US Intel Agency But Never Told Customers", *Ars Technica*, 12 November 2021, https://arstechnica.com/gadgets/2021/11/new-book-claims-us-intel-agency-hacked-booking-com-in-2016/ (diakses pada 21 Mei 2022).

APA ITU BOT?

Bot berasal dari kata *'robot'*, yakni aplikasi yang dapat melakukan dan mengulangi tugas tertentu lebih cepat daripada manusia. Ketika sejumlah besar bot menyebar ke beberapa komputer dan terhubung satu sama lain melalui internet, mereka membentuk grup yang disebut *botnet*, yang merupakan jaringan bot. *Botnet* berasal dari tiga elemen utama, yakni bot, *Command and Control* (C & C), dan *botmaster*. Bot dirancang untuk menginfeksi target (misalnya komputer atau ponsel), dan menjadikannya bagian dari *botnet* tanpa sepengetahuan pemiliknya di bawah kendali seseorang, yang dikenal sebagai *botmaster*. *Botmaster* mengirimkan perintah ke semua bot pada target yang terinfeksi dan mengontrol seluruh *botnet* melalui internet dan server C & C. *Botmaster* mencoba untuk mengendalikan target ini dan melakukan aktivitas jahat mereka. Dalam tinjauan berbagai jenis aktivitas jahat yang dilakukan oleh *botnet*, ditemukan bahwa mereka tidak hanya mengancam jaringan komputer dan internet, tetapi juga digunakan sebagai infrastruktur untuk melakukan jenis ancaman dan serangan lainnya (misalnya DDoS).[149]

[149]Meisam Eslahi, *et.al.*, "Bots and Botnets: An Overview of Characteristics, Detection and Challenges", *IEEE International Conference on Control System, Computing and Engineering*, 23-25 November 2021, Malaysia, pp. 349-354, DOI:10.1109/ICCSCE.2012.6487169, hlm. 349.

[Halaman ini sengaja dikosongkan]

BAB 2

JENIS-JENIS *SOCIAL ENGINEERING*

Commissum menyatakan bahwa terdapat beragam bentuk *social engineering,* namun dasar dari metode umum yang digunakan adalah: (1) *baiting;* (2); *quid pro quo;* (3) *pretexting;* (4) *trust/distrust.*[150] Beberapa ragam jenis serangan *social engineering* lainnya, yaitu:[151]

1. *phishing;*
2. *baiting*;
3. *pretexting*;
4. *tailgating*;
5. *ransomware*;
6. *impersonation on help desk*;
7. *diversion theft*;
8. *dumpster diving*;
9. *shoulder surfing*;
10. *quid pro quo*;
11. *pop-up* Windows;
12. *robocalls*;

[150]Commissum, "The History and Evolution of Social Engineering Attacks", *Commissum*, 24 Mei 2018, https://commissum.com/blog-articles/the-history-and-evolution-of-social-engineering-attacks (diakses pada 23 Mei 2022).

[151]Fatima Salahdine dan Naima Kaabouch, *Op. Cit.*, hlm. 4.

13. *reverse social engineering*;
14. *online social enginerring;*
15. *phone social engineering;*
16. *stealing important documents;*
17. *fake software;*
18. *pharming;*
19. *SMSishing;*
20. *whitelisting flow.*

Namun, terdapat lima serangan yang umum terjadi, yaitu: *phishing, baiting, quid pro quo, pretexting,* dan *piggybacking*.[152]

A. Phishing

Istilah *phishing* mengacu pada *'fishing'* di dunia fisik. *Phishing* adalah bentuk eksploitasi dunia maya yang melibatkan aksi penipuan korban untuk menjadi sukarelawan kredensial informasi sensitif, seperti rincian kartu kredit dan kata sandi, lalu kemudian menggunakan kredensial curian untuk keuntungan finansial. *Phishing* dibedakan dari jenis eksploitasi dunia maya lainnya karena menargetkan dan mengeksploitasi kerentanan pengguna manusia.[153] Definisi lainnya mengenai *phishing* secara *de facto* digambarkan sebagai proses menipu penerima untuk mengambil tindakan yang diinginkan penyerang. Sementara itu, beberapa definisi menyebutkan situs web sebagai satu-satunya media yang memungkinkan untuk melakukan serangan sehingga mendefinisikan *phishing* sebagai aktivitas penipuan yang melibatkan pembuatan replika halaman web yang ada untuk mengelabui pengguna agar mengirimkan data pribadi, keuangan, atau kata sandi. Definisi tersebut menjelaskan *phishing* sebagai upaya untuk menipu pengguna agar mengungkapkan informasi sensitif seperti detail bank dan nomor kartu kredit dengan mengirimkan tautan berbahaya ke pengguna yang mengarah ke pembuatan web palsu.[154]

---

[152]Hussain Aldawood dan Geoffrey Skinner, "Reviewing Cyber Security Social Engineering Training and Awareness Programs – Pitfalls and Ongoing Issues", *Future Internet*, Vol. 11, No. 73, 2019, DOI:10.3390/fi11030073, hlm. 4.

[153]Van Nguyen, *Op. Cit*., hlm. 3.

[154]Zainab Alkhalil, *et.al.*, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy", *Frontiers in Computers Science*, Vol. 3, March 2021, hlm. 3.

Selain itu, definisi lainnya menyebutkan *email* sebagai satu-satunya faktor serangan, sehingga menggambar *phishing* sebagai upaya penipuan yang umumnya dilakukan melalui *email* untuk mencuri informasi pribadi target. Tidak hanya itu *phishing* turut didefinisikan sebagai suatu bentuk pencurian identitas *online* yang bertujuan untuk mencuri informasi sensitif seperti *password* perbankan *online* dan informasi kartu kredit dari pengguna. Selanjutnya beberapa definisi menyoroti penggunaan gabungan keterampilan sosial dan teknis, seperti APWG yang mendefinisikan *phishing* sebagai mekanisme kriminal yang menggunakan rekayasa sosial dan dalih teknis untuk mencuri data identitas pribadi konsumen dan kredensial akun keuangan. Selain itu, definisi dari *The United States Computer Emergency Readiness Team* (US-CERT) menyatakan *phishing* sebagai suatu bentuk rekayasa sosial yang menggunakan *email* atau situs web berbahaya untuk meminta informasi pribadi dari individu atau perusahaan dengan menyamar sebagai organisasi atau entitas yang dapat dipercaya.[155]

Sebagian besar masyarakat, menilai istilah *phishing* identik dengan pengiriman *email* dengan maksud tujuan jahat. Namun, sesungguhnya terdapat beragam ancaman yang dilakukan melalui *email*. Barracuda mengidentifikasi 13 jenis ancaman serangan yang dilakukan melalui *email,* yakni:

Gambar 4. 13 Jenis Ancaman Serangan Melalui *Email*[156]

Dari gambar di atas, dapat terlihat bila ancaman serangan melalui *email* tidak selalu identik dengan *phishing,* bahkan terdapat beragam jenis *phishing*. Namun, saat ini akan dijelaskan bentuk *phishing* secara umum. *Phishing* merupakan salah satu masalah besar yang dihadapi oleh individu, perusahaan hingga negara dan bila tidak ditangani memiliki konsekuensi yang menghancurkan. Diperkirakan lebih

[155]*Ibid.*

[156]Barracuda, *Spear Phishing: Top Threats and Trends,* Vol. 5, Desember 2020, hlm. 2.

dari 80% organisasi telah mengalami serangan *phishing*. Korbannya tidak hanya perusahaan kecil dan non-IT, seperti yang dialami oleh JP Morgan, Target, Sony bahkan kantor manajemen personalia Pemerintah Amerika Serikat. Biaya kerugian yang dialami oleh Sony pada tahun 2014 sebesar US$ 171 juta.[157] Serangan *phishing* yang tengah ramai saat ini adalah *web phishing* dengan kedok penjualan tiket menonton pertandingan Olimpiade 2020 di Tokyo Jepang. Selain itu, terdapat penawaran layanan *streaming online* dan dukungan penggalangan dana palsu untuk atlet olimpiade.[158] Data yang dirilis oleh NTT Corporation, perusahaan yang menyediakan layanan telekomunikasi Olimpiade Tokyo mengungkapkan bila terdapat lebih dari 450 juta percobaan serangan siber selama acara berlangsung (meningkat 2,5 kali lipat dibandingkan dengan Olimpiade London 2012).[159] Serangan *web phishing* lainnya memanfaatkan perilisan film *superhero* Marvel "*Black Widow*" pada 9 Juli 2021. Penyerang menampilkan beberapa menit pertama film sebelum akhirnya meminta pengguna mendaftar dapat melihat kelanjutannya. Pengguna diminta untuk mengisi informasi pribadi, seperti nama, negara tempat tinggal, kode pos serta informasi kartu kredit. Namun, setelah pendaftaran selesai, film tersebut tidak dapat diputar, walaupun uang telah terpotong. Tidak hanya itu, penyerang turut mencoba menyebarkan file jahat yang dengan modus unduhan film.[160] Serupa dengan modus film *Black Widow*, penjahat siber turut memanfaatkan perilisan album terbaru Kanye West. Perusahaan

---

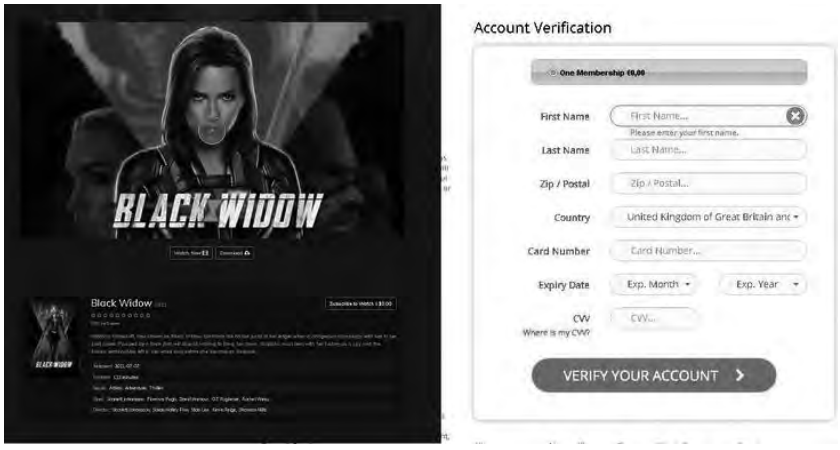
[157]Jason E. Thomas, "Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks", *International Journal of Business and Management*, Vol. 13, No. 6, 2018, pp. 1-24, DOI: 10.5539/ijbm.v13n6p1, hlm. 1.

[158]Veronica Combs, "Scammers Offer Streaming Service, Giveaways and a Fake Cyber Currency to Cash in on the Olympic Games", *TechRepublic*, 22 Juli 2021, https://www.techrepublic.com/article/scammers-offer-streaming-services-giveaways-and-a-fake-cyber-currency-to-cash-in-on-the-olympic-games/ (diakses pada 23 Juni 2022).

[159]Jonathan Greig, "450 Million Cyberattacks attempted on Japan Olympics Infrastructure: NTT", *Zdnet*, 22 Oktober 2021, https://www.zdnet.com/article/nearly-450-million-cyberattacks-attempted-on-japan-olympics-infrastructure-ntt/ (diakses pada 21 Mei 2022).

[160]Brandon Vigliarolo, "Black Widow Digital Premier a Cover for Malware and Scams, Says Kaspersky", *TechRepublic*, 8 Juli 2021, https://www.techrepublic.com/article/black-widow-digital-premier-a-cover-for-malware-and-scams-says-kaspersky/ (diakses pada 21 Mei 2022).

keamanan Kapersky menemukan unduhan palsu berisi file *adware* yang diberi nama **"Download-File-KanyeWestDONDA320.zip_88481.msi"** dan **"Kanye West_DONDA (Explicit) (2021) Mp3 320kbps [PMEDIA]__- Downloader.exe"**. Kapersky mendapati beberapa situs web penipuan (*scam)* yang menjebak orang untuk mengeklik tautan berbahaya tersebut.[161]



Gambar 5. *Web Phishing "Black Widow"*
Sumber: Kapersky

Bullee mendefinisikan *phishing* sebagai tindakan penipuan terukur di mana penipuan identitas digunakan untuk mendapatkan informasi dari target. Definisi tersebut mengandung dua bagian berikut.[162]

1. *Scalability* berkaitan dengan seberapa mudah bagi pelaku untuk mendekati target. Oleh karena itu, semua nonmedia massa (yaitu interaksi tatap muka atau panggilan telepon) bukan merupakan *phishing*.
2. Penipuan dengan penyamaran untuk memperoleh informasi, misalnya mengaku seseorang dari bank untuk mendapatkan informasi. Ketika pelaku tidak menggunakan peniruan identitas, itu

[161]Brandon Vigliarolo, "Kanye's Upcoming Album is a Scam Magnet, Kapersky Finds", *Techrepublic*, 25 Agustus 2021, https://www.techrepublic.com/article/kanyes-upcoming-album-is-a-scam-magnet-kaspersky-finds/#ftag=RSS56d97e7 (diakses pada 22 Mei 2022).

[162]Jan-Willem Bullee, *et.al.*, "Spear Phishing in Organitations Explained", *Information & Computer Security*, Vol. 25, No. 5, 2017, pp. 593-613, DOI: 10.1108/ICS-03-2017-0009, hlm. 595.

adalah permintaan informasi yang tidak menipu, dan oleh karena itu, tidak dapat diklasifikasikan sebagai *phishing*.

Phishing kerap ditujukan guna mengirimkan *malware*, *ransomware* atau untuk mendapatkan informasi pribadi dari penerima guna pencurian identitas. Serangan *phishing* terjadi dari tiga elemen, yaitu: (1) bujukan; (2) *hook;* dan (3) *catch*. Bujukan kerap melibatkan pesan *email* yang tampaknya berasal dari orang atau organisasi yang sah, dan kredibilitasnya diperkuat melalui eksploitasi,[163] antara lain:

1. keingintahuan, seperti *email* dengan isi tautan yang mengarah kepada video berita atau peristiwa terkini;
2. ketakutan, seperti *email* dari bank yang mendesak pengguna untuk memvalidasi informasi karena terjadi masalah dalam akunnya;
3. empati, seperti *email* yang menyamar sebagai teman atau kerabat yang membutuhkan bantuan keuangan atau informasi pribadi.

Keberhasilan serangan *phishing* bergantung pada 'kredibilitas". Seorang penyerang akan berjuang untuk memastikan korban percaya bahwa dirinya adalah pihak yang pantas untuk mendapatkan akses, baik melalui *email* yang tampak kredibel karena bersumber dari lembaga yang sah ataupun video rekayasa. Pada awal tahun 2021, FBI memperingatkan bahwa penyerang saat ini kemungkinan besar menggunakan *deepfake* sebagai taktik dalam aksinya. Teknologi *deepfake* berpotensi mengubah ancaman *phishing* sepenuhnya, karena memungkinkan penyerang beraksi di luar "dunia kata" dan memanfaatkan tingkat kepercayaan yang tinggi karena berkomunikasi melalui video.[164]

---

[163]Roderic Broadhurst, *et.al.,* "Phishing and Cybercrime Risk in a University Student Community"*, International Journal of Cybersecurity Intelligence & Cybercrime*, Volume 2, Issue 1, Article 2, 2019, hlm. 5.

[164]FBI, *Private Industry Notification*, 10 Maret 2021, https://www.ic3.gov/Media/News/2021/210310-2. pdf (diakses pada 22 Mei 2022).

***Deepfake* dan Perusahaan Energi Inggris**

Pada tahun 2019, seorang peretas menggunakan perangkat lunak berbasis *artificial intelligence* untuk meniru suara kepala eksekutif dan melakukan penipuan dengan meminta transfer dana sebesar €220.000 ($243.000). CEO sebuah perusahaan energi yang berbasis di Inggris mengira bila tengah berbicara di telepon dengan pimpinannya, kepala eksekutif perusahaan induk Jerman, yang memintanya untuk mengirim dana tersebut ke pemasok di Hungaria. Penelepon mengatakan permintaan itu mendesak, mengarahkan eksekutif untuk membayar dalam waktu satu jam.

Untuk informasi lebih lanjut terkait **Serangan *Deepfake* dan Perusahaan Inggris,** Anda dapat *scan QR code* di samping.[165]

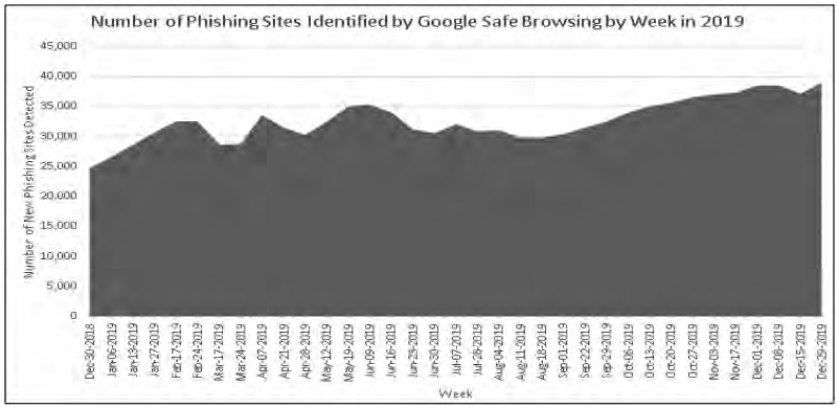
Dalam sebuah laporan, angka kejahatan *phishing* terlihat menurun, namun peningkatan *email* berbahaya dari 43% pada tahun 2017 menjadi 48% pada tahun 2018 sebagaimana yang dilaporkan oleh *Internet Security Threat Report* (ISTR) pada tahun 2018. Statistiknya dapat terlihat pada Gambar 6 berikut.

Gambar 6. Angka Kejahatan *Phishing* Tahun 2018[166]

[165]BBC NEWS, "Lancaster University Students' Data Stolen by Cyber-thieves", *BBC NEWS*, 23 Juli 2019, https://www.bbc.com/news/uk-england-lancashire-49081056 (diakses pada 22 Mei 2022).

[166]Tariq Rahim Soomro dan Mumtaz Hussain, "Social Media-Related Cybercrimes and Techniques for Their Prevention", *Applied Computer Systems*, Vol. 24, No. 1, Mei 2019, pp. 9-17, DOI: https://doi.org/10.2478/acss-2019-0002, hlm. 11.

Pada tahun 2019, *Google Safe Browsing* mendeteksi rata-rata terdapat 32.677 situs *phishing* baru setiap minggunya, yang menunjukkan tren kenaikan, seperti yang ditunjukkan pada gambar berikut.[167]



Gambar 7. Jumlah Situs *Phishing* yang Terdeteksi oleh *Google Safe Browsing* Setiap Minggunya pada Tahun 2019

Situs *web phishing* dapat di-*hosting* di mana saja. Beberapa lokasi memiliki konsentrasi situs *phishing* yang lebih tinggi daripada yang lain. **Tabel 3** di bawah, mengilustrasikan lokasi dengan konsentrasi situs *phishing* yang lebih tinggi dari rata-rata sebagaimana dipublikasikan dalam berbagai volume (v19, v21, v22, v23) Microsoft *Security Intelligence Report* (SIR) yang tersedia untuk diunduh pada www.microsoft.com/sir. Periode waktu yang tercermin meliputi kuartal pertama 2015 (1Q15), paruh pertama 2015 (1H15), paruh pertama 2016 (1H16), Maret 2017, dan paruh kedua 2017 (2H17), termasuk di Indonesia.[168]

Tabel 3. Lokasi dengan Konsentrasi Situs *Phishing* yang Lebih Tinggi dari Rata-rata pada Tahun 2015-2017[169]

Periode	Lokasi	Situs *Phising* per 1.000 *Host* Internet	Rata-rata Dunia	Sumber Data
1Q15	Bulgaria	98.5	5	Microsoft SIRv19
1H15	Libya	15.6	5	Microsoft SIRv19
1H15	Belize	14.5	5	Microsoft SIRv19

[167]Tim Rains, *Cybersecurity threats, Malware Trends, and Strategies* (Birmingham: Packt Publishing, 2020), hlm. 170.

[168]*Ibid.*, hlm. 172.

[169]*Ibid.*

Periode	Lokasi	Situs *Phising* per 1.000 *Host* Internet	Rata-rata Dunia	Sumber Data
1H16	Ukraina	18.8	9.1	Microsoft SIRv21
1H16	Afrika Selatan	15.4	9.1	Microsoft SIRv21
1H16	Australi	14.5	9.1	Microsoft SIRv21
Maret 2017	Ukraina	3.2	6.3	Microsoft SIRv22
Maret 2017	Afrika Selatan	10.3	6.3	Microsoft SIRv22
Maret 2017	Indonesia	9.6	6.3	Microsoft SIRv22
Maret 2017	Denmark	9.7	6.3	Microsoft SIRv22
2H17	Ukraina	19.1	5.8	Microsoft SIRv23
2H17	Belarus	12.3	5.8	Microsoft SIRv23
2H17	Bulgaria	12.2	5.8	Microsoft SIRv23
2H17	Indonesia	10.8	5.8	Microsoft SIRv23

Laporan *European Union Agency For Cybersecurity* (ENISA) pada tahun 2020 menerangkan perihal *Top Phishing Themes in 2019,* yaitu:[170]

1. *Generic Email Credential Harvesting.*
2. *Office 365 Account Phishing.*
3. *Financial Institution Phishing.*
4. *Microsoft OWA Phishing.*
5. *OneDrive Phishing.*
6. *American Express Phishing.*
7. *Chalbai Generic Phishing.*
8. *Adobe Account Phishing.*
9. *Docusing Phishing.*
10. *Netflix Phishing.*
11. *Dropbox Account Phishing.*
12. *LinkedIn Account Phishing.*

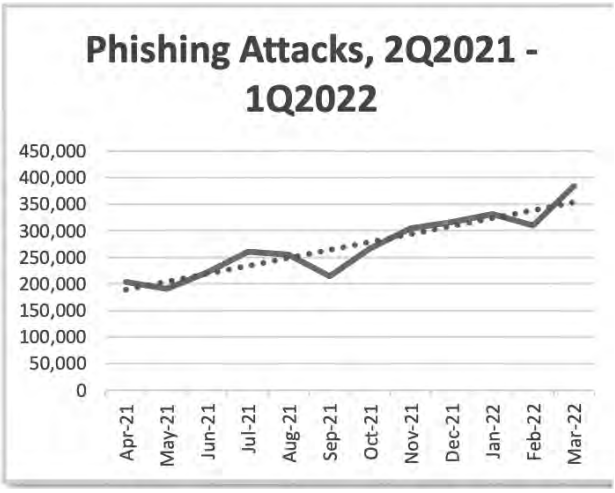
[170]Marco Barros Lourenco dan Louis Marinos (eds), *European Union Agency for Cybersecurity (ENISA)* (Phishing ENISA Threat Landscape, Attiki: ENISA, 2020), DOI: 10.2824/552242, hlm. 9.

13. *Apple Account Phishing*.
14. *Postal/Shipping Company Phishing*.
15. *Microsoft Online Document Phishing (Excel and Word)*.
16. *Windows Setting Phishing*.
17. *Google Drive Phishing*.
18. *PayPal Phishing*.

Dalam laporan *Data Breach Investigation Report* (DBIR) 2020, Verizon Enterprise menemukan bahwa *phishing* adalah variasi ancaman kedua teratas dalam insiden keamanan dan variasi ancaman teratas dalam pelanggaran data. Lebih dari seperlima (22%) pelanggaran data yang dianalisis oleh Verizon Enterprise melibatkan *phishing* dalam berbagai cara. Laporan Google menyebutkan bahwa situs *web phishing* meningkat 350% dari 149.195 pada Januari 2020 menjadi 522.495 hanya dalam dua bulan. Banyak dari situs web ini menggunakan Covid-19 sebagai iming-iming,[171] bahkan dalam laporan *Anti Phishing Working Group* yang dirilis pada 7 Juni 2022, diketahui sepanjang kuartal pertama tahun 2022 ditemukan 1.025.968 serangan *phishing,* dengan perusahaan finansial yang menjadi target utamanya (23.6%). Diketahui bahwa pada bulan Maret 2022 merupakan bulan tertinggi serangan *phishing* terjadi, seperti yang dijelaskan pada gambar berikut.[172]

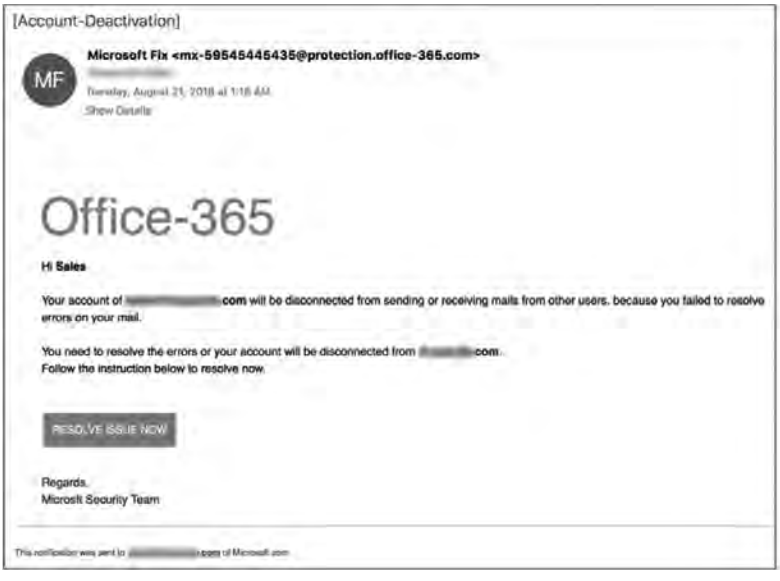
[171]David Bisson, "6 Common Phishing Attacks and How to Protect Against Them", *Tripwire*, 20 Oktober 2020, https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/ (diakses pada 22 Mei 2022).

[172]Anti Phishing Working Group, "Phishing Activity Trends Report, 1st Quarter 2022", *APWG*, 7 Juni 2022, hlm. 2.



Gambar 8. Serangan *Phishing* Sepanjang Kuartal 2 (2021) Hingga Kuartal 1 (2022)[173]

Berikut salah satu contoh, dari salah satu *Top Phishing Themes* yang sebelumnya telah disebutkan oleh ENISA, yakni *Office 365 phishing email*.



Gambar 9. Contoh *Office 365 Phishing Email*[174]

[173]*Ibid.*
[174]Marco Barros Lourenco dan Louis Marinos (eds), *Op. Cit.*, hlm. 10.

Kasus *Phishing "Office 365"*

Pada pertengahan Juni 2021, kelompok peretas yang dikenal dengan nama BazarCall menggunakan sebuah *malware "*BazarLoader" yang didesain untuk membawa dan mendistribusikan *ransomware*. Dalam serangan awalnya, kelompok ini menggunakan *email phishing* yang menargetkan pengguna *Office 365*. *Email* tersebut mengaku berasal dari perusahaan teknologi yang mengklaim bahwa target telah mengunduh versi demo yang akan kedaluwarsa dalam waktu 24 jam. Selanjutnya korban diberitahu bahwa akan ada pengenaan biaya untuk *software* secara otomatis, kecuali mereka menghubungi *call center* yang tersedia untuk pembatalan langganan. Ketika target menghubungi nomor tersebut, *call center* palsu akan mengarahkan target untuk mengunjungi situs web dan mengunduh file Excel untuk membatalkan layanan. File ini sebenarnya berisi macro jahat yang mengunduh *malware*. Pelaku turut menggunakan alat *pentest* Cobalt Strike untuk mencuri kredensial korban, termasuk *database Active Directory* (AD).

Untuk informasi lebih lanjut terkait **Kasus *Phishing Office 365,*** Anda dapat *scan QR code* di samping.

Peristiwa *Lancaster University*

Sebuah serangan *phishing* dialami oleh *Lancestery University* pada tahun 2019. Data pribadi siswa dan pelamar telah dicuri dalam serangan *phishing* tersebut, termasuk di antaranya adalah nama, catatan siswa, nomor telepon, *email*, dan dokumen identitas yang telah mendaftar pada tahun 2019 dan 2020. Pihak universitas mengatakan informasi tersebut telah digunakan untuk mengirim faktur palsu kepada pelamar sarjana. Serangan *phishing* tersebut melibatkan upaya untuk menipu pengguna web agar menyerahkan informasi sensitifnya.

Untuk informasi lebih lanjut terkait **Serangan *Phishing* terhadap Lancaster University,** Anda dapat *scan QR code* di samping.[175]

[175]BBC NEWS, "Lancaster University Students' Data Stolen by Cyber-thieves", *BBC NEWS*, 23 Juli 2019, https://www.bbc.com/news/uk-england-lancashire-49081056 (diakses pada 22 Mei 2022).

Dalam studinya, Alkhalil membagi proses serangan *phishing* menjadi empat fase, yaitu *planning*, *preparation*, *attack*, dan *valuables acquisition*. Pada fase ***planning***, *phisher* membuat keputusan tentang target dan mulai mengumpulkan informasi tentangnya (individu atau perusahaan). *Phisher* mengumpulkan informasi tentang korban untuk memancingnya berdasarkan kerentanan psikologis. Informasi ini dapat beragam seperti nama, alamat *email* untuk individu, atau pelanggan perusahaan. Korban juga dapat dipilih secara acak, dengan mengirimkan surat massal atau ditargetkan dengan mengumpulkan informasi dari media sosial, atau sumber lainnya. Target untuk *phishing* dapat berupa pengguna mana saja yang memiliki rekening bank dan memiliki komputer di internet. *Phisher* menargetkan bisnis seperti layanan keuangan, sektor ritel seperti eBay dan Amazon, dan penyedia layanan internet seperti MSN/Hotmail, dan Yahoo. Fase ini juga termasuk merancang metode serangan seperti membangun situs web palsu (dalam kasus tertentu *phisher* mendapatkan halaman *scam* yang telah dirancang atau digunakan), merancang *malware*, membuat *email phishing*.[176]

Pada fase ***preparation***, *phisher* mulai mengatur serangan dengan memindai kerentanan untuk dieksploitasi. Beberapa contoh kerentanan yang dieksploitasi oleh *phisher* misalnya adalah kerentanan *buffer overflow* untuk mengendalikan aplikasi target, membuat serangan DoS, atau membahayakan komputer. Selain itu, kerentanan perangkat lunak "*zero-day*", yang mengacu pada kerentanan yang baru ditemukan dalam program perangkat lunak atau sistem operasi dapat dieksploitasi secara langsung sebelum diperbaiki. Contoh lain adalah kerentanan *browser*, menambahkan fitur baru dan pembaharuan pada *browser* mungkin memperkenalkan kerentanan baru ke perangkat lunak *browser.* Selain merencanakan serangan untuk mengeksploitasi potensi kerentanan, *phisher* memilih media yang akan digunakan untuk menyampaikan ancaman kepada korban dan melakukan serangan. Media ini dapat berupa internet (jejaring sosial, situs web, *email*, komputasi awan, *e-banking*, sistem seluler), VoIP atau pesan teks. Salah satu contoh media yang aktif digunakan adalah *Cloud Computing* (CC). CC telah menjadi salah satu teknologi yang lebih menjanjikan dan populer menggantikan teknologi komputasi konvensional. Meskipun dinilai banyak keuntungan

[176]Zainab Alkhalil, *Op. Cit.,* hlm. 10-11.

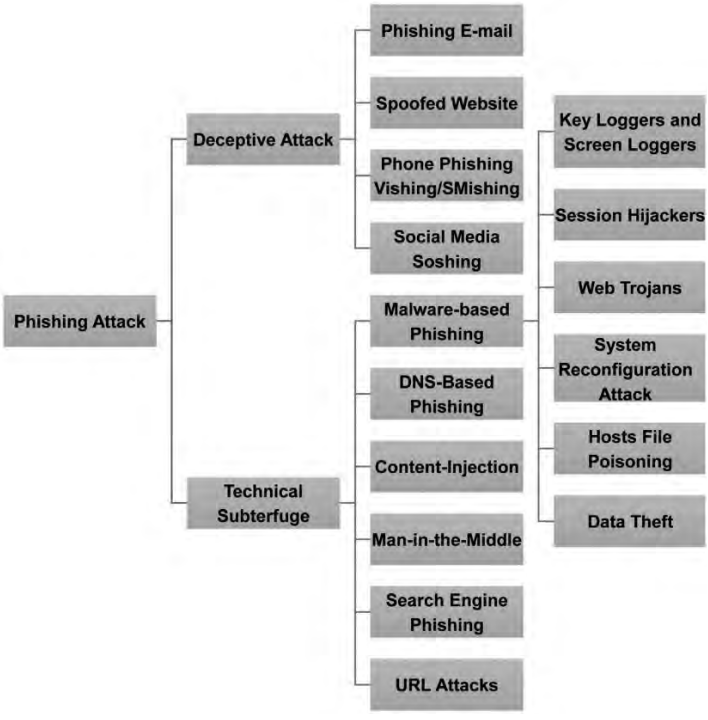
yang dihasilkan oleh CC, adopsi CC menghadapi beberapa kendala kontroversial termasuk privasi dan masalah keamanan. Misalnya pada September 2014, foto-foto rahasia beberapa selebritas beredar di internet dalam, yang diakibatkan aksi peretasan akun iCloud.[177]

Pada fase ***attack,*** ditemukan penggunaan teknik serangan untuk menyampaikan ancaman kepada korban serta interaksi korban dengan serangan dalam hal merespons atau tidak. Setelah korban merespons, sistem dapat disusupi oleh penyerang untuk mengumpulkan informasi pengguna. *Phisher* dapat mengkompromikan *host* tanpa pengetahuan teknis dengan membeli akses dari peretas. Ancamannya adalah eksploitasi kerentanan keamanan dan privasi orang atau menyebabkan kemungkinan kerusakan pada sistem komputer untuk tujuan jahat. Ancaman tersebut dapat berupa *malware*, *botnet*, penyadapan, *email* yang tidak diminta, dan tautan viral. Pada fase terakhir, yakni ***valuables acquisition,*** *phisher* mengumpulkan informasi atau barang berharga dari korban dan menggunakannya secara ilegal untuk membeli, mendanai uang tanpa sepengetahuan pengguna, atau menjual kredensial ini di pasar gelap. Penyerang menargetkan berbagai macam barang berharga dari korbannya mulai dari uang hingga nyawa orang. Misalnya, serangan terhadap sistem medis *online* dapat menyebabkan hilangnya nyawa. Data korban dapat dikumpulkan oleh *phisher* secara manual atau melalui teknik otomatis. Pengumpulan data dapat dilakukan baik selama atau setelah interaksi korban dengan penyerang. Namun, untuk mengumpulkan data secara manual teknik sederhana digunakan di mana korban berinteraksi langsung dengan *phisher* tergantung pada hubungan dalam jaringan sosial atau teknik penipuan manusia lainnya. Sementara itu, dalam pengumpulan data otomatis, beberapa teknik dapat digunakan seperti formulir web palsu yang digunakan dalam *spoofing web*. Selain itu, data publik korban seperti profil pengguna di jejaring sosial dapat digunakan untuk mengumpulkan informasi latar belakang korban yang diperlukan untuk menginisiasi serangan rekayasa sosial.[178]

Sebagaimana yang telah disinggung pada uraian sebelumnya perihal beragamnya jenis *phishing,* perusahaan keamanan Carbonite dan webroot

[177]*Ibid.*, hlm. 11-12.
[178]*Ibid.*

menjelaskan perihal 11 taktik *phishing* yang saat ini hadir, yakni: (1) *standard phishing;* (2) *malware phishing;* (3) *spear phishing;* (4) *smishing;* (5) *search engine phishing;* (6) *vishing*; (7) *pharming;* (8) *clone phishing;* (9) *man-in-the-middle phishing;* (10) BEC; (11) *malvertising*[179] dan jenis *phishing* lainnya yang sulit terdeteksi yakni *BitB Attack*. Sementara itu, Alkhalil membagi jenis *phishing* sebagaimana yang digambarkan berikut.



Gambar 10. Jenis dan Taktik Serangan *Phishing*[180]

Secara ringkas akan diuraikan dan disertai contoh beberapa *phishing* berikut.

1. Standard Phishing

Standard phishing yang paling umum adalah upaya untuk mencuri informasi rahasia dengan berpura-pura menjadi orang atau organisasi

[179]Carbonite dan Webroot, *11 Types of Phishing Attacks You Need to Know to Stay Safe,* 2020.
[180]Zainab Alkhalil, *Op. Cit.,* hlm. 13.

yang berwenang. Ini bukan serangan yang ditargetkan dan dapat dilakukan secara massal.


The White House Instruction for Coronavirus

Inbox ×

info@whcoronavirustaskforce.com Jun 8, 2020, 1:09 PM (10 days ago)

to me

STATEMENTS & RELEASES. The White House. April 2, 2020

Read the White House instruction for America about quarantine which will be prolonged till August 2020.

Protect yourself and your family from the pandemic by following official White House guidelines for slowing the spread of the virus.

Steps to Stay Safe During the Pandemic

Best,

White House Coronavirus Task Force

Gambar 11. Contoh *Standard Phishing*

Email phishing adalah salah satu bentuk *standard phishing*, yang berupa *email* palsu yang dikirim dari sumber yang tidak dipercaya ke ribuan korban secara acak. *Email* palsu ini mengaku berasal dari seseorang atau lembaga keuangan yang dipercaya penerima untuk meyakinkan penerima agar mengambil tindakan yang mengarahkan mereka untuk mengungkapkan informasi sensitif mereka. Sering kali *phisher* tidak menggunakan kredensial secara langsung, sebagai gantinya peretas menjual kembali kredensial atau informasi yang diperoleh di *dark web*.

2. Malware Phishing

Saat ini, *malware phishing* merupakan bentuk serangan *phishing* yang paling banyak digunakan. Seperti namanya, jenis serangan *phishing* ini dilakukan dengan menjalankan perangkat lunak berbahaya di mesin pengguna. *Malware* diunduh ke mesin korban, baik dengan salah satu trik rekayasa sosial atau secara teknis dengan mengeksploitasi kerentanan

dalam sistem keamanan (misalnya, kerentanan *browser*). *Malware* Panda adalah salah satu program *malware* yang berhasil ditemukan oleh Fox-IT Company pada tahun 2016. *Malware* ini menargetkan Sistem Operasi (OS) Windows, yang menyebar melalui kampanye *phishing* dan vektor serangan utamanya termasuk injeksi web, tangkapan layar aktivitas pengguna (hingga 100 per klik mouse), pencatatan *input* keyboard, *Clipboard Pastes* (untuk mengambil kata sandi dan menempelkannya pada formulir), dan mengeksploitasi pada sistem berbagi desktop *Virtual Network Computing* (VNC). Pada tahun 2018, *malware* Panda memperluas targetnya untuk memasukkan pertukaran mata uang kripto dan situs media. Ada banyak bentuk serangan *phishing* berbasis *malware*, beberapa di antaranya adalah sebagai berikut.[181]

a. *Key Loggers* dan *Screen Loggers*

Logger adalah jenis *malware* yang digunakan oleh *phisher* dan diinstal, baik melalui lampiran *email Trojan Horse* atau melalui unduhan langsung kepada komputer pribadi pengguna. Perangkat lunak ini memonitor data dan mencatat penekanan tombol pengguna, kemudian mengirimkannya kepada *phisher*. *Phisher* menggunakan *key logger* untuk menangkap informasi sensitif yang terkait dengan korban, seperti nama, alamat, kata sandi, dan data rahasia lainnya. *Key logger* juga dapat digunakan untuk tujuan *non-phishing* seperti memantau penggunaan internet oleh anak-anak. *Key logger* juga dapat diimplementasikan dengan banyak cara lain seperti mendeteksi perubahan URL dan informasi *log* sebagai *Browser Helper Object* (BHO) yang memungkinkan penyerang untuk mengontrol fitur semua IE, memantau *input* keyboard dan mouse sebagai *driver* perangkat dan memantau *input* dan tampilan pengguna sebagai *screen logger.*

b. *Viruses* dan *Worms*

Virus adalah jenis *malware*, yang merupakan bagian dari kode yang menyebar di aplikasi atau program lain dengan membuat salinan dirinya sendiri secara otomatis. *Worm* serupa dengan virus, tetapi berbeda dalam cara eksekusinya karena *worm* dijalankan dengan mengeksploitasi kerentanan sistem operasi tanpa perlu memodifikasi program lain. Virus mentransfer dari satu komputer

[181] *Ibid.*, hlm. 14-15.

ke komputer lain dengan dokumen yang dilampirkan, sementara *worm* mentransfer melalui file *host* yang terinfeksi. Baik virus maupun *worm* dapat menyebabkan kerusakan data dan perangkat lunak atau kondisi *Denial of Service* (DoS).

c. *Spyware*

Spying software adalah kode berbahaya yang dirancang untuk melacak situs web yang dikunjungi oleh pengguna untuk mencuri informasi sensitif dan melakukan serangan *phishing*. *Spyware* dapat dikirimkan melalui *email* dan setelah diinstal pada komputer, akan mengambil kendali atas perangkat dan mengubah pengaturannya atau mengumpulkan informasi seperti kata sandi dan nomor kartu kredit atau catatan perbankan yang dapat digunakan untuk pencurian identitas.

d. *Adware*

Adware juga dikenal sebagai perangkat lunak yang didukung iklan. *Adware* adalah jenis *malware* yang menunjukkan kepada pengguna jendela *pop-up* tanpa akhir dengan iklan yang dapat merusak kinerja perangkat. *Adware* dapat mengganggu, tetapi sebagian besar aman. Beberapa *adware* dapat digunakan untuk tujuan jahat seperti melacak situs internet yang dikunjungi pengguna atau bahkan merekam penekanan tombol pengguna.

e. *Ransomware*

Ransomware adalah jenis *malware* yang mengenkripsi data pengguna setelah mereka menjalankan program yang dapat dieksekusi pada perangkat. Dalam jenis serangan ini, kunci dekripsi ditahan hingga pengguna membayar uang tebusan. *Ransomware* bertanggung jawab atas pemerasan puluhan juta dolar setiap tahun. Lebih buruk lagi, *ransomware* sulit dideteksi dengan mengembangkan varian baru, memfasilitasi penghindaran banyak antivirus dan sistem deteksi intrusi. *Ransomware* umumnya dikirimkan kepada perangkat korban melalui *email phishing*.

f. *Rootkits*

Rootkit adalah kumpulan program, umumnya berbahaya, yang memungkinkan akses kepada komputer atau jaringan komputer. *Toolset* ini digunakan oleh penyusup untuk menyembunyikan tindakan mereka dari administrator sistem dengan memodifikasi

kode panggilan sistem dan mengubah fungsionalitas. Istilah "*rootkit*" memiliki konotasi negatif melalui hubungannya dengan *malware* dan digunakan oleh penyerang untuk memperingatkan alat sistem yang ada agar lolos dari deteksi. Kit ini memungkinkan individu dengan sedikit atau tanpa pengetahuan untuk meluncurkan eksploitasi *phishing*. *Rootkit* berisi pengodean, perangkat lunak *email* massal, perangkat lunak pengembangan web, dan alat desain grafis. Contoh *rootkit* adalah kit Kernel. KernelLevel Rootkit dibuat dengan mengganti bagian dari sistem operasi inti atau menambahkan kode baru melalui modul Kernel yang dapat dimuat di Linux atau driver perangkat di Windows.

g. Session Hijackers

Dalam jenis ini, penyerang memantau aktivitas pengguna dengan menyematkan perangkat lunak berbahaya di dalam komponen *browser* atau melalui *network sniffing*. Pemantauan bertujuan untuk membajak sesi, sehingga penyerang melakukan tindakan yang tidak sah dengan sesi yang dibajak seperti mentransfer keuangan, tanpa izin pengguna.

h. Web Trojans

Web Trojans adalah *malware* yang mengumpulkan kredensial pengguna dengan muncul secara tersembunyi di atas layar *login*. Ketika pengguna memasukkan kredensial, program ini menangkap dan mengirimkan kredensial yang dicuri langsung kepada penyerang.

i. Hosts File Poisoning

Ini adalah cara untuk mengelabui pengguna agar masuk ke situs *phisher* dengan meracuni (mengubah) file host. Saat pengguna mengetik alamat situs web tertentu pada URL, alamat web akan diterjemahkan ke dalam alamat numerik (IP) sebelum mengunjungi situs. Penyerang, untuk membawa pengguna ke situs web palsu untuk tujuan *phishing*, akan memodifikasi file ini, misalnya cache DNS.

j. System Reconfiguration Attack

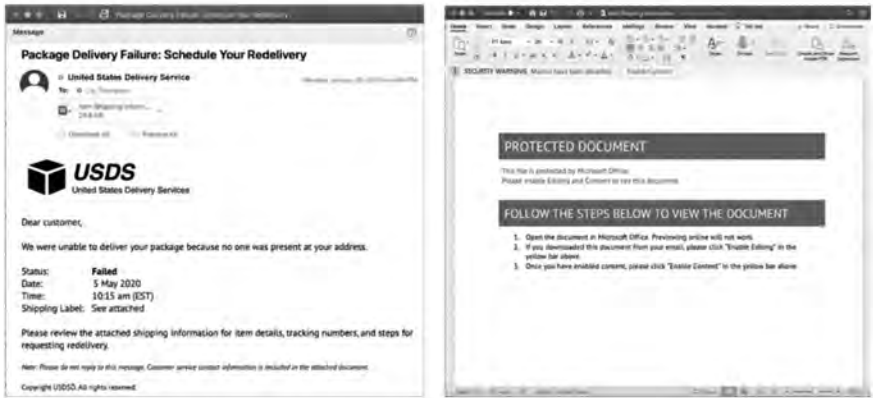
Dalam format serangan *phishing* ini, *phisher* memanipulasi pengaturan di komputer pengguna untuk aktivitas jahat sehingga informasi di PC ini akan disusupi. Konfigurasi ulang sistem dapat diubah menggunakan metode yang berbeda seperti mengonfigurasi ulang sistem operasi dan memodifikasi alamat server *Domain Name System* (DNS) pengguna. The Wireless Evil Twin adalah contoh

serangan konfigurasi ulang sistem di mana semua lalu lintas pengguna dipantau melalui *Access Point* (AP) nirkabel.

k. Data Theft

Data Theft adalah akses yang tidak sah dan pencurian informasi rahasia untuk bisnis atau individu. *Data Theft* dapat dilakukan melalui *email phishing* yang mengarah pada pengunduhan kode berbahaya kepada komputer pengguna yang kemudian mencuri informasi rahasia yang disimpan pada komputer tersebut secara langsung. Informasi curian seperti kata sandi, informasi kartu kredit, *email* sensitif, dan data pribadi lainnya dapat digunakan secara langsung oleh *phisher* atau secara tidak langsung dengan menjualnya untuk tujuan yang berbeda.

Salah satu ciri *malware phishing* adalah lampiran dokumen kosong yang mengharuskan target mengaktifkan makro untuk melihat isinya, seperti pada contoh umum "kegagalan pengiriman paket" di bawah ini.

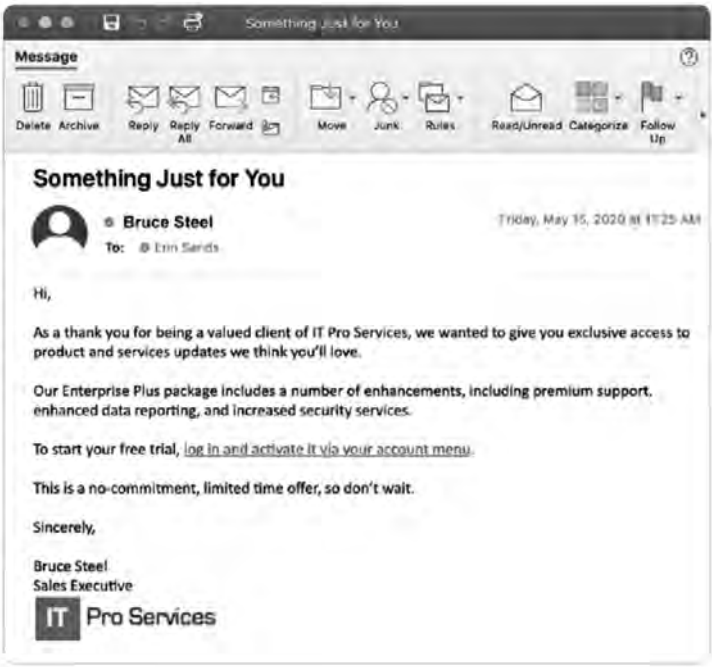


Gambar 12. Contoh *Malware Phishing*

3. Spear Phishing

Ketika sebagian besar serangan *phishing* dikirimkan secara luas, dengan harapan untuk menarik sebanyak mungkin pengguna terpancing, *spear phishing* melibatkan penelitian besar-besaran terhadap target bernilai tinggi yang telah ditentukan sebelumnya—seperti CEO, pendiri, atau persona publik—sering kali mengandalkan informasi publik yang tersedia di internet. Apabila targetnya cukup besar, *spear phishing*

terkadang disebut istilah *'whaling'*. Akan diuraikan lebih lanjut perihal *spear phishing* pada pembahasan selanjutnya.

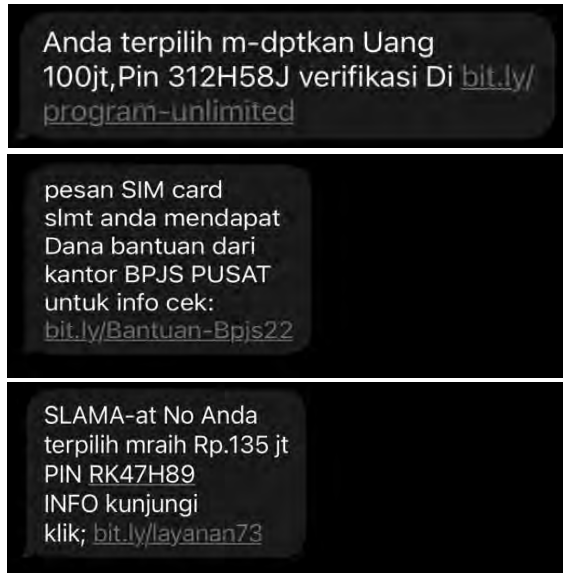


Gambar 13. Contoh *Spear Phishing*

4. Smishing

Smishing (SMS + *phishing*) menggunakan pesan teks sebagai metode untuk mengirimkan tautan berbahaya, sering kali dalam bentuk kode pendek, untuk menjerat pengguna ponsel dalam penipuan mereka. Apabila korban klik tautan yang dikirim, maka kemudian akan diarahkan pada situs untuk meyakinkan calon korban. Dalam situs tersebut, umumnya terdapat keterangan untuk menghubungi nomor pelaku. Setelah itu, pelaku akan meminta calon korban untuk transfer uang, dengan dalih pajak hadiah. Penipu tersebut umumnya menggunakan *SMS Gateway*, sebuah platform yang menyediakan mekanisme untuk mengirim SMS dari peralatan *mobile* melalui SMSC (*Short Message Service Center)*. Beberapa *SMS Gateway* yang kerap digunakan seperti SMSCaster. com, Gammu & Wammu, Kalkun, dan Play SMS. Untuk menjalankan modus ini, pelaku hanya membutuhkan alat PC/laptop, dongle GSM

atau HP dan *database* nomor HP yang dapat dicari di dunia maya. Via aplikasi ini, ribuan SMS dapat terkirim hanya dalam hitungan jam secara otomatis.[182]



Gambar 14. Contoh *Smishing*

Kasus *Smishing* di Inggris

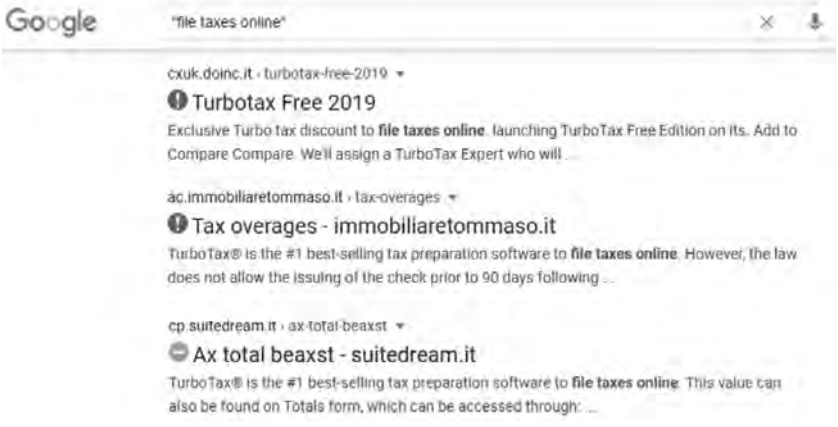
Pada Mei 2021, kepolisian Inggris menangkap 8 orang pelaku serangan siber dengan teknik *smishing*. Pelaku menyamar sebagai Royal mail dan meminta target untuk membayar biaya untuk mengambil sebuah parsel. Royal mail sendiri merupakan jasa pos nasional Inggris Raya. Dalam operandinya, pelaku mencuri informasi pribadi dan bank korban dengan membuatnya mengikuti tautan ke situs web palsu. Dengan begitu, korban akan memasukkan kata sandi, yang kemudian diretas oleh pelaku.

Untuk informasi lebih lanjut terkait **Kasus *Smishing* di Inggris,** Anda dapat *scan QR code* di samping.

[182]Yuni Astutik, "Terungkap! Ini Cara Penipu Sebarkan Ribuan SMS Spam per Jam", *CNBC Indonesia*, 13 Juli 2020, https://www.cnbcindonesia.com/news/20200713142625-4-172258/terungkap-ini-cara-penipu-sebarkan-ribuan-sms-spam-per-jam (diakses pada 24 Mei 2022).

5. *Search Engine Phishing*

Dalam jenis serangan ini, penjahat siber menunggu korban untuk datang. *Search engine phishing* menginjeksi situs penipuan, sering kali dalam bentuk iklan berbayar atau dalam hasil untuk istilah pencarian populer. Situs *search engine phishing* sering kali menjanjikan penawaran luar biasa, peluang kemajuan karier, atau suku bunga pinjaman yang rendah. Sering kali, satu-satunya perbedaan antara hasil penipuan dan yang seharusnya adalah .com yang seharusnya .org.



Gambar 15. Contoh *Search Engine Phishing*

***Malware* SolarMarker**

SolarMarker adalah perangkat lunak jahat *backdoor* yang mencuri data dan kredensial dari *browser*. Penyerang menggunakan ribuan file PDF yang diisi dengan kata kunci dan tautan yang mengarahkan orang yang tidak hati-hati pada web yang telah terpasang *malware.* Serangan tersebut bekerja dengan menggunakan dokumen PDF yang dirancang untuk menentukan peringkat pada hasil pencarian. Penyerang mengisi dokumen-dokumen ini dengan lebih dari 10 halaman kata kunci di berbagai topik, seperti '*insurance form'*, '*acceptance of contract'*, '*hot to join in SQL',* dan *'math answers'*. *Malware* ini sebagian besar menargetkan pengguna di Amerika Utara. Studi yang dilakukan oleh Microsoft, peretas meng-*hosting* halaman di Google Sites sebagai umpan untuk unduhan file berbahaya. Situs-situs web tersebut mempromosikan unduhan dokumen dan sering kali berperingkat tinggi dalam hasil pencarian. Temuan lainnya diketahui, bahwa penyerang telah menggunakan Amazon Web Service dan layanan Strikingly serta Google Sites. Ketika dibuka, terdapat permintaan kepada pengguna untuk mengunduh file .doc atau versi .pdf dari info yang korban inginkan. Korban yang mengeklik tautan akan diarahkan melalui 5 hingga 7 situs dengan TLD seperti .site, .tk, dan .ga. Penyerang lalu mencoba mengalihkan korban kepada situs web yang dikendalikan meniru Google Drive dan diminta untuk mengunduh file yang mengarah ke *malware* SolarMarker.

Untuk informasi lebih lanjut terkait ***Malware* SolarMarker,** Anda dapat *scan QR code* di samping.

6. Vishing

Vishing merupakan singkatan dari *voice phishing*. Dalam modus operandinya, serangan *vishing* melibatkan aktor penipuan yang menelepon korban dengan berpura-pura dari organisasi terkemuka dan mencoba mengekstrak informasi pribadi, seperti informasi perbankan atau kartu kredit. Umumnya "penelepon" terdengar seperti robot, tetapi seiring kemajuan teknologi, taktik ini menjadi lebih sulit untuk diidentifikasi. Tidak hanya itu serangan ini kerap dimulai dengan mengirimkan *email* dengan menggunakan toko *online* yang besar ataupun sistem pembayaran, seperti PayPal yang meminta penarikan uang dalam jumlah besar dari akun pengguna.

Gambar 16. Pemberitahuan Palsu dari PayPal

Sumber: https://www.kaspersky.com/about/press-releases/2022_tiktok-prank-based-on-real-fraud-scheme-how-cybercriminals-are-convincing-victims-to-call-them

Setelah itu, penyerangan akan meminta korban untuk menghubungi *customer support* yang tertera dalam *email*. Para pelaku kerap memilih serangan *vishing* karena ketika korban berbicara melalui telepon, mereka dihadapkan dengan situasi yang membingungkan dan memiliki tendensi untuk kehilangan fokus. Pada situasi ini, pelaku akan melakukan segala cara untuk memastikan korban tetap di bawah tekanan, dengan membuat korban merasa terburu-buru, mengintimidasi dan meminta untuk segera mengirimkan detail kartu kredit atau informasi kredensial lainnya. Perusahaan keamanan Kaspersky dalam studinya telah mendeteksi serangan *vishing* dan *email vishing* dan mengungkapkan jika pada bulan Juni-Juli 2022 terdapat 100.000 *email* dan 350.000 *email vishing*. Lebih lanjut diketahui bila serangan *vishing* tersebut telah mengancam para pengguna aplikasi TikTok.[183]

Salah satu contoh serangan *vishing*:

"Selamat siang, saya dari teknisi windows, saya menelepon karena komputer Anda terdeteksi terkena virus…"

[183]Kapersky, "TikTok Prank Based on Real Fraud Scheme: How Cybercriminals are Convincing Victims to Call Them", *Kapersky*, 11 Juli 2022, https://www.kaspersky.com/about/press-releases/2022_tiktok-prank-based-on-real-fraud-scheme-how-cybercriminals-are-convincing-victims-to-call-them (diakses pada 15 Juli 2022).

Penipuan Bermodus Aplikasi myBCA

Pada akhir September 2022, Kepolisian Daerah Istimewa Yogyakarta telah menangkap dan menetapkan tersangka atas dugaan pengurasan uang korban hingga lebih dari Rp500 juta. Para pelaku melakukan operandinya dengan terlebih dahulu menerima informasi *username* dan *password* korban. Selanjutnya pelaku menghubungi korban. Salah satu korban mengungkapkan bila dihubungi oleh seseorang dengan nomor telepon +1 (501) 2892989. Pelaku berpura-pura mengatasnamakan diri sebagai *Customer Service* (CS) Bank BCA. Kepada korban, pelaku mengatakan terdapat perubahan fitur dalam aplikasi myBCA dengan memberi tahu korban tentang biaya administrasi sebesar Rp300 ribu untuk penambahan fitur tersebut.

Pelaku juga mengatakan apabila nasabah memiliki lebih dari satu rekening, maka biaya tersebut akan dilipatkan setiap bulannya. Karena merasa keberatan, korban yang memiliki tiga rekening bermaksud menutup aplikasi tersebut. Dengan berpura-pura membantu menutup aplikasi tersebut, pelaku mengarahkan korban mengirimkan kode aktivasi aplikasi tersebut yang telah muncul melalui SMS pada telepon genggam korban. Tidak lama muncul dalam SMS bahwa terdapat *One Time Password* (OTP). Disebabkan tengah panik, korban menuruti keinginan tersangka dengan mengirimkan kode OTP sehingga rekening korban dapat dikuasai.

Untuk informasi lebih lanjut terkait **Kasus myBCA,** Anda dapat *scan QR code* di samping.

Kasus Morgan Stanley

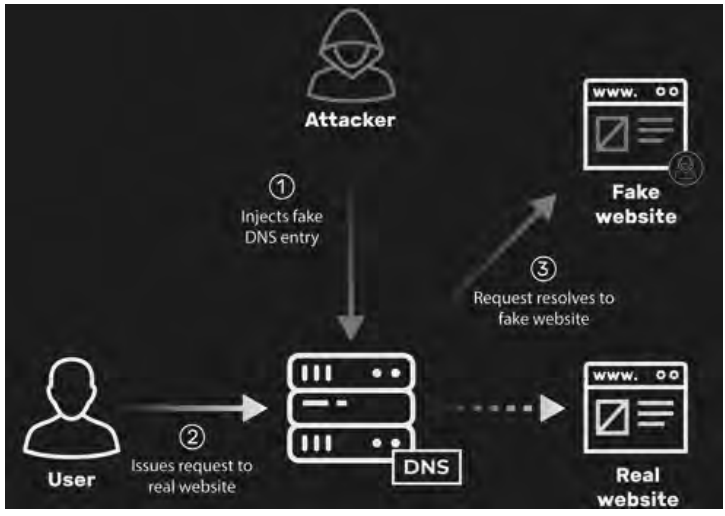
Pada awal tahun 2022, perusahaan Morgan Stanley mengungkapkan jika salah satu divisinya telah disusupi dengan menggunakan serangan *social engineering*. Serangan tersebut menggunakan teknik *vishing*, di mana penyerang menyamar sebagai figur Morgan Stanley dengan menggunakan panggilan suara guna meyakinkan target, agar mengungkapkan atau menyerahkan informasi sensitif seperti perbankan atau kredensial *login* berupa *username* dan kata sandi. Perusahaan mengungkapkan bahwa pada 11 Februari 2022, aktor peretas yang menyamar sebagai Morgan Stanley memperoleh akses ke akun mereka setelah menipu mereka untuk memberikan info akun Morgan Stanley *online*-nya. Pelaku kemudian mengakses akun tersebut dan melakukan pembayaran Zelle yang tidak sah.

Untuk informasi lebih lanjut terkait **Kasus Morgan Stanley,** Anda dapat *scan QR code* di samping.

7. Pharming

Dikenal juga sebagai 'DNS *poisoning*', *pharming* adalah bentuk *phishing* yang secara teknis mutakhir yang melibatkan *Domain Name System* (DNS). *Pharming* mengalihkan lalu lintas web yang sah kepada halaman palsu tanpa sepengetahuan pengguna, sering kali untuk mencuri informasi berharga. Secara pengertian *pharming* didefinisikan sebagai *an internet scamming practice in which malicious code is installed on a person computer or server misdirecting users to fraudulent website without knowledge or consent.*[184]

[184]Ibrahim S. Alfayoumi dan Tawfiq S. Barhoom, "Client – Side Pharming Attacks Detection Using Authoritative Domain Name Servers", *International Journal of Computer Applications*, Vol. 113, No. 10, Maret 2015, hlm. 26.



Gambar 17. Alur Teknik *Pharming*

Sumber: https://pmi-sesni.medium.com/introduction-to-dns-spoofing-c1abf8e67e2d

Kasus Bank di Mexico

Pada tahun 2008, salah satu bank di Mexico telah menerima serangan *pharming.* Dalam serangan tersebut, pelaku berpura-pura mengirimkan *email* dari sebuah perusahaan kartu ucapan berbahasa Spanyol, Gusanito.com. Dalam *email* tersebut terdapat tag gambar HTML, namun tidak menampilkan gambar justru mengirimkan permintaan pada *router* rumah untuk diubah. Diketahui bahwa, terdapat kode yang berusaha mengubah router 2 Wire DSL untuk mengarahkan *browser* pengguna kepada situs bank palsu yang meniru salah satu bank besar di Mexico.

Untuk informasi lebih lanjut terkait **Kasus Bank di Mexico,** Anda dapat *scan QR code* di samping.

8. Clone Phishing

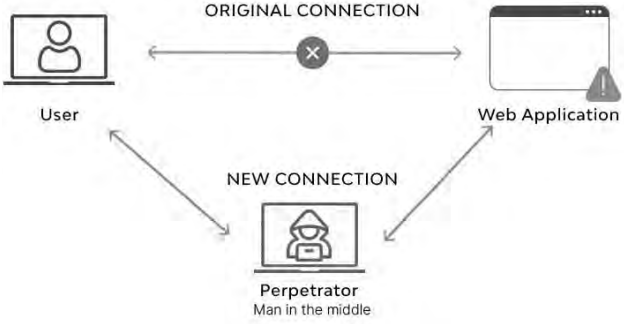
Dalam jenis serangan ini, pelaku membuat perubahan pada *email* yang ada, sehingga menghasilkan *email* yang hampir identik (dikloning), tetapi dengan tautan, lampiran, atau elemen lain yang sah kemudian ditukar dengan yang berbahaya. Di bawah ini adalah contoh betapa

rumitnya *clone phishing* untuk dikenali. Dengan memanfaatkan *social engineering*, peretas meningkatkan kemungkinan penyebaran infeksi.

Gambar 18. Contoh *Clone Phishing*

9. Man in the Middle

Serangan *man in the middle* atau dikenal *The Public WiFi Phisherman* melibatkan penyadap yang memantau korespondensi antara dua pihak yang tidak curiga. Ketika ini dilakukan untuk mencuri kredensial atau informasi sensitif lainnya, itu termasuk ke dalam *phishing man in the middle*. Serangan ini sering dilakukan dengan membuat jaringan WiFi publik palsu di kedai kopi, pusat perbelanjaan, dan lokasi publik lainnya. Setelah bergabung, *man in the middle* mencari informasi atau mendorong *malware* ke perangkat.



Gambar 19. Ilustrasi *Man in the Middle*
Sumber: https://www.wallarm.com/what/what-is-mitm-man-in-the-middle-attack

Kasus Mobil Pengintai

Pada pertengahan 2019, kasus "mobil van pengintai" ramai diperbincangkan setelah sebuah mobil van Chevrolet yang dikemas dengan peralatan senilai US$5-9 juta yang dapat meretas ponsel cerdas Android dan meretas data termasuk pesan WhatsApp dan Signal, ditempatkan di dekat bandara Larnaca. Majalah Forbes sebelumnya telah melaporkan keberadaan mobil pengintai yang disebut mampu meretas Iphone dari jarak 500 meter dan menyedot data-data penting di dalamnya. Perusahaan pemilik van tersebut, WiSpear membayar denda administrasi sebesar 925.000 euro atas pelanggaran GDPR.

Dalam sebuah laporannya, Forbes mengungkapkan bila peralatan pada mobil van tersebut dapat melacak, menyusup, dan mengekstrak konten dari perangkat seluler, termasuk obrolan (Facebook, WhatsApp), teks, panggilan, atau kontak. Kemampuan van tersebut telah didemonstrasikan terhadap salah seorang pengguna ponsel cerdas Huawei yang berada sejauh 500 meter dari mobil, dan dalam hitungan menit, ponsel tersebut telah berhasil diretas. Semua foto, nomor telepon, kontak panggilan, media sosial, video, pesan Facebook, WhatsApp, dan informasi berharga yang ada di dalam layar Huawei turut tampil pada layar monitor dalam mobil tersebut. Teknologi WiSpear menggunakan gelombang pancaran internet WiFi untuk menyerang, membobol, serta meretas.

Untuk informasi lebih lanjut terkait **Kasus Mobil Pengintai,** Anda dapat *scan QR code* di samping.[185]

Untuk informasi lebih lanjut terkait laporan Forbes terkait **Kasus Mobil Pengintai,** Anda dapat melihat video dengan *scan QR code* di samping.

10. Business Email Compromise (BEC)

Salah satu ancaman paling "mahal" yang dihadapi pelaku usaha saat ini adalah *Business Email Compromise*. Pusat Pelaporan dan Analisis

[185]Ionut Ilascu, "Surveillance Firm Pays $1 Million Fine After 'Spy Van' Scandal", *Bleeping Computer*, 13 November 2021, https://www.bleepingcomputer.com/news/security/surveillance-firm-pays-1-million-fine-after-spy-van-scandal/ (diakses pada 24 Mei 2022).

Transaksi Keuangan (PPATK) mengungkapkan bahwa kejahatan siber BEC di Indonesia selama periode Juli 2020 hingga Juli 2021 mencapai Rp300 miliar.[186] *Business Email Compromise* (BEC) atau yang juga dikenal dengan istilah *Email Account Compromise* (EAC) memanfaatkan fakta, bahwa begitu banyak dari pelaku usaha yang mengandalkan *email* untuk menjalankan bisnis — baik pribadi maupun profesional. Serangan ini melibatkan *email* palsu yang biasanya mengklaim sebagai permintaan mendesak untuk pembayaran atau pembelian dari seseorang di dalam atau terkait dengan perusahaan target, seperti contoh berikut.[187]

a. vendor yang selama ini telah bekerja sama mengirimkan faktur dengan alamat surat yang diperbaharui;
b. seorang CEO perusahaan, meminta asistennya untuk membeli lusinan *gift cards* untuk diberikan kepada karyawannya sebagai hadiah. Kemudian, pelaku meminta *serial numbers* sehingga dapat dikirimkan segera kepada karyawannya melalui *email;*
c. seseorang yang baru saja membeli rumah, menerima pesan dari pihak *developer* terkait instruksi mengenai cara mentransfer uang muka.

Langkah yang digunakan oleh pelaku BEC dalam menjalankan kejahatannya di antaranya:[188]

a. Menipu dengan Akun *Email* atau Situs Web Palsu

   Pada umumnya pelaku, melakukan sedikit variasi pada alamat yang sah, seperti rifqi.noval@perusahaancontoh.com dan rifqi.nofal@perusahaancontoh.com.

b. Mengirim *Spear Phishing Email*

   Pesan ini seolah-olah dikirim dari pengirim terpercaya untuk mengelabui korban agar mengungkapkan informasi rahasia. Informasi ini memungkinkan penjahat untuk mengakses akun

---

[186]Andi Nugroho, "Kejahatan Siber BEC di Indonesia Capai Rp. 300 Miliar, PPATK Baru Selamatkan Rp175 Miliar", *Cyberthreat*, 19 Agustus 2021, https://cyberthreat.id/read/12282/Kejahatan-Siber-BEC-di-Indonesia-Capai-Rp-300-miliar-PPATK-Baru-Selamatkan-Rp175-Miliar (diakses pada 24 Mei 2022).

[187]FBI, "Scam and Safety: Business Email Compromise", *FBI*, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise (diakses pada 25 Mei 2022).

[188]*Ibid.*

perusahaan, kalender, dan data yang memberi pelaku detail guna menjalankan skema BEC.

c. Menggunakan *Malware*

Malicious Software dapat menyusup pada jaringan perusahaan dan mendapatkan akses kepada daftar *email* yang sah tentang penagihan dan faktur. Informasi ini digunakan untuk meminta waktu atau mengirim pesan sehingga akuntan atau petugas keuangan tidak mempertanyakan permintaan pembayaran. *Malware* turut memungkinkan pelaku mendapatkan akses tanpa terdeteksi ketika mencuri data korban, termasuk kata sandi dan informasi keuangan.

Kasus Penipuan Jual Beli Ventilator Covid-19, Senilai Rp58 Miliar

Polisi berhasil membongkar penipuan penjualan ventilator dan monitoring Covid-19 dengan kerugian mencapai Rp58,83 miliar. Kasus tersebut terungkap setelah NCB Interpol Italia memberikan informasi NBV Interpol Indonesia. Kasus tersebut berawal dari kontrak jual beli antara perusahaan Althea Italia dan perusahaan di Shenzhen terkait pengadaan ventilator dan monitor Covid-19, yang sebelumnya telah beberapa kali melakukan transaksi jual beli. Para pelaku beraksi dengan modus meretas *email* atau yang dikenal dengan istilah *business email compromise*. Dengan cara mem-*bypass* komunikasi *email* antara perusahaan Italia, dalam hal ini Althea Italy S.p.A dengan perusahaan Tiongkok, Shenzen Mindray Bio Medical Electronics.

Modus yang digunakan oleh salah satu pelaku adalah dengan mengaku sebagai general manager perusahaan Shenzen. Melalui *email* tersebut, diinformasikan adanya perubahan rekening penerima pembayaran alat kesehatan tersebut menjadi rekening pada bank di Indonesia. Setelah tiga kali melakukan transfer, barang yang telah dibayar tidak kunjung diterima perusahaan Althea Italy. Total terdapat tiga transaksi senilai Rp58,831 miliar. Pelaku lainnya berperan menjadi Direktur Shenzen Mindray Bio Medical Electronics co LTD dan membuka rekening penampungan. Polisi telah menyita uang dari rekening penampungan sebesar Rp56,1 miliar serta mobil dan tanah yang dibeli pelaku dengan uang hasil kejahatan.

Tersangka dijerat Pasal 378, 263 KUHP, Pasal 85 Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana, Pasal 45A ayat 1 *jo.* Pasal 28 ayat 1 UU ITE *jo.* Pasal 55, 56 KUHP, Pasal 3, 4, 5, 6, 10 Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindakan Pidana Pencucian Uang.

Untuk informasi lebih lanjut terkait **Kasus Penipuan Jual Beli Ventilator,** Anda dapat *scan QR code* di samping.

Kasus BEC Senilai Rp84,8 Miliar

Pada Oktober 2021, Direktorat Tindak Pidana Siber Bareskrim Polri menangkap empat tersangka kasus penipuan dengan skema *Bussines Email Compromise* (BEC), yang merugikan perusahaan asal Korea Selatan dan Taiwan, yaitu Simwoon dan White Wood House Food dengan total kerugian senilai Rp84,8 miliar.

Para pelaku melakukan modus BEC yang ditujukan kepada manajer keuangan atau bagian keuangan dari perusahaan tersebut. Para pelaku meretas *email* dua perusahaan tersebut, dan mengganti data atau identitas, sehingga terjadi proses transfer dana. Uang itu semestinya masuk ke rekening perusahaan, namun ditransfer ke rekening pelaku. Barang bukti yang diamankan di antaranya 90 buku tabungan dari berbagai bank, kartu ATM, 9 buku cek, surat izin usaha, cap perusahaan, akta notaris pendirian perusahaan. Tersangka dijerat Pasal 378 KUHP, Pasal 82, Pasal 85 Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana, Pasal 45A ayat 1 *jo.* Pasal 28 ayat 1 UU No. 19 Tahun 2016, Pasal 3, 4, 5 Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindakan Pidana Pencucian Uang.

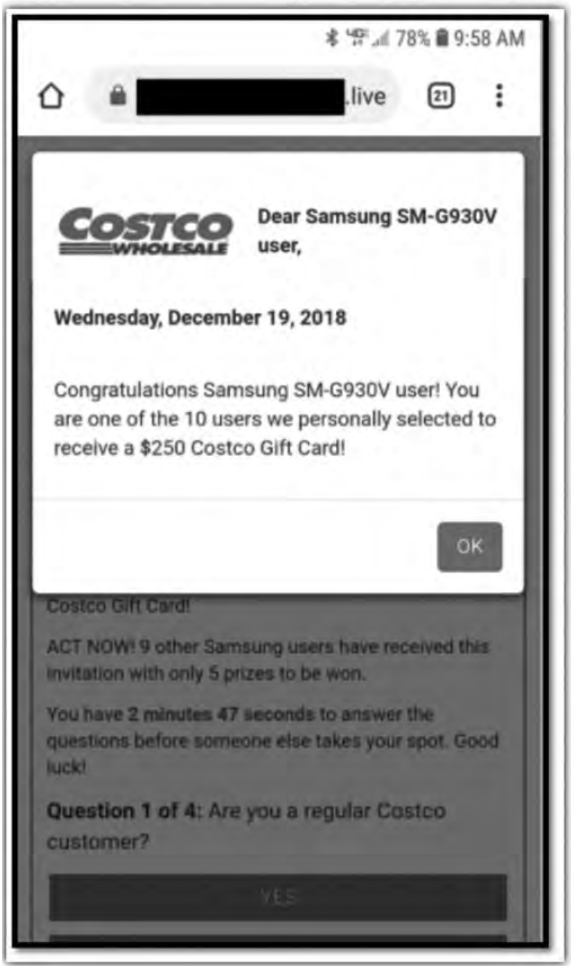
Untuk informasi lebih lanjut terkait **Kasus BEC,** Anda dapat *scan QR code* di samping.

Untuk dapat melihat secara lengkap Undang-Undang Republik Indonesia Nomor 3 Tahun 2011 tentang Transfer Dana, Anda dapat *scan QR code* di samping.

Gambar 20. Contoh *Business Email Compromise*

11. Malvertising (Malicious Advertising)

Jenis *phishing* ini memanfaatkan eksploitasi dalam perangkat lunak periklanan atau animasi untuk mencuri informasi dari pengguna yang ditargetkan. *Malvertising* biasanya disematkan dalam iklan yang tampak normal dan ditempatkan di situs web yang sah seperti Yahoo.com—tetapi dengan kode berbahaya yang ditanamkan di dalamnya.



Gambar 21. Contoh *Malvertising*

Sumber: https://www.prophet.ca/blog/malvertising-another-reason-not-click-web-ads

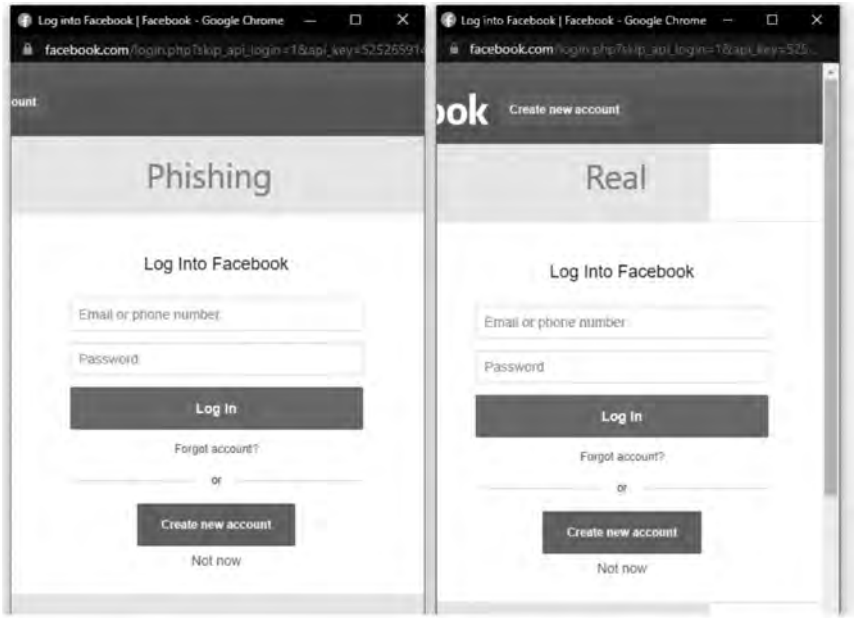
Kasus Peretasan Akun Iklan

Pada 29 Juni 2021, Facebook mengumumkan telah mengajukan dua gugatan hukum terkait pembajakan akun lalu menggunakannya untuk beriklan. Gugatan pertama terhadap sebuah perusahaan dan agennya. Gugatan lainnya terhadap empat warga Vietnam yang telah menggunakan teknis pencurian *cookie* untuk menyusuk ke akun karyawan agensi periklanan dan pemasaran, lalu membajaknya untuk menjalankan iklan tidak sah. Pelaku menggunakan aplikasi *"Ad Manager to Facebook"* untuk mengambil alih akun yang selanjutnya ditujukan agar korban menginstalnya. Aplikasi tersebut meminta pengguna untuk memberikan detail *login* Facebook, yang kemudian digunakan untuk mengakses akun Facebook korban dan menjalankan iklan, termasuk beberapa penawaran penipuan *online.* Iklan penipuan ditempatkan di Facebook untuk mempromosikan barang dagangan, namun setelah mengeklik iklan ini, pengguna diarahkan pada situs lainnya untuk melakukan transaksi. Korban yang telah membeli tidak pernah mendapatkan barang tersebut.

Untuk informasi lebih lanjut terkait **Kasus Peretasan Akun Iklan,** Anda dapat *scan QR code* di samping.

12. Browser-in-the-Browser Attack (BitB Attack)

Teknik *phishing* baru yang dikenal sebagai serangan *browser-in-the-browser* (BitB) dapat digunakan untuk meniru situs yang valid dengan mensimulasikan jendela *browser* di dalam *browser*, membuatnya lebih mudah untuk melakukan serangan *phishing* yang meyakinkan. Teknik ini memanfaatkan opsi *Single Sign On* (SSO) pihak ketiga seperti "Masuk dengan Google" (atau Facebook, Apple, atau Microsoft) yang terintegrasi pada situs web. Pelaku kemudian memanfaatkan celah ketika pengguna mencoba masuk, hingga kemudian disambut oleh jendela *pop-up* dalam menyelesaikan prosedur autentifikasi. Serangan *browser-in-the-browser* bermaksud untuk membuat ulang seluruh proses tersebut menggunakan kombinasi kode HTML dan CSS untuk menghasilkan *browser* yang dibuat sepenuhnya.

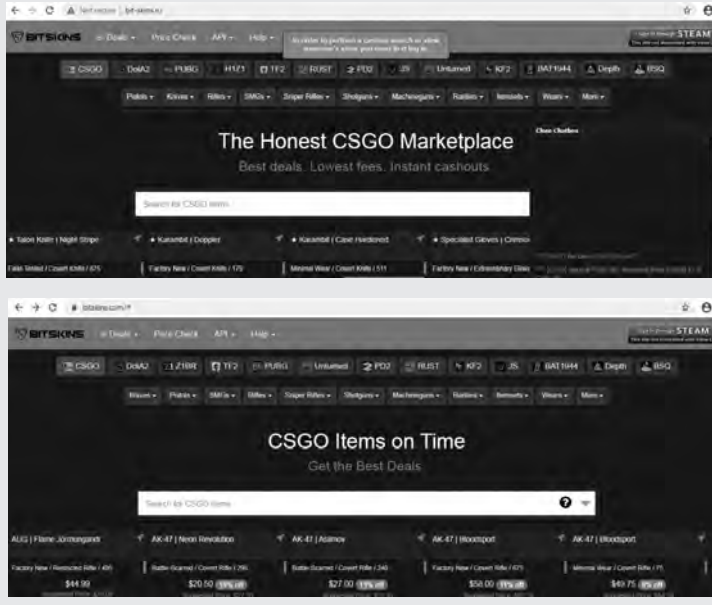


Gambar 22. Contoh *BitB Attack*

Sumber: https://www.gispp.org/2022/03/26/browser-in-the-browser-attack-bitb-new-type-of-phishing-campaigns/

Kasus Serangan BitB

Pada tahun 2020, tim Zscaler ThreatLabZ menemukan beberapa tampilan palsu *Counter-Strike: Global Offensive* (CS:GO) yang bertujuan untuk mencuri kredensial Steam. Steam adalah layanan distribusi digital *video game* yang menyediakan pembaruan otomatis untuk berbagai *game*. Steam juga telah berkembang menjadi etalase digital seluler dan berbasis web daring. Steam menawarkan *Digital Right Management* (DRM), *matchmaking servers*, *streaming* video, layanan jejaring sosial, dan menyediakan instalasi serta pembaruan otomatis *game*. Diketahui bila situs *phishing* tersebut terlihat sangat serupa dengan yang asli. Untuk membuat situs *phishing* tampak lebih sah, bahkan terdapat kotak obrolan palsu dengan frasa yang dipilih secara acak berdasarkan peristiwa terkini. Layar berikut menunjukkan situs CS:GO *phishing* (atas) dan situs CS:GO yang sebenarnya (bawah).



Gambar 23. Kasus *BitB Attack Counter-Strike*

Sumber: https://www.zscaler.com/blogs/security-research/fake-sites-stealing-steam-credentials

Untuk informasi lebih lanjut terkait **Kasus Serangan BitB Iklan,** Anda dapat *scan QR code* di samping.

Selanjutnya, perlu diketahui empat tipe penyerang dalam serangan *phishing,* yaitu sebagai berikut.[189]

a. *Script Kiddies*

Istilah *script kiddies* mewakili penyerang tanpa latar belakang teknis atau pengetahuan tentang menulis program canggih atau mengembangkan alat *phishing*, tetapi sebaliknya mereka menggunakan skrip yang dikembangkan oleh orang lain dalam serangan *phishing*-nya. Meskipun istilah ini berasal dari anak-anak yang menggunakan *kit phishing* yang tersedia untuk memecahkan kode permainan dengan menyebarkan *malware* menggunakan *toolkit* virus, istilah tersebut tidak berhubungan secara tepat dengan usia sebenarnya dari *phisher*. *Script kiddies* bisa mendapatkan akses ke hak istimewa administrasi situs web dan melakukan serangan *web cracking*. Selain itu, mereka dapat menggunakan alat peretasan untuk mengkompromikan komputer jarak jauh yang disebut botnet, komputer tunggal yang disusupi yang disebut komputer zombie. Penyerang ini tidak terbatas hanya duduk dan menikmati *phishing*, mereka dapat menyebabkan kerusakan serius seperti mencuri informasi atau mengunggah *Trojan* atau virus. Pada bulan Februari 2000, serangan yang diluncurkan oleh remaja Kanada Mike Calce mengakibatkan kerusakan sebesar 1,7 juta USD (dolar AS) dari serangan *Distributed Denial of Service* (DDoS) di CNN, eBay, Dell, Yahoo, dan Amazon.

b. *Serious Crackers*

Serious crackers turut dikenal dengan istilah *Black Hats*. Penyerang ini dapat melakukan serangan canggih dan mengembangkan *worm* maupun *Trojan* dalam serangannya. Penyerang akan membajak akun orang lain dengan tujuan jahat dan mencuri informasi kartu kredit, menghancurkan file penting, atau menjual kredensial yang disusupi untuk keuntungan pribadi.

c. *Organized Crime*

Organized crime adalah jenis penyerang yang paling terorganisir, efektif dan mereka dapat menimbulkan kerusakan yang signifikan pada korban. Penyerang ini menyewa *cracker* serius untuk

[189]Zainab Alkhalil, *Op. Cit.,* hlm. 11.

melakukan serangan *phishing*. Selain itu, mereka dapat benar-benar menghancurkan identitas korban dan melakukan penipuan yang menghancurkan karena memiliki keterampilan, alat, dan tenaga. *Organized crime* adalah tim peretas ahli yang berbagi keahlian untuk membangun serangan kompleks dan meluncurkan kampanye *phishing* terhadap individu dan organisasi. Kelompok-kelompok ini menawarkan pekerjaan mereka sebagai 'kejahatan sebagai layanan' dan mereka dapat disewa oleh kelompok, organisasi, atau individu teroris.

d. Terrorists

Oleh karena ketergantungan masyarakat pada internet dalam sebagian besar kegiatan, kelompok teroris dapat dengan mudah melakukan aksi teror dari jarak jauh yang dapat berdampak buruk. Jenis serangan ini berbahaya karena mereka tidak takut akan akibat apa pun, misalnya masuk penjara. Teroris dapat menggunakan internet secara maksimal untuk menciptakan ketakutan dan kekerasan karena membutuhkan dana, sumber daya, dan upaya yang terbatas dibandingkan dengan misalnya, membeli bom dan senjata dalam serangan tradisional. Sering kali, teroris menggunakan *spear phishing* untuk meluncurkan serangan mereka untuk tujuan yang berbeda seperti menimbulkan kerusakan, spionase dunia maya, mengumpulkan informasi, mencari individu, dan tujuan vandalisme lainnya. Spionase dunia maya telah digunakan secara luas oleh teroris dunia maya untuk mencuri informasi sensitif tentang keamanan nasional, informasi komersial, dan rahasia dagang yang dapat digunakan untuk kegiatan teroris. Jenis kejahatan ini dapat menargetkan pemerintah atau organisasi, atau individu.

B. Modus Nigerian SCAM (419 SCAM)

Modus ***Nigerian scam***, atau yang juga dikenal dengan "419 *scam*" merujuk kepada Pasal 419 dalam KUHP Nigeria (*Chapter 38: Obtaining Property by False Pretenses*), yang telah menjadi masalah selama beberapa dekade — juga dikenal sebagai *Advance Fee Fraud* (AFF). Awalnya, fenomena penipuan tersebut dimulai melalui surat pos, kemudian berkembang menjadi bisnis yang dijalankan melalui faks, dan saat ini

melalui *email*.[190] Kamus Etimologi *online* mengaitkan 419 *scam* dengan 'penipu' bahasa Inggris slang abad ke-19 *'scamp'*, yang berarti *'cheater'* atau *'swindler'*. Bahkan sejak tahun 1963, ketika beberapa sarjana mengatakan istilah *'scam'* dalam sastra tertulis untuk pertama kalinya, makna utamanya tetap tidak berubah — yaitu tipuan, *a ruse*, *a swindle*, *a racket*. Meskipun 419 *scam* dikenal sebagai fenomena global, namun praktik tersebut muncul dari Nigeria dan merupakan gagasan dari sekelompok warga Negara Nigeria. Banyak ahli dalam studi Afrika mengklaim tanpa mendukung rincian bahwa 419 *scam* dimulai pada 1980-an oleh perusahaan minyak Nigeria sebagai pelaku utama. Beberapa berpendapat sebaliknya, mempertahankan bahwa 419 *scam* berevolusi dari berbagai jenis trik yang dimainkan sejak lama, sebagian besar di tanah Igbo di Nigeria Tenggara.[191]

Secara historis, dekatnya Nigeria dengan istilah *Nigerian scam* dilatarbelakangi oleh kondisi Nigeria yang memperoleh kemerdekaannya pada tahun 1960. Pada tahun 1993, Jenderal Sani Abacha, sebagai kepala militer negara, mencuri miliaran dolar dari kekayaan negaranya. Setelah kematian Abacha, keluarganya mengembalikan $750 juta dari uang yang digelapkannya selama rezimnya. Pada tahun 1993, *Transparency International Corruption Perception Index* (CPI) mencatat Nigeria dengan skor 1,9 pada skala 1 hingga 10, di mana 1 adalah tingkat persepsi korupsi tertinggi. Pada tahun 1999, Nigeria mengadakan pemilihan demokratis pertamanya dalam 15 tahun dan memilih Olusegun Obasanjo, untuk menjabat sebagai presiden sipil Nigeria selama delapan tahun dari 1999 hingga 2007. Di bawah rezim Obasanjo, Nigeria mulai memberikan perhatian kepada teknologi, seperti telepon guna membantu komunikasi serta kegiatan bisnis. Teknologi ini memiliki dampak positif pada kehidupan Nigeria, namun warga Nigeria mengeksploitasinya, menggunakannya secara negatif untuk menipu orang, baik di dalam maupun di luar negeri.[192]

---

[190]Jelena Isacenkova, *et.al.,* "Inside the SCAM Jugle: A Closer Look at 419 Scam Email Operations", *EURASIP Journal on Information Security*, Vol. 1, 2014, pp. 143-150, DOI: 10.1109/SPW.2013.15, hlm. 143.

[191]Mohamed Chawki, "Nigerian Tackles Advance Fee Fraud", *Journal of Information, Law & Technology*, Vol. 1, 2009, pp. 1-20, hlm. 2-3.

[192]Richard G. Brody, *et.al.,* "An Insider's Look at the Rise of Nigerian 419 Scam", *Journal of Financial Crime*, Vol. ahead-of-print No. ahead-of-print, 2020, pp. 1-13, DOI: 10.1108/JFC-12-2019-0162, hlm. 2.

Literatur lainnya menjelaskan bahwa *Nigerian scam* adalah variasi dari penipuan yang secara historis dikenal sebagai *'Spanish Prisoner'*, yang berasal dari abad ke-16 merupakan awal dari ruang publik anonim di Eropa. Terdapat dua atribut kunci dari penipuan tersebut. *Pertama*, terjeratnya korban dengan nasib sosok tak dikenal. Dalam versi aslinya, yang dimaksud adalah tawanan Phillip II yang misterius dan "konon" kaya, yang akan memberikan imbalan atas janji remunerasi setelah mereka dibebaskan. Versi lainnya adalah kisah insinyur William Adams, seorang pedagang minyak/kontraktor dengan pemerintah federal Nigeria yang meninggal dalam kecelakaan udara yang mengerikan dan meninggalkan $22,2 juta dalam rekening di Union Bank PLC, Lagos. *Kedua,* perlunya menjaga kerahasiaan skema yang diusulkan. Umumnya terdapat penjelasan bahwa langkah transfer uang dari korban guna menghindari perampasan aset oleh negara atau orang lain yang bermaksud jahat.[193]

Nigerian scam kerap dianggap sebagai salah satu jenis spam. Namun, ketika sebagian besar spam saat ini dikirim oleh *botnet* dan oleh mesin yang dirilis dalam jumlah besar, aktivitas *Nigerian scam* sebagian besar masih dilakukan secara manual. Selain itu, model bisnis dan operasi yang mendasarinya berbeda. *Spammer* menjebak korbannya melalui upaya rekayasa, sedangkan *scammer* mengandalkan faktor manusia: rasa kasihan, keserakahan, dan teknik *social engineering*. *Scammers* menggunakan alat yang sangat primitif dibandingkan dengan bentuk lain dari *spam* di mana operasi sering kali sepenuhnya otomatis. Meskipun saat ini pesan *Nigerian scam* tidak sebanyak spam yang dikirim oleh *botnet*, namun tetap menjadi masalah yang menyebabkan kerugian finansial yang besar bagi sejumlah korban di seluruh dunia.[194]

Dalam modus *Nigerian scam* klasik, korban akan menerima *email* dari *scammer* yang meminta bantuan untuk mentransfer sejumlah uang ke luar negeri. Korban kemudian ditawari bagian dari uang tersebut jika setuju untuk memberi pelaku rincian rekening bank untuk membantu transfer. Pelaku kemudian akan meminta untuk membayar semua jenis pajak dan biaya sebelum korban dapat menerima "hadiah". Korban tidak

[193]Andrew Smith, "Nigerian Scam E-Mais and The Charms of Capital", *Cultural Studies*, Vol. 23, No. 1, 2008, pp. 27-47, DOI: 10.1080/09502380802016162, hlm. 28.

[194]Jelena Isacenkova, *et.al., Loc. Cit.*

akan pernah menerima kiriman uang apa pun, dan akan kehilangan biaya yang telah dikeluarkan. Modus lainnya berupa *email* penipuan yang mengaku dari pengacara atau perwakilan bank yang memberi tahu bahwa kerabat target yang telah lama hilang meninggal dunia dan meninggalkan target berupa warisan yang sangat besar. Pelaku dapat menceritakan kisah yang terdengar asli sehingga target dapat tertipu untuk memberikan dokumen pribadi serta detail rekening bank sehingga target dapat mengonfirmasi identitasnya dan mengklaim warisan. "Warisan" kemungkinan besar tidak ada, dan selain kehilangan uang yang mungkin telah korban bayarkan kepada *scammer* dalam bentuk biaya dan pajak, korban juga berisiko mengalami pencurian identitas.[195]

Penelitian yang dilakukan oleh Richard G. Brody memaparkan lebih jauh terkait *Nigerian scam* yakni sebagai berikut.[196]

Pelaku	
Usia	Pelaku *Nigeria scam* di Nigeria berusia muda di antara 15 dan 55 tahun. Mereka umumnya memasuki bisnis ilegal ini pada usia yang sangat muda. Beberapa pelaku tindakan ilegal ini sedang dilatih oleh *master* mereka selama studi sarjana mereka. Mereka menerapkan penipuan ini sebagai pekerjaan penuh waktu, segera setelah mereka menyelesaikan program gelar mereka karena tingginya tingkat pengangguran di pasar tenaga kerja.
Jenis Kelamin	95% dari pelaku *Nigerian scam* di Nigeria adalah laki-laki. Mereka kerap membuat halaman media sosial palsu, dengan gambar wanita cantik untuk melakukan tipu muslihat pada para korban. Setelah korban terperangkap, akun palsu akan ditutup oleh *scammers* yang kemudian akan membuka akun palsu lain untuk menangkap "*fish*" lainnya.
Pekerjaan	Sebelumnya, sebagian besar *scammers* menganggur dan mereka melakukan *Nigerian scam* untuk mencari nafkah. Saat ini, individu terpelajar seperti insinyur, pengacara, dan dokter terlibat dalam penipuan ini. Mereka menggunakan pekerjaan tetap mereka untuk membingungkan *Economic and Financial Crimes Commission* (EFCC), *Special Anti-Robbery Squads* (SARS), *Independent Corrupt Practices and Other Related Offences Commission* (ICPC) dan badan hukum lainnya yang bertanggung jawab untuk menangkap dan menyelidiki pelanggaran apa pun di masyarakat. Mereka percaya bahwa karena mereka adalah pekerja profesional, mereka akan dibebaskan atas dasar bahwa mereka adalah pekerja profesional.

[195]Competition Bureau Canada, *The Little Black Book of Scams: Your Guide to Protection Against Fraud* (Ottawa Competition Bureau Canada, 2012), hlm. 6.

[196]Richard G. Brody, *et.al., Op. Cit.*, hlm. 7-8.

Pelaku	
Cara berpakaian	Secara historis, pelaku *Nigerian scam* berpakaian berbeda dari warga negara lainnya. Mereka berpakaian dengan cara yang tidak pantas dan memiliki gaya rambut yang tidak rapi. SARS mulai menangkap orang-orang tak bersalah yang berpakaian tidak normal karena mengira mereka adalah pelaku tindakan ilegal ini. Untuk menghindari perhatian dari SARS, baru-baru ini pelaku *Nigerian scam* telah meningkatkan cara berpakaian mereka untuk menipu badan hukum. Mereka sekarang mencoba mengenakan pakaian resmi dan menampilkan diri mereka sebagai profesional.
Kesabaran	Pelaku memiliki tingkat kesabaran yang tinggi. *Scammers* menunggu waktu yang lama untuk kesepakatan mereka matang. Mereka mengirim permintaan pertemanan ke banyak orang asing melalui media sosial dan terkadang menargetkan individu terkemuka di luar negeri. Mereka meluangkan waktu agar orang-orang ini menerima permintaan mereka. Terkadang pelaku membutuhkan waktu lebih dari satu tahun untuk menipu korbannya.
Cara hidup	Para pelaku sering menjalani kehidupan yang boros. Sama seperti penipu di negara lain, mereka tidak memiliki tabungan, melainkan membeli mobil, perhiasan, serta pakaian mewah dan mahal. Mereka berpindah dari satu korban ke korban lain menghabiskan uang dengan boros mengharapkan lebih banyak uang akan masuk ke rekening mereka.
Korban	
Mudah tertipu	Terlepas dari publisitas tingkat tinggi *Nigerian scam* di seluruh dunia, beberapa orang masih menjadi korban penipuan ini. Para korban ini mudah dibujuk dan ditipu. Mereka dihubungi melalui berbagai cara, dan melalui cara ini para penipu memperoleh informasi yang relevan dari mereka. Peningkatan penggunaan media sosial telah meningkatkan ketersediaan informasi terkait tentang korban. *Scammers* menggunakan informasi ini untuk meyakinkan korban bahwa mereka mencoba berteman dengan mereka.
Status perkawinan	Sebagian besar korbannya telah menikah, meskipun terdapat beberapa korban yang telah berusia, tetapi masih lajang. Hal ini disebabkan pelaku lebih memilih menyasar kelompok usia tertentu.
Simpati	Beberapa kategori orang menjadi korban karena simpati. Penipu sering menipu kliennya (korban) untuk mengambil barang berharga darinya dengan berbohong bahwa salah satu anggota keluarga dekatnya mengalami kecelakaan fatal dan mereka membutuhkan uang untuk melakukan operasi bedah. Setelah mendengar ini, pikiran untuk membantu orang tersebut akan menyerang pikiran "klien" dan ini akan mengakibatkan korban mengirimkan sejumlah besar uang untuk melakukan operasi palsu.
Jenis kelamin	Para korban terdiri dari kedua jenis kelamin, 50% adalah perempuan dan 50% adalah laki-laki. Penipu ini percaya bahwa wanita umumnya mudah ditipu karena perhatian dan hati mereka yang fleksibel dan pria adalah sasaran empuk karena keinginan mereka untuk menarik perhatian wanita cantik.

Nice to Know You

Naomi Surugaba [azlin@moa.gov.my] Actions

Inbox Monday, March 10, 2014 1:18 PM

Dear Beloved Friend,
I know this message will come to you as surprised but permit me of my desire to go into business relationship with you.
I am Miss Naomi Surugaba a daughter to late Al-badari Surugaba of Libya whom was murdered during the recent civil war in Libya in March 2011, before his death my late father was a strong supporter and a member of late Moammar Gadhafi Government in Tripoli. Meanwhile before the incident, my late Father came to Cotonou Benin republic with the sum of USD4, 200,000.00 (US$4.2M) which he deposited in a Bank here in Cotonou Benin Republic West Africa for safe keeping.
I am here seeking for an avenue to transfer the fund to you in only you`re reliable and trustworthy person to Investment the fund. I am here in Benin Republic because of the death of my parent`s and I want you to help me transfer the fund into your bank account for investment purpose.
Please I will offer you 20% of the total sum of USD4.2M for your assistance. Please I wish to transfer the fund urgently without delay into your account and also wish to relocate to your country due to the poor condition in Benin, as to enable me continue my education as I was a medical student before the sudden death of my parent`s. Reply to my alternative email:missnaomisurugaba2@hotmail.com, Your immediate response would be appreciated.
Remain blessed,
Miss Naomi Surugaba.

Gambar 24. Contoh *Email Nigerian Scam*[197]

[197]Erika Eichleberger, "What I Learned Hanging Out with Nigerian Eial Scammers", *Mother Jones*, 20 Maret 2014, https://www.motherjones.com/politics/2014/03/what-i-learned-from-nigerian-scammers/ (diakses pada 24 Mei 2022).

Kasus OPAP *Investment Limited*

Pada bulan Agustus 2019, Kepolisian RI melakukan penangkapan terhadap 5 warga Negara Indonesia, pelaku *Nigerian scam* yang dilakukan terhadap bendahara perusahaan OPAP *Investment Limited* yang berkewarganegaraan Yunani.
Pelaku berhasil mendapatkan uang dari saldo rekening korban sebesar 6,9 juta euro atau sekitar Rp113 miliar. Kejadian ini pertama kali diketahui pada tanggal 31 Mei 2019, ketika perusahaan melakukan audit keuangan dan menemukan transaksi pembayaran dengan nominal 4,9 juta euro pada 16 Mei 2019 dan 2 juta euro pada 23 Mei 2019.
Polisi menjerat para tersangka dengan Pasal 82; dan/atau Pasal 85 Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana; dan/atau Pasal 46 ayat (1), ayat (2), dan ayat (3) *juncto* Pasal 30 ayat (1), ayat (2), dan ayat (3); dan/atau Pasal 51 ayat (1) dan ayat (2) *juncto* Pasal 35; dan/atau Pasal 36 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; dan/atau Pasal 3, Pasal 5, dan Pasal 10 Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang; dan/atau Pasal 378 KUHP; dan/atau Pasal 263 KUHP.

Untuk informasi lebih lanjut terkait **Kasus OPAP *Investment Limited,*** Anda dapat *scan QR code* di samping.[198]

Untuk dapat melihat secara lengkap Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Anda dapat *scan QR code* di samping.

Ted Claypoole dan Theresa Payton menguraikan tujuh langkah bagi korban untuk mengembalikan akunnya dari serangan *phishing*

[198]Audrey Santoso, "Gasak Rp113 M, Sindikat Nigerian Scam Dibekuk Polisi", *Detik News*, 07 Agustus 2019, https://news.detik.com/berita/d-4655840/gasak-rp-113-m-sindikat-nigerian-scam-dibekuk-polisi (diakses pada 25 Mei 2022).

atau mencegah peretas memilikinya sejak awal, yaitu sebagai berikut.[199]

1. **Hubungi *service providers***. Apabila akun korban telah terkunci, korban dapat mencoba mendapatkan kembali akses dari *service provider*.
2. **Ubah kata sandi**. Apabila penyerang mengambil akun korban, tetapi korban masih dapat masuk, segera ubah kata sandi akun tersebut.
3. **Periksa pengaturan**. Setelah korban telah mendapatkan kembali akses akun, periksa semua pengaturan. Peretas mungkin telah mengubah pengaturan seperti "teruskan semua email ke akun xxx@xxxxxxx.com".
4. **Periksa *login* otomatis dari *email* ke aplikasi atau akun lain**. Apabila korban *login* otomatis untuk aplikasi atau akun lain, sebaiknya korban mengubah kata sandi untuk aplikasi tersebut dan memeriksa pengaturannya juga.
5. **Beri tahu teman dan keluarga**. Beri tahu semua orang bahwa akun telah diretas dan jangan membalas *email* dari akun tersebut, mengeklik tautan, atau membuka lampiran.
6. **Gunakan *two-factor authentication***. Sebelum yang terburuk terjadi, coba aktifkan *two-factor authentication*. *Two-factor authentication* umumnya berkaitan dengan ponsel dan sebagian perusahaan internet akan mengirim kode pendek ke ponsel ketika mereka melihat *login* yang tidak sesuai dengan pola yang biasa (misalnya, lokasi yang berbeda atau perangkat yang berbeda).
7. **Jalankan perangkat lunak *antimalware* dan *antivirus***. Pastikan tidak memiliki *malware* yang mencatat penekanan tombol pengguna.

C. Spear Phishing

Spear phishing adalah bentuk *phishing* yang ditargetkan, lazimnya berupa serangan *email* dengan menggunakan metode *social engineering* khusus untuk mencoba memengaruhi pengguna agar mengekspos

[199]Ted Claypoole dan Theresa Payton, *Protecting your Internet Identity: Are You Naked Online* (London: Rowman & Littlefield, 2017), hlm. 55-56.

akun sensitif, informasi pribadi atau bisnis serta upaya intrusi ke dalam infrastruktur komputer. *Spear phishing* sulit dideteksi karena menggunakan pendekatan yang ditargetkan untuk menarik pengguna agar menurunkan kewaspadaan dan bertindak berdasarkan persepsi urgensi atau melalui komunikasi dari kontak penting, bahkan atasan dalam organisasi seseorang. *Spear phishing* umumnya melibatkan penelitian pada target dengan membuat pesan yang dipersonalisasi untuk menipu penerima agar mengambil tindakan yang akan merugikan dalam beberapa cara. Intinya, *spear phishing* adalah serangan pribadi yang mencoba membuat target percaya bahwa mereka berinteraksi dengan seseorang yang mereka kenal atau dengan otoritas resmi dalam upaya untuk meminta pengguna menyerahkan informasi sensitif.[200]

Salah satu kelemahan serangan *phishing* adalah bahwa 'umpan' yang sama didistribusikan ke sejumlah besar calon korban. Dengan demikian, *email phishing* tidak terlalu berhasil dalam menjangkau dan meyakinkan para korban — distribusi massal membuat *email phishing* relatif mudah dideteksi dan difilter menggunakan sistem otomatis, serta informasi yang tidak relevan terkandung dalam *email phishing* kerap menyebabkan diabaikannya atau dihapusnya pesan oleh penerima. Misalnya, *email phishing* yang meminta penerima untuk melakukan beberapa tindakan untuk mengamankan rekening bank ABC-nya akan gagal membujuk pemegang rekening XYZ. *Spear phishing* adalah upaya untuk menghilangkan kelemahan tersebut. Tidak seperti '*blanket phishing*' (atau hanya *'phishing'*), yang mengambil pendekatan oportunistik — *phisher* melemparkan 'jaring lebar' dengan harapan untuk mengaitkan beberapa *'phish'* yang tidak bersalah atau tidak beruntung — *spear phishing* mengambil pendekatan yang disesuaikan: penargetan dan *spearing* dari *'phish'* tertentu. Dengan *spear phishing*, seorang *phisher* bersedia menginvestasikan lebih banyak usaha dan waktu untuk menyusun skema serangannya guna memaksimalkan kemungkinan keberhasilan.[201]

S*pear phishing* mewarisi banyak fitur *phishing*, tetapi jauh lebih kuat dan efisien karena penggabungan informasi kontekstual dan waktu ke dalam skema *phishing*. Oleh karena itu, *spear phishing* juga disebut

[200]Jason E. Thomas, *Op. Cit.,* hlm. 3.
[201]Van Nguyen, *Op. Cit*., hlm. 5.

sebagai *context-aware phishing* atau *targeted phishing*. Sebagai contoh untuk ilustrasi, bila seseorang, setelah menyelesaikan pendaftarannya untuk akun *online* ABC, menerima *email phishing* yang tampaknya berasal dari bank ABC dan memintanya untuk mengaktifkan akun *online* ABC-nya menggunakan fitur yang disediakan (*malicious*), serangan ini memiliki peluang keberhasilan yang jauh lebih tinggi dibandingkan serangan yang ditujukan kepada orang yang tidak memiliki akun ABC, atau yang mendaftar untuk akun ABC beberapa waktu sebelumnya, terlepas dari seberapa paham teknologi korban tersebut. Angka statistik sebuah studi menunjukkan bahwa tingkat respons untuk skema *blanket phishing* adalah sekitar 3%-5%, sedangkan tingkat respons untuk skema *spear phishing* setinggi 80%. Ini menunjukkan bahwa skema *spear phishing*, bila diciptakan dengan hati-hati, memiliki tingkat keberhasilan yang sangat tinggi.[202]

Dua dampak yang paling ditakutkan dari *spear phishing* adalah pencurian identitas serta infeksi serangan *ransomware*. Pada tahun 2013, lebih dari 13 juta orang menjadi korban pencurian identitas serta menimbulkan kerugian hingga US$ 18 miliar. Selama periode tersebut, *Federal Trade Commission* (FTC) menerima lebih dari 290.000 pengaduan terkait pencurian identitas. Sementara itu, *ransomware* dinilai sangat merusak karena dapat mengenkripsi data sensitif dan membuat sistem tidak dapat digunakan. *Ransomware* WannaCry pada tahun 2017 telah menginfeksi lebih dari 100.000 organisasi di seluruh dunia.[203]

Bullee menilai bahwa *email spear phishing* berhasil karena personalisasi menciptakan kepercayaan. Teori pilihan rasional memberikan landasan untuk pandangannya. Tindakan dalam teori ini didasarkan pada evaluasi sadar kegunaan bertindak dengan cara tertentu (yaitu biaya vs manfaat). Di bidang kejahatan dan keamanan, ini diterjemahkan ke dalam penimbangan nilai yang akan diperoleh dengan melakukan tindakan versus konsekuensi negatif. Pelaku mengubah fokus mereka dari sasaran yang luas ke sasaran yang sempit. Pelaku kerap mengirim *email* massal, berharap untuk menipu siapa pun; sekarang pelaku lebih selektif dan menggunakan informasi konteks yang relevan dalam *email* untuk mengelabui target tertentu. Berdasarkan teori ini,

[202]*Ibid.*
[203]Jason E. Thomas, *Loc. Cit.*

Bullee berhipotesis bahwa *spear phishing* lebih menarik karena dua alasan berikut.[204]

1. Ini melibatkan penargetan lebih sedikit orang daripada *phishing* umum, kemungkinan konsekuensi negatif lebih rendah karena jumlah upaya yang harus dilakukan pelaku lebih rendah.
2. Oleh karena *email* dipersonalisasi, target lebih cenderung menganggap bahwa *email* itu sah, yang berarti tingkat kepatuhan yang lebih tinggi.

Keberhasilan *spear phishing* dapat tergambarkan dalam dua studi lapangan berikut. Dalam studi lapangan pertama, efek *spear phishing* diuji pada 581 mahasiswa (usia 18-24 tahun). Mereka yang berada di grup kontrol (94 orang) menerima *email phishing* dari orang fiktif yang meminta untuk memasukkan kredensial *login* mereka di situs web yang tidak terpercaya, sedangkan mereka yang berada di grup eksperimen (487 orang) menerima *email* yang sama yang diduga dari salah satu teman mereka. Subjek yang menerima *email* dari "teman" memasukkan kredensial mereka 4,5 kali lebih sering daripada mereka yang menerima *email* dari orang asing (16% vs 72%). Dalam studi lapangan kedua, 158 karyawan yang tersebar di lima organisasi di Swedia didekati dalam dua kondisi. Semua karyawan pertama-tama menerima *email* umum (ditulis dalam bahasa Inggris) dengan permintaan untuk mengunduh perangkat lunak dari situs web yang tidak terpercaya. Kemudian, semua karyawan menerima *email* lain (ditulis dalam bahasa Swedia), menggunakan nama karyawan, nama organisasi, dan nama eksekutif untuk membujuk mereka mengunduh *add-on* ke pemindai virus. Mereka yang menerima *email spear phishing* memiliki kemungkinan 5,3 kali lebih besar untuk mengeklik tautan di *email* (27,2% vs 5,1%) dan 2,8 kali lebih mungkin untuk mengeksekusi biner (8,9% vs 3,2%) daripada mereka yang menerima *email phishing* umum.[205]

Laporan yang dirilis oleh perusahaan keamanan Barracuda menunjukkan sebagai berikut.[206]

---

[204]Jan-Willem Bullee, *Op. Cit.*, hlm. 595.
[205]*Ibid.*, hlm. 596.
[206]Barracuda, *Op. Cit.*, hlm. 1.

1. 12% serangan *spear phishing* adalah serangan *Business Email Compromise* (BEC).

   BEC merupakan 12% dari serangan *spear phishing* yang dianalisis, meningkat dari hanya 7% pada tahun 2019.

2. Hanya 30% serangan BEC yang menyertakan tautan.

   Peretas yang menggunakan BEC ingin membangun kepercayaan dengan korbannya dan mengharapkan balasan ke *email* mereka, dan kurangnya URL membuat lebih sulit untuk mendeteksi serangan.

3. Serangan BEC menyebabkan kerugian lebih dari $3,5 miliar pada tahun 2019.

   Merujuk pada laporan FBI selama dua tahun terakhir, telah terjadi sejumlah serangan BEC yang terkenal, seperti Toyota Boshoku Corporation Jepang kehilangan $37 juta pada 2019 dan Pemerintah Puerto Rico kehilangan $2,6 juta pada awal 2020. Sementara sepanjang tahun 2016 hingga 2019 kerugian mencapai $26 miliar.

4. 71% serangan *spear phishing* termasuk URL berbahaya.

   Peretas menggunakan banyak taktik untuk menyamarkan tautan berbahaya dan menghindari deteksi oleh solusi perlindungan URL.

5. 13% dari semua serangan *spear phishing* berasal dari akun yang disusupi secara internal.

   Organisasi perlu berinvestasi dalam melindungi lalu lintas *email* internal mereka sebanyak yang mereka lakukan dalam melindungi dari pengirim eksternal.

6. 72% serangan terkait Covid-19 adalah penipuan *scam*.

   Sebagai perbandingan, 36% dari keseluruhan serangan adalah penipuan. Penyerang lebih suka menggunakan Covid-19 dalam serangan penipuan yang tidak terlalu ditargetkan yang berfokus pada pengobatan dan donasi palsu.

Sebagian besar *email phishing* akan menyertakan URL, dan serangan *spear phishing* yang lebih bertarget tidak terkecuali. Peretas menggunakan taktik *social engineering* yang dirancang dengan cermat untuk menipu pengguna agar mengeklik URL berbahaya yang disertakan dalam pesan *email*. Sekitar 71% dari seluruh serangan *spear phishing* menyertakan setidaknya satu URL di badan *email*. URL ini biasanya mengarah ke situs *phishing* yang digunakan oleh peretas untuk mencuri kredensial

login atau mendistribusikan *malware*. Meskipun banyak organisasi saat ini memiliki beberapa bentuk perlindungan tautan, banyak dari URL ini tidak diperhatikan oleh filter *gateway* tradisional. Penjahat dunia maya menggunakan situs web yang diretas atau situs yang baru terdaftar untuk membuat replika yang hampir sempurna dari halaman *login* resmi. Pesan-pesan ini melewati pemindai yang mencari konten berbahaya untuk berada di kotak masuk pengguna. Penjahat dunia maya semakin banyak menggunakan layanan peringkas URL populer seperti t.co, bit.ly, tinyurl.com, dan lainnya untuk menyematkan tautan berbahaya dalam *email phishing*. Peringkas URL memadatkan tautan, sehingga tautan situs yang sebenarnya menjadi kabur dengan huruf atau angka acak. Menggunakan taktik ini dapat menyamarkan tujuan sebenarnya dari tautan, sehingga memudahkan peretas untuk mengelabui korbannya.[207]

1. Ransomware

Cyber Threat Alliance, sebuah aliansi sekelompok perusahaan keamanan siber yang dibentuk pada tahun 2014 untuk melacak ancaman siber, memperkenalkan definisi *ransomware* yang diterbitkannya pada tahun 2015 sebagai jenis *malware* yang mengenkripsi file korban dan kemudian menuntut pembayaran sebagai imbalan atas kunci yang dapat mendekripsi file tersebut. Ketika *ransomware* pertama kali diinstal pada mesin korban, biasanya akan menargetkan file sensitif seperti data keuangan penting, catatan bisnis, *database*, file pribadi, dan banyak lagi. File pribadi, seperti foto dan film rumahan, mungkin memiliki nilai sentimental bagi korban.[208]

Ransomware mulai muncul sekitar tahun 2004, tetapi volume serangan *ransomware* tidak signifikan sampai sekitar sepuluh tahun kemudian ketika *ransomware* menjadi berita utama pada tahun 2013. Kejahatan memeras uang dari *malware* komputer dimulai pada tahun 1989 ketika *malware* pertama menginfeksi komputer dengan mengganti file "autoexec.bat" lama dengan file yang berbeda. "autoexec.bat" baru akan menunggu beberapa saat sebelum menemukan komputer dan menampilkan pesan yang menuntut pembayaran. Komputer akan tetap

[207]*Ibid.*, hlm. 9-11.

[208]Azad Ali, "Ransomeware: A Research and A Personal Case Study of Dealing with this Nasty Malware", *Issue in Informing Science and Information Technology*, Vol. 14, 2017, pp. 87-99, hlm. 88-89.

terkunci sampai sebuah kotak pos di Panama menerima pembayaran dan kemudian mereka mengirim *floppy disk* yang berisi solusi untuk masalah penguncian. Dua laporan yang diterbitkan oleh *Cyber Threat Alliance* pada tahun 2015 dan 2016, menunjukkan bahwa *Cryptowall 3* dan *Cryptowall 4* (*ransomware*) mulai muncul pada tahun 2014 dan 2015 secara terpisah.[209]

Serangan *ransomware* menjadi perhatian dunia pada tahun 2017, ketika varian *"WannCry"* menyandera ratusan komputer organisasi di dunia, termasuk di dalamnya 2 rumah sakit di Jakarta — Rumah Sakit Harapan Kita dan Dharmais. Perusahaan migas AS, Colonial Pipeline dan perusahaan perangkat lunak SolarWinds turut menjadi korban serangan ini. Salah satu kelompok peretas yang terkenal dengan serangan *ransomware* adalah GandCrab, yang menyatakan telah pensiun pada tahun 2019. Kelompok ini mendominasi serangan *ransomware* yang telah terjadi sebesar 50% dan mengklaim telah mendapatkan keuntungan lebih dari US$2 miliar.[210]

Kasus yang tengah menjadi sorotan terkait *ransomware* dialami oleh perusahaan perangkat lunak asal Florida, Kaseya. Serangan *ransomware* menyusup melalui perangkat lunak manajemen TI Kaseya VSA. Pola serangan ini dikenal dengan istilah *supply chain attack*. Penyerangan menargetkan pemasok perangkat lunaknya, yang berdampak ke semua perusahaan pengguna perangkat lunak tersebut. Pada serangan yang terjadi pada 2 Juli 2021 tersebut, sedikitnya 1.000 bisnis dan organisasi publik mengalami serangan *ransomware* REvil sehingga membuat pelayanan tidak dapat beroperasi. Jaringan supermarket asal Swedia, Coop, terpaksa menutup 500 toko karena mesin kasir yang tidak berfungsi. Penyerang meminta uang tebusan sebesar US$70 juta dalam bentuk bitcoin. Namun, pada akhir Juli, Kaseya mendapatkan *decryptor* yang telah mengunci file-file milik para pelanggannya.[211] *Ransomware* yang sama ini sebelumnya telah menyandera sistem jaringan komputer terhadap 22 pemerintah kota di Texas. Serangan tersebut terjadi pada

---

[209]*Ibid.*, hlm. 89-90.

[210]Bitdefender, *Mid-Year Threats Landscape Report,* 2019, hlm. 3-4.

[211]Frank Bajak, "Kaseya Gets Master Decryption Key After July 4 Global Attack", *Apnews*, 23 Juli 2021, https://apnews.com/article/lifestyle-technology-joe-biden-europe-business-bb7298b31b7157640fbd5f90fc19c224 (diakses pada 24 Mei 2022).

16 Agustus 2019 ketika peretas meminta tebusan kolektif dari seluruh kota senilai US$2,5 juta dalam bitcoin.[212] Sementara itu, pada tahun 2020, penyedia layanan valuta asing yang berbasis di Inggris, Travelex, terpaksa membayar tebusan sebesar US$2,3 juta akibat serangan yang melumpuhkan jaringannya, bahkan kejadian tersebut membuat 1.300 karyawannya diberhentikan.[213] Serupa dengan Travelex, produsen daging sapi di Brasil, JBS telah membayar tebusan sebesar US$11 juta kepada geng REvil dalam bentuk bitcoin pada 1 Juni 2021, akibat serangan yang dilakukannya pada Mei 2021.[214]

Berbagai laporan mencatat secara berbeda mengenai jumlah uang yang dikumpulkan dari serangan *ransomware*. American Bankers Association pada tahun 2016, memperkirakan bahwa jumlah yang dikumpulkan untuk melepaskan kunci dekripsi dari serangan *ransomware* dapat berkisar dari beberapa ratus hingga ribuan dolar tergantung pada siapa yang terinfeksi *malware*. Laporan lainnya memberikan informasi spesifik tentang jumlah yang dikenakan saat pemerasan dunia maya pertama kali dimulai. Tercatat bahwa tebusan pertama yang dikumpulkan dari para korban adalah pada tahun 1989 ketika mereka harus mengirimkan $189 ke PC Cyborg Corp di sebuah kotak pos di Panama. Harga itu telah berubah karena komunikasi menjadi lebih mudah melalui dunia maya dan mata uang digital yang berbeda telah muncul dalam pertukaran uang. Proses *ransomware* mengambil arah yang berbeda tergantung pada tindakan pengguna dan jalur yang dihasilkan dari penjahat setelah mereka menerima uang tebusan. Berikut ini adalah langkah-langkah yang umumnya dilakukan dalam proses *ransomware*.[215]

---

[212]Bobby Allyn, "22 Texas Towns Hit With Ransomeware Attack In 'New Front' of Cyberassault", *NPR*, 20 Agustus 2019, https://www.npr.org/2019/08/20/752695554/23-texas-towns-hit-with-ransomware-attack-in-new-front-of-cyberassault (diakses pada 24 Mei 2022).

[213]Dan Sabbagh, "Ransomeware is Biggest Online Threat to People in UK, Spy Agency Chief to Warn", *The Guardian*, 14 Juni 2021, https://www.theguardian.com/technology/2021/jun/14/ransomware-is-biggest-online-threat-to-people-in-uk-spy-agency-chief-to-warn (diakses pada 24 Mei 2022).

[214]Lawrence Abrams, "JBS Paid $11 Million to REvil Ransomeware, $22,5 M First Demanded", *Bleeping Computers*, 10 Juni 2021, https://www.bleepingcomputer.com/news/security/jbs-paid-11-million-to-revil-ransomware-225m-first-demanded/ (diaskes pada 24 Mei 2022).

[215]Azad Ali, *Op.Cit.*, hlm. 91-93.

a. Virus menginfeksi komputer.
b. Fungsionalitas hilang – pengguna membaca catatan tebusan.
c. Pengguna memutuskan untuk membayar tebusan (atau tidak).
d. Batas waktu diperpanjang.
e. Pengguna memutuskan untuk membayar setelah melewati batas waktu yang diperpanjang.
f. Fungsionalitas dikembalikan atau hilang untuk selamanya tergantung jika dibayar atau tidak dibayar.

Saat ini, serangan *ransomware* telah mengalami perubahan. Bila pada awalnya, pelaku melakukan serangan dengan menyusup pada jaringan korban dan mengunci file-file penting dari komputer korban. Kemudian selanjutnya meminta uang tebusan kepada korban bila menghendaki file-file yang terkunci dapat dikembalikan seperti semula. Namun, saat ini, bila korban tidak membayar maka penyerang mengancam akan merilis data tersebut ke publik dan menghancurkan citra perusahaan korban. Tidak hanya itu, penyerangan turut menambahkan serangan DDoS ke perusahaan korban, sehingga klien atau pelanggan tidak dapat menggunakan layanan perusahaan. DDoS sendiri merupakan serangan dengan membanjiri situs web yang ditargetkan dengan lalu lintas palsu, umumnya menggunakan *botnet* dari berbagai lokasi, dengan tujuan untuk memperlemah situs web atau membuat lumpuh server karena lonjakan permintaan yang begitu besar,[216] seperti yang dialami oleh situs **projectmultatuli.org** pada awal Oktober 2021 sehingga mengakibatkan situs tersebut tidak dapat diakses oleh penggunanya. Peretasan dengan menggunakan DDoS tersebut diduga terkait karya jurnalistik Project Multatuli, setelah mengunggah reportase dugaan kasus pemerkosaan pada tiga anak kandung oleh ayahnya di Luwu Timur, Sulawesi Selatan.[217]

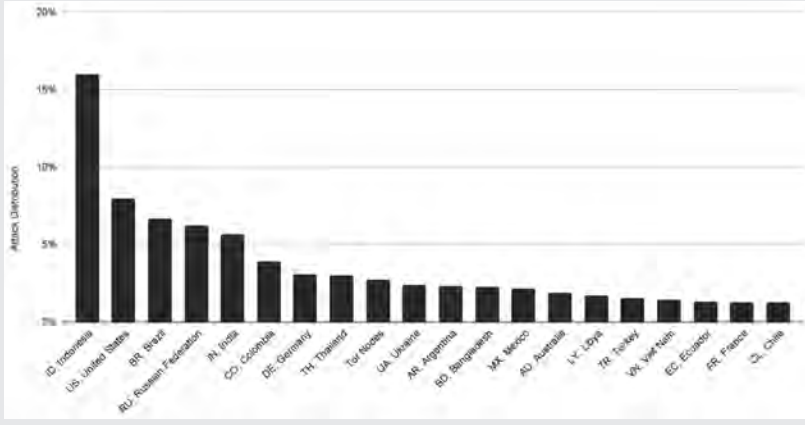
---

[216]Daniel Miessler, "Ransomware Groups Add a Third Threat Vector: DDos", 4 Oktober 2020, https://danielmiessler.com/blog/ransomware-groups-add-a-third-threat-vector-ddos/ (diakses pada 24 Mei 2022).

[217]Tatang Guritono, "Usai Dapat Serangan Siber, Situs Project Multatuli Belum Pulih Sepenuhnya", *Kompas*, 8 Oktober 2021, https://nasional.kompas.com/read/2021/10/08/16093581/usai-dapat-serangan-siber-situs-project-multatuli-belum-pulih-sepenuhnya?page=all (diakses pada 25 Mei 2022).

Serangan DDoS Terbesar di Dunia

Perusahaan teknologi Cloudfare, pada bulan Juni 2022 mengungkap terjadinya serangan *Distributed Denial of Service* (DDos) yang terbesar di Dunia. Serangan tersebut, mencapai 26 juta permintaan/detik. Dalam serangan berdurasi kurang dari 30 detik itu, terdapat permintaan HTTPS yang berasal lebih dari 1.500 jaringan tersebar di 121 negara dan negara teratas adalah Indonesia.[218]



Data sumber negara

Sumber tempat orang mengunduh dan menginstal *malware* begitu beragam. Pengguna dapat saja mengunduh dan menginstal *malware* di komputer mereka dari *drive-by download,* mengeklik tautan *pop-up* iklan, maupun serangan *phishing* melalui lampiran *email*. Umumnya, seseorang tidak menyadari sepenuhnya bila telah menjadi korban, karena seseorang jelas tidak ingin mengunduh virus ke dalam perangkatnya. Namun demikian, banyak pengguna di berbagai tingkat keahlian tanpa sadar mengunduh *malware* ke komputernya dan terdapat beragam faktor yang membuat itu terjadi, di antaranya:[219]

a. minimnya pengetahuan;
b. mengabaikan ancaman ketika mengunjungi situs tertentu;
c. instalasi antivirus yang tidak tepat;
d. *software* tidak diperbaharui;
e. menggunakan perangkat yang telah lama;

[218]Omer Yoachimik, "Cloudflare Mitigates 26 Million Request Per Second DDoS Attack", *Cloudfare*, 14 Juni 2022, https://blog.cloudflare.com/26m-rps-ddos/ (diakses pada 20 Juni 2022).

[219]Azad Ali, *Loc. Cit*.

f. putus asa dalam menyelesaikan masalah yang berkaitan dengan komputer.

Pemerintah Amerika Serikat saat ini telah mengumumkan upaya baru untuk memerangi *ransomware* dengan meluncurkan situs web ***StopRansomeware.gov*** yang dirancang sebagai hub pusat yang menghubungkan sumber daya *ransomware* dari semua lembaga pemerintah, termasuk *Cybersecurity & Infrastructure Security Agency* (CISA), FBI, *Secret Service,* NIST, Departemen Keuangan, dan HHS. Tujuannya adalah untuk menyediakan sumber daya yang berguna bagi individu, bisnis dan organisasi lainnya. Situs ini memberikan informasi tentang apa yang harus dilakukan jika seseorang terkena *ransomware*, menghindari *ransomware* dan melaporkan insiden siber kepada pihak berwenang. Sebagai bagian dari perang melawan *ransomware* dan ancaman dunia maya lainnya, Departemen Luar Negeri AS turut menawarkan US$10 juta untuk informasi yang mengarah pada identifikasi atau lokasi siapa pun yang bertindak atas arahan atau di bawah kendali pemerintah asing, berpartisipasi dalam aktivitas kejahatan siber terhadap infrastruktur penting AS.

DRIVE-BY DOWNLOAD?

Ketika pengguna internet mengunjungi halaman web berbahaya, server web mengirimkan dokumen HTML termasuk konten berbahaya ke sistem komputer pengguna. Konten berbahaya kemudian mengeksploitasi kerentanan pada sistem komputer pengunjung, yang mencakup kerentanan di *browser* web, *plug-in*, dan sistem operasi. Eksploitasi mengarah pada eksekusi kode berbahaya yang diberikan oleh penyerang dan pemasangan *malware* pada sistem komputer pengunjung. Proses ini terjadi tanpa persetujuan atau pemberitahuan pengguna internet. Jenis serangan ini dikenal dengan istilah *drive-by download*. Salah satu tahapan serangan tersebut adalah dengan mengarahkan korban ke server web yang dimiliki oleh penyerang ataupun dengan menumbangkan server web yang sah. Menumbangkan situs yang sah memungkinkan penyerang untuk memperkuat jangkauan serangan mereka karena situs ini dipercaya dan dikunjungi oleh banyak pengunjung. Faktor lain yang menyebabkan meningkatnya dampak serangan *drive-by download* adalah ketersediaan paket eksploit yang mengurangi tingkat keterampilan yang dibutuhkan untuk menyebarkan serangan tersebut.[220]

Oleh karena *drive-by download* dapat mengeksekusi kode berbahaya pada mesin korban tanpa interaksi korban, menjadikannya serangan yang paling signifikan dan populer di internet. Serangan *drive-by download* selanjutnya memungkinkan penyerang untuk menjalankan perangkat lunak yang dapat merekam penekanan tombol, mencuri kredensial *login*, dan rentan terhadap kebocoran informasi dari sistem. Sistem yang terinfeksi tersebut dapat digunakan sebagai *botnet*, yang merupakan kumpulan host yang terinfeksi yang dikendalikan oleh penyerang. Skenario serangan untuk mengeksekusi *drive-by download* diawali oleh penyerang yang akan mengkompromikan server web asli dan mengunggah kode skrip berbahaya. Setiap kali situs web yang disusupi dikunjungi oleh korban, *browser* korban akan mengunduh dan mengeksekusi kode skrip yang disematkan. Skrip yang dikodekan akan mengeksploitasi kerentanan mesin korban dengan menginstal *plug in browser* dan akan memberikan kontrol penuh kepada penyerang.[221]

2. Kasus *Ransomware*

Tahun 2019, menjadi waktu penting karena tercatat pertama kali *hacker* dengan modus *ransomware* tertangkap oleh Kepolisian Indonesia. Polisi menangkap pelaku yang berasal dari Yogyakarta ini pada 18 Oktober 2019. Selama ini pelaku menargetkan sejumlah perusahaan Amerika

[220]Van Lam Le, *et.al.*, "Anatomy of Druve-by Download Attack", *Proceedings of the Eleventh Australasian Information Security Conference*, Adelaide, Australia, 2013, pp. 49-58, hlm. 49.

[221]Chirag R. Desai dan Narendra M. Shekokar, "VILEEAR: Detection of Drive by Download Attack on Malicious Web Pages", *International Journal of Science and Research*, Vol. 4, Issue 4, 2015, pp. 2302-2306, hlm. 2302-2303.

Serikat. Kasus tersebut terungkap dari laporan tim Biro Investigasi Federal (FBI) AS kepada Polri. Informasi yang diterima bahwa, terdapat perusahaan asal San Antonio, Texas yang terkena serangan *ransomware* dan terdeteksi berasal dari Indonesia. Pelaku diketahui melakukan peretasan dengan teknik *ransomware* sejak 2014. Dalam kasus ini, pelaku meminta tebusan sebesar 3 bitcoin. Sejak 2014, pelaku telah mengumpulkan 300 bitcoin. Sepanjang tahun 2019, pelaku menargetkan 500 perusahaan di sejumlah negara dengan mengirimkan *email phishing* yang mengarahkan korban untuk mengeklik tautan berisi *ransomware*.[222]

Selain itu, pada awal September 2020, Proofpoint mengungkapkan bila telah mendeteksi dua serangan *spear phishing* yang melibatkan Group TA413 yang berbasis di Tiongkok. Serangan pertama terjadi pada bulan Maret dan menargetkan entitas Pemerintahan Eropa, organisasi penelitian, dan perusahaan global yang terkait dengan urusan ekonomi dengan modus menggoda penerima pesan untuk membuka file *'WHO's Critical preparedness, readiness and responce actions for Covid-19'*. Serangan kedua menargetkan *'Tibetian dissident'* dengan mengirimkan file PowerPoint dengan judul *Tibetian being hit by deadly virus that carries a gun and speaks chinese.ppsx*.[223]

Pemerintah Kota Tulsa di Oklahama, pada bulan Juni 2021 memperingatkan warganya bila data pribadinya mungkin telah terungkap setelah kelompok *ransomware* mempublikasikan sejumlah dokumen dan surat tilang polisi secara *online*. Pada bulan Mei, Tulsa mengalami serangan *ransomware* yang menyebabkan pemerintah kota menutup jaringannya untuk mencegah penyebaran *malware*. Serangan tersebut telah mengganggu sistem pembayaran tagihan *online,* tagihan utilitas, *email* Tusla, situs web Kota Tusla, Dewan Kota Tusla, serta Kepolisian Tusla. Sebuah kelompok bernama **Conti Ransomware** mengaku bertanggung jawab dan menerbitkan 18.938 file milik pemerintah kota, terutama dokumen tilang polisi dan dokumen internal dalam bentuk file Word. Surat tilang polisi berisi beberapa informasi pribadi, seperti nama, tanggal lahir, alamat, dan nomor SIM.[224]

---

[222]Oktarina Paramitha Sandy, "Pertama Kali dalam Sejarah, Polri Tangkap Hacker Ransomeware", *Cyberthreat*, 25 Oktober 2019, https://cyberthreat.id/read/3532/Pertama-Kali-dalam-Sejarah-Polri-Tangkap-Hacker-Ransomware (diakses pada 25 Mei 2022).

[223]David Bisson, *6 Common Phishing Attacks and How to Protect Against Them, Ibid.*

[224]Lawrence Abrams, "City of Tulsa's Online Services Disrupted in Ransomeware Incident", *Bleeping Computer*, 10 Mei 2021, https://www.

Instansi lainnya yang mengalami serangan *ransomware* adalah perusahaan diagnosis medis Brasil Grupo Fleury sehingga mengakibatkan perusahaan mematikan layanannya. Hal ini menyebabkan pasien tidak dapat menjadwalkan tes laboratorium ataupun ujian klinis lainnya secara *online*. Operator REvil yang mengklaim bertanggung jawab terhadap serangan ini menuntut US$5 juta untuk *decyrptor* dan tidak membocorkan file yang diretas.[225]

Pada 7 Juli 2021, perusahaan penyedia informasi konsumen asal Swiss, Comparis mengalami serangan yang mengakibatkan sejumlah sistem teknologi informasinya terblokir. Pelaku diketahui memiliki akses ke data terkait pelanggan. Comparis yang mengumpulkan sekitar 80 juta kunjungan per tahun, sempat tak dapat diakses. Pada tahun 2020, perusahaan kereta api Swiss, Stadler turut menjadi korban serangan *ransomware*. Pelaku mempublikasikan data curian di internet karena perusahaan menolak untuk membayar uang tebusan.[226] Peretas lainnya memanfaatkan popularitas kartun *"Rick and Morty"* untuk melakukan teknik *phishing* dengan dalih memberikan episode terbaru serial tersebut. Kapersky menemukan setidaknya 350 file yang disamarkan sebagai film, yang ketika diunduh berkas tersebut akan mendistribusikan berbagai jenis *malware,* termasuk *exploit* dan *ransomware*.[227]

---

bleepingcomputer.com/news/security/city-of-tulsas-online-services-disrupted-in-ransomware-incident/ (diakses pada 26 Mei 2022).

[225]Duncan Riley, "REvil Ransomeware Gang Targets French Connection and Grupo Fleury*", Silicon Angle*, 24 Juni 2021, https://siliconangle.com/2021/06/24/revil-ransomware-gang-targets-french-connection-grupo-fleury/ (diakses pada 27 Mei 2022).

[226]Michael Shields, "Ransomeware Attack Hits Swiss Consumer Outlet Comparis*", Reuters*, 10 Juli 2021, https://www.reuters.com/technology/ransomware-attack-hits-swiss-consumer-outlet-comparis-2021-07-09/ (diakses pada 27 Mei 2022).

[227]Newsbeezer, "New Season of Rick and Morty Creates a Wave of Ransomeware Attacks"*, Newsbeezer*, 29 Juni 2021, https://newsbeezer.com/portugaleng/new-season-of-rick-and-morty-creates-a-wave-of-ransomware-attacks/ (diakses pada 27 Mei 2022).

Kasus Operator *Ransomware* Clop

Setelah sebelumnya beberapa anggotanya tertangkap, anggota *ransomware* Clop tetap melakukan serangannya. Dalam salah satu video yang dirilis oleh Kepolisian Ukraina, terlihat aparat penegak hukum tengah menggeledah rumah dan melakukan penyitaan, di antaranya 500 juta Hryvnia Ukraina, peralatan komputer, dokumen serta mobil dengan merek Tesla dan Mercedes. Namun, berselang beberapa minggu penangkapan, kelompok ini kembali merilis data milik dua korban baru pada situsnya. Kelompok Clop ini telah beroperasi sejak Maret 2019, ketika pertama kali menargetkan perusahaan menggunakan *ransomware* CryptoMix. Clop telah bertanggung jawab atas beberapa serangan *ransomware* besar seperti Universitas Maastricht, Software AG IT, ExecuPharm, dan Indiabulls. Sebelumnya, Clop telah mencuri data dari perangkat transfer file *Accellion FTA* menggunakan kerentanan *zero-day* dan kemudian mengancam akan merilis data jika tidak membayar $10 juta.[228]

Untuk melihat video penggeledahan kediaman kelompok operator Clop Anda dapat *scan QR code* di samping.

Sebuah catatan yang perlu diperhatikan terkait serangan *ransomware* yang meminta uang tebusan dari korban agar pelaku menyerahkan *decryptor*. Pilihan membayar uang tebusan, yang kerap dalam bentuk bitcoin tidak selalu menuntaskan masalah dengan segera. Perusahaan operator pipa *Colonial Pipline*, yang telah menerima *decryptor* setelah mentransfer uang tebusan, tidak serta pemulihannya berjalan dengan lancar sehingga tidak menjamin bila membayar tebusan, sistem akan pulih kembali atau data curian dihapus. Survei yang dilakukan terhadap 1.300 profesional keamanan yang dilakukan oleh *Cybereason* menungkapkan bahwa 84% perusahaan memutuskan membayar uang tebusan ketika serangan kedua. Lalu dari 50% kasus, mereka mendapatkan serangan kembali oleh pelaku yang sama. 43% korban melaporkan bahwa sebagian data yang diambil dalam kondisi rusak selama pemulihan. 51% organisasi diminta uang tebusan berkisar US$350.000 hingga US$1,4 juta, sementara 4% meminta lebih dari US$1,4 juta.[229]

---

[228]Sergiu Gatlan, "Ukraine Arrest Clop Ransomware Gang Members, Seizes Servers", *Bleeping Computer*, 16 Juni 2021, https://www.bleepingcomputer.com/news/security/ukraine-arrests-clop-ransomware-gang-members-seizes-servers/ (diakses pada 27 Mei 2022).

[229]Sead Fadilpasic, "Majority of Ransomeware Victims are Hit with a Second Attack After Paying Up", *IT ProPortal*, 16 Juni 2021, https://www.itproportal.com/

D. Baiting

Serangan *baiting*, atau istilah lainnya *road apples*, adalah serangan *phishing* yang mengundang pengguna untuk mengeklik tautan guna mendapatkan barang gratis. Misalnya, menjanjikan musik gratis, telepon, hadiah uang, dan untuk mendapatkannya target hanya perlu masuk ke halaman atau membagikan beberapa informasi pribadinya. Operandi lainnya adalah pelaku bertindak seperti *Trojan Horse* dengan memanfaatkan materi komputer yang tidak aman seperti media penyimpanan atau *drive* USB yang berisi *malware* di kedai kopi untuk ditemukan oleh korban. Ketika korban mencolokkan *drive* USB ke komputernya, *drive* tersebut bertindak seperti *Trojan Horse* dunia nyata dan menyerang komputer.[230]


Reader's digest

READER'S DIGEST
B-45, SECTOR-57, NOIDA - 201301

FINANCE DEPARTMENT - GUARANTEE OF PAYMENT TO PRIZE WINNERS

To: shivam lohani
From: Ravi G.L.
Subject: Finance Department Payout Notice

TOTAL SUPER GRAND PRIZE ELIGIBILITY

₹ 15,00,000.00 Click Here to Confirm

CHANCE TO WIN FOR:

shivam lohani

ACTIVE STATUS:

SELECTION STAGE STATUS	[?] PASSED
ENTRY ALLOCATION STAGE	[?] PASSED
WINNERS DRAW	[X] PENDING

This notice is to guarantee that Reader's Digest Finance has established arrangements to disburse a CASH TRANSFER of Rs. 15,00,000.00 to Full_Name in the event of a win. To ensure there is no delay in awarding the payment with the preferred option to you if you are chosen the winner, decide how you would like to receive your prize today.

Approved,
Ravi G.L.
Director Sweepstakes - Reader's Digest India

Gambar 25. Contoh *Email Baiting*[231]

news/majority-of-ransomware-victims-are-hit-with-a-second-attack-after-paying-ransom/ (diakses pada 28 Mei 2022).

[230]Fatima Salahdine dan Naima Kaabouch, *Op. Cit.*, hlm. 6.

[231]Shivam Lohani, "Social Engineering: Hacking into Humans", *Proceedings of 4th International Conference on Cyber Security (ICSS)*, 2018, pp. 385-393, hlm. 388.

Pada Juni 2021, divisi riset dari perusahaan keamanan siber Quick Heal Technologies Ltd menemukan sejumlah aplikasi Android di Google Play Store yang mengandung *malware* "Joker". Joker termasuk ke dalam keluarga *Trojan*, menyamar layaknya aplikasi yang sah. *Malware* ini diam-diam mengumpulkan data dan mendaftarkan ke layanan berlangganan premium tanpa izin pengguna. Delapan aplikasi yang mengandung Joker yaitu ***Auxiliary Message, Fast Magic* SMS*, Free CamScanner, Super Message, Element Scanner, Go Messages, Travel Wallpapers,*** dan ***Super* SMS.** Dalam operandinya, aplikasi tersebut meminta akses notifikasi, yang digunakan untuk mendapatkan data notifikasi. Aplikasi kemudian mengambil alih data SMS dari notifikasi, dan meminta akses kontak. Ketika akses diberikan, aplikasi membuat dan mengelola izin panggilan telepon. Joker telah menargetkan pengguna di 37 negara, termasuk Amerika Serikat, Inggris, Australia, serta Negara UNI Eropa dan Asia.[232]

Sementara pada Juli 2021, perusahaan keamanan siber Rusia, Dr. Web merilis laporan perihal 9 aplikasi *Trojan* pada Google Play Store. *Software* tersebut mampu mencuri informasi *login*, termasuk kata sandi pengguna media sosial, Facebook. *Stealer Trojan* telah diunduh lebih dari 5,8 juta kali. Aplikasi-aplikasi ini meminta korban untuk masuk pada akun Facebook. Berikut 9 aplikasi *Trojan* yang ditemukan Dr. Web, yakni: (1) aplikasi edit foto, ***Processing Photo, PIP Photo,*** (2) aplikasi pembatasan akses, ***App Lock Keep, App Lock Manager,*** dan ***Lockit Master,*** (3) aplikasi ***Rubbish Cleaner,*** (4) aplikasi astrologi, ***Horoscope Daily, Horoscope Pi,*** (5) aplikasi kebugaran, ***Inwell Fitness.***[233]

[232]Danny Cyril D C, "Android Smartphone Users Alert! Remove These 8 Apps Laced with 'Joker' Malware", *Livemint*, 19 Juni 2021, https://www.livemint.com/technology/apps/android-smartphone-users-alert-remove-these-8-apps-laced-with-joker-malware-11624103586505.html (diakses pada 28 Mei 2022).

[233]Dr. Web, "Android Trojan Steal Facebook Users's Logins and Passwords", 1 Juli 2021, https://news.drweb.com/show/?i=14244&lng=en (diakses pada 28 Mei 2022).

APA ITU *TROJAN HORSE*?[234]

Sebuah kisah legendaris tentang kuda kayu berlubang yang digunakan orang Yunani untuk menyelundupkan tentara mereka ke Troy, ***Trojan Horse*** adalah program jahat yang merusak dan menyamar sebagai file atau aplikasi yang sah untuk mendapatkan akses ke komputer (baru-baru ini, ponsel atau perangkat *game*). Setelah berada dalam sistem, *Trojan Horse* dapat melakukan sejumlah tindakan yang tidak diinginkan, termasuk menghapus atau merusak file, atau bahkan *denial of service attack* (yaitu mencegah penggunaan komputer atau internet yang ditargetkan), membuat bunyi bip, memulai dan menghentikan proses, mencuri informasi (misalnya kata sandi), dan membuka *back door* yang memungkinkan penyerang luar untuk mengontrol komputer yang disusupi dari jarak jauh dan melakukan tindakan seperti meluncurkan *denial of service attack,* di mana semua komputer yang terinfeksi diubah menjadi zombie yang membanjiri situs web yang ditargetkan dengan permintaan informasi secara simultan atau dengan mengirimkan data dalam jumlah besar. Serangan ini pernah dialami oleh Yahoo!, CNN, Microsoft, dan beberapa situs *e-commerce* besar, termasuk Amazon, eBay, dan lainnya. Serangan *Trojan Horse* pertama, *PC-write*, muncul pada tahun 1986 dengan menyamar sebagai versi terbaru dari aplikasi pengolah kata populer. *Trojan* diunduh ke banyak komputer pengguna yang tidak curiga, yang *hard drive*-nya kemudian diformat ulang dan dihapus (yaitu semua file hilang). *Trojan Horse* yang lebih baru juga mengganggu operasi normal komputer, meskipun tidak selalu pada tingkat yang sama atau menggunakan metode yang sama. Namun, setelah pertumbuhan internet dan konektivitas pengguna, fungsi *Trojan Horse* semakin diperluas untuk mencakup pelepasan informasi dan aktivitas lain yang tampaknya berorientasi pada tujuan yang lebih instrumental. Selain penandaan siber dan vandalisme, pencurian, pelanggaran privasi dan kerusakan langsung lainnya yang disebabkan oleh *Trojan Horse*, maka penting untuk mengenali peran yang mungkin dimainkan oleh ancaman ini dalam kelanjutan tindakan kejahatan tersebut, seperti penipuan, pencurian identitas, dan bahkan pemerasan.

E. Quid Pro Quo

Quid pro quo adalah frasa Latin yang secara harfiah berarti "sesuatu untuk sesuatu". Ungkapan tersebut biasanya menunjukkan pertukaran barang atau jasa dengan nilai yang kurang lebih setara. *Quid pro quo* adalah salah satu istilah hukum Latin yang paling umum digunakan. Dalam setiap transaksi, hukum, politik atau lainnya, akan sangat membantu untuk mengetahui *quid pro quo,* yaitu keseimbangan nilai layanan atau barang dan kompensasi finansial yang ditawarkan. Dalam perspektif hukum, *quid pro quo* menunjukkan bahwa suatu barang atau jasa telah diperdagangkan untuk sesuatu yang bernilai sama. Secara khusus, *quid pro quo* digunakan secara eksplisit untuk menunjukkan bahwa telah

[234]Lorine A. Hughes, "Viruses, Worms, and Trojan Horses: Serious Crimes, Nuisance, or Both?", *Social Science Computer Review*, Vol. 25, No. 1, 2007, pp. 78-98, DOI: 10.1177/0894439306292346, hlm. 81-82.

ada "pertimbangan" dalam suatu kontrak, yang berarti bahwa terdapat barang atau jasa yang dikirimkan dan pembayaran yang dapat diterima diperuntukkan untuk barang atau jasa tersebut. Tanpa pertimbangan atau *quid pro quo*, misalnya suatu kontrak dapat dianggap tidak mengikat dan tidak sah. Dalam dunia politik, misalnya *quid pro quo* sering kali mengacu pada pemberian dukungan, finansial atau lainnya, terhadap seorang kandidat politik dengan imbalan harapan dukungan langsung untuk aktivitas politik. *Quid pro quo* kerap muncul sebagai suap dalam kasus ini dan dukungan tersebut harus selalu diuji untuk konflik kepentingan.[235] Dalam lingkup serangan *social engineering, quid pro quo* didefinisikan sebagai serangan yang bergantung pada rasa timbal balik orang-orang, dengan modus penyerang menawarkan sesuatu sebagai imbalan informasi.[236]

Jenis serangan ini umumnya terjadi dengan cara menghubungi nomor seseorang secara acak dan berpura-pura untuk membantu persoalan teknis. Sayangnya, teknik ini tampaknya kerap berhasil karena pelaku kerap muncul ketika korban tengah benar-benar mengalami masalah. Korban menjadi merasa bersyukur bahwa seseorang menelepon kembali untuk membantu mereka menyelesaikan masalah. Pelaku kemudian akan mulai menyelesaikan masalah, tetapi meminta pengguna mengetikkan perintah yang memberikan akses untuk menyerang atau meluncurkan *malware* selama panggilan.[237]

F. Pretexting

Serangan *pretexting* diawali dengan menciptakan skenario palsu dan meyakinkan untuk mencuri informasi pribadi korban. Skenario tersebut didasarkan pada keadaan yang membuat korban memercayai penyerang. Serangan dapat dilakukan melalui panggilan telepon, *email*, atau media fisik. Penyerang dapat menggunakan informasi dari buku telepon,

---

[235]Sruthy Santhosh, "Social Engineering Attacks", *The Bit: The Bullettin of Information Technology*, Rajagiri School of Engineering & Technology, April-August 2015, hlm. 6-7.

[236]IT Governance, "Social Engineering Attacks", *IT Governance*, https://www.itgovernance.co.uk/social-engineering-attacks (diakses pada 28 Mei 2022).

[237]Hussain Aldawood dan Geoffrey Skinner, "An Advanced Taxonomy for Social Engineering Attacks", *International Journal of Computer Application*, Vol. 177, No. 30, Januari 2020, pp. 1-11, hlm. 4.

halaman web publik, atau konferensi di mana kolaborator di bidang yang sama bertemu untuk melakukan serangan mereka. Dalihnya dapat berupa tawaran untuk melakukan layanan atau mendapatkan pekerjaan, menanyakan informasi pribadi, membantu teman untuk mendapatkan akses ke sesuatu, atau memenangkan lotre.[238]

Kasus Kantor Presiden Afghanistan

Pada pertengahan tahun 2021, kelompok peretas berbahasa China melakukan serangan siber terhadap Pemerintah Afghanistan dengan menyamar sebagai presiden. Kantor Presiden Afghanistan digunakan sebagai umpan *email phishing* yang dirancang untuk menyusup ke lembaga pemerintah. Serangan tersebut berhasil meretas Dewan Keamanan Nasional Afghanistan. Kelompok yang dijuluki IndigoZebra diduga bertanggung jawab atas serangan tersebut. Dalam *email phishing* tersebut, terdapat permintaan dari kantor presiden untuk dilakukan peninjauan mendesak atas perubahan dokumen terkait dengan konferensi pers yang akan datang. File tersebut adalah arsip. RAR yang dilindungi kata sandi bernama NSC Press Conference.rar. Apabila korban membuka file, maka akan menerima *executable windows* yang menyebarkan pengunduhan *malware* dan *backdoor "xCaon"*. *Backdoor* dapat mengunduh dan mengunggah file, menjalankan perintah dari *server command-and-control* yang dikuasai peretas dan mencuri data. Penyerang turut menyebarkan alat pemindai NetBIOS yang diadopsi oleh APT10/Stone Panda yang dapat menjalankan alat utilitas jaringan untuk pengintaian dalam pencarian target lebih lanjut.

Untuk informasi lebih lanjut terkait **Kasus Kantor Presiden Afghanistan,** Anda dapat *scan QR code* di samping.

[238]Fatima Salahdine dan Naima Kaabouch, *Op. Cit.*, hlm. 5.

Kasus Kate Middleton

Pada 2012, ketika mengandung Pangeran George, Duchess Kate Middleton dirawat di rumah sakit karena mual di pagi hari yang ekstrem. Publik dan media segera mengetahuinya, dan pada pukul 5.30 pagi, sepasang penyiar pada sebuah acara radio Australia menghubungi (menelepon) rumah sakit, menyamar sebagai Ratu Inggris dan Pangeran Charles. Penyiar tersebut menirukan aksen mereka dan meminta perkembangan keadaan Middleton. Perawat yang bekerja di bagian penerima tamu menjawab telepon memercayai bahwa panggilan itu sah, dan menghubungkannya kepada perawat pribadi Middleton, yang memberikan berbagai detail tentang kondisinya. Para penyiar merekam panggilan tersebut dan memutarnya di radio. Program ini mendapat perhatian internasional. Sebelum rumah sakit dapat mengambil tindakan apa pun, perawat itu ditemukan tewas karena bunuh diri. Pangeran William dan Duchess Kate merilis pernyataan tentang kesedihan mendalam mereka atas insiden tersebut dan menyampaikan belasungkawa kepada mereka yang dekat dengan perawat. Acara radio tersebut telah dibatalkan, dan akun Twitter acara serta pembawa acara telah dihapus. Stasiun radio mengeluarkan permintaan maaf publik secara resmi.[239]

Untuk informasi lebih lanjut terkait **Kasus Kate Middleton,** Anda dapat *scan QR code* di samping.[240]

[239]Joe Gray, *Practical Social Engineering* (San Franciso: No starch Press, 2021), hlm. 17.

[240]Caroline Davies, "Royal Baby Hoax Call Leaves Duchess's Hospital Unamused", *The Guardian*, 5 Desember 2012, https://www.theguardian.com/uk/2012/dec/05/royal-baby-hoax-call-hospital (diakses pada 28 Mei 2022).

Kasus Kane Gamble

Salah satu kasus *pretexting* yang mendapatkan perhatian dunia dilakukan oleh seorang remaja berusia 15 tahun yang berasal dari Inggris dan bernama Kane Gamble yang mengakses sejumlah data rahasia *Central Intelligence Agency* (CIA) dan dilakukannya dalam kurun waktu 2015-2016. Aksinya tersebut Kane lakukan di kamar rumahnya yang terletak di Leicestershire. Dalam aksinya, Kane menyamar sebagai John Brennan, Kepala CIA pada saat itu dan menipu panggilan di perusahaan komunikasi Comcast dan Verizon agar membuka informasi pribadi Brennan. Pada akhirnya Kane berhasil membobol akun *email* AOL milik Brennan yang memuat banyak nomor kontak dan *email* agen CIA. Bahkan Kane mendapatkan akses dokumen rahasia negara seperti operasi militer dan intelijen di Afghanistan dan Iran. Kane lantas mengunggah dokumen tersebut di Twitter serta memberikannya kepada WikiLeaks.

Tidak hanya CIA, Kane juga berhasil menyamar sebagai Clapper, Direktur Intelijen Nasional Pemerintahan Barack Obama. Kane telah mengalihkan seluruh panggilan yang masuk ke telepon rumah Clapper ke Gerakan Palestina Merdeka. Korban lainnya adalah Vonna Weir Heaton, mantan pejabat Badan Intelijen Geospasial AS, yang berhasil dibajak akun media sosialnya. Kane juga meneror keluarga Jeh Johnson, yang saat itu adalah Menteri Keamanan Dalam Negeri AS. Kane berhasil meretas jaringan internet rumah Johnson, mengetahui kata sandi TV kabelnya, mendengarkan pesan suara dan mengirim teks dari ponselnya. Penasihat Teknologi dan Ilmu Pengetahuan Obama, John Holdren turut menjadi korban peretasan. Kane meretas akun serta informasi pribadi Holdren, dan akhirnya membuat telepon palsu ke kantor polisi, mengatakan terjadi kekerasan di rumah Holdren, hingga akhirnya tim SWAT datang. Kane ditangkap pada Februari 2016 di rumahnya atas permintaan dari FBI setelah berhasil meretas jaringan Kementerian Kehakiman AS dan FBI serta mengakses informasi 20 ribu agen FBI. Salah satu dokumen rahasia FBI yang dicurinya adalah dokumen berjudul *Deepwater Horizon Oil Spil.*

Kane menjalani pengadilan pertamanya di Old Bailey, London dan menghadapi 10 dakwaan pelanggaran undang-undang penyalahgunaan komputer Inggris dan divonis 2 tahun atas kejahatannya. Dalam laporan persidangan diketahui bila Kane berhasil mengakses *email* dan jaringan telepon pribadi Avril Haines, wakil penasihat keamanan nasional Gedung Putih dan agen FBI Amy Hess. Kane mengunduh banyak film ke dalam komputer Hess, termasuk berbagai film porno.

Untuk informasi lebih lanjut terkait **Kasus Kane Gamble,** Anda dapat *scan QR code* di samping.[241]

[241]BBC News, "Two years for teen 'cyber terrorist' who targeted US officials", *BBC News*, 20 April 2018, https://www.bbc.com/news/uk-england-leicestershire-43840075, diakses pada 28 Mei 2022.

Kasus PopCall

Pada akhir tahun 2020, pengguna Jenius mengeluhkan adanya upaya penipuan yang dialami. Pelaku menggunakan layanan PopCall agar terlihat pesan yang diterima datang dari perusahaan resmi. PopCall merupakan layanan yang memungkinkan pelanggan untuk menampilkan teks berupa *pop up* pada layar ponsel penerima. Pesan ini akan muncul sesaat sebelum telepon berdering. Upaya penipuan ini diketahui setelah beberapa orang yang mengaku korban mengeluhkan pengalamannya di media sosial. Pengguna Twitter Adiyat Hanif Kautsar menuliskan bahwa rekening Jenius temannya yang bernama Anggita Wahyuningtyas dibobol sehingga merugi Rp50 juta. Anggita mendapatkan panggilan telepon dari seseorang yang seolah-olah bertindak sebagai *call center* Jenius. Penipu menyatakan, bila terdapat pembaharuan sistem dan penggantian kartu ATM. Data yang diminta pelaku mengakibatkan Anggita tidak dapat mengakses akun Jeniusnya. Keluhan lainnya disampaikan akun @jeffyoung97 yang mengisahkan bila terdapat seseorang yang mengatasnamakan Jenius dari BTPN meminta untuk mengganti kartu Jenius.

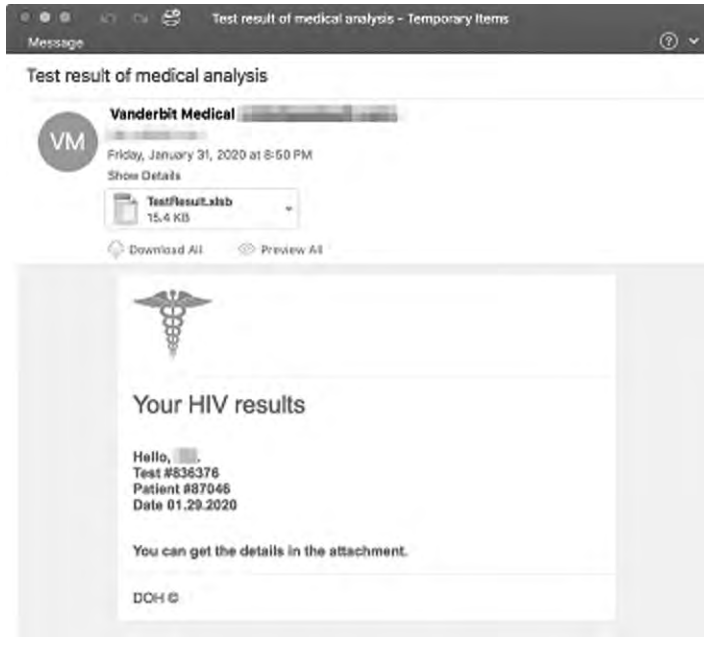
Untuk informasi lebih lanjut terkait **Kasus PopCall,** Anda dapat *scan QR code* di samping.

Potensi ancaman *pretexting* semakin besar, mengingat mudahnya seseorang untuk mendapatkan informasi dari internet saat ini. Terdapat beberapa forum maupun *website* yang secara terbuka memberikan informasi yang detail terkait skenario serangan *pretexting*, sehingga tidak menutup kemungkinan, orang yang tidak bertanggung jawab dapat menggunakannya. Salah satunya adalah **https://pretext-project.github.io/**, yang memberikan beberapa contoh *pretexting* lengkap dengan contoh dan langkah-langkahnya, serta **https://www.proofpoint.com** yang merupakan perusahaan keamanan yang salah satu agendanya melakukan penelitian terkait kejahatan siber. Berikut beberapa contoh yang terdapat dalam kedua situs tersebut **(catatan penulis: informasi ini ditujukan agar pembaca dapat terhindar menjadi korban dari serangan *pretexting* tersebut, dan tidak diperuntukkan untuk disalahgunakan).**

1. Skenario Hasil Tes Medis

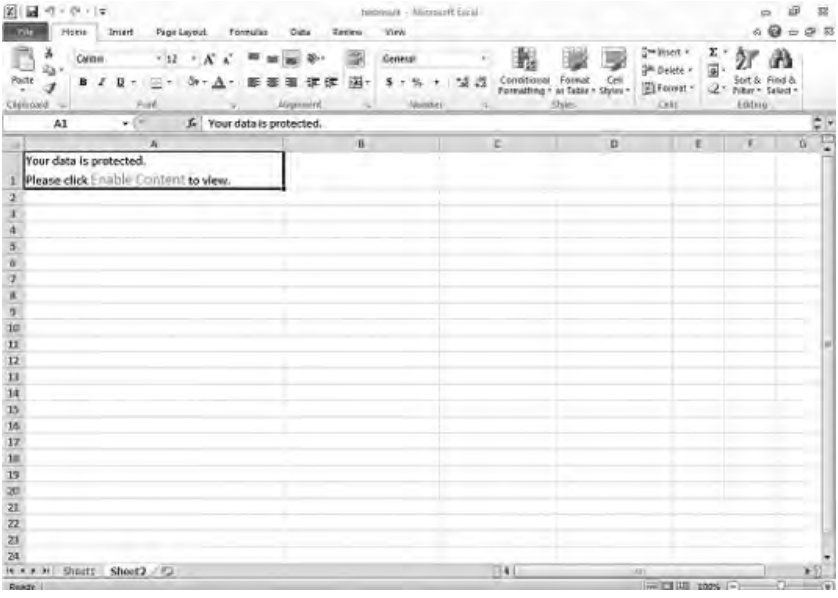
Seorang korban menerima *email* yang tidak diminta dan berisi data analisis medis dari unit kesehatan. Dengan dalih ini, penyerang tidak mengirim *email* ke korban yang mereka yakini sedang menunggu hasil tes medis. Sebaliknya, *email* tersebut dirancang untuk memancing rasa ingin tahu penerima untuk melihat hasil tes medis orang lain. Tes kesehatan yang dimaksud dalam *email* dapat bervariasi: Coronavirus, HIV, tes darah, dan lain-lain. *Email* tersebut berisi lampiran hasil tes medis, yang sesungguhnya adalah *malware*.

Peneliti Proofpoint menemukan serangan *pretexting* yang mengaku dari Pusat Medis Universitas Vanderbilt yang mengirimkan hasil tes HIV dan memikat korban untuk membuka file berbahaya yang dilampirkan dalam *email,* berupa file Microsoft Excel dengan judul "TetsResults.xslb" dan menyatakan bahwa hasil HIV penerima terdapat di dalamnya. Serangan ini memanfaatkan Koadic RAT, yang bila berhasil dan Koadic diinstal, penyerang dapat menjalankan program dan mengakses data korban, termasuk informasi pribadi dan keuangan.



Gambar 26. *Email* Mengatasnamakan *Venderbit Medical*

Apabila korban membuka lampiran, dokumen Excel akan terbuka dan meminta pengguna untuk mengaktifkan makro seperti yang ditunjukkan pada gambar di bawah ini.



Gambar 27. Lampiran File Excel

Apabila korban mengaktifkan makro, dokumen kemudian akan mengunduh Koadic. Koadic memungkinkan penyerang untuk mengambil kendali penuh sistem korban. Dalam beberapa tahun terakhir ini Koadic telah digunakan oleh berbagai pelaku dari berbagai negara, termasuk kelompok yang disponsori Negara China dan Rusia, serta penyerang yang terkait dengan Iran.

Proofpoint mengutarakan bila informasi sensitif terkait kesehatan umumnya disampaikan dengan aman menggunakan portal pesan aman, melalui telepon, atau secara langsung. Jika seseorang menerima *email* yang mengklaim memiliki informasi sensitif terkait kesehatan, jangan buka lampirannya, namun segera kunjungi portal pasien penyedia medis secara langsung, hubungi dokter, atau buat janji untuk secara langsung mengonfirmasi diagnosis medis atau hasil tes apa pun.

Perlu menjadi perhatian penting, bila saat ini data kesehatan merupakan informasi penting, sensitif yang wajib mendapatkan perlindungan khusus, mengingat perkembangan teknologi telah

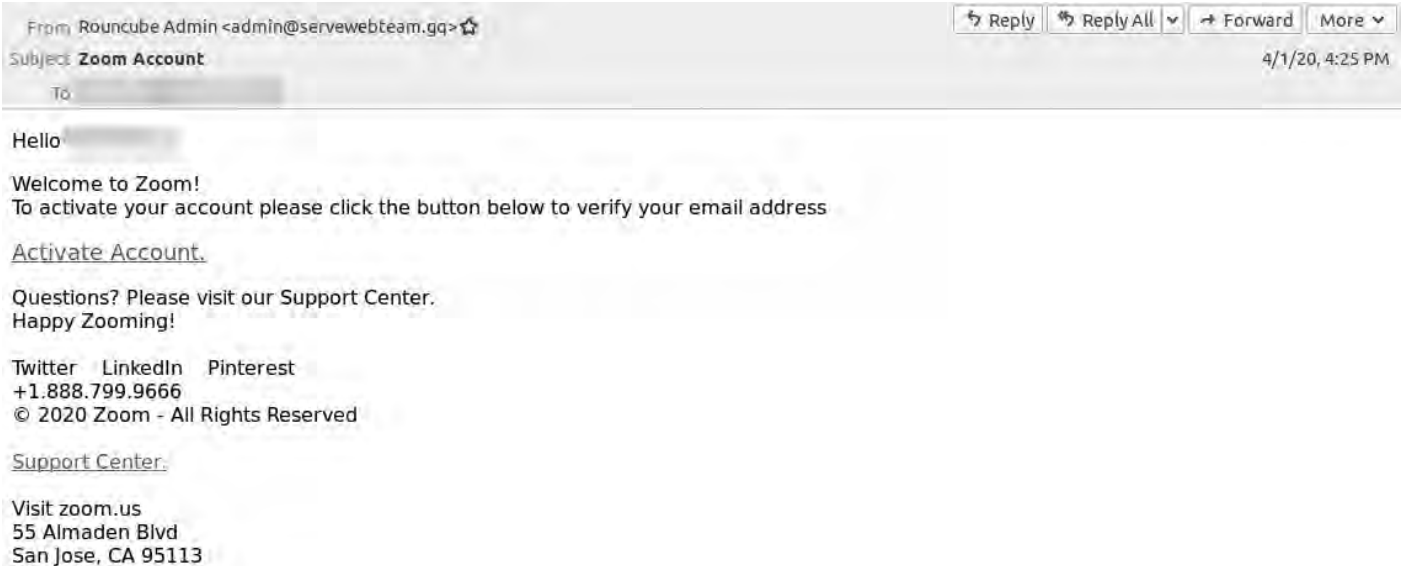
membuka peluang besar terjadinya pelanggaran maupun kejahatan yang memanfaatkan informasi maupun data pribadi. Diskursus perihal *genetic data* dan privasi saat ini telah menjadi tema utama setelah diketahui pelanggaran yang memanfaatkan data biometric, seperti sidik jari dan pengenalan wajah telah menjadi modus operandi kejahatan saat ini.[242]

2. Skenario Rapat Virtual (Zoom)

Serangan ini tidak memanfaatkan atau menyerang perangkat lunak konferensi video secara langsung. Pelaku menggunakan nama dan merek perusahaan konferensi video sebagai tema dalam umpan *social engineering*, yang mengarah pada pencurian berbagai kredensial akun, distribusi *malware*, atau pengambilan kredensial untuk akun konferensi video palsu ini.

Serangan dengan menggunakan zoom sebagai umpan, terjadi di Amerika Serikat dengan target perusahaan di bidang energi, manufaktur, dan layanan bisnis. Serangan ini dirancang untuk mencuri kredensial pengguna. Isi pesan menyertakan iming-iming yang mengklaim untuk menyambut pengguna ke akun Zoom baru mereka.

[242]Roisin A Costello, "Genetic Data and The Right to Privacy: Towards a Relational Theory of Privacy?", *Human Right Law Review*, Vol. 22, Issue 1, 2022, hlm. 2.

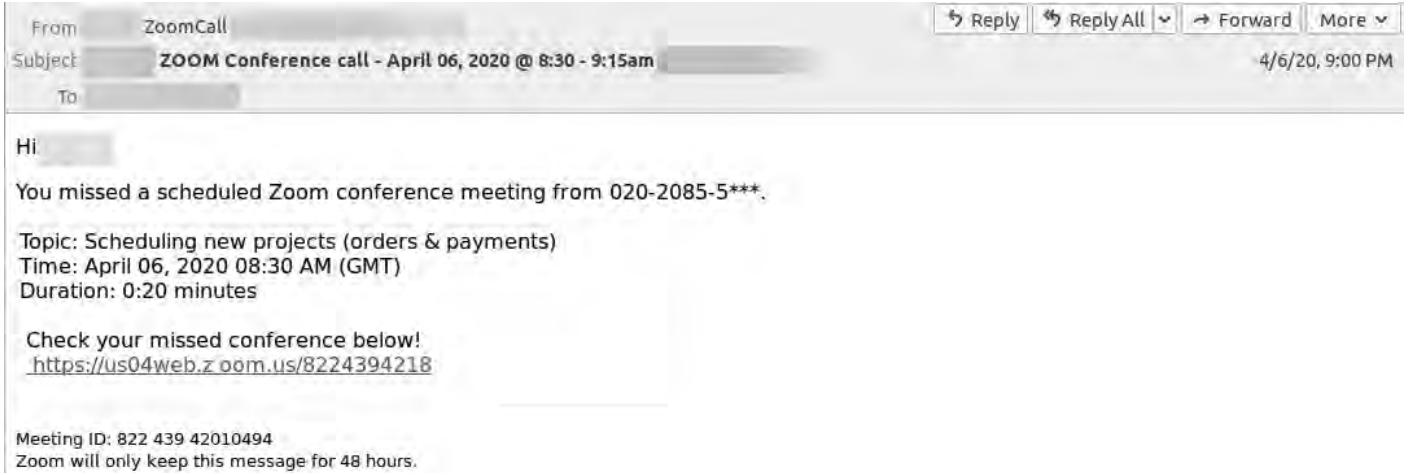


Gambar 28. Pesan Perihal Aktivasi Akun

Serangan *email phishing* Zoom ini berisi subjek "Akun Zoom" dan mengaku berasal dari akun admin. Dalam contoh, pesan mengklaim berasal dari "Rouncube Admin". Umpan *email* lainnya mengklaim berasal dari "admin@servewebteam[.]gq".

Isi pesan menyertakan tawaran yang menyambut korban ke akun Zoom baru dan berisi tautan, yang mendesak untuk diklik oleh korban untuk mengaktifkan akun Zoomnya. Ketika diklik, korban dibawa ke halaman arahan webmail umum dan diminta untuk memasukkan kredensial mereka.

Skenario lainnya hadir, dengan menargetkan perusahaan transportasi, teknologi serta dirgantara di Amerika Serikat guna mencuri kredensial pengguna dengan dalih pertemuan Zoom yang telah terlewat dan menyertakan tautan yang dapat digunakan korban untuk memeriksa konferensi yang terlewat. Apabila korban mengeklik tautan, maka akan diarahkan ke halaman Zoom palsu dan meminta kredensial Zoom.



Gambar 29. Pesan Perihal Agenda Zoom yang Terlewat

3. Undangan Menjadi Pembicara

Skenario serangan ini pada umumnya menargetkan praktisi maupun akademisi dengan berisi permintaan menjadi narasumber atau bahkan *keynote speaker* pada sebuah seminar atau konferensi. Pelaku mempersiapkan informasi palsu terkait sebuah agenda seminar yang berkaitan dengan bidang keahlian korban. Pelaku kemudian menghubungi korban melalui *email* atau telepon dan mengundang korban sebagai narasumber. Skenario ini sangat bergantung pada kejelian pelaku untuk meneliti kepakaran bidang korban dan meluluhkan hati korban dengan menggunakan kata-kata "wawasan Anda", "Anda sangat direkomendasikan", "terbaik pada bidangnya", dan lainnya. Pelaku kemudian akan membuat *website* konferensi palsu dengan informasi yang detail dan menginformasikan kepada korbannya melalui *email*.

Gambar 30. Pesan Perihal Undangan Menjadi Narasumber

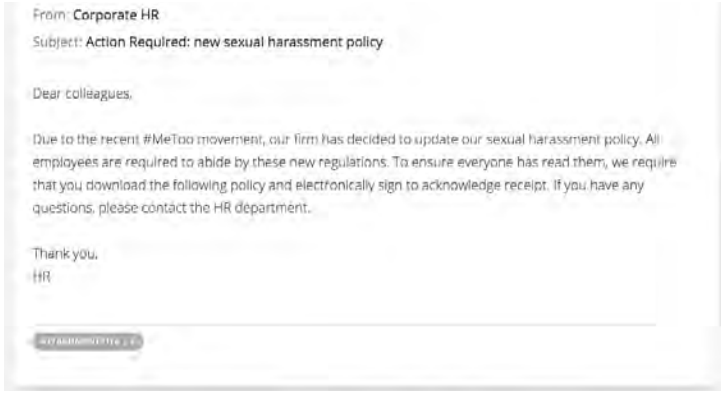
Operandi lain dilakukan dengan menghubungi langsung target sebagai langkah awal, hingga akhirnya mengarahkan target untuk menerima dan membuka pesan yang dikirimkan melalui *email* oleh penyerang. Salah satu contoh skenario tersebut, yakni:

Korban:	Selamat siang.
Pelaku:	Selamat siang, Pak (korban), saya (pelaku) dari Konferensi Internasioal Kejahatan Siber. Apa kabarnya Pak (korban)?
Korban:	Baik, ada yang bisa saya bantu?
Pelaku:	Saya tidak yakin, apakah bapak sebelumnya telah mendengar Konferensi Internasional Kejahatan Siber, tetapi ini adalah tahun ketiga kami menjalankan konferensi ini. Kami mengumpulkan praktisi serta akademi terbaik dalam bidang kejahatan siber. Saat ini, kami tengah mencari pembicara serta *keynote speaker,* dan panelis serta komite merekomendasikan nama bapak. Apakah bapak bersedia untuk kami undang sebagai *keynote speaker* pada konferensi tersebut?
Korban:	Mungkin.
Pelaku:	Baik pak, apakah saya boleh mengirimkan informasi terkait kegiatan tersebut melalui *email* dan berdiskusi selanjutnya untuk membahas lebih detail?

4. Gerakan #MeToo

Serangan ini memanfaatkan gerakan #MeToo yang ketika itu tengah ramai menjadi sorotan, perihal pelecehan seksual yang dilakukan oleh Harvey Weinsten. Gerakan tersebut mendorong para korban untuk berani bersuara menyampaikan pelecehan yang pernah dialaminya, setelah selama ini diam karena rasa takut maupun malu yang dihadapinya.

Sejak gerakan tersebut, beberapa perusahaan mulai memperbaharui regulasi internal guna mengurangi risiko terjadinya pelecehan seksual di lingkungannya. Penyerang memanfaatkan kondisi ini dengan mengirimkan *malware* melalui lampiran yang terdapat dalam *email* dengan tajuk peraturan perusahaan terbaru perihal pelecehan seksual. Penyerang mengaku dari bagian HRD dan menghubungi karyawannya untuk menyampaikan informasi peraturan tersebut.


From: Corporate HR
Subject: Action Required: new sexual harassment policy

Dear colleagues,

Due to the recent #MeToo movement, our firm has decided to update our sexual harassment policy. All employees are required to abide by these new regulations. To ensure everyone has read them, we require that you download the following policy and electronically sign to acknowledge receipt. If you have any questions, please contact the HR department.

Thank you,
HR

Gambar 31. Pesan Perihal Regulasi Kekerasan Seksual di Tempat Kerja

Kasus Harvey Weinstein

Pada 5 Oktober 2017, New York Times menerbitkan laporan perihal tuduhan pelecehan seksual yang dilakukan oleh produsen film Amerika, Harvey Weinstein, diikuti oleh artikel New Yorker yang turut menuduh tindakan pelecehan seksual serta pemerkosaan lainnya yang dilakukan oleh Harvey. Setelah laporan tersebut, lebih dari delapan puluh wanita yang bergerak di industri film menyuarakan pelanggaran seksual yang pernah dialaminya. Weinstein kemudian mundur dari perusahaannya, produksi filmnya diberhentikan dan keanggotaannya di sejumlah organisasi film dicabut. Setelah enam bulan laporan tersebut terbit, Harvey didakwa pada pengadilan New York pada Mei 2018 atas tuduhan pemerkosaan dan pelecehan seksual.[243]

Gerakan #MeToo pada kasus Harvey diinisiasi oleh aktris Alyssa Milano dengan mendorong pengguna Twitter untuk menyampaikan kisahnya jika pernah mengalami aksi pelecehan seksual. Dalam waktu dua puluh empat jam, setelah tweet Milano, terdapat 500.000 tanggapan yang hadir dan dalam satu tahun, tagar (#) tersebut dilaporkan telah digunakan lebih dari delapan belas juta tweet. Gerakan *multi-platform* internasional menggunakan tagar '#MeToo', diciptakan oleh aktivis Tarana Burke pada tahun 2006.[244] Saat ini, #MeToo tidak hanya menolong korban di lingkungan Hollywood, tetapi membantu pekerja wanita di seluruh dunia.[245]

Untuk informasi lebih lanjut terkait **Kasus Harvey,** Anda dapat *scan QR code* di samping.

[243]Natalie Dugan, "#TimesUp On Individual Litigation Reform : Combatting Sexual Harassment Through Employee-Driven Action and Private Regulation", *Colombia Journal of Law and Social Problem*, Vol. 53, No. 2, 2020, pp. 247-281, hlm. 248-250.

[244]Elanor Dierking, "The Weinstein Effect and Mediated Non-Apologies", *Media@LSE, London School of Economics and Political Sciene,* 2019, hlm. 4.

[245]Daniel Otero, "How "Me Too" Hollywood Types Destroyed Feminism", *Journal of Arts & Humanities*, Vol. 7, Issue 11, 2018. pp. 50-57, DOI: http://dx.doi.org/10.18533/journal.v7i10.1525, hlm. 50.

G. Piggybacking

Serangan *piggybacking*, yang juga disebut *tailgating* merupakan salah satu jenis *social engineering* yang sedikit berbeda dengan jenis lainnya karena teknik ini mengharuskan penyerang untuk berinteraksi secara eksklusif dan fisik dengan target. Jenis serangan ini melibatkan pelaku yang meminta akses ke area atau ruang yang dibatasi secara fisik, atau organisasi digital. Skenario umum yang dilaporkan dalam pengaturan organisasi adalah bahwa penyerang meminta karyawan untuk "menahan pintu" ke area terlarang karena mereka lupa akses atau kartu identitas mereka, atau meminta karyawan untuk meminjam alat yang tidak mereka miliki. Serangan ini akan sangat berguna dalam organisasi besar di mana karyawan tidak mengenali rekan kerja mereka, sehingga target sering kali mudah tertipu. Seseorang tanpa autentikasi yang tepat mengikuti karyawan yang diautentikasi ke area terlarang; penyerang mungkin menyamar sebagai sopir pengiriman dan menunggu di luar gedung, dan ketika seorang karyawan mendapatkan akses keamanan dan membuka pintu, penyerang meminta karyawan untuk menahan pintu, sehingga mendapatkan akses ke gedung. *Piggybacking* tidak selalu berhasil di semua pengaturan organisasi seperti perusahaan besar yang membutuhkan kartu akses untuk masuk. Namun, di perusahaan menengah atau keamanan rendah, penyerang dapat dengan mudah memulai percakapan dengan karyawan dan mengandalkan penampilan untuk melewati resepsionis dan memasuki lokasi perusahaan.[246]

[246]Michelle Adi Nugraha, *et.al.,* "Insight on Media Literacy and Social Engineering Vulnerability Predictors: Lifelong Learning Gravity"*, Cypriot Journal of Educational Sciences*, Vol. 15, Issue 5, 2020, pp. 955-975, DOI: https://doi.org/10.18844/cjes.v15i5.5124, hlm. 958.

Kasus Colin Greenless

Colin menjadi perhatian ketika diketahui dapat menyusup ke perusahaan jasa keuangan FTSE. Colin, konsultan keamanan di Siemens Enterprise Communication, diminta oleh direktur perusahaan untuk memeriksa keamanan kantornya. Tanpa bantuan pegawai FTSE dan peralatan khusus, Colin berhasil menyusup ke dalam kantor selama satu minggu lamanya. Colin menghabiskan hari pertamanya dengan mengamati orang-orang yang keluar masuk untuk mendapatkan gambaran tentang informasi keamanan. Setelah makan siang, Colin memutuskan untuk mendapatkan akses dengan membuntuti orang-orang saat mereka menggesek kartu akses. Colin berpura-pura menelepon dan memberi isyarat kepada orang-orang bahwa dia menginginkan naik ke lantai 3. Colin memasuki ruang pertemuan kaca, dengan tenang menggantungkan jaketnya dan mulai bekerja dengan laptopnya. Dalam waktu 20 menit, Colin telah melihat sebuah dokumen rahasia yang ditinggalkan di atas meja. Dokumen ini menyangkut proses merger dua perusahaan senilai £434 juta. Colin mengakses berbagai lantai, ruangan, lemari arsip. Dengan menggunakan trik memegang dua cangkir kopi, membuat orang di sekitarnya membuka pintu ketika Colin hendak masuk. Colin mendapatkan akses ke ruangan data dengan berpura-pura melakukan audit keamanan. Colin diberikan informasi tentang jaringan perusahaan dan sebagai hasilnya, membuat Colin dapat menghubungkannya dengan laptop pribadinya. Ini memberikan Colin akses data rahasia pelanggan, karyawan dan perusahaan. Colin mendapatkan direktori telepon internal dan menggunakan telepon internal untuk berpura-pura menjadi pekerja teknis bidang IT. Tidak hanya itu, Colin berhasil mendapatkan *username* dan kata sandi 17 dari 20 orang yang dimintanya. Bahkan, Colin menyelundupkan konsultan lain untuk membantu analisis sistem IT.

Untuk informasi lebih lanjut terkait **Kasus Colin Greenlees,** Anda dapat *scan QR code* di samping.

Untuk informasi lebih lanjut terkait contoh *piggybacking*, Anda dapat melihat video dengan *scan QR code* di samping.

H. Dumpster Diving

Dumpster diving merupakan istilah yang menggambarkan aktivitas "mengais-ngais" sampah target untuk mencari informasi berharga. Tidak banyak yang mengetahui jumlah informasi yang mungkin didapatkan dengan cara ini. Sebagian orang tidak terlalu memikirkan perihal barang yang dibuang di rumah; laporan mutasi kartu kredit, botol resep medis, laporan mutasi bank, materi terkait pekerjaan dan lainnya. Pada tempat kerja, pegawai perlu diberikan pemahaman bahwa terdapat orang yang memanfaatkan sampah untuk mendapatkan informasi yang bermanfaat bagi mereka.[247]

Jangan Buang Sampah Paket Sembarangan !!!!

Meningkatnya angka transaksi pembelian secara daring, melahirkan potensi hadirnya kejahatan terhadap konsumen. Konsumen kerap membuang sampah paket barang tersebut yang terdapat informasi detail seperti nama lengkap, alamat rumah, nomor telepon, *email* dan lainnya. Tidak menutup kemungkinan informasi ini akan digunakan oleh penyerang dan merugikan korban. Untuk itu pastikan sebelum membuang sampah paket, informasi telah digunting hingga tidak dapat tersusun serta mencoretnya hingga tidak dapat terbaca.

Untuk informasi lebih lanjut terkait cara pencegahannya, Anda dapat *scan QR code* di samping.

Bentuk serangan ini populer selama tahun 1980-an, ketika keamanan belum sebaik saat ini. Pelaku *dumpster diving* pada awalnya dilakukan oleh individu yang memiliki rasa ingin tahu tentang sesuatu. Orang-orang ini ingin mengetahui lebih banyak tentang bagaimana suatu produk atau teknologi bekerja. Mereka merasa bahwa cara terbaik untuk mengetahuinya adalah dengan pergi ke sumbernya. Cara konvensional untuk masuk ke kantor perusahaan, dengan cara meminta informasi sensitif tentang produk tertentu, benar-benar tidak

[247]Kevin D. Mitnick dan William L. Simon, *The Art of Deception: Controlling the Human Element of Security* (Indianapolis: Wiley Publishing, 2002), hlm. 156.

mungkin. Satu-satunya cara lain untuk mengakses informasi tersebut adalah dengan menelusurinya di tempat sampah. Awalnya, orang-orang yang merasa perlu mengeluarkan rasa ingin tahu mereka dengan cara menelusuri tempat sampah dianggap sebagai peretas atau *cracker*. Peretas dapat dicirikan sebagai "orang yang senang menggunakan komputer dan menjelajahi infrastruktur informasi dan sistem yang terhubung dengannya". *Cracker* di sisi lain diklasifikasikan sebagai "orang yang dengan jahat membobol sistem informasi dan dengan sengaja menyebabkan kerugian dalam melakukannya.[248]

Pada tahun 1982 Geraldo Rivera telah memperingatkan perihal *electronic delinquents* yang melakukan peretasan komputer. Rivera membongkar langkahnya dan mengungkapkan jika itu semua bermula dari tempat sampah yang terletak di belakang sebuah perusahaan. Dari sinilah Rivera mendapatkan seluruh informasi yang dibutuhkan guna mengakses sistem komputer sebuah perusahaan telepon. Ketika itu istilah yang digunakan dalam modus ini adalah *garbology,* istilah yang menggambarkan penulusuran sampah perusahaan dan menemukan informasi penting seperti sandi maupun catatan penting lainnya yang ditulis oleh seseorang. *Trashing* adalah praktik yang dibagikan oleh peretas dengan detektif swasta, paparazi, pemulung yang semuanya menilai tempat sampah sebagai sumber bahan berharga, termasuk informasi.[249]

Seseorang yang telah terbiasa melakukan *dumpster diving*, akan memahami bahwa yang dilakukannya tidak menyenangkan, namun merupakan sebuah tantangan. Mereka adalah pembuat teka-teki, sehingga sekalipun dokumen-dokumen tersebut telah disobek, mereka akan menyusun kembali karena menduga bahwa dokumen tersebut pasti memiliki informasi yang berharga. Pertimbangan lainnya adalah, kegiatan tersebut jarang mendapatkan kendala. Sebagian besar orang tidak keberatan ketika sampahnya diambil, karena lazim dilakukan oleh pemulung dan kemungkinan perbuatannya tersebut legal — selama tidak memasuki wilayah tanpa izin.

---

[248]Robert B. Fried, "Dumspter: Beware of Treasure, Crime and Clues: The Art and Science of Criminal Investigation", https://social-engineer.org/wiki/archives/DumpsterDiving/CrimeandClues_dumpster_diving.htm (diakses pada 28 Mei 2022).

[249]Robert W Gehl dan Sean T. Lawson, *Social Engineering: How Crowdmasters, Phreaks, Hackers, and Trolls Created a New Form of Manipulative Communication* (Cambridge, MA: MIT Press, 2022), hlm. 70-72.

Bagi seorang *social engineer*, *dumpster diving* memiliki keuntungan tersendiri. Dia bisa mendapatkan informasi yang cukup untuk memandu serangannya terhadap perusahaan target, termasuk memo, agenda rapat, surat dan sejenisnya yang mengungkapkan nama, departemen, jabatan, nomor telepon, dan tugas proyek. Sampah dapat menghasilkan bagan organisasi perusahaan, informasi tentang struktur perusahaan, jadwal perjalanan, dan sebagainya. Semua detail itu mungkin tampak sepele bagi orang dalam, namun mungkin merupakan informasi yang sangat berharga bagi penyerang. Bahkan seseorang dapat menemukan seluruh laporan yang dibuang karena salah ketik, kata sandi yang ditulis di secarik kertas, seluruh folder file dengan dokumen masih di dalamnya, yang semuanya dapat membantu seseorang untuk menyerang targetnya,[250] seperti data sensitif riwayat medis yang dibuang pada tempat sampah,[251] sementara Siddiqi menguraikan beberapa dokumen yang dapat ditemukan adalah: *(1) financial reports; (2) access codes; (3) passwords; (4) meeting calendars; (5) equipment purchase slip; (6) phone numbers; (7) network/application diagram; (8) printed email; (9) printed meeting documents; (10) employees and their designation; (11) credit card reciepts; (12) employee names*.[252] Sebuah studi lainnya yang dilakukan terhadap 25 praktisi IT di New Zealand sempat mengungkapkan jika dampak dari *dumpster diving* salah satunya adalah kehilangan informasi rahasia hingga dana.[253]

Kerentanan lainnya dalam serangan *social engineering* adalah kebiasaan seseorang yang kerap membuang dokumen berupa tagihan laporan keuangan yang kerap mengungkapkan informasi sensitif seperti nomor rekening, nomor kartu kredit dan sebagainya yang berpotensi digunakan oleh penyerang untuk berpura-pura menjadi korban untuk mendapatkan akses ke rekening bank atau kartu kredit.

---

[250]Kevin D. Mitnick dan William L. Simon, *Op.Cit*., hlm. 157.

[251]Wtae, "Medical Record Found Trahsed In Dumpster", *WTAE*, 21 Maret 2017, https://www.wtae.com/article/medical-records-found-trashed-in-dumpster/9160857 (diakses pada 29 Mei 2022).

[252]Murtaza Ahmed Siddiqi, *et.al.*, "A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures", *Applied Science*, Vol. 12, 2022, hlm. 4.

[253]Lech J. Janczewski dan Lingyan Fu, "Social Engineering-Based Attacks: Model and New Zealand Perspective", *Proceedings of the International Multiconference on Computer Science and Information Technology*, 2010, hlm. 851.

Terkait target perusahaan, baik perusahaan di bidang teknologi, firma hukum maupun farmasi memiliki kerentanan yang serupa. Perusahaan pengembang aplikasi dapat membuang dokumen berharga terkait kode program, firma hukum dapat membuat dokumen yang berkaitan dengan kasus tertentu dan perusahaan farmasi dapat memiliki *bluprints* komposisi kimia obat baru yang telah dalam pengembangan dan belum dipasarkan.[254]

Tidak hanya dokumen, beberapa orang dan perusahaan kerap membuang komputer, laptop atau *flashdisk* yang telah tidak terpakai. Sebagian besar orang menilai, sukar untuk memanfaatkan data yang berada dalam perangkat tersebut karena telah rusak atau telah dihapus. Namun, perlu diketahui bahwa beragam peralatan dan *software* saat ini dengan mudah untuk dapat memulihkannya, bahkan diketahui untuk dapat memastikan data yang terhapus sepenuhnya, seseorang perlu melakukan hingga 7 proses tahapan melalui program khusus. *Hard drive* yang diproduksi saat ini telah memiliki program bawaan untuk melakukan penghapusan data secara aman, yakni *secure erase*. Namun, sebelum dapat digunakan, perlu dilakukan pengaktifan pada BIOS *motherboard* karena sebagian besar sistem menonaktifkan fitur tersebut secara *default*.[255]

[254]Robert B. Fried, *Loc. Cit*.

[255]Robert M. Weaver dan Joseph A. Cazier, *Dumpster Diving: A Study on Data Recovery and Exploitation* (Southeast Institute for Operation Research and the Management Science Conference, 2007), pp. 1-4, hlm. 1-2.

Kasus Oracle

Pada tahun 2020, perusahaan pesaing Microsoft, Oracle telah mengakui melakukan aksi memata-matai Microsoft serta rekanannya dengan cara menggali informasi melalui sampah perusahaannya. Oracle diduga merupakan aktor yang membiayai aksi seseorang yang diketahui telah menyuap petugas kebersihan untuk mendapatkan sampah yang dibuang oleh perusahaan rekanan Microsoft, yakni *Association for Competitive Technology* (ACT). Seorang wanita yang mengidentifikasi dirinya sebagai Blanca Lopes menawarkan uang tunai $700 kepada petugas kebersihan untuk dokumen sampah milik ACT.

Oracle mengakui apabila telah menggunakan jasa detektif dari *Investigative Group International* (IGI) untuk mendapatkan informasi perihal aksi penentangan gugatan antimonopoli yang ditujukan kepada Microsoft. CEO Oracle, Larry Ellison adalah pendukung gugatan antimonopoli tersebut, dan kerap memberikan dokumen kepada pemerintah untuk membantu proses penyelidikan.

Oracle mendapatkan manfaat dari gugatan tersebut, saham Oracle ketika itu naik sekitar 4%, serta menjadikan Ellison orang terkaya di dunia saat itu.

Untuk informasi lebih lanjut terkait **Kasus Oracle,** Anda dapat *scan QR code* di samping.[256]

Tim Tiger

Sebuah kelompok *social engineering* dalam satu episode Tim Tiger menunjukkan bagaimana mereka menggunakan kantong sampah untuk menemukan detail berharga tentang target. Di tempat sampah tim menemukan nama tim teknisi. Kemudian, mereka dapat mengirim anggota untuk bertindak sebagai karyawan teknisi dan diberi akses penuh ke server mereka.[257]

Untuk informasi lebih lanjut terkait **Tim Tiger**, Anda dapat melihat video dengan *scan QR code* di samping.

[256]Declan Mccullagh, "Twas Oracle That Spied on MS", *Wired*, 28 Juni 2000, https://www.wired.com/2000/06/twas-oracle-that-spied-on-ms/ (diakses pada 29 Mei 2022).

[257]Security Through Education, "Dumpster Diving", *Social Engineer Org*, https://www.social-engineer.org/framework/information-gathering/dumpster-diving/ (diakses pada 29 Mei 2022).

Kasus Greenwood

Pada tahun 1988 Mahkamah Agung Amerika Serikat menyidangkan kasus California v. Greenwood. William Greenwood, seorang tersangka pengedar narkoba, sampahnya telah diperiksa oleh petugas kebersihan atas permintaan petugas polisi Laguna Beach California. Setelah pemeriksaan sampah oleh penegak hukum, bukti yang berkaitan dengan penyalahgunaan narkoba ditemukan. Setelah penemuan ini, surat perintah dikeluarkan untuk memungkinkan penggeledahan di rumah Greenwood. Penggeledahan ini menghasilkan temuan barang bukti terkait penyalahgunaan narkoba. Greenwood ditangkap atas tuduhan kejahatan narkoba. Ketika proses persidangan di Mahkamah Agung California, dinyatakan bahwa, "inspeksi sampah yang tidak berperikemanusiaan melanggar *the Fourth Amandment"*. Selanjutnya, pengadilan menyimpulkan, "kemungkinan penyebab penggeledahan kediaman Greenwood tidak akan ada tanpa bukti yang diperoleh dari pemeriksaan sampah ilegal, dan oleh karena itu, semua bukti yang disita dari kediaman harus dihentikan dan semua tuduhan terhadap Greenwood dibatalkan."

Mahkamah Agung Amerika Serikat akhirnya membatalkan keputusan Mahkamah Agung California dengan suara 6-2. Majelis Hakim Mahkamah Agung Amerika Serikat merasa bahwa seseorang tidak boleh mengharapkan privasi apa pun dalam sampah yang ditinggalkan untuk diambil. Majelis Hakim menyatakan, "telah menjadi rahasia umum bila kantong sampah plastik yang ditinggalkan atau ditaruh pada sisi jalan umum mudah diakses oleh hewan, anak-anak, pemulung, pengintai, dan anggota masyarakat lainnya." Selanjutnya dinyatakan, "Apa yang secara sadar diekspos ke publik, bahkan di rumah atau kantornya sendiri, bukanlah subjek perlindungan *the Fourth Amandment"*.

Untuk informasi lebih lanjut terkait **Kasus Greenwood,** Anda dapat *scan QR code* di samping.

Kasus Modul Pemalsuan Dokumen

Dua pelaku pembobolan tiga bank daerah tertangkap pada tahun 2020 oleh Polda Sumatra Selatan. Modus yang dilakukan oleh para pelaku adalah dengan cara memanfaatkan struk sampah yang ditinggalkan di ATM. Apabila saldo yang tertera besar, pelaku akan langsung mengambilnya. Setelah itu pelaku akan memalsukan identitas korban, berupa KTP dan buku tabungan milik korban. Hingga akhirnya pelaku menarik uang di bank dengan modus tertinggal kartu ATM. Aksi ini pertama kali dilakukan pada tahun 2018 di BPD Lampung senilai Rp70 juta, kemudian Bank Sultra di Kendari senilai Rp120 juta, dan terakhir Bank Sumsel Babel senilai Rp116 juta. Diketahui bahwa, pelaku mendapatkan data korban dari *website* pemilih milik Komisi Pemilihan Umum (KPU). Atas perbuatannya pelaku terancam Pasal 372, 378, dan 263 KUHP.

Untuk informasi lebih lanjut terkait **Kasus Pemalsuan Dokumen,** Anda dapat *scan QR code* di samping.[258]

I. Shoulder Surfing

Shoulder surfing didefinisikan sebagai tindakan pengamatan terhadap seseorang yang tengah memasukkan kata sandi tanpa sepengetahuannya. Secara historis, lazimnya tindakan dilakukan dengan melihat kata sandi dari balik bahu seseorang ketika tengah duduk di terminal.[259] Peristiwa yang sangat mungkin dilakukan dan diduga pernah dilakukan sebagian orang dengan niat jahat atau iseng belaka. Namun, terdapat ketimpangan studi perihal penyerangan *shoulder surfing* dan upaya menciptakan sistem yang dapat mengurangi penyerangan *shoulder surfing*. Penelusuran yang dilakukan melalui Google Scholar ditemukan setidaknya 4.640 karya tulis yang telah diterbitkan sejak 2007 tentang *shoulder surfing*, namun informasi kasus *shoulder surfing* minim untuk diketahui. Laporan pada

[258]Candra Setia Budi, "Fakta Kasus Pembobolan Rp 300 Juta dari 3 Bank, Manfaatkan Sampah Struk ATM, Gunakan Data dari Website KPU", *Kompas*, 24 Juli 2020, https://regional.kompas.com/read/2020/07/24/16242951/fakta-kasus-pembobolan-rp-300-juta-dari-3-bank-manfaatkan-sampah-struk-atm?page=all (diakses pada 30 Mei 2022).

[259]Furkan Tari, *et.al.*, "A Comparison of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical Passords", *Proceedings of the 2nd Symposium on Usable Privacy and Security (SOUPA)*, Pennsylvania, 12-14 Juli 2014, DOI: 10.1145/1143120.1143128, hlm. 2.

tahun 2014 menunjukkan 11 pengguna ponsel yang merasakan risiko dari serangan *shoulder surfing* dari jumlah 3.410 responden (0,3%).[260]

Studi yang dilakukan oleh Malin Eiband menggambarkan temuan terkait serangan *shoulder surfing* yang hadir,[261] yakni sebagai berikut.

1. *Shoulder surfing* sesungguhnya terjadi dalam banyak peristiwa, namun korban kerap tidak menyadari.
2. Penyerang bersifat oportunistik dan jarang bertindak karena alasan di luar rasa ingin tahu dan bosan.
3. *Shoulder surfing* memberikan dampak pada informasi pribadi dan membangkitkan perasaan negatif pada korban.
4. Teks diamati dalam banyak kasus, diikuti oleh gambar dan permainan. Umumnya terjadi pada pesan instan dan aktivitas media sosial.
5. *Shoulder surfing* menempatkan kredensial autentifikasi seperti PIN, kata sandi, dan pola lainnya dalam keadaan terancam.
6. Korban menyesuaikan strategi koping terhadap penyerang berdasarkan pengamatan yang terjadi.
7. *Shoulder surfing* membocorkan informasi pribadi tentang orang ketiga melalui konten yang berinteraksi dengan korban.

[260]Malin Eiband, *et.al.,* "Understanding Shoulder Surfing in the Wild: Stories from User and Observers"*, Procedings of the 2017 CHI Conference on Human Factors in Computing Systems,* Denver, Mei 2017, pp. 4254-4265, DOI: 10.1145/3025453.3025636, hlm. 4254.

[261]*Ibid.,* hlm. 4261-4262.

Gambar 32. Ilustrasi *Shoulder Surfing*[262]

Beragam upaya telah dikaji guna memastikan berkurangnya kerentanan seseorang ketika menggunakan kata sandi agar terhindar dari praktik *shoulder surfing*, salah satunya dengan konsep *graphical password*. Namun, metode ini pun tidak sepenuhnya tanpa celah. Arash mengungkap setidaknya 16 pembahasan terkait dengan *shoulder surfing* dan alternatif autentifikasi menggunakan *graphical password*, yaitu sebagai berikut.[263]

1. Metode autentikasi komputer yang paling umum adalah menggunakan nama pengguna dan kata sandi alfanumerik. Metode ini telah terbukti memiliki kelemahan yang signifikan. Misalnya, pengguna cenderung memilih kata sandi yang mudah ditebak. Di sisi lain, bila kata sandi sulit ditebak, maka sering kali sulit untuk diingat.
2. *Graphical password* mengatasi masalah *shoulder surfing* tanpa memberikan kerumitan ekstra dalam prosedur autentifikasi.

[262]Anastasia Shuraeva, "Woman in White Long Sleeve Shirt Holding Black Smartphone", *Pexels*, https://www.pexels.com/photo/woman-relaxation-internet-writing-5704404/ (diakses pada 30 Mei 2022). Gambar digunakan sesuai dengan ketentuan Pexels "*free to use*".

[263]Arash Habibi Laskhari, *et.al.,* "Shoulder Surfing Attack in Graphical Password Authentication", *International Journal of Computer Science and Information Security*, Vol. 6, No. 2, 2009, pp. 145-154, hlm. 145-152.

3. Sebuah langkah lainnya yang dikenal dengan *pass-thought*, yang memungkinkan pengguna melakukan autentifikasi pada perangkat dengan "mentransmisikan" pikirannya. Transmisi ini dilakukan melalui *Brain Computer Interface* (BCI) yang dirancang khusus. Keuntungan dari *pass-thought* adalah kekuatan dalam menghadapi serangan *shoulder surfing*, akan tetapi kebutuhan perangkat serta berbiaya tinggi menjadi kendala.
4. Penyerang dapat memperoleh kata sandi dengan pengamatan langsung atau dengan merekam proses autentifikasi saat seseorang memasukkan kata sandi di depan umum.
5. Sebuah studi menunjukkan bahwa kata sandi grafis lebih mudah diingat daripada kata sandi non-kamus atau kata sandi alfanumerik yang kuat. Ditemukan dalam studi tersebut bahwa saat ini lahir keprihatinan perihal peningkatan daya ingat yang dapat menyebabkan peningkatan kerentanan kata sandi grafis dari serangan *shoulder surfing*.
6. Kelemahan potensial dari skema kata sandi grafis adalah bahwa langkah tersebut lebih rentan terhadap serangan *shoulder surfing* dibandingkan kata sandi teks alfanumerik konvensional.
7. Serangan *shoulder surfing* merupakan masalah yang sukar diatasi.
8. Untuk mendapatkan akses pada suatu sistem komputer, seorang pengguna memerlukan proses autentifikasi. Umumnya, pengguna diminta untuk memasukkan nama pengguna dan kata sandi alfanumerik. Pengguna biasanya diminta untuk mengingat beberapa kata sandi untuk sistem yang berbeda dan keadaan ini menimbulkan masalah seperti peruntukan, daya ingat serta keamanan.
9. Sandi tekstual rentan terhadap serangan *shoulder surfing*, kamera tersembunyi, dan *spyware*. Skema kata sandi grafis telah diusulkan sebagai alternatif yang memungkinkan untuk skema berbasis teks.
10. Upaya menggunakan kata sandi berbasis gambar belum berfokus pada upaya mempertahankan tingkat entropi yang tinggi. Karena sistem kata sandi biasanya memungkinkan pemilihan kata sandi oleh pengguna, entropi mereka yang sebenarnya tetap tidak diketahui.
11. Salah satu praktik umum yang terkait dengan kata sandi alfanumerik adalah menuliskannya atau membaginya dengan teman atau kolega

terpercaya. Skema kata sandi grafis sering mengklaim keuntungan bahwa mereka secara signifikan lebih aman sehubungan dengan pengungkapan verbal dan penulisan.

12. Autentikasi pengguna adalah salah satu topik penting dalam keamanan informasi. Skema kata sandi tradisional yang kuat dapat memberikan tingkat keamanan tertentu. Namun, fakta bahwa kata sandi yang kuat sulit untuk dihafal sering membuat pemiliknya menuliskannya di kertas atau bahkan menyimpannya di file komputer. Akibatnya, keamanan menjadi sangat terganggu.
13. Kata sandi alfanumerik banyak digunakan dalam autentikasi komputer dan jaringan untuk melindungi privasi pengguna. Namun, sudah diketahui bahwa kata sandi berbasis teks yang panjang sulit diingat orang, sedangkan kata sandi yang lebih pendek rentan terhadap serangan.
14. Ancaman seperti *key-loggers*, kata sandi yang lemah, dan *shoulder surfing*, memaksa pengguna untuk mengingat kata sandi yang berbeda atau membawa token yang berbeda, proses "pembiasaan" atau "pengaturan kata sandi" yang panjang adalah kelemahan sistem autentikasi saat ini.
15. Mekanisme *two factor authentication* dinilai aman untuk mengautentikasi pengguna di lingkungan berbasis internet. Oleh karena jumlah layanan yang disediakan secara *online* semakin hari semakin meningkat, pengguna yang ingin menggunakan berbagai layanan *online* juga semakin meningkat. Dengan setiap layanan yang mengharuskan pengguna untuk mendaftar secara terpisah, upaya mengingat banyak pasangan ID/sandi telah menyebabkan masalah daya ingat. Untuk mengatasi hal ini, para peneliti telah mengusulkan mekanisme untuk lingkungan *multi-server* di mana pengguna perlu mendaftar dengan satu pusat pendaftaran menggunakan satu pasangan ID/sandi dan dengan demikian mengakses semua layanan yang terdaftar melalui server itu.
16. Untuk mengatasi kerentanan metode tradisional, skema kata sandi visual atau grafis telah dikembangkan. Walaupun mengadopsi autentikasi kata sandi grafis juga memiliki beberapa kelemahan, beberapa skema hibrida berdasarkan grafik dan teks tengah dikembangkan.

Kelemahan lain yang diketahui terkait kata sandi terhadap serangan *shoulder surfing* adalah terbatasnya ruang kata sandi yang dimiliki oleh sistem berbasis *seacrhmetrics*. Karena penyerang dapat meluncurkan *brute-forcing attack* dengan menggunakan data dari beberapa informasi untuk menyimpulkan kata sandi. Salah satu upaya untuk mengurangi *brute-forcing attack* adalah dengan menambah ruang kata sandi karena sukarnya sistem untuk memiliki jumlah memori yang dibutuhkan untuk merekam sebagian besar dari semua kemungkinan kata sandi.[264]

Data yang diungkap oleh Kapersky menyebutkan bila terdapat 2.847.706 kali upaya serangan *brute force attack* terhadap penggunaan *Remote Desktop Protocol* (RDP) di Indonesia pada semester pertama 2021.[265] Penelitian yang dilakukan oleh Nord Pass pada 50 negara, mengungkap 200 *password* yang umum dipakai oleh pengguna internet pada 2021. Sepuluh peringkat teratas *password* yang ditemukan, dan dapat dipecahkan dalam waktu kurang dari 1 detik yakni:[266]

1. 123456;
2. 123456789;
3. 12345;
4. qwerty;
5. *password*;
6. 12345678;
7. 111111;
8. 123123;
9. 1234567890;
10. 1234567.

---

[264]Peng Foong Ho, *et.al.*, "Preventing Shoulder-Surfing Attack with the Concept of Concealing the Password Object' Information", *The Scientific World Journal*, Vol. 2014, pp. 1-12, DOI: 10.1155/2014/838623, hlm. 10.

[265]Faisal Hafis, "Lebih dari 20 Juta Kali Terdeteksi Upaya 'Brute Force Attack' di Indonesia", *Cyberthreat*, 16 November 2021, https://cyberthreat.id/read/12852/Lebih-dari-20-Juta-Kali-Terdeteksi-Upaya-Brute-Force-Attack-di-Indonesia (diakses pada 30 Mei 2022).

[266]Nord Pass, "Top 200 Most Common Passwords", *Nord Pass*, https://nordpass.com/most-common-passwords-list/ (diakses pada 2 Juni 2022).

APA ITU *BRUTE FORCE ATTACK?*[267]

Histori nama *brute force* sebenarnya adalah sebuah *game* untuk PC yang dirilis pada tahun 2000. *Brute force* adalah sebuah *third-person shooter* dan terdiri dari beberapa karakter. Masing-masing dengan kekuatan dan kemampuannya sendiri. Tujuannya adalah untuk menemukan beberapa karakter lain yang dapat diandalkan untuk bersatu. Sebuah tim dibentuk bernama "tim *brute force*" untuk menandakan perkumpulan tersebut. Misi tim adalah untuk menemukan dan bertarung dengan alien dan angkatan bersenjata. Setiap kali alien ini terlihat, anggota tim *brute force* bertarung dengan mereka. *Brute force attack* sendiri merupakan serangan yang menggunakan metode "*Trial and Error*" untuk menebak *password*. Penyerang pertama-tama mengumpulkan informasi mendasar tentang pengguna. Misalnya, nama lengkap pengguna, nomor kamar, nomor kendaraan, nama anak, dan lain-lain.

Penyerang terus mencoba kata sandi acak berdasarkan informasi pribadi pengguna. Penyerang mencoba ini sampai dia berhasil. Ini mungkin memakan waktu berjam-jam, berhari-hari, berbulan-bulan, dan bertahun-tahun juga. Semakin tinggi jenis skema enkripsi (32, 64, 128, 168-bit, dan lain-lain) yang digunakan, semakin banyak waktu yang dibutuhkan. *Brute force attack* juga dikenal sebagai "*Dictionary Attack*" atau "*Hybrid Brute-Force Attack"*.

Apabila situs web memerlukan autentikasi pengguna untuk melewatinya maka itu akan menjadi target yang bagus untuk *brute force attack*. Serangan tersebut merupakan upaya untuk menentukan kata sandi dengan secara analitis mencoba setiap kemungkinan kombinasi huruf, angka, simbol, dan lain-lain. Akan tetapi, hambatannya adalah bahwa perlu waktu yang lama (yaitu tahun) untuk menemukannya, tergantung pada kompleksitas dan lamanya kata sandi. Banyak orang ingin memilih kata kamus yang bermakna daripada memilih kata sandi acak. Apabila penyerang menyerang berdasarkan kata-kata kamus yang tepat, maka itu dikenal sebagai "*Dictionary attack"*. Dan bila penyerang sedikit memodifikasi kata-kata kamus dan melakukan serangan, dikenal sebagai "*Hybrid Brute-Force Attack"*.

[267]Konark Truptiben Dave, "Brute-force Attack "Seeking but Distressing", *International Journal of Innovations in Engineering and Technology*, Vol. 2, Issue 3, Juni 2013, pp. 75-78, hlm. 75-76.

Kasus ATM Milpitas

Pada Januari 2015, seorang karyawan Bank of America melaporkan seorang wanita yang berkeliaran di dekat mesin ATM. Diduga wanita tersebut tengah mengawasi pengguna ATM dari dalam mobil yang tengah diparkir. Petugas kepolisian, mengonfirmasi kepada wanita tersebut dengan bantuan pihak bank untuk mengetahui apakah terdapat aktivitas kejahatan yang terjadi. Akhirnya diketahui bila terdapat dua korban penipuan penarikan ATM yang terjadi. Dalam penyelidikan awal, diketahui bahwa korban menggunakan ATM di bank pada 2 Januari 2015 dan mungkin secara tidak sengaja meninggalkan ATM sebelum proses selesai sepenuhnya. Setelah korban menyelesaikan transaksi dan mendapatkan tanda bukti, segera bergegas keluar dari ATM karena menduga proses telah selesai. Namun, terdapat *prompt* di layar ATM yang menanyakan apakah terdapat transaksi lain yang diinginkan dan *prompt* tersebut mungkin akan tetap ada di layar selama beberapa detik, bahkan setelah pengguna ATM pergi. Hanya PIN yang diperlukan untuk melakukan transaksi lain, dan apabila seseorang mengawasi pengguna ATM, maka PIN dapat diperoleh.

Untuk informasi lebih lanjut terkait **Kasus ATM Milpitas,** Anda dapat *scan QR code* di samping.[268]

Kasus Ayanna Bastain

Pada 25 Januari 2015, detektif dari Walnut Creek *Police Department* melakukan operasi penangkapan di Bank of America guna mengidentifikasi orang yang bertanggung jawab dalam beberapa peristiwa kejahatan melalui *shoulder surfing* dari ATM. Akhirnya, kecurigaan ditujukan kepada Ayanna Bastain dari Pittsburg, karena teridentifikasi melalui foto pengawasan dari aksi *shoulder surfing* terjadi sebelumnya di Walnut Creek pada November dan Desember 2014 dan ditangkap. Bastain ditahan atas tuduhan pencurian identitas dan penyalahgunaan.

Untuk informasi lebih lanjut terkait **Kasus Ayanna Bastain,** Anda dapat *scan QR code* di samping.

[268]Lieutenant Henry Kwong, *ATM Shoulder Surfing,* Press Release, Milpits Police Department, Case 15-002-067, 15 Januari 2015.

Kasus pada Kepolisian Fremont

Kepolisian Fremont menyelidiki aktivitas penipuan yang terjadi pada dua mesin ATM Bank of America yang terjadi pada 17 dan 18 Maret 2015. Selama insiden tersebut, pelaku memperoleh kode akses korban dengan teknik *shoulder surfing* pada mesin ATM. Pada tanggal 17 Maret 2015, peristiwa tersebut terjadi di cabang Irvington dan pada tanggal 18 Maret terjadi di lokasi Beacon Street. Petugas telah menemukan dua korban, namun meyakini terdapat korban lain yang tidak menyadarinya.

Untuk informasi lebih lanjut terkait **Kasus pada Kepolisian Fremont,** Anda dapat *scan QR code* di samping.

Kasus Daniel Jermaine Usher

Hakim federal telah menghukum Daniel Jermaine Usher dari Los Angeles atas tiga tuduhan pencurian identitas berat dengan menggunakan kode rahasia Bank of America untuk melakukan penarikan ilegal pada mesin ATM yang berlokasi di Los Angeles dan Orange Country. Daniel mengakui bila telah melakukan kejahatannya, dengan teknik *shoulder surfing* dalam mendapatkan nomor PIN korbannya. Daniel berkeliaran di dekat ATM Bank of America dan diam-diam mengawasi korban saat memasukkan PIN dalam bertransaksi. Ketika korban meninggalkan ATM tanpa menyelesaikan seluruh proses hingga akhir, Daniel dengan cepat memasukkan kembali PIN yang dia dapatkan dan kemudian menarik uang tersebut. Korban yang menjadi target Daniel adalah orang lanjut usia dan minoritas, tiga korbannya membutuhkan penerjemahan dalam proses persidangan.

Untuk informasi lebih lanjut terkait **Kasus Daniel Jermaine Usher,** Anda dapat *scan QR code* di samping.[269]

[269]Thom Mrozek, "L.A. Man Convicted of ATM 'Shoulder Surfing' that Allowed Him to Withdraw Cash after Bank Customers Left ATMs", *The United States Attorney's Office Central District of California,* 26 Februari 2018, https://www.justice.gov/usao-cdca/pr/la-man-convicted-atm-shoulder-surfing-allowed-him-withdraw-cash-after-bank-customers (diakses pada 2 Juni 2022).

Kasus *Shoulder Surfing* di Indonesia

November 2019, aksi komplotan yang menguras isi ATM korbannya ditangkap di Surabaya. Kelompok tersebut beranggotakan empat orang, yang salah satunya bertugas untuk mengintip PIN ATM korban ketika mengambil uang setelah sebelumnya ditawari investasi menarik dari tiga anggota komplotan lainnya. Target korbannya adalah penghuni hotel yang teridentifikasi karena menggunakan sandal hotel. Eko Supriyanto, warga Kalimantan Tengah kehilangan Rp60 juta setelah sebelumnya bertemu komplotan tersebut di lobi hotel.[270]

Kasus lainnya terjadi di Kota Makassar pada tahun 2021, yang dilakukan oleh seorang karyawan rumah sakit terhadap rekannya. Pelaku telah mencuri kartu ATM korban sejak lama. Ketika menginap di kamar kost korban, dan ketika korban mandi, pelaku mengambil kartu ATM dalam tas korban. Pelaku mengetahui PIN ATM, ketika menemani korban menarik uang. Pelaku mengambil Rp5 juta dari ATM korban. Kejadian ini terungkap, setelah melihat CCTV minimarket dan mengetahui aktivitas pelaku ketika menggunakan ATM korban.[271]

Kasus serupa dengan jumlah kerugian yang besar terjadi pada tahun 2020. Komplotan pelaku berhasil mencuri uang korban hingga Rp1,14 miliar. Komplotan pelaku yang berjumlah 6 orang melakukan aksinya pada pertengahan Januari 2020. Korban bertemu pelaku pada salah satu hotel mewah dan mengaku berasal dari Brunei Darussalam. Pelaku menawarkan kerja sama bisnis gawai, dengan tawaran keuntungan 15% dari setiap penjualan gawai. Dengan dalih tidak memiliki rekening di Indonesia, salah satu pelaku meminjam rekening korban. Korban dan pelaku akhirnya mengecek rekening korban pada mesin ATM, dan salah satu pelaku mengintip PIN yang dimasukkan oleh korban. Dalam perjalanannya pelaku sempat menukar kartu ATM korban dengan kartu palsu. Pelaku dijerat Pasal 30 ayat 3, Pasal 46 ayat 3, Pasal 363 KUHP, Pasal 55 ayat 1, Pasal 56 KUHP, serta Pasal 3, 4, dan 5 Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.[272]

Untuk dapat melihat secara lengkap Undang-Undang Republik Indonesia Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, Anda dapat *scan QR code* di samping.

[270]Wijayanto, "Komplotan Penipuan Bermodus ATM Rp. 1 M Dibekuk", *Radar Surabaya*, 6 November 2019, https://radarsurabaya.jawapos.com/read/2019/11/06/164853/komplotan-penipuan-bermodus-atm-rp-1-m-dibekuk (diakses pada 2 Juni 2022).

[271]Faisal Mustafa, "Setelah Mengintip PIN ATM, Karyawan Rumah Sakit di Makassar Kuras Tabungan Teman", *I News Sulsel*, https://sulsel.inews.id/berita/setelah-mengintip-pin-atm-karyawan-rumah-sakit-di-makassar-kuras-tabungan-teman (diakses pada 2 Juni 2022).

[272]Siti Yona Hukmana, "Sindikat Pembobol Rekening Rp. 1,14 Miliar Ditangkap", *Medcom*, 10 Maret 2020, https://www.medcom.id/nasional/hukum/aNraLz1K-sindikat-pembobol-rekening-rp1-14-miliar-ditangkap (diakses pada 3 Juni 2022).

J. Femme Fatale

Istilah *femme fatale* kerap melekat sebagai penggambaran sosok perempuan dalam dunia sastra, sinematik, dan budaya. Sebagai figur umum dalam budaya populer, *femme fatale* dianggap rakus secara seksual, tak tertahankan dan berbahaya, karena membawa pria ke dalam kehancuran.[273] Sementara Dennon menjelaskan *femme fatale* sebagai seorang wanita yang menjalankan aktivitasnya berangkat dari keinginannya untuk kekuasaan, kekayaan, kepuasan, dan dominasi. *Femme fatale* menunjukkan ambisi umum pada sebuah kelas sosial. Metode yang kerap digunakan oleh *femme fatale* untuk mencapai tujuan kerap merusak struktur sosial yang hendak coba dinaiki.[274] Pandangan lainnya menjelaskan bahwa akar *femme fatale* dari *fin-de-siècle* Inggris yang ditandai oleh kecemasan atas emansipasi perempuan, dan minat pada klasifikasi hukuman seksualitas perempuan, sebuah proyek yang sesuai dengan pemetaan imperialis kontemporer dari yang tidak diketahui. Pada akhirnya, *femme fatale* adalah tanda, sosok yang melintasi batas-batas wacana, yang dapat ditemukan di persimpangan kecemasan rasial dan seksual.[275]

Di dunia nyata, contoh nyata *femme fatale* adalah seorang wanita bernama Mata Hari yang dihukum mati karena dugaan pekerjaannya sebagai mata-mata. Mitologi Mata Hari memengaruhi proyeksi, teror, dan kecemasan tentang perempuan dan modernitas yang muncul di akhir abad ke-19.[276] *Femme fatale* dalam media fiksi Barat merupakan salah satu contoh kiasan bagi wanita populer yang memanfaatkan aspek seksismenya guna menutupi aktivitasnya sebagai pihak "musuh". Karakter-karakter ini mengerahkan kekuatan dan seksualitas, seperti yang umumnya digambarkan dalam film Amerika noir. *Femme fatale* muncul di sinema AS pasca-Perang Dunia II, ketika wanita mengalami

---

[273]Maysaa Jaber, "Sirens in Command: The Criminal Femme Fatale in American Hardboile Crime Fiction", *Thesis*, University of Manchester for the Degree of Doctor of Philosophy in the Faculty of Humanities, 2011, hlm. 8.

[274]Anne Dennon, "The Emergence of the Feminist Fatele in American Film Noir", *Master's Thesis*, Central Washington University, 2017, hlm. 2.

[275]Helen Hanson dan Catherine O'Rawe, *The Femme Fatale: Images, Histories, Contexts* (UK: Palgrave Macmillan, 2010), hlm. 3.

[276]Sandra Widya Resti dan Titien Diah Selistyarini, "From Enchantress to Murderess: The Portrayal of Amy Dunne as "Femee Fatale" in Gillian Flynn's Gone Girl", *Allusion*, Vol. 5, No. 2, 2016, hlm. 134.

kekuatan dan status baru dalam tatanan sosial. Kekhawatiran tentang peran seks, pernikahan, dan seksualitas yang memunculkan sinematik *femme fatale* yang menarik, tetapi berbahaya mencerminkan keengganan masyarakat pada gagasan tentang perempuan yang merebut masyarakat Amerika yang secara tradisional didominasi laki-laki. *Femme fatale* menyampaikan karakteristik yang mencerminkan sikap bermusuhan terhadap peran perempuan dalam budaya Barat.[277]

Dalam kaitannya dengan *social engineering*, istilah *femme fatale* sesuai dengan pandangan Sheppard yang menggambarkannya sebagai wanita yang menggunakan kekuatan manipulatif untuk membuat pria melakukan kehendak atau perintahnya, yang sering kali dengan tujuan membawa malapetaka atau bahkan fatal. Seperti Sirene yang digambarkan dalam mitologi Yunani adalah makhluk wanita cantik dan berbahaya yang memikat para pelaut untuk mengarahkan perahu mereka ke bebatuan bergerigi dengan keindahan dan manisnya lagu mereka. Dalam *The Odyssey* karya Homer, Odysseus teralihkan dari perjalanannya pulang ke Ithaca oleh Circe, seorang dewi cantik. Dia merayu dan menganggapnya sebagai kekasihnya selama setahun sebelum mengizinkannya pulang ke istrinya.[278] Maka, *femme fatale* yang dimaksud dalam buku ini menggambarkan upaya memanipulasi target atau korban yang dilakukan oleh wanita atau memanipulasi informasi sebagai wanita yang memanfaatkan daya tariknya. Beberapa contoh kasusnya adalah sebagai berikut.

[277]Jessica E. Tompkins, *et.al.,* "Kawaii Killers and Femme Fatale: A Textual Analysis of Female Characters Signifying Benevolent and Hostile Sexism in Video Games"*, Journal of Broadcasting & Electronic Media*, Vol. 6, Issue 2, 2020, hlm. 238.

[278]Leah D. Sheppard dan Stefanie K. Johnson, "The Femme Fatale Effect: Attractiveness is a Liability for Businesswomen's Perceived Thruthfulness, Trust, and Deservingness of Termination"*, Sex Roles*, Vol. 81, No. 4, 2019, hlm. 4.

Kasus Safeena Malik

Pada tahun 2017, seseorang mengakui dirinya sebagai Safeena Malik, sesosok wanita yang terlihat seperti hipster milenial dalam foto profil Facebook-nya, akustik string nilon di tangan dan semua senyum di taman, serta mengaku memiliki beberapa rahasia sensitif. Pada suatu waktu, dalam sebuah pesan kepada Konfederasi Serikat Buruh Internasional, sebuah federasi serikat pekerja yang berbasis di Brussels dan memiliki 168 juta anggota, Malik menawarkan penelitian tentang pendanaan kelompok teroris ISIS. Tahun sebelumnya, Malik menjanjikan materi tentang hak-hak pekerja Qatar kepada seorang jurnalis investigasi, sehubungan dengan laporan yang mengutuk perlakuan terhadap para migran yang membantu membangun stadion untuk Piala Dunia FIFA 2020. Pada tahun yang sama, Malik meminta bantuan untuk presentasi tentang perdagangan manusia, mengirimkan PDF ke para aktivis yang dia yakini dapat berkontribusi.

Dalam semua kasus, Malik meminta penerima untuk membuka tautan Google Documents. Namun, siapa pun yang mengekliknya berada dalam bahaya, kehidupan digital mereka akan terekspos, karena ternyata itu merupakan sebuah upaya *phishing*. Tautan tersebut mengarahkan target ke halaman *login* Google yang meyakinkan, tetapi palsu. Segera setelah kredensial dimasukkan, target dibawa ke dokumen yang di-*hosting* Google yang tampak asli. Sementara itu, di latar belakang, *username* dan *password* Google korban dikirim kembali kepada Malik.

Pada akhir 2016, diketahuilah bahwa Safeena Malik adalah sosok palsu yang memiliki tujuan untuk memata-matai para aktivis, jurnalis, dan serikat pekerja yang menangani masalah hak asasi manusia di seluruh Qatar. Sementara satu tautan teknis menunjukkan lokasi peretas yang berbasis di Qatar. Selama dua tahun terakhir, persona Malik telah berusaha mencuri *login* Google dari sebanyak 38 target yang berbeda. Amnesty dan FORBES merahasiakan nama-nama mereka yang ditargetkan karena kekhawatiran tentang dampak pengungkapan identitas. ITUC setuju untuk disebut sebagai target, mencatat bahwa mereka tidak percaya akun Google pekerjanya berhasil dilanggar.

Selama waktu itu, guna memberinya kredibilitas dengan targetnya, Malik mengembangkan kehadiran *online* yang rumit. Sejak pertama kali muncul secara *online* pada tahun 2014, Malik membangun profil LinkedIn dengan lebih dari 500 koneksi dan ratusan dukungan. Diyakini bahwa Malik turut membeli teman dan kontak, karena akun Google Plusnya tertaut ke berbagai layanan untuk meningkatkan profil *online*, termasuk pengoptimalan mesin telusur dan komentar berbayar, di antara ratusan iklan untuk banyak sekali produk seperti alat peretas WhatsApp, aplikasi untuk memata-matai orang yang dicintai dan terapi pijat.

Untuk informasi lebih lanjut terkait **Kasus Safeena Malik,** Anda dapat *scan QR code* di samping.[279]

[279]Thomas Brewster, "This Fake Femme Fatale Is Stealing Google Accounts From Journalists and Human Rights Activists", *Forbes*, 14 Februari 2017, https://www.forbes.com/sites/thomasbrewster/2017/02/14/safeena-malik-qatar-fake-cyberespionage-hacking-campaign/?sh=5e134f99435a (diakses pada 2 Juli 2022.

Tes Emily Williams

Dua orang peneliti berhasil melancarkan serangan siber terhadap badan pemerintah AS yang tidak dikenal hanya dengan memanfaatkan akun LinkedIn dan Facebook palsu yang menyamar sebagai wanita muda yang menarik dan cerdas. Peneliti tersebut membuat profil media sosial sebagai seorang gadis cantik berusia 28 tahun bernama Emily Williams. Melalui aksinya, mereka berhasil menipu pegawai pemerintah dari laptop dan kredensial jaringan yang sangat rahasia. Tidak hanya itu, mereka berhasil membujuk staf pada institusi yang dikenal dengan pertahanan dunia mayanya, untuk mengeklik *e-card* rusak dan memperoleh kata sandi, dokumen rahasia termasuk informasi tentang serangan yang disponsori negara dan pemimpin negara.
Aksi ini merupakan langkah uji keamanan, yang dilakukan oleh karyawan World Wide Technology Aamir Lakhani dan Joseph Muniz. Tes tersebut dimulai dengan menciptakan Emily Williams, 28 tahun, lulusan MIT fiktif dengan 10 tahun pengalaman TI, lengkap dengan profil media sosial palsu yang berfungsi penuh. Untuk ini Lakhani mencari dan mendapatkan izin dari seorang pramusaji lokal di sebuah Hooters dekat dengan petugas agen yang ditargetkan. Tidak hanya itu, para peneliti memperkuat profil palsunya dengan membuat profil palsu di situs web dan forum lain, hingga mem-*posting* di MIT dengan menggunakan namanya.

Untuk informasi lebih lanjut terkait **Tes Emily Williams,** Anda dapat *scan QR code* di samping.[280]

[280]James Nye, "How 'High-Level U.S. Government Agency' Fell for Fake Femme Fatale Created by Two Hackers", *Dailymail*, 4 November 2013, https://www.dailymail.co.uk/news/article-2486975/How-fake-Femme-fatale-created-hackers-carried-cyber-attack-high-level-U-S-government-agency.html (diakses pada 2 Juli 2022).

BAB 3
POTENSI MASALAH AKIBAT SERANGAN

A. Dampak Mengeklik Tautan pada Serangan *Phishing*

Pada laporan yang dirilis oleh Keepnet Labs dengan tajuk *Phishing Trend Report 2020*, diketahui bahwa dari 410.000 *email phishing* yang dianalisis, ditemukan bahwa 1 dari 2 karyawan cenderung membuka dan membaca *email phishing*, 1 dari 3 cenderung mengeklik tautan pada *email phishing* atau mengunduh lampiran, dan 1 dari 8 karyawan membagikan informasi yang diminta dalam *email phishing*.[281] Penelitian dengan hasil yang mendekati turut dilakukan oleh Alwanain yang melakukan *experiment* dengan mengirimkan 1.500 *email phishing* kepada 1.500 orang dan ternyata *email* tersebut dibuka oleh 580 orang.[282] Tidak hanya itu, dalam sebuah penelitian dalam bidang kesehatan diketahui bahwa 14,2% dari *email phishing* diklik oleh karyawan. Sekalipun organisasi telah mengambil langkah-langkah untuk mengatasi masalah ini dengan menyediakan program pelatihan untuk mendidik dan meningkatkan kesadaran keamanan siber, tetapi upaya ini tetap tidak cukup. Oleh karena diketahui bahwa program pelatihan wajib tidak membuat perbedaan besar dalam mengurangi tingkat klik pada tautan *phishing*.

[281]Keepnet Labs, *Phishing Trends Report 2020,* 2020, hlm. 4-5.

[282]Mohammed I. Alwanain, *"*An Evaluation of User Awareness for the Detection of Phishing Emails*", International Journal of Advanced Computer Science and Applications*, Vol. 10, No. 10, 2019, hlm. 326.

Hasil penelitian menemukan 70% rumah sakit gagal menetapkan atau menegakkan privasi dan tindakan keamanan yang memadai.[283]

Sebagian besar tautan *phishing* dikirim melalui *email* dan dirancang untuk menipu penerima agar mengunduh virus, memberikan nomor kartu kredit, memberikan informasi pribadi (seperti nomor induk kependudukan) atau menawarkan informasi akun atau *login* kepada situs web tertentu. Sering kali, *email* ini dibuat dengan baik agar terlihat persis seperti pemberitahuan resmi dari situs yang dikenal dan nyaman oleh target, yang dapat menyulitkan untuk mengetahui apakah seseorang telah mengeklik tautan *phishing* atau tidak. Untuk menentukan apakah seseorang telah menerima tautan *phishing*, pastikan inkonsistensi pada alamat *email*, tautan, dan domain pengirim. Arahkan kursor ke atas tautan sebelum mengeklik untuk melihat pratinjau URL yang dituju (kemungkinan dalam *pop-up* dekat kursor atau sudut bawah layar). Apabila domain tidak ada, dimungkinkan merupakan tautan *phishing*.

Tanda bahaya lain yang dapat mengidentifikasi tautan *phishing* adalah permintaan yang tidak biasa atau mendesak dan bahasa yang berisi kesalahan di dalam *email* itu sendiri. Mengeklik tautan *phishing* atau membuka lampiran (*attachment)* pada pesan diterima seseorang dapat membuka peluang terpasangnya (*install) malware*, seperti virus, *spyware*, atau *ransomware* pada perangkatnya. Ini semua dilakukan di belakang layar, sehingga sukar terdeteksi oleh rata-rata pengguna. Perlu diketahui, sukar atau tidak mungkin bagi peretas untuk dapat mencuri data target atau memasang virus di komputer hanya dengan membuka *email spam*. Pada umumnya, pemrograman di balik *email* mengharuskan pengguna mengunduh lampiran atau mengeklik tautan *phishing* di dalam *email* untuk menginfeksi perangkat.

Sehingga dampak yang terjadi setelah mengeklik tautan *phishing* akan sangat bergantung situasi spesifik yang dialami oleh korban. Terdapat beberapa hal yang mungkin terjadi setelah mengeklik tautan *phishing*, yakni sebagai berikut.

1. Peretas Dapat Menerima Informasi dari atau tentang Korban

   Apabila seseorang telah mengeklik tautan *phishing*, penyerang akan secara otomatis menerima beberapa data dasar, seperti statistik

[283]Mohammad S. Jalali, *et.al.*, "Why Employees (Still) Click on Phishing Links: Investigation in Hospitals"*, Journal of Medical Internet Research*, Vol. 22, No. 1, January 2020, hlm. 2.

perangkat, perkiraan lokasi, dan informasi lain yang mungkin diberikan secara sukarela.

2. Kemungkinan *Malware* Terpasang pada Perangkat Korban

   Perangkat lunak berbahaya, seperti *spyware*, *ransomware*, atau virus dapat diinstal tanpa sepengetahuan pengguna. File berbahaya ini dapat menginfeksi perangkat korban dan mengumpulkan data rahasia bagi peretas.

3. Jaringan dan Kontak Korban Dapat Dieksploitasi

   Pelanggaran ke seluruh jaringan korban dapat terjadi jika korban mengeklik tautan *phishing* saat peretas mulai mengirim *email phishing* lebih lanjut kepada orang-orang di daftar kontak korban, atau lebih buruk lagi, mendapatkan akses jarak jauh ke komputer korban.

Sayangnya, saat ini pesan *phishing* menjadi kian sulit untuk diidentifikasi, karena berkembangnya modus tersebut. Apabila seseorang telah luput atau tidak sadar telah mengeklik tautan *phishing* ataupun mengunduh lampiran berbahaya, maka beberapa saran dapat dilakukan guna meminimalisir risikonya, yakni sebagai berikut.[284]

1. Putuskan Sambungan Perangkat yang Digunakan

   Hal pertama yang perlu seseorang lakukan adalah segera memutuskan sambungan perangkat yang disusupi dari internet. Apabila menggunakan koneksi kabel, langkah termudah untuk melakukannya adalah dengan mencabut kabel internet (kabel ethernet) dari komputer. Apabila terhubung melalui Wi-Fi, temukan pengaturan Wi-Fi pada perangkat dan putuskan sambungan dari jaringan tersebut. Apabila tidak dapat menemukan pengaturan jaringan Wi-Fi pada perangkat, dapat secara langsung membuka router Wi-Fi dan mematikannya. Langkah ini akan mengurangi risiko penyebaran *malware* ke perangkat lain pada jaringan dan mencegah *malware* mengirimkan informasi sensitif dari perangkat dan mencegah seseorang mengakses perangkat dari jarak jauh.

---

[284]Carrie Kerskie, "5 Step to Take After Clicking on Phishing link", *Aging Care*, 24 September 2021, https://www.agingcare.com/articles/5-steps-to-take-after-clicking-on-a-phishing-link-178044.htm#:~:text=What%20Happens%20If%20You%20Click,undetectable%20to%20the%20average%20user (diakses pada 3 Juli 2022).

2. Lakukan *Backup* Data

   Setelah perangkat terputus dari koneksi internet, langkah selanjutnya adalah mencadangkan (*back up*) file. Data dapat dihancurkan atau dihapus dalam proses pemulihan dari serangan *phishing*. Apabila secara teratur mencadangkan file menggunakan metode seperti *hard drive* eksternal, USB, atau penyimpanan *cloud*, maka hanya perlu mencadangkan file yang telah diperbarui atau dibuat sejak pencadangan terakhir. Berfokuslah untuk melindungi dokumen dan informasi yang sangat sensitif serta file yang tak tergantikan seperti foto dan video keluarga. Namun, apabila belum pernah menyalin file kepada perangkat atau program cadangan, disarankan memilih salah satu metode penyimpanan yang disebutkan di atas.

3. Pindai Sistem Anda dari *Malware*

   Apabila tidak memahami secara baik perihal pindai sistem, disarankan untuk berkonsultasi ataupun meminta bantuan kepada ahli di bidangnya. Namun, bila ingin menanganinya sendiri maka lakukan pemindaian secara menyeluruh pada sistem. Lakukan pemindaian dengan menggunakan program antivirus. Apabila terdapat peringatan terhadap temuan hasil pemindaian, pastikan untuk menghapus atau mengarantina file tersebut.

   Perlu diketahui bila beberapa *malware* mungkin menyamar sebagai file operasi yang sah, sehingga sukar bagi program antivirus untuk mendeteksinya. Apabila masih mengalami masalah dengan perangkat atau ingin memastikan bahwa sistem Anda bersih, sebaiknya proaktif dan bawa perangkat ke ahlinya untuk memastikan.

4. Ubah Kredensial

   Malware dapat digunakan untuk mengumpulkan informasi sensitif, termasuk nama pengguna dan kata sandi, nomor kartu kredit, nomor rekening bank, dan informasi pengenal lainnya. Apabila seseorang merasa telah ditipu untuk bertindak berdasarkan pesan *phishing*, segera ubah kredensial. Ini berlaku untuk semua akun *online—email*, *online banking*, media sosial, dan lainnya. Hindari menggunakan nama pengguna dan kata sandi yang serupa untuk seluruh akun *online*, karena hal tersebut memberi kemudahan bagi

penjahat untuk mencuri kredensial, mengakses informasi pribadi, bahkan mencuri dana.

5. Hapus Pesan

   Pesan teks dan *email phishing* telah menjadi ancaman berbahaya, namun tak terhindarkan di era digital saat ini. Perlindungan terbaik adalah dengan berhati-hati dan segera menghapus pesan pada *email* dan teks yang tampak meragukan. Organisasi atau bisnis yang sah tidak akan pernah meminta seseorang untuk membagikan informasi pribadi yang sensitif melalui saluran yang tidak aman seperti *email*, teks, atau pesan *pop-up*. Apabila pesan tersebut benar-benar penting, pengirim akan mencoba menghubungi melalui metode terverifikasi seperti telepon.

Dalam studi lainnya, penanggulangan *phishing* dapat diterapkan pada beberapa tahap selama serangan. Solusi awal yang dapat diterapkan adalah ***filtering***. Solusi tersebut memproses dan menganalisis semua pesan *email* yang masuk dan berdasarkan aturan atau *Machine Learning* (ML) mengklasifikasikannya sebagai *phishing* atau tidak. Teknik penyaringan ML telah menjadi seni dan klasifikasi situs *web phishing* yang dapat digunakan untuk dimasukkan dalam *blacklist*. Pendekatan tersebut dapat mencegah pesan *phishing* mencapai pengguna target, tetapi penyerang turut dapat menggunakan teknik ML untuk melewati sistem deteksi *Artificial Intelligence* (AI) tersebut. Selanjutnya, penanggulangan berbasis ML dapat lebih diadaptasi dan dioptimalkan untuk lingkungan operasional yang berbeda guna meningkatkan kinerja dan mengatasi tantangan implementasi.[285]

Penanggulangan lainnya adalah ***education of users*** yang merupakan pendekatan proaktif. Dengan kata lain, pengguna sendiri dapat dididik untuk mengidentifikasi penipuan *phishing*. Dengan menciptakan kesadaran akan serangan *phishing* dan melatih pengguna untuk dapat mengidentifikasinya, metode ini dapat mencegah karyawan menjadi korban penipuan *phishing*, oleh karena itu mencegah kemungkinan kebocoran informasi. Selain itu, ***web filtering software or a specific firewall*** turut dapat digunakan untuk menganalisis semua situs web

[285]Daniel Jampen, *et.al.,* "Don't Click: Towards an Effective Anti-Phishing Training. A Comparative Literature Review", *Human-Centric Computing and Information Science*, Vol. 10, Issue 33, 2020, hlm. 7-8.

yang dikunjungi oleh karyawan dan berupaya mencegah akses kepada situs dengan maksud jahat. Ini dapat mencegah pengguna membocorkan informasi secara tidak sengaja. Pendekatan yang lebih aktif adalah *take-down of phishing websites* oleh pihak ketiga seperti lembaga penegak hukum atau layanan *hosting* guna mencegah calon korban mengakses situs web tersebut. Beberapa penstudi menyatakan durasi seluruh proses *take-down* rata-rata sekitar 62 jam. Persyaratan penting untuk upaya mitigasi yang efisien adalah partisipasi multi-lembaga (misalnya pengguna internet, *brand enterprises*, *browser manufactures*, dan otoritas) dengan format berbagi data yang seragam dan saluran berbagi yang tidak terhalang untuk pelaporan *phishing* umum. Salah satu cara untuk mencapai ini adalah dengan platform berbagi data *phishing* multi-pihak berdasarkan *blockchain*.

Perlu diketahui terdapat beberapa tujuan penyerang dalam mengirimkan *email phishing*, sehingga beberapa tindakan yang perlu dilakukan dapat saja berbeda, di antaranya sebagai berikut.

1. *Phishing* untuk Data

   Untuk jenis *phishing* ini, isi *email* kerap mengandung penawaran atau *voucher* menarik yang terkait dengannya. Penyerang mungkin akan meminta target untuk memberikan informasi detail agar dapat mengajukan voucher, penawaran atau sejenisnya. Mengeklik tautan *email phishing* ini akan membawa target menuju halaman web dengan formulir yang perlu diisi. Target akan diarahkan kepada halaman web palsu. Apabila itu adalah *email* dari perusahaan ternama seperti Starbucks, maka halaman tersebut akan sangat menyerupai web resmi Starbucks. Halaman web ini akan meminta target untuk memasukkan beberapa data, di antaranya detail pribadi seperti nama, alamat ataupun detail kartu kredit.

   Maka, hindari untuk memasukkan data yang diminta, dan segera putuskan sambungan perangkat Anda dari internet. Sekalipun target memasukkan data yang tidak sesuai, penyerang dimungkinkan akan mengetahui informasi seperti IP address dan akan digunakan oleh penyerangan untuk melakukan serangan selanjutnya.

2. *Phishing* untuk Detail *Log In*

   Untuk jenis *phishing* ini, umumnya merupakan *email* dari perusahaan ternama yang mengingatkan target bila akunnya telah diretas

sehingga diperlukan langkah pembaharuan, sehingga mengarahkan target untuk mengeklik tautan pembaharuannya. Apabila tautan tersebut diklik, maka target akan diarahkan pada halaman *login* yang serupa dengan perusahaan ternama seperti Instagram ataupun Twitter. Target akan diminta untuk memasukkan kredensial *login*, seperti nama pengguna dan kata sandi.

Maka, hindari untuk memasukkan kredensial *login* apa pun karena informasi itu akan segera disebar atau digunakan oleh penyerang untuk masuk pada akun target.

3. *Phishing* untuk Menginfeksi

   Untuk jenis *phishing* ini, situs web yang terinfeksi *malware* dapat berada di akhir tautan yang target klik. Tautan akan *phishing* membawa target menuju situs *spoof*. Pada saat target tiba di situs tersebut, kerusakan mungkin telah terjadi. *Ransomware* yang dikenal sebagai *CryptoLocker* atau *Cryptowall*, serta jenis *malware* lainnya, menggunakan metode ini untuk menginfeksi perangkat pengguna. URL yang terhubung dengan tautan membawa kode yang terinfeksi. Apabila perangkat target rentan (kerentanan keamanan pada *browser* atau perangkat lunak lain di komputer), *malware* dapat memanfaatkan ini dan menginstal. Oleh karena itu, disarankan untuk segera memutuskan sambungan perangkat dari internet. Baik dengan mematikan koneksi jaringan pada perangkat atau mencabut kabel jaringan. Ini akan membantu untuk menahan infeksi *malware*. Lalu pindai perangkat dengan menggunakan antivirus/anti-*malware*. Gunakan mode pemindaian penuh dan usahakan untuk tetap terputus dari internet selama pemindaian.

Perlu menjadi perhatian, bahwa tautan *phishing* tidak hanya berbentuk *email*. Tautan berbahaya yang mengarah kepada pencurian data dan upaya menginfeksi perangkat turut dapat ditemukan pada pesan teks (SMS), *posting*-an dalam media sosial.

Situs Pinjaman *Online*

115 nasabah bank BRI tertipu oleh *website* palsu hingga miliaran rupiah yang dilakukan oleh Suparman dan Sudirman. Pelaku melakukan aksinya di daerah Sulawesi Selatan dengan modus membuat *website* pinjaman *online* yang disebarkan secara acak. Pelaku menyebarkan SMS yang berisikan pinjaman *online* dengan syarat mudah serta mudah melalui creditrupiah.com. Kemudian bila terdapat korban yang tertarik, selanjutnya pelaku menghubungi korban dan meminta korban untuk memiliki rekening BRI yang terdaftar di *internet banking.* Kemudian pelaku mengirim *link website* palsu BRI dan meminta korban mengisi data-data pribadi termasuk nomor PIN nasabah. Dengan terisinya data korban pada web palsu tersebut, maka seluruh informasi tersebut terekam yang membuat pelaku dapat mengambil uang yang terdapat dalam rekening korban.

Untuk informasi lebih lanjut terkait **Kasus Situs Pinjaman Online,** Anda dapat *scan QR code* di samping.[286]

Remaja Inggris Mendapatkan £2 Juta Melalui Situs Palsu

Remaja berusia 17 tahun di Inggris, mendapatkan keuntungan sebesar £2 juta melalui sebuah situs palsu yang meniru "Love2Shop", sebuah situs penyedia voucher belanja. Remaja tersebut mengumpulkan informasi pembayaran orang-orang, lalu menggunakan data mereka untuk mendapatkan keuntungan. Para korban yang terjebak memasukkan alamat *email* dan detail akun Love2Shop pada situs palsu tersebut, lalu data tersebut dikumpulkan untuk mengonversi voucher pada akun Love2Shop miliknya. Dalam penyelidikan, diketahui setidaknya terdapat 12.000 nomor kartu kredit serta 197 akun PayPal. Akhirnya, remaja tersebut dijatuhi hukuman satu tahun direhabilitasi remaja karena penipuan dan pencucian uang. Hakim Catarina Sjolin Knight memutuskan bahwa remaja tersebut diuntungkan dari kejahatannya sebesar £2.141.720 dan memerintahkan penyitaan aset dengan nilai yang sama.

Untuk informasi lebih lanjut terkait **Kasus Situs Palsu Remaja Inggris,** Anda dapat *scan QR code* di samping.[287]

[286]Muhammad Taufiqqurahman, "Ratusan Nasabah BRI Tertipu Kredit Online di Sulsel", *Detik News*, 11 Januari 2019, https://news.detik.com/berita/d-4380083/ratusan-nasabah-bri-tertipu-kredit-online-di-sulsel (diakses pada 2 Juli 2022).

[287]Donald Nannestad, "Lincolnshire Teenager Ordered to Hand Over £ 2M After Gift Voucher Fraud", *Lincolnshire Live*, 27 Oktober 2021, https://www.lincolnshirelive.co.uk/news/lincolnshire-teenager-makes-2m-fake-6116584 (diakses pada 3 Juni 2022).

B. Dampak *Streaming* Film Secara Ilegal

Illegal streaming adalah *streaming* ilegal film, acara TV, atau konten olahraga premium, tanpa izin pemilik hak cipta. Ini dapat mencakup menonton konten ilegal menggunakan *add-on* yang diakses dari perangkat seperti dekoder atau stik, *streaming* dari situs web yang tidak sah, atau *streaming* melalui aplikasi (smart TV, ponsel, tablet, laptop, atau *game console*). Perlu diingat, *streaming* yang memungkinkan seseorang untuk mendengarkan dan menonton program secara *online* tanpa harus mengunduhnya, bukanlah tindakan ilegal. Platform web utama, seperti YouTube, Deezer, Netflix, dan lainnya kerap digunakan. Namun, sejumlah besar platform lain menyediakan program, film, dan serial TV kepada publik tanpa izin. Perangkat keras *streaming* seperti dekoder atau Amazon Firesticks/Google Chromecast dalam bentuk yang tidak diubah adalah sah — tetapi marak yang dimodifikasi dan kemudian dijual, dengan pengaya tidak resmi yang telah dipasang sebelumnya yang memungkinkan orang untuk mengakses, *streaming*, dan menonton konten berhak cipta secara ilegal. Pada sisi lain, melalui penggunaan situs media sosial seperti Facebook dan YouTube, tautan dan aliran ilegal ke konten film/TV dan olahraga bajakan di-*posting* tanpa izin pemegang hak cipta.[288]

Para pengguna internet saat ini pun kerap menggunakan *Virtual Private Network* (VPN), tidak hanya sebagai upaya memberikan perlindungan ekstra pada data *online,* dan ini adalah hal yang legal. Namun, menggunakan VPN untuk membuka konten yang secara khusus tidak tersedia di negara seseorang adalah ilegal. Beberapa contoh konten bajakan adalah film yang belum dirilis secara resmi, program TV yang belum ditayangkan atau yang hanya ditayangkan pada saluran tertentu. Maka, apabila seseorang *streaming* dan menonton film, TV atau konten olahraga melalui sumber yang tidak sah atau gratis, pengguna tersebut tengah *streaming* secara ilegal.[289]

Setiap kali pengguna mengakses konten ilegal, baik itu untuk menonton film, olahraga, atau acara TV favorit menggunakan *box* atau

[288]Crime Stoppers, "Streaming Online – Know The Risks: How to Stay Safe Online", https://crimestoppers-uk.org/keeping-safe/online-safety/streaming-online-know-the-risks#:~:text=Every%20time%20you%20access%20illegal,of%20fraud%20and%20data%20theft (diakses pada 3 Juni 2022).

[289]*Ibid.*

stick yang dimodifikasi atau melalui situs web, aplikasi, *add-on*, atau sumber ilegal lainnya yang tidak sah. Maka pengguna berisiko terkena *malware* berbahaya dan/atau menjadi korban penipuan serta pencurian data. Risiko ini meningkat secara signifikan ketika pengguna bertukar informasi kartu kredit atau debit untuk melihat konten di situs web dijalankan oleh peretas. Selain itu, menonton konten melalui sumber yang tidak sah dapat mengekspos penonton yang lebih muda kepada iklan eksplisit dan konten yang tidak sesuai usianya. Tidak seperti kebanyakan sumber legal, situs web, perangkat, aplikasi, *add-on*, dan konten yang tidak sah ini tidak memiliki kontrol orang tua yang efektif.[290]

Oleh karena itu, beberapa ahli berpendapat jika *streaming*, merupakan faktor kunci dalam penyebaran *malware*. Dengan mengeklik iklan yang menyesatkan, pengguna web secara khusus membuka diri terhadap terminal mereka yang terinfeksi oleh virus komputer (*ransomware*, Trojan, *cryptomining*). Peringatan kepada pengguna konten bajakan dari *Federation Against Copyright Theft* (FACT), badan Inggris terhadap pembajakan audiovisual mengungkapkan, bila seseorang 28 kali lebih mungkin terinfeksi oleh perangkat lunak berbahaya saat menggunakan *streaming* ilegal. Seseorang dapat terkena tindakan *phishing* dengan masuk ke situs *streaming* yang terlihat persis serupa dengan situs aslinya (desain yang sama, tipografi yang sama, URL koneksi yang serupa atau bahkan identik), dan ketika itu sebenarnya penyerangan tengah mencoba mencuri sesuatu, yaitu data pribadi. Bahkan, perlu diperhatikan teknik *false track* yang membuat seseorang mengeklik *pop-up* dengan menghasut untuk mengunduh *software* keamanan. Pesan kesalahan palsu ini membuat seseorang percaya bahwa dirinya tengah memiliki masalah teknis dan mendorong pengguna untuk mengunduh antivirus[291] atau telah melanggar standar komunitas.

[290]*Ibid.*

[291]Victor Poitevin, "Illegal Streaming: Beware of the Backlash"*, Strom Shield*, 18 November 2021, https://www.stormshield.com/news/illegal-streaming-beware-of-the-backlash/ (diakses pada 5 Juli 2022).

Phishing – Chatbots Messenger

Pada bulan Juni 2022, peneliti keamanan siber dari TrustWave menemukan kampanye *phishing* baru yang menggunakan *chatbot* Facebook Messenger untuk menyamar sebagai tim dukungan perusahaan dan mencuri kredensial yang digunakan untuk mengelola halaman Facebook.

Pelaku ancaman menggunakan *chatbot* untuk mencuri kredensial bagi pengelola halaman Facebook, yang biasanya digunakan oleh perusahaan untuk memberikan dukungan atau mempromosikan layanan mereka. Serangan *phishing* dimulai dengan *email* yang memberi tahu penerima bahwa halaman Facebook mereka telah melanggar standar komunitas. Pengguna hanya diberi waktu 48 jam untuk mengajukan banding atas keputusan tersebut, atau halaman mereka akan dihapus.

Pengguna akan ditawari kesempatan untuk menyelesaikan masalah pada Facebook's Support Center, dan untuk mengaksesnya pengguna didesak untuk mengeklik tombol "*Appeal Now*". Saat mengeklik tombol tersebut korban akan dibawa ke percakapan Messenger di mana *chatbot* menyamar sebagai *Facebook customer support agent*.

Chatbot tersebut akan mengirimkan tombol "*Appeal Now*" di Messenger kepada korban, yang membawa korban ke situs web yang disamarkan sebagai *Facebook Support Inbox*, tetapi URL-nya bukan bagian dari domain Facebook. Selanjutnya penyerang akan meminta pengguna yang ingin mengajukan banding atas keputusan penghapusan halaman untuk memasukkan alamat *email*, nama lengkap, nama halaman, dan nomor telepon.

Setelah data ini dimasukkan ke dalam kolom dan tombol "Kirim" ditekan, akan muncul *pop-up* yang meminta kata sandi akun. Setelah itu, semua informasi dikirim ke *database* aktor ancaman melalui permintaan POST. Akhirnya, korban diarahkan ke halaman 2FA palsu dan selanjutnya didesak untuk memasukkan OTP yang mereka terima melalui SMS di nomor telepon yang diberikan.

Untuk informasi lebih lanjut terkait **Kasus Chatbot Messenger Inggris,** Anda dapat *scan QR code* di samping.

Perlu turut diketahui, bila terdapat garis tipis antara *streaming* dan pengunduhan. Beberapa aplikasi *streaming* bahkan menyarankan untuk mengunduh episode atau program di komputer pengguna. Dalam hal ini pengguna harus sangat berhati-hati karena sangat sering file yang akan diinstal di komputer pengguna mungkin berisi program jenis *adware* atau pengunduh. Selain menerima versi yang tidak sesuai dengan sub-judul, sangat dimungkinkan pengguna menerima semua jenis *malware*.[292] *Malware* sendiri biasanya menyerang sistem *codec* atau *plugin*.

[292]*Ibid.*

Codec merupakan sebuah jenis file yang digunakan untuk memainkan file audio atau video yang memiliki format lain seperti avi, 3gp, dan lainnya. *Codec* dapat disebut juga sebagai *compressor-decompressor* atau *coder-decoder.* Jika pengguna tidak menginstal sistem ini, maka tidak dapat menikmati film yang telah diunduh.

Sebuah studi yang dilakukan di Inggris mengungkapkan bila 3 juta orang yang melakukan *streaming* secara ilegal telah diretas pada tahun 2021, 2,4 juta orang mengungkap bila perangkatnya telah terinfeksi virus dan 1 juta orang menyatakannya jika terjadinya pencurian dana akibat menonton *streaming* ilegal.[293] Sementara laporan yang dirilis oleh Walnut Unlimited mengungkapkan bahwa pada tahun 2020 diketahui sebagai berikut.[294]

1. 3,029 juta *streamer* ilegal telah diretas.
2. 2,495 juta *streamer* ilegal terinfeksi virus.
3. 1,069 juta *streamer* ilegal uang mereka dicuri karena menonton *streaming* ilegal.
4. 4,812 juta *streamer* ilegal mengalami virus, penipuan, atau pencurian data pribadi.

Penggunaan *box* atau *stick* semakin berbahaya, karena perangkat tersebut dinilai membantu proses peretasan dengan "mengawal" peretas melewati jaringan keamanan vital. Ketika pengguna membeli perangkat yang memuat aplikasi dan menawarkan akses gratis film terbaru di bioskop atau siaran langsung pertandingan olahraga, sesungguhnya perangkat tersebut telah menautkan pada aplikasi peretasan. Perangkat tersebut kerap ditawarkan melalui Facebook, ataupun *marketplace*. Setelah dibeli, pengguna didorong untuk menambahkan aplikasi baru yang menawarkan akses kepada berbagai konten "bajakan" yang semakin luas, termasuk film terbaru di bioskop atau acara lainnya. Namun, ini yang perlu diketahui bahwa dengan menghubungkan perangkat kepada jaringan rumah, maka memungkinkan peretas untuk melewati keamanan (seperti *router's firewall*) yang dirancang untuk melindungi sistem.[295]

---

[293]Claire Reid, "Huge Risk Million Face When Illegally Streaming At Home", *Lad Bible*, 7 Juni 2022, https://www.ladbible.com/news/huge-risks-millions-face-when-illegally-streaming-at-home-20220607 (diakses pada 5 Juli 2022).

[294]Crime Stoppers, *Ibid*.

[295]Digital Citizens Alliance, "Fishing in the Piracy Stream: How the Dark Web of Entertainment is Exposing Consumers to Harm", April 2019, hlm. 3.

Lembaga peneliti, Digital Citizens bekerja sama dengan perusahaan keamanan siber GroupSense guna mencari informasi perihal modus peretasan pada ruang diskusi pada *dark web* dan menemukan bahwa para peretas menggunakan *malware* untuk mengeksploitasi daya komputasi perangkat seperti memasukkannya ke dalam *botnet* untuk kemudian menyerang komputer lain atau menambang *cryptocurrency*, hingga kemudian mengakses informasi yang tersimpan di perangkat, termasuk foto, kata sandi, dan kartu kredit. Taktik yang kerap digunakan oleh peretas adalah dengan memancing pengguna dengan tawaran konten gratis, hingga kemudian menginfeksi pengguna yang terpancing melalui *malware* dan mencuri informasi pribadi. Pada tahun 2015, investigasi Digital Citizens menemukan bahwa 1 dari 3 situs web yang menawarkan konten bajakan mengekspos pengguna melalui *malware* yang dapat mencuri informasi pribadi dan keuangan dan mengambil alih komputer mereka untuk meluncurkan serangan.[296]

Selain itu, perusahaan keamanan siber Kaspersky merilis laporan terperinci pada awal April 2019 yang mengungkapkan bahwa banyak situs torrent yang menawarkan acara TV yang berisi *malware*, *adware*, dan *Trojan* yang mampu membajak komputer. Kaspersky secara khusus berfokus pada Game of Thrones HBO dan menemukan 9.986 ancaman *malware-laced* dari keseluruhan serangan secara umum (129.819 serangan).[297]

[296]*Ibid.*, hlm. 4-5.
[297]*Ibid.*, hlm. 6.

Peretas iCloud - Foto Telanjang

Pria asal California, Hao Kuo Chi, pelaku peretasan ribuan akun Apple iCloud pada Juni 2022 dijatuhi hukuman 9 tahun penjara setelah mengakui aksi peretasannya pada Oktober 2021. Dalam modus operandinya, pelaku menggunakan *email* yang memungkinkannya untuk menyamar sebagai perwakilan dukungan pelanggan Apple. Pelaku menipu target agar menyerahkan ID dan kata sandi Applenya. Pelaku kemudian membagikan foto tersebut kepada beberapa orang termasuk dalam situs porno yang dibuatnya. Pelaku berhasil memperoleh akses tidak sah kepada ratusan akun iCloud penggunanya dari seluruh Amerika Serikat, termasuk Arizona, California, Florida, Kentucky, Louisiana, Maine, Massachusetts, Ohio, Pennsylvania, Carolina Selatan, dan Texas. Jumlah korbannya sekitar 4.700 orang, dengan besar file 3,5 Terabyte.

Untuk informasi lebih lanjut terkait **Kasus Peretas iCloud Inggris,** Anda dapat *scan QR code* di samping.

BAB 4

LANGKAH ANTISIPASI SERANGAN *SOCIAL ENGINEERING*

Beragam studi telah marak dilakukan guna menguraikan langkah pencegahan agar terhindar menjadi korban serangan *social engineering*, di antaranya Alsufyani yang memberikan delapan jenis langkah pencegahan, yakni: (1) *security policies;* (2) *education and training;* (3) *inspections and obedience;* (4) *authentication and permission measures;* (5) *shredded and burning;* (6) *checked your state;* (7) *anti-phish;* (8) *using accurate software*.[298] Sementara Wenjun Fan memberikan langkah pencegahan dengan memisahkan dalam dua kategori, yakni kategori *objective defense measures*, berupa *using standards security policies, updating facilities, detecting malicious data*, dan kategori *subjective defense measures* berupa *training human awareness* dan *detecting human emotion*.[299]

Odeh turut menjelaskan langkah pencegahan berdasarkan jenis serangan *social engineering*, sebagai berikut.[300]

---

[298]Asma. A. Alsufyani, *et.al.,* "Social Engineering, New Era of Stealth and Fraud Common Attack Techniques and How to Prevent Against"*, International Journal of Scientific & Technology Research*, Vol. 9, Issue 10, 2020, hlm. 374.

[299]Wenjun Fan, *et.al.,* "Social Engineering: I-E Based Model of Human Weakness for Attack and Defense Investigations"*, International Journal Network and Information Security*, Vol. 1, 2017, hlm. 8-9.

[300]Noor Ammar Odeh, *et.al.,* "A Survey of Social Engineering Attacks: Detection and Prevention Tools"*, Journal of Theoritical and Applied Information Technology*, Vol. 99, No. 18, 2021, hlm. 4382-4383.

Jenis Serangan	Tindakan Pencegahan
Impersonation	– Jangan pernah membuka lampiran *email* yang dikirim dari orang yang tidak dikenal sebelum memverifikasi sumber pengiriman karena penyerang kerap menggunakan metode ini untuk menyebarkan *malware* dan mendapatkan informasi untuk melakukan serangan mereka. – Hindari mengeklik iklan dan situs web yang tidak dikenal.
Shoulder Surfing	– Tidak memasukkan detail kartu kredit atau kata sandi akun saat berada di tempat umum dan menggunakan kata sandi yang kuat sehingga sulit bagi penipu untuk mengingat jika melihatnya. – Jangan biarkan siapa pun menggunakan ponsel atau komputer pribadi, bahkan teman atau kerabat dan jangan pernah membiarkannya terbuka di tempat umum. Pastikan untuk tetap terkunci setiap saat.
Dumster Diving	– Merobek atau membakar salinan cetak data atau informasi rahasia sebelum membuangnya ke tempat sampah sehingga penyerang tidak dapat menyaring sampah dan mengumpulkan informasi rahasia seperti nama pengguna dan kata sandi. – Pastikan bahwa semua informasi dan data yang dapat diidentifikasi dihapus dari perangkat sebelum membuangnya, baik dengan menjualnya atau menghancurkannya.
Phishing Attacks	– Didiklah diri sendiri dan kembangkan pengetahuan teknologi secara permanen untuk dapat menangani serangan semacam dengan baik. – Jangan mengeklik *email* atau pesan instan. – Selalu pastikan menggunakan situs resmi https. – Ubah kata sandi secara berkala, jangan gunakan kembali kata sandi pada beberapa akun, dan buat agar sulit ditebak dengan menggunakan huruf, angka, dan simbol alih-alih informasi pribadi. – Pembaruan terus-menerus dari perangkat lunak antivirus, aplikasi perangkat lunak, sistem operasi, selain menginstal *firewall*. – Lindungi privasi data dan informasi dengan tidak mengungkapkan informasi pribadi apa pun seperti nama orang penting, nomor telepon, tanggal, tempat lahir, atau informasi pribadi lainnya melalui internet.
Baitin Attacks	– Berhati-hatilah untuk mengeklik tautan yang diterima melalui pesan yang tidak dikenal karena kerap kali berisi program dan file berbahaya. – Hindari klik pada pemberitahuan pembaruan perangkat lunak dan aplikasi atau kiriman hadiah dan skandal, karena sebagian besar ditujukan untuk penipuan.

Pretextin Attacks	– Pastikan bahwa individu dan karyawan terus-menerus dilatih dan dididik tentang penipuan dalih dan cara menanganinya. – Gunakan filter spam untuk memfilter pesan *email*, mendeteksi virus, dan menggunakan filter web untuk memblokir situs web berbahaya.
Tailgaiting Attacks	– Pertahankan pengawasan konstan dan keamanan yang ketat pada pintu masuk dan keluar organisasi untuk memastikan masuk dan keluar organisasi serta untuk mencegah non-pekerja masuk tanpa pengawasan dan persetujuan dari mereka yang diizinkan ke organisasi untuk menghindari serangan. – Menetapkan kebijakan, prosedur, dan langkah-langkah keamanan yang diperlukan untuk memandu karyawan dalam menangani informasi dan data perusahaan atau lembaga secara tepat dan melakukan audit untuk memastikan kepatuhan mereka terhadapnya dan untuk menetapkan hukuman bagi ketidakpatuhan. – Selalu verifikasi identitas orang yang mencurigakan dan verifikasi datanya untuk melihat apakah memiliki hak akses resmi di area itu atau tidak. – Pastikan untuk keluar dari komputer atau perangkat lain saat jauh dari mereka.
Ransomware Attacks	– Berhati-hatilah untuk membuat salinan cadangan semua data. – Melatih dan mendidik individu di lembaga dan organisasi untuk menghadapi serangan. – Hindari mengeklik tautan dan lampiran yang tidak terpercaya. – Menggunakan autentikasi dua faktor untuk membuat akun lebih aman, karena fitur ini menyediakan lapisan tambahan untuk memverifikasi identitas saat masuk, sehingga penyerang tidak mungkin mendapatkan akses ke akun, bahkan jika nama pengguna dan kata sandi telah disusupi.
Pop-up Windows	– Gunakan program keamanan dan perlindungan seperti program antivirus dan *malware*, serta perbarui program tersebut untuk menghilangkan semua sumber bahaya dan serangan. – Hindari mengeklik iklan, *pop-up,* atau situs web yang mencurigakan dan menutupnya.
Scareware	– Hindari mengeklik pemberitahuan pembaruan perangkat lunak dan aplikasi atau kiriman hadiah dan skandal, karena sebagian besar ditujukan untuk penipuan. – Penggunaan program perlindungan dan keamanan yang sering diperbarui dan menginstal *firewall*.

Phone/Email Scam Attacks	– Selalu verifikasi sumber panggilan telepon sebelum menjawabnya, terutama panggilan yang tidak terduga dan dicurigai, atau ajukan pertanyaan untuk memverifikasi identitas penelepon atau tidak untuk menjawab panggilan tersebut. – Tidak membuka lampiran *email* yang dikirim dari orang yang tidak dikenal sebelum memeriksanya karena penyerang sering menggunakan metode ini untuk menyebarkan program jahat dan memperoleh informasi untuk melakukan serangan mereka.
Quid Pro Quo	– Pastikan untuk sering mengubah kata sandi untuk akun. – Jangan pernah mengungkapkan informasi pribadi atau informasi apa pun yang terkait dengan akun.

Selanjutnya akan dijelaskan beberapa langkah pencegahan guna terhindar dari serangan *social engineering* secara umum.

A. Belajar untuk Mengenali Serangan *Social Engineering*

Erdal Ozkaya menguraikan beberapa informasi sebagai upaya pencegahan agar terhindar dari serangan *social engineering* yang berasal dari beberapa *platform*, yakni sebagai berikut.[301]

1. *Email*

   Terdapat efek bola salju ketika pelaku berhasil meretas akun *email* korban, salah satunya adalah mengeksplorasi teman-teman korban. Beberapa jenis pesan yang ditujukan untuk mengeksploitasi teman korban adalah: (a) *email* yang berisi tautan; (b) *email* yang berisi file yang dapat diunduh; (c) *email* dengan mendesak meminta bantuan; (d) *email* yang meminta sumbangan.

2. *Baiting*

   Pelaku terkadang memancing korban yang kerap mengunduh konten "bajakan". Di balik langkah mengunduh secara ilegal konten di internet, terdapat kerentanan untuk mengunduh *malware* yang korban tidak sadari. Pada tahun 2015, diperkirakan 12 juta komputer terinfeksi *malware* setiap bulannya. Torrent telah menjadi cara yang umum digunakan pengguna internet untuk mengunduh file secara gratis, seperti film, game dan program. Dari 1.000

[301]Erdal Ozkaya, *Learn Social Engineering* (Birmingham: Packt Publishing, 2018), hlm. 280-286

situs torrent, sepertinya mengandung *malware* yang diunduh oleh penggunanya.

3. Menanggapi Pertanyaan

   Para pelaku, kerap berpura-pura mewakili perusahaan besar seperti Gmail, PayPal atau IRS dan memberikan pertanyaan kepada korban dengan mengiming-imingi korban layanan atau produk gratis. Pelaku akan meminta korban untuk mengautentifikasi diri dengan *login* ke sistem melalui tautan yang telah dipersiapkan.

4. Menciptakan Ketidakpercayaan

   Pelaku kerap menyusun skenario dengan menempatkan dirinya sebagai pahlawan bagi korban yang tengah menghadapi kendala. Terkadang pelakulah yang menyusun keadaan dengan menyerang korban dan menawarkan upaya pemecahannya. Setelah terbangun kepercayaan, pelaku secara perlahan akan menjebak korban agar memberikan informasi pribadinya.

5. Tata Bahasa yang Buruk

   Beberapa pelaku berasal dari negara yang tidak berkomunikasi dengan bahasa Inggris sebagai bahasa utama. Oleh karena itu, mereka cenderung kesulitan dalam menggunakan bahasa Inggris yang baik dan benar.

6. Sikap

   Perusahaan besar tentu akan memberikan pelayanan yang baik kepada konsumennya. Apabila terdapat seseorang yang mengakui mewakili sebuah perusahaan, tetapi menunjukkan tanda-tanda kasar dan agresif, besar kemungkinan orang tersebut adalah pelaku *social engineering*.

7. Permintaan Tidak Secara Formal

   Sangat tidak lazim bila perusahaan PayPal meminta nasabahnya untuk membacakan kata sandi, atau mengirimkan informasi pribadinya melalui media sosial seperti Facebook. Seorang CEO tidak akan meminta kepada akuntannya untuk mengirim sejumlah uang kepada rekening pribadinya untuk kemudian dikembalikan. Permintaan tidak secara formal merupakan indikator bahwa permintaan tersebut tidak dilakukan oleh orang yang sah.

8. Pujian yang Tidak Umum

   Pelaku kerap memberikan pujian yang tidak umum untuk meluluhkan korban agar mematuhi permintaan mereka.

9. Tidak Memiliki Nomor Kontak yang Valid

   Pelaku kerap menggunakan nomor yang berbeda ketika melakukan penyerangan. Oleh karena itu, jika korban menghubungi kembali nomor tersebut, sulit untuk dapat tersambung dengan pelaku.

10. Tergesa-gesa

    Pelaku sangat menghargai waktu yang mereka gunakan untuk menyerang korban. Sehingga terkadang mereka ingin tindakannya terjadi dengan cepat sebelum korban tersadar. Oleh karena itu, taktik yang digunakan pelaku adalah dengan meminta korban memenuhi permintaannya sesegera mungkin.

Sementara peneliti dari MDSNY menguraikan lima hal yang perlu diperhatikan terkait serangan *social engineering,* yakni:[302]

1. *Think Before You Click*

   Penyerang menggunakan suasana penting atau urgen untuk membuat korban bertindak lebih dulu dan berpikir kemudian dalam serangan *phishing*. Ketika korban mendapatkan pesan yang sangat mendesak dan bertekanan tinggi, pastikan untuk meluangkan waktu sejenak untuk memeriksa apakah sumbernya kredibel terlebih dahulu. Cara terbaik adalah menggunakan metode komunikasi lain yang berbeda dari tempat asal pesan — seperti mengirim pesan teks kepada orang tersebut untuk melihat apakah mereka mengirimi pengguna pesan penting atau dari penyerang.

2. *Research the Source*

   Selalu berhati-hati terhadap pesan yang tidak diinginkan. Periksa tautan *domain* untuk melihat apakah asli dan orang yang mengirimi *email* adalah anggota organisasi yang sebenarnya. Umumnya, kesalahan ketik/ejaan adalah kata kuci. Manfaatkan mesin pencari, buka situs web perusahaan, periksa direktori telepon mereka. Ini semua adalah cara sederhana dan mudah untuk menghindari

[302]Jen Trang Nguyen, "Five Ways to Prevent Social Engineering Attacks", *MDSNY*, https://www.mdsny.com/5-ways-to-prevent-social-engineering-attacks/ (diakses pada 7 Juli 2022).

penipuan. Mengarahkan kursor pada tautan sebelum benar-benar mengekliknya akan mengungkapkan tautan di bagian bawah, dan merupakan cara lain untuk memastikan pengguna diarahkan ke situs web perusahaan yang benar.

3. *Email Spoofing is Ubiquitous*

   Peretas, *spammer* berupaya untuk mendapatkan informasi korban dan mengambil alih kendali akun orang. Begitu mereka mendapatkan akses, mereka akan memangsa kontak korban. Bahkan ketika pengirim tampaknya adalah seseorang yang korban kenal, tetap merupakan praktik terbaik untuk menghubungi mereka jika korban tidak mengharapkan tautan *email* atau file apa pun dari mereka.

4. *Don't Download Files You Don't Know*

   Apabila pengguna tidak mengenal pengirimnya dan tidak mengharapkan apa pun dari pengirimnya serta tidak tahu apakah pengguna harus melihat file yang mereka kirimkan dengan "URGENT" pada judul email, aman untuk tidak membuka pesan tersebut sama sekali.

5. *Offers and Prize are Fake*

   Apabila Anda dari seorang pangeran Nigeria yang menjanjikan sebuah uang, atau mendapatkan pesan dari keluarga kaya di Afrika yang akan memberikan uang dalam jumlah besar dengan syarat Anda membantunya, maka kemungkinan itu adalah penipuan.

1. Antisipasi SIM-*Swap*

Serangan SIM (*Subscriber Identity Module)-Swap* merupakan tindakan peretasan yang dilakukan dengan mendapatkan kendali tidak sah atas nomor telepon seseorang untuk menggunakan pesan teks dan mengatur ulang kata sandi untuk kemudian mencuri aset berharga dari akun penting.[303] Dalam beberapa kasus, para penyerang menggunakan informasi ponsel untuk mentransfer dana bank secara ilegal. Pelaku berhasil mentransfer dana dari rekening bank *online* pelanggan dengan mengganti kartu SIM yang ada dengan yang baru. Penggantian ini

[303]Nathanael Andrews, ""Can I Get Your Digits?": Illegal Acquisition of Wireless Phone Numbers For SIM-Swap Attacks and Wireless Provider Liability", *Northwestern Journal of Technology and Intellectual Property*, Vol. 16, Issue 2, 2018, pp. 79-106, Hlm. 81.

memungkinkan penipu untuk mengambil alih nomor ponsel korban dan menggunakannya untuk penipuan.[304] Serangan SIM-*Swap* memiliki karakter khusus yang membedakan dari serangan terhadap data lainnya yakni, *pertama*, serangan SIM-*Swap* adalah serangan yang ditargetkan pada individu, berbeda; *kedua*, serangan SIM-*Swap* kerap mengakibatkan pencurian aset digital, seperti bitcoin yang memiliki nilai finansial substansial dan terukur, berbeda dengan kerugian yang lebih sulit untuk diukur dan tidak berwujud dari pelanggaran privasi dan peningkatan risiko pencurian identitas yang terkait dengan sebagian besar pelanggaran data skala besar.[305]

Cara pelaku melakukan kejahatan SIM-*Swap* adalah dengan menghubungi operator penyedia layanan ponsel dan menggunakan identitas palsu. Pelaku mengaku nomornya rusak atau hilang, kemudian meminta penggantian kartu SIM. Setelah melakukan verifikasi identitas, operator seluler akan menerbitkan kartu SIM pengganti dan menonaktifkan kartu SIM yang masih berada di tangan pemilik yang sah. Setelah mereka menguasai kartu SIM pengganti, pelaku kejahatan kemudian melakukan transaksi finansial, umumnya dengan menggunakan kartu kredit atau nomor rekening bank. Lalu, bank penerbit akan mengirimkan sandi sekali pakai (*One Time Password* atau OTP) ke nomor SIM tersebut. Kemudian transaksi finansial pun akan dianggap sah tanpa sepengetahuan korban. Seperti kasus yang terjadi pada nasabah Bank Permata yaitu Tjho Winarto dalam putusan 227/PID/2016/PT.DKI.[306]

Kebocoran data memberikan peluang besar bagi penjahat untuk melakukan SIM-*Swap*. Untuk mencegah terjadinya SIM-*Swap*, berikut beberapa langkah pengamanan yang dapat dilakukan.

a. Selalu perbarui *software*, termasuk *browser*, antivirus, dan sistem operasi.
b. Batasi informasi pribadi terkait dengan media sosial.

---

[304]Nada Ibrahim, *et.al.,* "SIM Card Forensic: Digital Evidance"*, Proceedings Annual ADFSL Conference on Digital Forensic, Security and Law*, 2016, pp. 219-234, hlm. 220.

[305]Nathanael Andrews, *Loc. Cit*.

[306]Winda Handayani Sinambela, *et.al.,* "Analisis Yuridis Pemalsuan Identitas oleh Penjual Kartu Subscriber Indentity Module Internet"*, Jom Fakultas Hukum*, Vol. V, Edisi 2, 2018, pp. 1-15, hlm. 4-5.

c. Tidak pernah membuka tautan atau lampiran mencurigakan yang diterima melalui *email* atau pesan teks.
d. Tidak membalas *email* yang mencurigakan atau terlibat melalui telepon dengan penelepon yang meminta informasi pribadi.
e. Perbarui kata sandi secara teratur.
f. Ganti 2FA berbasis SMS dengan aplikasi autentikator atau kunci keamanan fisik.
g. Unduh aplikasi hanya dari penyedia resmi dan selalu membaca izin aplikasi.
h. Apabila memungkinkan, tidak mengaitkan nomor telepon dengan akun *online* yang sensitif.
i. Tidak membagikan PIN kepada siapa pun.
j. Rutin memeriksa laporan keuangan.
k. Bila dimungkinkan, hindari memberikan *fotocopy* KTP/KK atau meng-*input* pada *online* form untuk kegiatan pengumpulan data.

Remaja Kanada Ditangkap Terkait Pencurian Uang Kripto Senilai $36,5 Juta

Remaja Kanada ditangkap atas dugaan pencurian uang kripto senilai $36,5 juta. Polisi Kota Hamilton mengungkapkan seorang korban berkewarganegaraan Amerika Serikat menjadi target setelah nomor ponselnya (kartu SIM) dibajak. Pelaku menipu petugas operator telekomunikasi agar dapat menggandakan nomor telepon korban. Setelah menguasai nomor tersebut, pelaku dapat mencegat permintaan autentifikasi dua faktor yang dikirim ke ponsel dan mendapatkan akses ke akun korban.

Untuk informasi lebih lanjut terkait **Kasus SIM-*Swap* Remaja Kanada,** Anda dapat *scan QR code* di samping.[307]

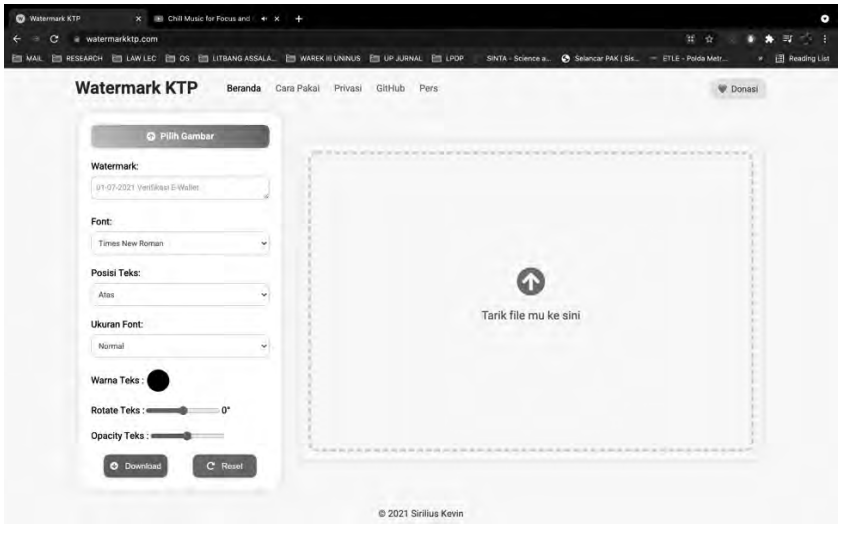
[307]Katyanna Quach, "Canadian Teen Nabbed in $36.5M Crypto Heis-Possibly The Biggest Haul Yet by a Single Individual", *The Register*, 18 November 2021, https://www.theregister.com/2021/11/18/canadian_cryptocurrency_heist/ (diakses pada 4 Juni 2022).

Kasus SIM-*Swap* Ilham Bintang

Februari 2020, Polda Metro Jaya telah menangkap delapan tersangka kasus pembobolan rekening bank milik Ilham Bintang. Pembobolan rekening tersebut dilakukan setelah tersangka menduplikasi kartu SIM dengan register Ilham Bintang, yang data pribadinya didapatkan dari tersangka yang memiliki akses ke layanan informasi keuangan milik Otoritas Jasa Keuangan (OJK).

Untuk informasi lebih lanjut terkait **Kasus SIM-*Swap* Ilham Bintang,** Anda dapat *scan QR code* di samping.[308]

Salah satu upaya yang dapat dipertimbangkan jika akan *share* KTP di dunia maya, maka gunakan *watermark* pada gambar KTP tersebut. Salah satunya dapat memanfaatkan aplikasi pembuatan *watermark* yang diciptakan oleh Sirilus Kevin pada situs https://watermarkktp.com/.



Gambar 33. Tampilan Situs Watermarkktp.com

[308]CNN Indonesia, "Pembobolan Rekening Ilham Bintang, Data Dijual Orang Bank", *CNN Indonesia*, 06 Februari 2020, https://www.cnnindonesia.com/nasional/20200205211241-12-472073/pembobolan-rekening-ilham-bintang-data-dijual-orang-bank (diakses pada 6 Juni 2022).

2. Deteksi Alamat Web dengan *Toolsdetect*

Dalam beberapa kasus, penyerang telah mempersiapkan situs web palsu yang menyerupai situs asli guna menipu korbannya. Untuk itu, sebagai langkah pencegahan, dapat terlebih dahulu dipastikan dengan beberapa *toolsdetect* apakah situs tersebut asli atau palsu. Beberapa *toolsdetect* yang dapat digunakan, yaitu sebagai berikut.[309]

a. PhishShield

   PhishShield merupakan aplikasi *desktop* yang berkonsentrasi pada URL dan konten situs *web phishing*. Cara kerjanya dengan mengambil URL sebagai masukan dan *output*-nya berupa status yang mengonfirmasi URL termasuk *phishing* atau situs asli. Tingkat akurasi yang diperolah oleh PhishShield adalah 96,57% dan mencakup berbagai situs *phishing* yang dihasilkan dengan tingkat kepalsuan negatif dan positif.

b. LinkGuard Algoritma

   LingGuard Algoritma digunakan untuk menganalisis dua URL dan akhirnya akan bergantung pada hasil yang diberikan oleh algoritma. URL tersebut adalah URL yang melibatkan ekstrasi URL yang sebenarnya dan URL visual (yang dilihat oleh pengguna).

c. Phish Detector

   Phish Detector adalah ekstensi *browser* yang digunakan untuk mendeteksi serangan *phishing* dengan menggunakan pencocokan algoritma pencocokan *string* perkiraan guna menentukan hubungan antara konten dan URL suatu halaman web.

3. Pencegahan Serangan *Phishing*

Miller mengenalkan *three-pillared approach* dalam memerangi serangan *phishing*, yaitu sebagai berikut.[310]

---

[309]Mia Haryati Wibowo dan Nur Fatimah, "Ancaman Phishing Terhadap Pengguna Sosial Media dalam Dunia Cyber Crime", *Journal of Education and Information Communication Technology*, Vol. 1, No. 1, 2017, hlm. 4.

[310]Bryon Miller, *et.al.*, "Prevention of Phishing Attacks: A Three-Pillared Approach", *Issue in Information System*, Vol. 21, No. 2, 2020, hlm. 2-4.

a. *One Time Password*

One Time Password (OTP) adalah metode yang umum digunakan untuk mengamankan sistem *online*. OTP pada dasarnya adalah kata sandi jangka pendek yang dibuat sesuai kebutuhan dan tidak lagi efektif setelah penggunaan pertama. Ini biasanya berupa bermacam-macam angka dan/atau huruf yang tampak acak dan secara otomatis akan kedaluwarsa jika tidak digunakan dalam waktu yang relatif singkat. OTP memaksa pengguna untuk mengambil langkah lain selain memasukkan nama pengguna dan kata sandi. Bahkan jika *scammer* dapat memperoleh kata sandi pengguna, mereka biasanya tidak dapat melewati langkah autentikasi kedua. *Scammers* dapat dengan mudah memangsa *email*, nama pengguna, dan kata sandi. Oleh karena itu, memiliki autentikasi sekunder adalah salah satu praktik terbaik untuk menjaga keamanan informasi pengguna.

Para penstudi mengusulkan sistem OTP yang memanfaatkan *Short Message Service* atau SMS. Dalam model tersebut, pesan SMS dikirim ke pelanggan pada saat dirinya siap untuk menyelesaikan transaksi. Apabila pelanggan gagal memasukkan OTP dalam interval waktu yang ditentukan, transaksi ditolak. Saat ini, transaksi nasabah dengan perbankan, saham, pajak, dan lainnya telah dengan mengirimkan OTP untuk verifikasi menggunakan pesan SMS atau *email*. Perhatian utama dengan strategi ini adalah berbasis pengguna, bukan berbasis keamanan. Misalnya, pelanggan dapat salah membaca OTP dan terpaksa mengulang proses konfirmasi. Demikian pula, apabila pelanggan terlalu lambat dalam memasukkan OTP, sistem dapat kehabisan waktu dan memaksa proses untuk diulang. Terkadang, perusahaan memilih untuk tidak menggunakan OTP karena ketidaknyamanan yang ditimbulkannya kepada pelanggan. OTP, bagaimanapun menawarkan keamanan sistem yang ekstrem dengan kemungkinan minimal peretasan dapat terjadi, namun pelanggan mungkin merasa tidak nyaman, tetapi mereka dapat merasa tenang karena informasi mereka aman.

b. *Multi-Level Desktop Barriers*

Beberapa ahli mengusulkan aplikasi *five-level desktop barrier* yang dirancang untuk mencegah pengguna membuka halaman web yang mencurigakan. *Phisher* termotivasi oleh pengakuan, keuntungan moneter, atau peningkatan identitas. Aplikasi *Multi-Level Desktop*

Barriers dapat mendeteksi motivasi ini sebagai kelemahan. Aplikasi ini membantu mencegah upaya *phishing* agar tidak berhasil. Lima *barriers* yang dimaksud adalah sebagai berikut.

1) *Verification Barrier*

   Essentially a whitelist in which suspicious webpages are checked against to find potentially dangerous sites.

2) *Text Field Barrier*

   Raises suspicion and alerts anytime an insert text field is found within the webpage. This leaves an open door for secure information to pass through to a potential scammer.

3) *The Anchor Tag Endorsement Barrier*

   Detects the existence of hyperlinks against the existence of text fields. There is cause for alarm if a website has a text field such as a login form (as found in the text barrier phase), but with no hyperlink such as 'login', 'sign up', or 'forgot password' leading a user elsewhere.

4) *The Null (#) Link Barrier*

   Tracks links directing to its own webpage, which raises red flags because the phisher typically wants to try to keep the user on the susceptible page for as long as they can in order to contract large amounts of information from them.

5) *Webpage Identity Barrier*

   Analyzes the structure of the hyperlink and how frequent a hyperlink points to the webpage's own domain. Many phishers use hyperlinks with different domains to conduct their scam.

c. *Behavior Modification*

Selain mengandalkan strategi berbasis perangkat lunak, pengguna harus dididik untuk mengenali potensi serangan *phishing*. Metode yang paling umum dan diterima secara luas untuk mengurangi tingkat keberhasilan upaya *phishing* adalah modifikasi perilaku. Ini bisa menjadi tantangan, karena perilaku sangat sulit untuk diubah. Beberapa penstudi menyarankan agar pengguna dididik tentang psikologi upaya *phishing*, serta teknik yang digunakan. Modifikasi perilaku mungkin mulai memprioritaskan pelatihan untuk semua karyawan, tetapi upaya turut harus dilakukan untuk mengidentifikasi karyawan yang paling rentan untuk

mengeklik *email phishing*. Orang-orang dari berbagai demografi mungkin lebih rentan terhadap penipuan *phishing*. Misalnya, siswa lebih mengandalkan informasi dari internet dan mereka tidak memverifikasi informasi sesering non-siswa. Usia juga tampaknya menjadi faktor penting. Studi lain menemukan bahwa wanita dan orang-orang berusia antara 18 dan 25 tahun kurang curiga terhadap *phishing*. Organisasi dapat menggunakan sejumlah teknik untuk membantu mengidentifikasi demografi yang paling rentan, termasuk penggunaan penipuan *phishing* palsu, menggunakan kuesioner untuk menguji pengetahuan keamanan karyawan, dan meninjau jumlah upaya *phishing* aktual yang dilakukan pada individu atau departemen tertentu.

Ini juga akan meningkatkan pelatihan jika manajer dan staf teknologi informasi (TI) mengenali proses pemikiran yang mengarah pada perilaku berisiko. Misalnya, penelitian menunjukkan bahwa orang lebih rentan terhadap *phishing* ketika mereka memproses informasi dengan lebih memperhatikan elemen dalam *email* seperti logo perusahaan, nomor telepon, atau tanda tangan. Manajer dan staf TI juga perlu mengajari karyawan mereka untuk mengidentifikasi penipuan *phishing* dengan mencari tanda-tanda khas, termasuk salah eja, urgensi yang tinggi, ancaman, salam atau tanda tangan umum, dan permintaan informasi pribadi atau terkait pekerjaan. Ketika karyawan dilatih untuk mengenali tanda-tanda ini, mereka cenderung tidak membuka *email* atau mengeklik tautan *phishing*.

B. Batasi Publikasi Informasi Sensitif di Sosial Media

Apabila dahulu, para pelaku melalukan *dumpster diving*, dengan membongkar tempat sampah fisik untuk mendapatkan informasi, saat ini ketika orang-orang memublikasikan begitu banyak informasi di media sosial yang tidak mereka sadari dapat digunakan dalam serangan *social engineering*. Namun, memeriksa tempat pembuangan data digital tidak serta-merta disebut sebagai *digital dumpster diving*.[311] Istilah yang lazim digunakan saat ini adalah *Open Source Intelligence* (OSINT) yang dimanfaatkan penyerang ketika melakukan serangan *social engineering*. OSINT merupakan data apa pun

[311]Robert W. Gehl dan Sean T. Lawson, *Op. Cit.*, hlm. 86.

yang dapat ditemukan, tersedia untuk umum dan tidak disembunyikan.[312] OSINT sesungguhnya diambil dari istilah militer yang mengacu pada pengumpulan *Open Source Intelligence,* yaitu penggunaan kembali catatan publik untuk intelijen dan investigasi, termasuk konten media sosial yang tidak dilindungi oleh pengaturan privasi.[313]

Tripwire merekomendasikan beberapa langkah agar terhindar dari serangan *social engineering* akibat *oversharing* di dunia maya, yaitu sebagai berikut.[314]

1. Jangan membuka *email* apa pun dari sumber yang tidak terpercaya. Hubungi teman atau anggota keluarga langsung atau melalui telepon bila pesan yang dicurigakan menggunakan nama mereka.
2. Jangan menerima tawaran dari orang asing yang mengiming-imingi keuntungan.
3. Kunci laptop setiap kali Anda meninggalkannya.
4. Beli *software* antivirus. Tidak ada AV yang dapat bertahan melawan semua serangan, namun dapat membantu melindungi dari beberapa serangan.
5. Baca dan pahami kebijakan privasi perusahaan, agar mengetahui dalam keadaan apa saja yang diperbolehkan membawa orang asing masuk ke dalam gedung.

Apabila foto pribadi telah terlanjur terpublikasi di dunia maya, saat ini Google merilis fitur keamanan baru yang memungkinkan pengguna berusia di bawah 18 tahun dapat meminta Google untuk menghapus hasil pencarian gambar dan foto diri sendiri. Dalam pengumumannya, seseorang diminta untuk mengajukan laporan dengan menyertai URL dari gambar yang hendak dihapus. Kemudian sertakan informasi nama, usia, umur, dan hubungan (orang tua atau wali) yang melaporkan, dan Google akan mengirimkan surel konfirmasi bahwa permintaan tengah dipelajari untuk ditindaklanjuti.[315]

---

[312]Joe Gray, *Op. Cit.*, hlm. 35.

[313]Robert W. Gehl dan Sean T. Lawson, *Loc. Cit*.

[314]David Bisson, "5 Social Engineering Attacks to Watch Out For"*, Tripwire*, 5 November 2019, https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/ (diakses pada 6 Juni 2022).

[315]James Vincent, "You Can Now Ack Google to Remove Images of Under-

Hal lainnya yang perlu dilakukan adalah dengan mempertimbangkan untuk menghapus riwayat penjelajahan di internet jika tidak bermanfaat, atau menghapus jejak digital. Bagi pengguna yang lazim menggunakan *browser* Google, terdapat menu yang dapat diakses untuk mengetahui informasi pribadi yang dibagikan oleh Google, langkahnya sebagai berikut.

1. Buka *browser* dan akses https:myaccount.google.com/.
2. Ketikkan nama pengguna Google.
3. Pada menu tersebut, pilih informasi pribadi dan lakukan peninjauan terhadap informasi. Pengguna dapat mengubah atau menghapus foto, nama, tanggal lahir, jenis kelamin, kata sandi, *email,* nomor telepon, dan lainnya.
4. Apabila hendak melihat informasi pengguna yang tersedia untuk umum, dapat menuju fitur *"go to about me"*.
5. Pada fitur ini, pengguna dapat mengatur informasi apa saja yang dapat dilihat oleh publik, semi publik atau pribadi.

Terdapat beberapa fitur lainnya yang memberikan perlindungan penggunanya dengan mengatur riwayat tersebut, yakni sebagai berikut.

1. Mengelola Data Lokasi Pengguna
    a. Masuk pada **akun Google** dan pilih **data & personalisasi** pada menu navigasi.
    b. Untuk melihat seluruh data lokasi yang telah tercatat oleh Google, dapat dilihat pada menu **control aktivitas**, lalu pilih **riwayat lokasi**.
    c. Apabila hendak mengatur agar Google berhenti melacak lokasi pengguna, maka dapat dimatikan fungsinya pada menu tersebut.
    d. Untuk mengatur Google agar secara otomatis menghapus data jenis ini, maka dapat memilih **hapus otomatis**, lalu pilih jangka waktu yang dirasa paling baik.

18s from its Search Result", *The Verge*, 27 Oktober 2021, https://www.theverge.com/2021/10/27/22748240/remove-images-google-search-results-under-18-request-how-to (diakses pada 6 Juni 2022).

e. Selanjutnya masuk pada **kelola aktivitas**, untuk melihat seluruh informasi lokasi yang telah Google kumpulkan, termasuk tempat-tempat yang pengguna kunjungi, rute yang diambil, serta frekuensi dan tanggal kunjungan.

2. Menghapus Data Lokasi Pengguna
   a. Untuk menghapus seluruh riwayat permanen, pilih **hapus riwayat.**
   b. Lakukan pencarian pada Google dengan nama pengguna untuk mengetahui seberapa banyak informasi yang memuat nama pengguna di Google.
   c. Lakukan penghapusan ataupun *deactive* akun media sosial yang telah tidak dipergunakan.
   d. Atur ulang pengaturan keamanan pada seluruh media sosial dan batasi izin aplikasi untuk mengakses fitur tertentu pada saat menginstal aplikasi.
   e. Dapat pula menggunakan metode *incognito* pada saat melakukan penelusuran di internet dan pastikan untuk menghapus *cookie* dan riwayat pencarian pada *browser* yang digunakan.

[Halaman ini sengaja dikosongkan]

DAFTAR PUSTAKA

Buku

Arnauld, Andreas Von (ed). *The Cambridge Handbook of New Human Rights: Recognition, Novelty, Rhetoric*. UK: Cambridge University Press. 2020. DOI: 10.1017/9781108676106.

Atmasasmita, Romli. *Teori Hukum Intergratif: Rekonstruksi terhadap Teori Hukum Pembangunan dan Teori Hukum Progresif*. Yogyakarta: Genta Publishing. 2012.

Claypoole, Ted & Theresa Payton. *Protecting Your Internet Identity: Are You Naked Online*. London: Rowman & Littlefield. 2017.

Competition Bureau Canada. *The Little Black Book of Scams: Your Guide to Protection Against Fraud*. Ottawa Competition Bureau Canada. 2012.

Dowd, Rebekah. *The Birth of Digital Human Rights: Digitized Data Governance as a Human Rights Issue in the EU*. Cham: Palgrave Macmillan, Springer. 2022.

Fuady, Munir. *Teori-Teori Besar (Grand Theory) dalam Hukum*. Jakarta: Kencana. 2013.

Gehl, Robert W. & Sean T. Lawson. *Social Engineering: How Crowdmasters, Phreaks, Hackers, and Trolls Created a New Form of Manipulative Communication*. Cambridge, MA: MIT Press. 2022. DOI: https://doi.org/10.7551/mitpress/12984.001.0001.

Gray, Joe. *Practical Social Engineering*. San Franciso: No Starch Press. 2021.

Green, James A. (ed). *Cyber Warfare: A Multidisciplinary Analysis*. New York: Routledge. 2015.

Hadnagy, Christopher. *Social Engineering: The Art of Human Hacking*. Indianapolis: Wiley Publishing. 2011.

Hanson, Helen & Catherine O'Rawe. *The Femme Fatale: Images, Histories, Contexts*. UK: Palgrave Macmillan. 2010.

Kusumaatmadja, Mochtar. *Konsep-Konsep Hukum dalam Pembangunan*. Bandung: Alumni. 2006.

McAlaney, John, *et.al.* (Eds). *Psychological and Behavioral Examinations in Cyber Security*. Hersey: IGI Global. 2018. DOI: http://doi.org/10.4018/978-1-5225-4053-3.ch003.

Mitnick, Kevin D. & William L. Simon. *The Art of Deception: Controlling the Human Element of Security*. Indianapolis: Wiley Publishing. 2002.

Ozkaya, Erdal. *Learn Social Engineering*. Birmingham: Packt Publishing. 2018.

Pond, Roscoe. *Contemporarty Juristic Theory*. Claremont CA: Pamona College. 1940.

Rains, Tim. *Cybersecurity Threats, Malware Trends, and Strategies*. Birmingham: Packt Publishing. 2020.

Rakhmat, Jalaluddin. *Rekayasa Sosial: Reformasi, Revolusi, atau Manusia Besar?*. Bandung: Rosdakarya. 1999.

Rodriguez, Rosana Montanez, *et.al. Cybersecurity and Cognitive Science, Chapter 1 - Social Engineering Attacks and Defense in the Physical World vs. Cyberspace: A Contrast Study*. UK: Academic Press. 2022. https://doi.org/10.1016/B978-0-323-90570-1.00012-7.

Tanya, Bernard L., *et.al. Teori Hukum: Strategi Tertib Manusia Lintas Ruang dan Generasi*. Yogyakarta: Genta Publishing. 2013.

Jurnal

Ahuja, Mehak & Anshdha Sharma. "Right to Internet: Fundamental Right". *IOSR Journal of Humanities and Social Science*, Vol. 25, Issue 12, Series 8, 2020, pp. 1-12. DOI: 10.9790/0837-2512080112.

Aldawood, Hussain & Geoffrey Skinner. "An Advanced Taxonomy for Social Engineering Attacks". *International Journal of Computer Application*, Vol. 177, No. 30, Januari 2020.

_____. "Reviewing Cyber Security Social Engineering Training and Awareness Programs – Pitfalls and Ongoing Issues". *Future Internet*, Vol. 11, No. 73, 2019, DOI: 10.3390/fi11030073.

Alfayoumi, Ibrahim S. & Tawfiq S. Barhoom. "Client – Side Pharming Attacks Detection Using Authoritative Domain Name Servers". *International Journal of Computer Applications*, Vol. 113, No. 10, Maret 2015. DOI: 10.5120/19862-1820.

Ali, Azad. "Ransomeware: A Research and A Personal Case Study of Dealing with this Nasty Malware". *Issue in Informing Science and Information Technology*, Vol. 14, 2017.

Alkhalil, Zainab, *et.al*. "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy". *Frontiers in Computers Science*, Vol. 3, March 2021. https://doi.org/10.3389/fcomp.2021.563060.

Alsufyani, Asma A., *et.al*. "Social Engineering, New Era of Stealth and Fraud Common Attack Techniques and How to Prevent Against". *International Journal of Scientific & Technology Research*, Vol. 9, Issue 10, 2020.

Alunge, Rogers. "Breach of Security vs Personal data Breach: Effect on EU Data Subject Notification Requirements". *International Data Privacy Law*, Vol. 11, Issue 2, April 2021. https://doi-org.eres.qnl.qa/10.1093/idpl/ipaa021.

Alwanain, Mohammed I. "An Evaluation of User Awareness for the Detection of Phishing Emails". *International Journal of Advanced Computer Science and Applications*, Vol. 10, No. 10, 2019.

Andrews, Nathanael. ""Can I Get Your Digits?": Illegal Acquisition of Wireless Phone Numbers For SIM-Swap Attacks and Wireless Provider Liability". *Northwestern Journal of Technology and Intellectual Property*, Vol. 16, Issue 2, 2018.

Anthony, Mark & Ambay, *et.al*. "Dystopia is Now: Digital Authoritarianism and Human Rights in Asia". *Global Campus Human Rights Journal*, Vol. 3, No. 2, 2019. http://doi.org/20.500.11825/1575.

Atkins, Brandon & Wilson Huang. "A Study of Social Engineering in Online Frauds". *Open Journal of Social Science,* Vol. 1, No. 3, 2013. DOI: 10.4236/jss.2013.13004.

Ayalew, Yohannes Eneyew. "Untrodden Paths Towards the Right to Privacy in The Digital Era Under African Human Right Law". *International Data Privacy Law*, Vol. 12, Issue 1, February 2022.

Bansla, Neetu, *et.al.* "Social Engineering: A Technique for Managing Human Behavior". *Journal of Information Technology and Science*, Vol. 5, Issue 1, 2019.

Broadhurst, Roderic, *et.al.* "Phishing and Cybercrime Risk in a University Student Community". *International Journal of Cybersecurity Intelligence & Cybercrime*, Volume 2, Issue 1, Article 2, 2019.

Brody, Richard G., *et.al.* "An Insider's Look at the Rise of Nigerian 419 Scam". *Journal of Financial Crime*, Vol. ahead-of-print, No. ahead-of-print, 2020. DOI: 10.1108/JFC-12-2019-0162.

Bullee, Jan-Willem, *et.al.* "Spear Phishing in Organitations Explained". *Information & Computer Security*, Vol. 25, No. 5, 2017, pp. 593-613. DOI: 10.1108/ICS-03-2017-0009.

Burruss, George W. *et.al.* "Website Defacer Classification: A Finite Mixture Model Approach". *Social Science Computer Review*, 2021, pp. 1-13. DOI: https://doi.org/10.1177/0894439321994232.

Camri, Elinor. "Regulating Behaviours on the European Union Internet, the Case of Spam Versus Cookies". *International Review of Law, Computers & Technology*, Vol. 31, Issue 3, 2017. https://doi.org/10.1080/13600869.2017.1304616.

Chawki, Mohamed. "Nigerian Tackles Advance Fee Fraud". *Journal of Information, Law & Technology*, Vol. 1, 2009.

Conteh, Nabie Y. & Malcolm D. Royer. "The Rise in Cybercrime and the Dynamics of Exploiting the Human Vulnerability Factor". *International Journal of Computer (IJC)*, Vol. 20, No. 1, 2016.

Costello, Roisin A. "Genetic Data and The Right to Privacy: Towards a Relational Theory of Privacy?". *Human Right Law Review*, Vol. 22, Issue 1, 2022. https://doi.org/10.1093/hrlr/ngab031.

Custers, Bart. "New Digital Rights: Imagining Additional Fundamental Rights for the Digital Era". *Computer Law & Security Review*, Vol. 44, 2022, pp. 1-13. DOI: https://doi.org/10.1016/j.clsr.2021.105636.

Daly, Angela. "The Introduction of Data Breach Notification Legislation in Australia: A Comparative View". *Computer Law and Security Review*, Vol. 34, Issue 3, June 2018. https://doi.org/10.1016/j.clsr.2018.01.005.

Dave, Konark Truptiben. "Brute-force Attack "Seeking but Distressing"". *International Journal of Innovations in Engineering and Technology*, Vol. 2, Issue 3, Juni 2013.

Desai, Chirag R. & Narendra M. Shekokar. "VILEEAR: Detection of Drive by Download attack on Malicious Web Pages". *International Journal of Science and Research*, Vol. 4, Issue 4, 2015.

Dror-Shpoliansky, Dafna & Yuval Shany. "It's The End of The (Offline) World as We Know it: From Human Rights to Digital Human Rights – a Proposed Typology". *Hebrew University of Jerusalem Legal Research Paper,* No. 20-36, 2020.

Dugan, Natalie "#TimesUp On Individual Litigation Reform: Combatting Sexual Harassment Through Employee-Driven Action and Private Regulation". *Colombia Journal of Law and Social Problem*, Vol. 53, No. 2, 2020.

Fan, Wenjun, *et.al.* "Social Engineering: I-E Based Model of Human Weakness for Attack and Defense Investigations". *International Journal Network and Information Security*, Vol. 1, 2017. DOI: 10.5815/ijcnis.2017.01.01.

Fauji, Asep Ahmad. "Penerapan Prinsip UNCITRAL Model Law dalam Pembuktian Kasus Transaksi Elektronik di Indonesia". *Universitas of Bengkulu Law Journal,* Vol. 1, No. 1, April 2017. https://doi.org/10.33369/ubelaj.2.1.90-102.

Gibson, Dennis & Clive Harfield. "Contradictions and Inconsistencies in Australia's Mandatory Data Breach Notification Laws". *Computer Law and Security Review*, Vol. 42, September 2021. https://doi.org/10.1016/j.clsr.2021.105600.

Ho, Peng Foong, *et.al.* "Preventing Shoulder-Surfing Attack with the Concept of Concealing the Password Object' Information". *The Scientific World Journal*, 2014. DOI: 10.1155/2014/838623.

Howell, C. Jordan, *et.al.* "Website Defacement and Routine Activities: Considering the Important oh Hackers' Valuations of Potential Targets". *Journal of Crime and Justice*, Vol. 42, Issue 5, 2019, pp. 536-550. DOI: https://doi.org/10.1080/0735648X.2019.1691859.

Hughes, Lorine A. "Viruses, Worms, and Trojan Horses: Serious Crimes, Nuisance, or Both?". *Social Science Computer Review*, Vol. 25, No. 1, 2007. DOI: 10.1177/0894439306292346.

Isacenkova, Jelena, *et.al.* "Inside the SCAM Jugle: A Closer Look at 419 Scam Email Operations". *EURASIP Journal on Information Security*, Vol. 1, 2014. DOI: 10.1109/SPW.2013.15.

Jalali, Mohammad S., *et.al.* "Why Employees (Still) Click on Phishing Links: Investigation in Hospitals". *Journal of Medical Internet Research*, Vol. 22, No. 1, January 2020. DOI: 10.2196/16775.

Jampen, Daniel *et.al.* "Don't Click: Towards an Effective Anti-Phishing Training. A Comparative Literature Review". *Human-Centric Computing and Information Science*, Vol. 10, Issue 33, 2020. https://doi.org/10.1186/s13673-020-00237-7.

Jang-Jaccard, Julian & Surya Nepal. "A Survey of Emerging Threats in Cybersecurity". *Journal of Computer and System Sciences*, Vol. 80, Issue 5, August 2014. DOI: https://doi.org/10.1016/j.jcss.2014.02.005.

Kigerl, Alex. "Routine Activity Theory and Malware, Fraud, and Spam at the National Level". *Crime, Law and Social Change,* Vol. 76, Issue 2, September 2021. https://doi.org/10.1007/s10611-021-09957-y.

Kim, Jawon, *et.al.* "Research on Behavior-Based Data Leakage Incidents for the Sustainable Growth of an Organization". *Journal Sustainability*, Vol. 12, No. 15, 2020. DOI: https://doi.org/10.3390/su12156217.

Laskhari, Arash Habibi, *et.al.* "Shoulder Surfing Attack in Graphical Password Authentication". *International Journal of Computer Science and Information Security*, Vol. 6, No. 2, 2009.

Latipulhayat, Atip. "Khazanah: Mochtar Kusumaatmadja". *Padjajaran Jurnal Ilmu Hukum*, Vol. 1, No. 3, 2014.

_____. "Khazanah: Roscoe Pound". *Padjajaran Jurnal Ilmu Hukum*, Vol. 1, No. 2, 2014.

Makarov, Timofey Grigorievich & Elena Vassilievna Kobchikova. "Digital Rights". *Utopia y Praxis Latinoamericana*, Vol. 25, No. 12, 2020. DOI: https://doi.org/10.5281/zenodo.4280122.

Malar, M. Neela. "Impact of Cyber Crimes on Social Networking Pattern of Girls". *International Journal of Internet of Things*, Vol. 1, No. 1, 2012. DOI: 10.5923/j.ijit.20120101.02.

Mathiesen, Kay. "Human Rights for the Digital Age". *Journal of Mass Media Ethics*, Vol. 29, Issue 1, 2014. https://doi.org/10.1080/08900523.2014.863124.

Mehmonov, Kambariddin M. & Elbek T. Musaev. "Legal Regime of Digital Rights". *Elementary Education Online*, Vol. 21, Issue 2, 2022. DOI: 10.17051/ilkonline.2021.03.193.

Miller, Bryon, *et.al.* "Prevention of Phishing Attacks: A Three-Pillared Approach". *Issue in Information System*, Vol. 21, No. 2, 2020. https://doi.org/10.48009/2_iis_2020_1-8.

Nugraha, Michelle Adi, *et.al.* "Insight on Media Literacy and Social Engineering Vulnerability Predictors: Lifelong Learning Gravity". *Cypriot Journal of Educational Sciences*, Vol. 15, Issue 5, 2020, pp. 955-975. DOI: https://doi.org/10.18844/cjes.v15i5.5124.

Odeh, Noor Ammar, *et.al.* "A Survey of Social Engineering Attacks: Detection and Prevention Tools". *Journal of Theoritical and Applied Information Technology*, Vol. 99, No. 18, 2021.

Ong, Rebecca & Sandy Sabapathy. "Hong Kong's Data Breach Notification Scheme: From the Stakeholder Perspective". *Computer Law and Security Review*, Vol. 42, September 2021. https://doi.org/10.1016/j.clsr.2021.105579.

Otero, Daniel. "How "Me Too" Hollywood Types Destroyed Feminism". *Journal of Arts & Humanities*, Vol. 7, Issue 11, 2018. DOI: http://dx.doi.org/10.18533/journal.v7i10.1525.

Pangrazio, Luci & Julian Sefton Green. "Digital Rights, Digital Citizenship and Digital Literacy: What's the Difference?". *Journal*

of New Approaches in Educational Research, Vol. 10, No. 1, 2021. https://doi.org/10.7821/naer.2021.1.616.

Papazov, Yavor. "Social Engineering". *Educational Notes Paper*, North Atlantic Treaty Organization (NATO) dan Science and Technology Organization, 2016, pp. 1-18. DOI: 10.14339/STO-EN-IST-143-08-PDF.

Pirnau, Mironela. "Considerations on Preventing Social Engineering Over the Internet". *Memoirs of the Scientific Sections of The Romanian Academy*, 2017.

Prudentov, Roman V. "Private Life and Surveillance in a Digital Era: Human Rights in European Perspective". *Digital Law Journal*, Vol. 1, No. 2, 2020. https://doi.org/10.38044/2686-9136-2020-1-2-41-52.

Resti, Sandra Widya & Titien Diah Selistyarini. "From Enchantress to Murderess: The Portrayal of Amy Dunne as "Femee Fatale" in Gillian Flynn's Gone Girl". *Allusion*, Vol. 5, No. 2, 2016.

Richardson, Michael D., *et.al.* "Planning for Cyber Security in Schools: The Human Factor". *Education Planning Journal*, Vol. 27, No. 3, 2020.

Rochel, Johan. "Connecting the Dots: Digital Integrity as a Human Right". *Human Rights Law Review*, Vol. 21, Issue 2, 2021. https://doi.org/10.1093/hrlr/ngaa063.

Salahdine, Fatima & Naima Kaabouch. "Social Engineering Attacks: A Survey". *Future Internet*, Vol. 11, No. 89, 2019. DOI: 10.3390/fi11040089.

Sanders, Cynthia K. & Edward Scanlon. "The Digital Divide Is a Human Right Issue: Advancing Social Incluision Through Social Work Advocacy". *Journal of Human Rights and Social Work*, Vol. 6, Issue 2, 2021. https://doi.org/10.1007/s41134-020-00147-9.

Sheppard, Leah D. & Stefanie K. Johnson. "The Femme Fatale Effect: Attractiveness is a Liability for Businesswomen's Perceived Thruthfulness, Trust, and Deservingness of Termination". *Sex Roles*, Vol. 81, No. 4, 2019, https://doi.org/10.1007/s11199-019-01031-1.

Siddiqi, Murtaza Ahmed, *et.al.* "A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures". *Applied Science*, Vol. 12, 2022. https://doi.org/10.3390/app12126042.

Sinambela, Winda Handayani, *et.al.* "Analisis Yuridis Pemalsuan Identitas oleh Penjual Kartu Subscriber Indentity Module Internet". *Jom Fakultas Hukum*, Vol. V, Edisi 2, 2018.

Smith, Andrew. "Nigerian Scam E-Mais and The Charms of Capital". *Cultural Studies*, Vol. 23, No. 1, 2008. DOI: 10.1080/09502380802016162.

Soomro, Tariq Rahim & Mumtaz Hussain. "Social Media-Related Cybercrimes and Tehcniques for Their Prevention". *Applied Computer Systems*, Vol. 24, No. 1, Mei 2019. DOI: https://doi.org/10.2478/acss-2019-0002.

Struthers, Alison E. C. "Human Rights: A Topic Too Controversial for Mainstream Education?". *Human Rights Law Review*, Vol. 16, Issue 1, 2016. https://doi.org/10.1093/hrlr/ngv040.

Tampubolon, Kartini Eliva Angel. "Perbedaan Cyber Attack, Cybercrime, dan Cyber Warfare". *Jurist-Diction*, Vol. 2, No. 2, Maret 2019.

Tompkins, Jessica E., *et.al.* "Kawaii Killers and Femme Fatale: A Textual Analysis of Female Characters Signifying Benevolent and Hostile Sexism in Video Games". *Journal of Broadcasting & Electronic Media*, Vol. 6, Issue 2, 2020. https://doi.org/10.1080/08838151.2020.1718960.

Ulbashev, Alim K. "The Right to a Name: Back to the Future". *Digital Law Journal*, Vol. 1, No. 3, 2020. https://doi.org/10.38044/2686-9136-2020-1-3-40-50.

Wang, Victoria, *et.al.* "Internet Banking in Nigeria: Cybersecurity Breaches, Practice and Capability". *International Journal of Law*, Vol. 62, September 2020. https://doi.org/10.1016/j.ijlcj.2020.100415.

Wang, Zuoguang, *et.al.* "Defining Social Engineering in Cybersecurity". *IEEE Access*, Volume 8, 2020, pp. 85094-85115. DOI: 10.1109/ACCESS.2020.2992807.

_____. "Social in Cybersecurity: A Domain Ontology and Knowledge Graph Applicatioan Examples". *Journal Cybersecurity*, Vol. 4, Issue 31, 2001, pp. 1-21. DOI: https://doi.org/10.1186/s42400-021-00094-6.

Washo, Amy Hetro. "An Interdisciplinary View of Social Engineering: A Call to Action for Research". *Computers in Human Behavior Reports*, Vol. 4, 2021. https://doi.org/10.1016/j.chbr.2021.100126.

Wibowo, Mia Haryati & Nur Fatimah. "Ancaman Phishing Terhadap Pengguna Sosial Media dalam Dunia Cyber Crime". *Jurnal of Education and Information Communication Technology*, Vol. 1, No. 1, 2017.

Prosiding

Eiband, Malin, *et.al*. "Understanding Shoulder Surfing in the Wild: Stories from User and Observers". *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, Denver, Mei 2017. DOI: 10.1145/3025453.3025636.

Eslahi, Meisam, *et.al*. "Bots and Botnets: An Overview of Characteristics, Detection and Challenges". *IEEE International Conference on Control System, Computing and Engineering*, 23-25 November 2021, Malaysia, pp. 349-354. DOI: 10.1109/ICCSCE.2012.6487169.

Ibrahim, Nada, *et.al*. "SIM Card Forensic: Digital Evidance". *Proceedings Annual ADFSL Conference on Digital Forensic, Security and Law*, 2016.

Janczewski, Lech J. & Lingyan Fu. "Social Engineering-Based Attacks: Model and New Zealand Perspective". *Proceedings of the International Multiconference on Computer Science and Information Technology*, 2010.

Le, Van Lam, *et.al*. "Anatomy of Druve-by Download Attack". *Proceedings of the Eleventh Australasian Information Security Conference*, Adelaide, Australia, 2013.

Lohani, Shivam. "Social Engineering: Hacking into Humans". *Proceedings of 4th International Conference on Cyber Security (ICSS)*, 2018.

Tari, Furkan, *et.al*. "A Comparison of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical Passords".

Proceedings of the 2nd Symposium on Usable Privacy and Security (SOUPA), Pennsylvania, 12-14 Juli 2014. DOI: 10.1145/1143120.1143128.

TS, Korobeinikova. "Digital Rights as an Object of Civil Rights". *Prosiding Advances in Economic, Business and Management Research*, Vol. 138, 2nd International Scientific and Practical Conference Modern Management Trends and the Digital Economy: From Regional Development to Global Economic Growth (MTDE 2020).

Weaver, Robert M. & Joseph A. Cazier. "Dumpster Diving: A Study on Data Recovery and Exploitation". *Southeast Institute for Operation Research and the Management Science Conference*, 2007.

Tesis/Disertasi

Dennon, Anne. "The Emergence of the Feminist Fatele in American Film Noir". *Master's Thesis*, Central Washington University, 2017.

Hove, Lindiwe T. "Strategies Used to Mitigate Social Engineering Attacks". *Dissertations*, College of Management and technology, Walden University, 2020.

Jaber, Maysaa. "Sirens in Command: The Criminal Femme Fatale in American Hardboile Crime Fiction". *Thesis*, University of Manchester for the Degree of Doctor of Philosophy in the Faculty of Humanities, 2011.

Papadopoulos, Sofia. "Human Trafficking for Sexual Exploitation Purpose". *Thesis*, Institute for International Law of Peace and Armed Conflict, Ruhr University Bochum, 2021.

Laporan/Majalah

Anti Phishing Working Group. *Phishing Activity Trends Report, 1st Quarter 2022*. APWG. 7 Juni 2022.

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). *Profil Internet Indonesia 2022*. Juni 2022.

Barracuda. *Spear Phishing: Top Threats and* Trends. Vol. 5. Desember 2020.

Bitdefender. *Mid-Year Threats Landscape Report*. 2019.

Carbonite & Webroot. *11 Types of Phishing Attacks You Need to Know to Stay Safe*. 2020.

Damen, Juliane, *et.al*. "The Human Right of Privacy in the Digital Age". *Staat, Recht und Politik - Forschungs - und Diskussionpapiere, Working Paper,* Universitatsverlag Potsdam, 2017. http://nbn-resolving.de/urn:nbn:de:kobv:517-opus4-399265.

Diaz, Rodrigo Mariano. "Cybersecurity in the Time of Covid-19 and the Transition to Cyberimmunity". *Bulletin FAL: Facilitation of Transport and Trade in Latin America and the Caribbean*, Bulletin 382, Number 6, 2020.

Dierking, Elanor. *The Weinstein Effect and Mediated Non-Apologies*. Media@LSE, London School of Economics and Political Sciene. 2019.

Ebner, Nick. *Cyber Space, Cyber Attack and Cyber Weapons: A Contribution to the Terminology*. Institute for Peace Research and Security Policy. University of Hamburg, October 2015.

Fraklin, Marianne, *et.al. The Charter of Human Rights and Principles for the Internet*. Internet Governance Forum dan United Nation. August 2014.

Hathaway, Oona A., *et.al*. "The Law of Cyber-Attack". *California Law Review*, Vol. 100, 2012.

Keepnet Labs. *Phishing Trends Report 2020*. 2020.

Kwong, Lieutenant Henry. *ATM Shoulder Surfing*. Press Release. Milpitas Police Department. Case 15-002-067. 15 Januari 2015.

Lourenco, Marco Barros & Louis Marinos (eds). *European Union Agency for Cybersecurity* (ENISA), *Phishing ENISA Threat Landscape*. Attiki: ENISA. 2020. DOI: 10.2824/552242.

Mitnik, Kevin & The Global Ghost Team. *The History of: Social Engineering & How to Stay Safe*. Las Vegas: Mitnick Security Consulting. 2020.

Myers, Nick. *Cyber Security: Cyber Crime, Attacks and Terrorism*. Old Dominion University UN Day 2020 Issue Brief, GA First Committee (DISC). 2020.

National Cyber Security Centre. *Common Cyber Attacks: Reducing the Impact*. Cyber Attacks White Paper. Januari 2016.

Nguyen, Van. *Attribution of Spear Phishing Attacks: A Literature Survey*.

Australian Government, Department of Defence, Cyber and Electronic Warfare Division, Defense Science and Technology Organisation, South Australia: DSTOP Defence Science and Technology Organisation, 2013.

Papazov, Yavor. "Social Engineering". *Science and Technology Organization, Educational Notes Paper,* North Atlantic Treaty Organization, 2016. DOI: 10.14339/STO-EN-IST-143-08-PDF.

Santhosh, Sruthy. "Social Engineering Attacks". *The Bit: The Bullettin of Information Technology, Rajagiri School of Engineering & Technology,* April-August 2015.

Peraturan Perundang-undangan

Kitab Undang-Undang Hukum Pidana (KUHP) Republik Indonesia.

Peraturan Menteri Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi.

Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 3 Tahun 2011 tentang Transfer Dana.

Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.

Sumber Elektronik

Abrams, Lawrence. 10 Juni 2021. "JBS Paid $11 Million to REvil Ransomeware, $22,5 M First Demanded". *Bleeping Computers*. Diakses dari https://www.bleepingcomputer.com/news/security/jbs-paid-11-million-to-revil-ransomware-225m-first-demanded/ (diakses pada 24 Mei 2022).

_____. 10 Mei 2021. "City of Tulsa's Online Services Disrupted in Ransomeware Incident". *Bleeping Computer*. Diakses dari https://www.bleepingcomputer.com/news/security/city-of-tulsas-online-services-disrupted-in-ransomware-incident/ (diakses pada 26 Mei 2022).

_____. 15 Agustus 2021. "Hacker Claims to Steal Data of 100 Million T-Mobile Customers". *Bleeping Computer*. Diakses

dari https://www.bleepingcomputer.com/news/security/hacker-claims-to-steal-data-of-100-million-t-mobile-customers/ (diakses pada 18 Mei 2022).

_____. 21 Mei 2022. "Ransomware Attack Exposes Data of 500,000 Chicago Students". *Bleeping Computers*. Diakses dari https://www.bleepingcomputer.com/news/security/ransomware-attack-exposes-data-of-500-000-chicago-students/ (diakses pada 9 Juni 2022).

_____. 27 Mei 2021. "Canada Post Hit by Data Breach After Supplier Ransomeware Attack". *Bleeping Computer*. Diakses dari https://www.bleepingcomputer.com/news/security/canada-post-hit-by-data-breach-after-supplier-ransomware-attack/ (diakses pada 21 Mei 2022).

_____. 8 November 2021. "Robinhood Discloses Data Breach Impacting 7 Million Customers". *Bleeping Computer*. Diakses dari https://www.bleepingcomputer.com/news/security/robinhood-discloses-data-breach-impacting-7-million-customers/ (diakses pada 17 Mei 2022).

_____. 9 Juli 2022. "Mangatoon Data Breach Exposes Data Form 23 Million Accounts". *Bleeping Computer*. Diakses dari https://www.bleepingcomputer.com/news/security/mangatoon-data-breach-exposes-data-from-23-million-accounts/ (diakses pada 15 Juli 2022).

Allyn, Bobby. 20 Agustus 2019. "22 Texas Towns Hit With Ransomeware Attack In 'New Front' of Cyberassault". *NPR*. Diakses dari https://www.npr.org/2019/08/20/752695554/23-texas-towns-hit-with-ransomware-attack-in-new-front-of-cyberassault (diakses pada 24 Mei 2022).

Astutik, Yuni. 13 Juli 2020. "Terungkap! Ini Cara Penipu Sebarkan Ribuan SMS Spam Per Jam". *CNBC Indonesia*. Diakses dari https://www.cnbcindonesia.com/news/20200713142625-4-172258/terungkap-ini-cara-penipu-sebarkan-ribuan-sms-spam-per-jam (diakses pada 24 Mei 2022).

Bajak, Frank. 23 Juli 2021. "Kaseya Gets Master Decryption Key After Jult 4 Global Attack". *Apnews*. Diakses dari https://apnews.com/article/lifestyle-technology-joe-biden-europe-business-bb7298b31b7157640fbd5f90fc19c224 (diakses pada 24 Mei 2022).

Balu, Nivedita. 7 Oktober 2021. "Amazon's Twitch Hit by Data Breach". *Reuters*. Diakses dari https://www.reuters.com/technology/amazons-twitch-hit-by-data-breach-2021-10-06/ (diakses pada 18 Mei 2022).

BBC NEWS. 20 April 2018. "Two Years For Teen 'Cyber Terrorist' Who Targeted Us Officials". *BBC News*. Diakses dari https://www.bbc.com/news/uk-england-leicestershire-43840075 (diakses pada 28 Mei 2022).

_____. 23 Juli 2019. "Lancaster University Students' Data Stolen by Cyber-Thieves". *BBC News*. Diakses dari https://www.bbc.com/news/uk-england-lancashire-49081056 (diakses pada 22 Mei 2022).

Bisson, David. 5 November 2019. "5 Social Engineering Attacks to Watch Out For". *Tripwire*. Diakses dari https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/.

Bracken, Becky. 11 Juni 2022. "Baby Clothes Giant Carter's Leaks 410K Customer Records". *Threat Post*. Diakses dari https://threatpost.com/baby-clothes-carters-leaks-customer-records/166866/ (diakses pada 21 Mei 2022).

Brewster, Thomas. 14 Februari 2017. "This Fake Femme Fatale Is Stealing Google Accounts From Journalists and Human Rights Activists". *Forbes*. Diakses dari https://www.forbes.com/sites/thomasbrewster/2017/02/14/safeena-malik-qatar-fake-cyberespionage-hacking-campaign/?sh=5e134f99435a (diakses pada 2 Juli 2022).

Budi, Candra Setia. 24 Juli 2020. "Fakta Kasus Pembobolan Rp 300 Juta dari 3 Bank, Manfaatkan Sampah Struk ATM, Gunakan Data dari Website KPU". *Kompas*. Diakses dari https://regional.kompas.com/read/2020/07/24/16242951/fakta-kasus-pembobolan-rp-300-juta-dari-3-bank-manfaatkan-sampah-struk-atm?page=all (diakses pada 30 Mei 2022).

Castle, Stephen. 18 Maret 2007. "Thief Woos Bank Staff Which Chocolates- Then Steals Diamonds Worth £14m". *Independent*. Diakses dari https://www.independent.co.uk/news/world/europe/thief-woos-bank-staff-chocolates-then-steals-

diamonds-worth-163-14m-5332414.html (diakses pada 11 Mei 2022).

CNN Indonesia. 06 Februari 2020. "Pembobolan Rekening Ilham Bintang, Data Dijual Orang Bank". *CNN Indonesia*. Diakses dari https://www.cnnindonesia.com/nasional/20200205211241-12-472073/pembobolan-rekening-ilham-bintang-data-dijual-orang-bank (diakses pada 6 Juni 2022).

_____. 23 Januari 2020. "Penipuan Online, Kejahatan Paling Banyak di 2019". *CNN Indonesia*. Diakses dari https://www.cnnindonesia.com/teknologi/20200123164303-185-468075/penipuan-online-kejahatan-paling-banyak-di-2019 (diakses pada 13 Mei 2022).

Combs, Veronica. 22 Juli 2021. "Scammers Offer Streaming Service, Giveaways and a Fake Cyber Currency to Cash in on the Olympic Games". *TechRepublic*. Diakses dari https://www.techrepublic.com/article/scammers-offer-streaming-services-giveaways-and-a-fake-cyber-currency-to-cash-in-on-the-olympic-games/ (diakses pada 23 Juni 2022).

Cruze, Danny Cyril D. 19 Juni 2021. "Android Smartphone users alert! Remove these 8 Apps laced with 'Joker' Malware". *Livemint*. Diakses dari https://www.livemint.com/technology/apps/android-smartphone-users-alert-remove-these-8-apps-laced-with-joker-malware-11624103586505.html (diakses pada 28 Mei 2022).

Cukier, Michel. 9 Februari 2007. "Study: Hackers Attack Every 39 Seconds". University of Maryland. Diakses dari https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds (diakses pada 5 Mei 2022).

David, Benjamin. 24 Mei 2022. "US Car Giant General Motors Hit by Cyber-Attack Exposing Car Owners Personal Info". *Info Security Magazine*. Diakses dari https://www.infosecurity-magazine.com/news/general-motors-hit-by-cyber-attack/ (diakses pada 9 Juni 2022).

Davies, Caroline. 5 Desember 2012. "Royal Baby Hoax Call Leaves Duchess's Hospital Unamused". *The Guardian*. Diakses dari https://www.theguardian.com/uk/2012/dec/05/royal-baby-hoax-call-hospital (diakses pada 28 Mei 2022).

Dr. Web. 1 Juli 2021. "Android Trojan Steal Facebook Users's Logins and Passwords". Diakses dari https://news.drweb.com/show/?i=14244&lng=en (diakses pada 28 Mei 2022).

Eichleberger, Erika. 20 Maret 2014. "What I Learned Hanging Out With Nigerian Eial Scammers". *Mother Jones*. Diakses dari https://www.motherjones.com/politics/2014/03/what-i-learned-from-nigerian-scammers/ (diakses pada 24 Mei 2022).

European Commission. 22 Januari 2022. "Commission Puts Forward Declaration on Digital Rights and Principles for Everyone in the EU". *Press Release*. Diakses dari https://ec.europa.eu/commission/presscorner/detail/en/ip_22_452 (diakses pada 27 Juni 2022).

FBI. 1 Agustus 2018. "How Cyber Crime Group FIN7 Attacked and Stole Data form Hundreds of U.S Companies". *FBI*. Diakses dari https://www.fbi.gov/contact-us/field-offices/seattle/news/stories/how-cyber-crime-group-fin7-attacked-and-stole-data-from-hundreds-of-us-companies (diakses pada 10 Mei 2022).

_____. "Scam and Safety: Business Email Compromise". *FBI*. Diakses dari https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise (diakses pada 25 Mei 2022).

Franedya, Roy. 16 Juli 2020. "Twitter Ungkap Sebab Akun Bill Gates Hingga Obama Bisa Diretas". *CNBC Indonesia*. Diakses dari https://www.cnbcindonesia.com/tech/20200716124829-37-173232/twitter-ungkap-sebab-akun-bill-gates-hingga-obama-bisa-dihack (diakses pada 13 Mei 2022).

Fried, Robert B. "Dumspter: Beware of Treasure". *Crime and Clues: The Art and Science of Criminal Investigation*. Diakses dari https://social-engineer.org/wiki/archives/DumpsterDiving/CrimeandClues_dumpster_diving.htm (diakses pada 28 Mei 2022).

Gatlan, Sergiu. 12 November 2021. "Costco Disclose Data Breach After Finding Credit Card Skimmer". *Bleeping Computer*. Diakses dari https://www.bleepingcomputer.com/news/security/costco-discloses-data-breach-after-finding-credit-card-skimmer/ (diakses pada 15 Mei 2022).

_____. 16 Juni 2021. "Ukraine Arrest Clop Ransomeware Gang Members, Seizes Servers". *Bleeping Computer*. Diakses dari

https://www.bleepingcomputer.com/news/security/ukraine-arrests-clop-ransomware-gang-members-seizes-servers/ (diakses pada 27 Mei 2022).

_____. 21 Mei 2021. "Air India Data Breach Impacts 4.5 Million Costumers". *Bleeping Computer*. Diakses dari https://www.bleepingcomputer.com/news/security/air-india-data-breach-impacts-45-million-customers/ (diakses pada 19 Mei 2022).

_____. 30 Juni 2022. "OpeanSea Discloses Data Breach, Warn Users of Phising Attacks". *Bleeping Computers*. Diakses dari https://www.bleepingcomputer.com/news/security/opensea-discloses-data-breach-warns-users-of-phishing-attacks/ (diakses pada 7 Juli 2022).

Ginting, Nanda Sagita. 7 Juni 2015. "Diskominfo Kabupaten Magelang Masih Lakukan Penyelidikan Terkait Kebocoran Data Penduduknya". *Tribun Jogja*. Diakses dari https://jogja.tribunnews.com/2021/06/07/diskominfo-kabupaten-magelang-masih-lakukan-penyelidikan-terkait-kebocoran-data-penduduknya (diakses pada 9 Mei 2022).

Gobel, Tenri & Paramitha Sandy. 9 Desember 2021. "Pakai Internet tanpa Budaya Keamanan Siber, Kita akan Hancur". *Cyberthreat*. Diakses dari https://cyberthreat.id/insightdetil/9548/Menyoroti-Budaya-Keamanan-Siber (diakses pada 9 Mei 2022).

Goddard, William. 27 Mei 2021. "Cyber Security Statistics 2020". *IT Chronicles*. Diakses dari https://itchronicles.com/information-security/cyber-security-statistics-2020/ (diakses pada 6 Mei 2022).

Goodin, Dan. 12 November 2021. "Booking.com Was Reportedly Hacked by a Us Intel Agency But Never Told Customers". *Ars Technica*. Diakses dari https://arstechnica.com/gadgets/2021/11/new-book-claims-us-intel-agency-hacked-booking-com-in-2016/ (diakses pada 21 Mei 2022).

Greig, Jonathan. 22 Oktober 2021. "450 Million Cyberattacks Attempted on Japan Olympics Infrastructure: NTT". *Zdnet*. Diakses dari https://www.zdnet.com/article/nearly-450-million-cyberattacks-attempted-on-japan-olympics-infrastructure-ntt/ (diakses pada 21 Mei 2022).

Guritono, Tatang. 8 Oktober 2021. "Usai Dapat Serangan Siber, Situs Project Multatuli Belum Pulih Sepenuhnya". *Kompas*. Diakses dari https://nasional.kompas.com/read/2021/10/08/16093581/usai-dapat-serangan-siber-situs-project-multatuli-belum-pulih-sepenuhnya?page=all (diakses pada 25 Mei 2022).

Hafis, Faisal. 16 November 2021. "Lebih dari 20 Juta Kali Terdeteksi Upaya 'Brute Force Attack' di Indonesia". *Cyberthreat*. Diakses dari https://cyberthreat.id/read/12852/Lebih-dari-20-Juta-Kali-Terdeteksi-Upaya-Brute-Force-Attack-di-Indonesia (diakses pada 30 Mei 2022).

Higgins, David. 20 Oktober 2020. "6 Common Phishing Attacks and How to Protect Against Them". *Tripwire*. Diakses dari https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/ (diakses pada 22 Mei 2022).

Hukmana, Siti Yona. 10 Maret 2020. "Sindikat Pembobol Rekening Rp. 1,14 Miliar Ditangkap". *Medcom*. Diakses dari https://www.medcom.id/nasional/hukum/aNraLz1K-sindikat-pembobol-rekening-rp1-14-miliar-ditangkap (diakses pada 3 Juni 2022).

Ilascu, Iounut. 1 September 2021. "Lockbit Gang Leaks Bangkok Airways Data, Hits Accenture Customers". *Bleeping Computer*. Diakses dari https://www.bleepingcomputer.com/news/security/lockbit-gang-leaks-bangkok-airways-data-hits-accenture-customers/ (diakses pada 18 Mei 2022).

_____. 13 November 2021. "Surveillance Firm Pays $1 Million fine after 'Spy Van' Scandal". *Bleeping Computer*. Diakses dari https://www.bleepingcomputer.com/news/security/surveillance-firm-pays-1-million-fine-after-spy-van-scandal/ (diakses pada 24 Mei 2022).

Institute for Internet & the Just Society. "Digital Human Rights". Diakses dari https://www.internetjustsociety.org/digital-human-rights (diakses pada 2 Juli 2022).

Jie, Yang & Liza Lin. 15 Juni 2021. "Alibaba Falls Victim to Chinese Web Crawler in Large Data Leak". *The Wall Street Journal*. Diakses dari https://www.wsj.com/articles/alibaba-falls-victim-to-

chinese-web-crawler-in-large-data-leak-11623774850 (diakses pada 21 Mei 2022).

Kapersky. 11 Juli 2022. "TikTok Prank Based on Real Fraud Scheme: How Cybercriminals Are Convincing Victims to Call Them". *Kapersky*. Diakses dari https://www.kaspersky.com/about/press-releases/2022_tiktok-prank-based-on-real-fraud-scheme-how-cybercriminals-are-convincing-victims-to-call-them (diakses pada 15 Juli 2022).

Kelley, Diana. 30 Juni 2020. "The Psychology of Social Engineering-the "Soft" Side of Cybercrime". *Microsoft*. Diakses dari https://www.microsoft.com/security/blog/2020/06/30/psychology-social-engineering-soft-side-cybercrime/ (diakses pada 10 Mei 2022).

Kerskie, Carrie. 24 September 2021. "5 Step to Take After Clicking on Phishing Link". *Aging Care*. Diakses dari https://www.agingcare.com/articles/5-steps-to-take-after-clicking-on-a-phishing-link-178044.htm#:~:text=What%20Happens%20If%20You%20Click,undetectable%20to%20the%20average%20user (diakses pada 3 Juli 2022).

Kok, Kim Fai. 8 Desember 2020. "Truecaller Insight: Top 20 Countries Affected By Spam Calls in 2020". *Truecalles*. Diakses dari https://truecaller.blog/2020/12/08/truecaller-insights-top-20-countries-affected-by-spam-calls-in-2020-2/ (diakses pada 13 Mei 2022).

Mccullagh, Declan. 28 Juni 2000. "Twas Oracle That Spied on MS". *Wired*. Diakses dari https://www.wired.com/2000/06/twas-oracle-that-spied-on-ms/ (diakses pada 29 Mei 2022).

Mercedes-Benz. 24 Juni 2021. "Mercedes-Benz USA Announce Initial Findings of Data Investigation Affecting Customers and Interested Buyers". Diakses dari https://media.mbusa.com/releases/release-ee5a810c1007117e79e1c871352a4afa-mercedes-benz-usa-announces-initial-findings-of-data-investigation-affecting-customers-and-interested-buyers (diakses pada 20 Mei 2022).

Miessler, Daniel. 4 Oktober 2020. "Ransomware Groups Add a Third Threat Vector: DDos". Diakses dari https://danielmiessler.com/blog/ransomware-groups-add-a-third-threat-vector-ddos/ (diakses pada 24 Mei 2022).

Mitnick Security. 5 April 2021. "6 Types of Social Engineering Attacks". *Mitnick Security*. Diakses dari https://www.mitnicksecurity.com/blog/6-types-of-social-engineering-attacks (diakses pada 10 Mei 2022).

Mrozek, Thom. 26 Februari 2018. "L.A. Man Convicted of ATM 'Shoulder Surfing' that Allowed Him to Withdraw Cash after Bank Customers Left ATMs". *The United States Attorney's Office Central District of California*. Diakses dari https://www.justice.gov/usao-cdca/pr/la-man-convicted-atm-shoulder-surfing-allowed-him-withdraw-cash-after-bank-customers (diakses pada 2 Juni 2022).

Mustafa, Faisal. "Setelah Mengintip PIN ATM, Karyawan Rumah Sakit di Makassar Kuras Tabungan Teman". *I News Sulsel*. Diakses dari https://sulsel.inews.id/berita/setelah-mengintip-pin-atm-karyawan-rumah-sakit-di-makassar-kuras-tabungan-teman (diakses pada 2 Juni 2022).

Nannestad, Donald. 27 Oktober 2021. "Lincolnshire Teenager Ordered to Hand Over £2M After Gift Voucher Fraud". *Lincolnshire Live*. Diakses dari https://www.lincolnshirelive.co.uk/news/lincolnshire-teenager-makes-2m-fake-6116584 (diakses pada 3 Juni 2022).

Newsbeezer. 29 Juni 2021. "New Season of Rick and Morty Creates a Wave of Ransomeware Attacks". *Newsbeezer*. Diakses dari https://newsbeezer.com/portugaleng/new-season-of-rick-and-morty-creates-a-wave-of-ransomware-attacks/ (diakses pada 27 Mei 2022).

Nguyen, Jen Trang. "Five Ways to Prevent Social Engineering Attacks". *MDSNY*. Diakses dari https://www.mdsny.com/5-ways-to-prevent-social-engineering-attacks/ (diakses pada 7 Juli 2022).

Nistanto, Reska K. 21 Mei 2021. "Data 279 Juta Penduduk yang Bocor Identik dengan Milik BPJS, Kominfo Panggil Direksi". *Kompas*. Diakses dari https://tekno.kompas.com/read/2021/05/21/14351007/data-279-juta-penduduk-yang-bocor-identik-dengan-milik-bpjs-kominfo-panggil?page=all (diakses pada 9 Mei 2022).

Nord Pass. "Top 200 Most Common Passwords". *Nord Pass*. Diakses dari https://nordpass.com/most-common-passwords-list/ (diakses pada 2 Juni 2022).

Nugroho, Andi. 19 Agustus 2021. "Kejahatan Siber BEC di Indonesia Capai Rp. 300 Miliar, PPATK Baru Selamatkan Rp. 175 Miliar". *Cyberthreat*. Diakses dari https://cyberthreat.id/read/12282/Kejahatan-Siber-BEC-di-Indonesia-Capai-Rp-300-miliar-PPATK-Baru-Selamatkan-Rp175-Miliar (diakses pada 24 Mei 2022).

_____. 19 November 2021. "Peretas Brasil 'son1x' Serang Subdomain Propam Polri, Satu Server Web Ditanam Backdoor". *Cyberthrat*. Diakses dari https://cyberthreat.id/read/12886/Peretas-Brasil-son1x-Serang-Subdomain-Propam-Polri-Satu-Server-Web-Ditanam-Backdoor (diakses pada 15 Mei 2022).

_____. 22 Oktober 2021. "Basis Data Pengaduan KPAI Dijual di Internet, BSSN: Ada Kebocoran Akun Server". Diakses dari https://cyberthreat.id/read/12625/Basis-Data-Pengaduan-KPAI-Dijual-di-Internet-BSSN-Ada-Kebocoran-Akun-Server (diakses pada 17 Mei 2022).

_____. 24 Agustus 2021. "Paruh Pertama 2021, Jumlah Serangan Siber di Indonesia Capai 741,44 Juta, Melebihi Total Serangan Tahun Lalu". *Cyberthreat*. Diakses dari https://cyberthreat.id/read/12306/Paruh-Pertama-2021-Jumlah-Serangan-Siber-di-Indonesia-Capai-74144-Juta-Melebihi-Total-Serangan-Tahun-Lalu (diakses pada 7 Mei 2022).

_____. 25 Oktober 2021. "*Pusat Malware Nasional BSSN Terkena Deface, Hacker Brasil: Ini Serangan Balasan*". Diakses dari https://cyberthreat.id/read/12634/Pusat-Malware-Nasional-BSSN-Terkena-Deface-Hacker-Brasil-Ini-Serangan-Balasan (diakses pada 8 Mei 2022).

_____. 29 Juli 2021. "Yang Perlu Diketahui Seputar Peretasan Sistem BRI Life". *Cyberthreat*. Diakses dari https://cyberthreat.id/read/12171/Yang-Perlu-Diketahui-Seputar-Peretasan-Sistem-BRI-Life (diakses pada 18 Mei 2022).

Nye, James. 4 November 2013. "How 'High-Level U.S. Government Agency' Fell for Fake Femme Fatale Created by Two Hackers". *Dailymail*. Diakses dari https://www.dailymail.co.uk/news/

article-2486975/How-fake-Femme-fatale-created-hackers-carried-cyber-attack-high-level-U-S-government-agency.html (diakses pada 2 Juli 2022).

Partida, Devin. 21 Desember 2020. "Social Engineering Cyberattacks and How They're Impacting Business". *Security Infowatch*. Diakses dari https://www.securityinfowatch.com/cybersecurity/article/21203580/social-engineering-cyberattacks-and-how-theyre-impacting-businesses (diakses pada 10 Mei 2022).

Poitevin, Victor. 18 November 2021. "Illegal Streaming: Beware of the Backlash". *Strom Shield*. Diakses dari https://www.stormshield.com/news/illegal-streaming-beware-of-the-backlash/ (diakses pada 5 Juli 2022).

Prima, Erwin. 24 Oktober 2021. "Studi Cisco: 60 Persen UKM Indonesia Alami Pencurian Informasi". Diakses dari https://tekno.tempo.co/read/1520571/studi-cisco-60-persen-ukm-indonesia-alami-pencurian-informasi/full&view=ok (diakses pada 10 Mei 2022).

Purple Sec. "2021 Cyber Security Statistic: The Ultimate List of Stats, Data & Thrends". *Purple Sec*. Diakses dari https://purplesec.us/resources/cyber-security-statistics/#SocialEngineering (diakses pada 9 Mei 2022).

Putra, Rhazes. 14 Juni 2022. "Kemenkumham Terima Serangan Siber 385.980 Kali, Terbanyak dari AS". *Detik News*. Diakses dari https://news.detik.com/berita/d-6126722/kemenkumham-terima-serangan-siber-385980-kali-terbanyak-dari-as (diakses pada 20 Juni 2022).

Quach, Katyanna. 18 November 2021. "Canadian Teen Nabbed in $36.5M Crypto Heis-Possibly The Biggest Haul Yet by a Single Individual". *The Register*. Diakses dari https://www.theregister.com/2021/11/18/canadian_cryptocurrency_heist/ (diakses pada 4 Juni 2022).

Reeds, Craig. "The Seven Phases of a Cyber Attack". *DNV*. Diakses dari https://www.dnv.com/article/the-seven-phases-of-a-cyber-attack-118270 (diakses pada 8 Mei 2022).

Reid, Claire. 7 Juni 2022. "Huge Risk Million Face When Illegally Streaming At Home". *Lad Bible*. Diakses dari https://www.

ladbible.com/news/huge-risks-millions-face-when-illegally-streaming-at-home-20220607 (diakses pada 5 Juli 2022).

Reuters. 14 November 2021. "Hackers Compromise FBI Email System, Send Thousands of Messages". *Reuters*. Diakses dari https://www.reuters.com/world/us/hackers-compromise-fbis-external-email-system-bloomberg-news-2021-11-13/ (diakses pada 17 Mei 2022).

Sabbagh, Dan. 14 Juni 2021. "Ransomeware is Biggest Online Threat to People in UK, Spy Agency Chief To Warn". *The Guardian*. Diakses dari https://www.theguardian.com/technology/2021/jun/14/ransomware-is-biggest-online-threat-to-people-in-uk-spy-agency-chief-to-warn (diakses pada 24 Mei 2022).

Sandy, Oktarina Paramitha. 19 Januari 2022. "Data Pelamar Pertamina PTC Bocor, ELSAM Soroti Notifikasi Pemilih Data hingga Posko Pengaduan". *Cyberthreat*. Diakses dari https://cyberthreat.id/read/13341/Data-Pelamar-Pertamina-PTC-Bocor-ELSAM-Soroti-Notifikasi-Pemilik-Data-hingga-Posko-Pengaduan (diakses pada 15 Mei 2022).

_____. 25 Oktober 2019. "Pertama Kali dalam Sejarah, Polri Tangkap Hacker Ransomeware". *Cyberthreat*. Diakses dari https://cyberthreat.id/read/3532/Pertama-Kali-dalam-Sejarah-Polri-Tangkap-Hacker-Ransomware (diakses pada 25 Mei 2022).

Santoso, Audrey. 07 Agustus 2019. "Gasak Rp 113 M, Sindikat Nigerian Scam Dibekuk Polisi". *Detik News*. Diakses dari https://news.detik.com/berita/d-4655840/gasak-rp-113-m-sindikat-nigerian-scam-dibekuk-polisi (diakses pada 25 Mei 2022).

Sead Fadilpasic. 16 Juni 2021. "Majority of Ransomeware Victims are Hit with a Second Attack After Paying Up". *IT ProPortal*. Diakses dari https://www.itproportal.com/news/majority-of-ransomware-victims-are-hit-with-a-second-attack-after-paying-ransom/ (diakses pada 28 Mei 2022).

Security Through Education. "Dumpster Diving". *Social Engineer Org*. Diakses dari https://www.social-engineer.org/framework/information-gathering/dumpster-diving/ (diakses pada 29 Mei 2022).

Shabong, Yadarisa. 7 Juli 2021. "British Airways Settles with 2018 Breach Victims". *Reuters*. Diakses dari https://www.reuters.com/business/aerospace-defense/british-airways-reaches-settlement-with-customers-over-2018-data-breach-2021-07-06/ (diakses pada 21 Mei 2022).

Shields, Michael. 10 Juli 2021. "Ransomeware attack hits Swiss consumer outlet Comparis". *Reuters*. Diakses dari https://www.reuters.com/technology/ransomware-attack-hits-swiss-consumer-outlet-comparis-2021-07-09/ (diakses pada 27 Mei 2022).

Shuraeva, Anastasia. "Woman in White Long Sleeve Shirt Holding Black Smartphone". *Pexels*. Diakses dari https://www.pexels.com/photo/woman-relaxation-internet-writing-5704404/ (diakses pada 30 Mei 2022).

Stoppers, Crime. "Streaming Online: Know the Risks". Diakses dari https://crimestoppers-uk.org/keeping-safe/online-safety/streaming-online-know-the-risks#:~:text=Every%20time%20you%20access%20illegal,of%20fraud%20and%20data%20theft (diakses pada 3 Juni 2022).

Suud, Yuswardi A. 26 Oktober 2020. "Tangkal Rekayasa Sosial di Platform Digital, Gojek Tempuh Jalan Apa?". *Cyberthreat*. Diakses dari https://cyberthreat.id/insightdetil/8973/Tangkal-Rekayasa-Sosial-Gojek-Tempuh-Jalan-Apa (diakses pada 10 Mei 2022).

Taufiqqurahman, Muhammad. 11 Januari 2019. "Ratusan Nasabah BRI Tertipu Kredit Online di Sulsel". *Detik News*. Diakses dari https://news.detik.com/berita/d-4380083/ratusan-nasabah-bri-tertipu-kredit-online-di-sulsel (diakses pada 2 Juli 2022).

Taylor, Sven. 27 Juni 2021. "New LinkedIn Data Leak Leaves 700 Million Users Exposed". *Restore Privacy*. Diakses dari https://restoreprivacy.com/linkedin-data-leak-700-million-users/ (diakses pada 19 Mei 2022).

Toulas, Bill. 29 Juni 2022. "Ukraine Arrests Cybercrime Gang Operating Over 400 Phishing Sites". *Bleeping Computer*. Diakses dari https://www.bleepingcomputer.com/news/security/ukraine-arrests-cybercrime-gang-operating-over-400-phishing-sites/ (diakses pada 7 Juli 2022).

Vigliarolo, Brandon. 25 Agustus 2021. "Kanye's Upcoming Album is a Scam Magnet, Kapersky Finds". *Techrepublic*. Diakses dari https://www.techrepublic.com/article/kanyes-upcoming-album-is-a-scam-magnet-kaspersky-finds/#ftag=RSS56d97e7 (diakses pada 22 Mei 2022).

_____. 8 Juli 2021. "Black Widow" Digital Premier a Cover for Malware and Scams, Says Kaspersky". *TechRepublic*. Diakses dari https://www.techrepublic.com/article/black-widow-digital-premier-a-cover-for-malware-and-scams-says-kaspersky/ (diakses pada 21 Mei 2022).

Vincent, James. 27 Oktober 2021. "You Can Now Ack Google to Remove Images of Under-18S From Its Search Result". *The Verge*. Diakses dari https://www.theverge.com/2021/10/27/22748240/remove-images-google-search-results-under-18-request-how-to (diakses pada 6 Juni 2022).

Wardani, Agustin Setyo. 24 Januari 2021. "Makin Parah, Serangan Ransomeware BI Ternyata Hantam 200 Komputer di 20 Cabang". *Liputan 6*. Diakses dari https://www.liputan6.com/tekno/read/4867855/makin-parah-serangan-ransomware-bi-ternyata-hantam-200-komputer-di-20-cabang (diakses pada 14 Mei 2022).

Whittaker, Zack. 1 Juni 2021. "Volkswagen Says a Vendor's Security Lapse Exposed 3,3 Milion Drivers's Details". *TechCrunch*. Diakses dari https://techcrunch.com/2021/06/11/volkswagen-says-a-vendors-security-lapse-exposed-3-3-million-drivers-details/ (diakses pada 19 Mei 2022).

Wijayanto. 6 November 2019. "Komplotan Penipuan Bermodus ATM Rp. 1 M Dibekuk". *Radar Surabaya*. Diakses dari https://radarsurabaya.jawapos.com/read/2019/11/06/164853/komplotan-penipuan-bermodus-atm-rp-1-m-dibekuk (diakses pada 2 Juni 2022).

Wtae. 21 Maret 2017. "Medical Record Found Trahsed in Dumpster". *WTAE*. Diakses dari https://www.wtae.com/article/medical-records-found-trashed-in-dumpster/9160857 (diakses pada 29 Mei 2022).

Yang, Yingzhi, *et.al*. 16 Juli 2021. "Chinese Regulators Send Teams to Didi For Cybersecurity Review". *Reuters*. Diakses dari https://

www.reuters.com/technology/chinese-regulators-send-on-site-teams-conduct-cybersecurity-review-didi-2021-07-16/ (diakses pada 18 Mei 2022).

Yoachimik, Omer. 14 Juni 2022. "Cloudflare Mitigates 26 Million Request Per Second DDoS Attack". *Cloudfare*. Diakses dari https://blog.cloudflare.com/26m-rps-ddos/ (diakses pada 20 Juni 2022).

Putusan Pengadilan

Putusan PN Sengkang Nomor 30/Pid.Sus/2019/PN.Skg.

[Halaman ini sengaja dikosongkan]

LAMPIRAN

Brussels, 26.1.2022 COM(2022) 28 final

European Declaration on Digital Rights and Principles for the Digital Decade

The European Parliament, the Council and the Commission solemnly proclaim the following joint Declaration on Digital Rights and Principles for the Digital Decade

Preamble

Whereas:

(1) The digital transformation affects every aspect of people's lives. It offers significant opportunities for a better quality of life, innovation, economic growth and sustainability, but it also presents new challenges for the fabric, security and stability of our societies and economies. With the acceleration of the digital transformation, the time has come for the European Union (EU) to spell out how its values and fundamental rights should be applied in the online world.

(2) The Parliament has made several calls for ensuring the full compliance of the Union's approach to the digital transformation with fundamental rights such as data protection or non-discrimination, and with principles such as technological and net neutrality, and inclusiveness. It has also called for a strengthened protection of users' rights in the digital environment.

(3) Building on previous initiatives such as the "Tallinn Declaration on eGovernment" and the "Berlin Declaration on Digital Society and Value-based Digital Government", the Council has called, through the "Lisbon Declaration – Digital Democracy with a Purpose" for a model of digital transformation that strengthens the human dimension of the digital ecosystem with the Digital Single Market as its core. The Council also called for a model of digital transition that ensures that technology assists in the need to take climate action and protect the environment.

(4) The EU vision for digital transformation puts people at the centre, empowers individuals and fosters innovative businesses. The Commission has recently presented a Proposal for a Decision on a "Path to the Digital Decade", which sets out the concrete digital targets based on four cardinal points (digital skills, digital infrastructures, digitalisation of businesses and of public services) that will help us achieve this vision. The Union way for the digital transformation of our societies and economy should encompass digital sovereignty, inclusion, equality, sustainability, resilience, security, trust, improving quality of life, respect of people' rights and aspirations and should contribute to a dynamic, resource-efficient and fair economy and society in the Union.

(5) The Declaration aims to explain shared political intentions. Not only does it recall the most relevant rights in the context of the digital transformation, it should also serve as a reference point for businesses and other relevant actors when developing and deploying new technologies. The Declaration should also guide policy makers when reflecting on their vision of the digital transformation: putting people at the centre of the digital transformation; underlying solidarity and inclusion; restating the importance of freedom of choice; participation in the digital public space; safety, security, and empowerment; and sustainability.

(6) The democratic oversight of the digital society and economy should be further strengthened, in full respect of the rule of law principles, effective justice, and law enforcement. This Declaration does not affect lawful limits on the exercise of legal rights, in order to reconcile them with the exercise of other rights, or necessary and proportionate restrictions in the public interest. The Union should promote the Declaration in its relations with other international organisations and third countries with the ambition that the principles serve as an inspiration for international partners to guide a digital transformation which puts people and their human rights at the centre throughout the world.

(7) This Declaration notably builds on primary EU law, in particular in the Treaty on European Union, the Treaty on the Functioning of the European Union, the EU Charter of Fundamental Rights and the case-law of the Court of Justice of the EU, as well as in

secondary law. It also builds on and complements the European Pillar of Social Rights. It has a declaratory nature and does not as such affect the content of legal rules or their application.

(8) The promotion and implementation of the digital principles is a shared political commitment and responsibility of the Union and its Member States within their respective competences and in full compliance with Union law. The Commission has proposed that the annual report on the "State of the Digital Decade", to be submitted to the Parliament and Council, would cover the monitoring of the digital principles.

Declaration on Digital Rights and Principles for the Digital Decade

We aim to promote a European way for the digital transition, putting people at the centre. It shall be based on European values and benefiting all individuals and businesses.

We therefore declare:

Chapter I: Putting people at the centre of the digital transformation

People are at the centre of the digital transformation in the European Union. Technology should serve and benefit all Europeans and empower them to pursue their aspirations, in full security and respect of their fundamental rights.

We commit to:

- strengthening the democratic framework for a digital transformation that benefits everyone and improves the lives of all Europeans;
- taking necessary measures to ensure that the values of the Union and the rights of individuals as recognised by Union law are respected online as well as offline;
- fostering responsible and diligent action by all digital actors, public and private, for a safe and secure digital environment;
- actively promoting this vision of the digital transformation, also in our international relations.

Chapter II: Solidarity and inclusion

Everyone should have access to technology that aims at uniting, and not dividing, people. The digital transformation should contribute to a fair society and economy in the Union.

We commit to:

- making sure that technological solutions respect people's rights, enable their exercise and promote inclusion.
- a digital transformation that leaves nobody behind. It should notably include elderly people, persons with disabilities, or marginalised, vulnerable or disenfranchised people and those who act on their behalf.
- developing adequate frameworks so that all market actors benefiting from the digital transformation assume their social responsibilities and make a fair and proportionate contribution to the costs of public goods, services and infrastructures, for the benefit of all Europeans.

Connectivity

Everyone, everywhere in the EU, should have access to affordable and high-speed digital connectivity.

We commit to:

– ensuring access to excellent connectivity for everyone, wherever they live and whatever their income;
– protecting a neutral and open internet where content, services, and applications are not unjustifiably blocked or degraded.

Digital education and skills

Everyone has the right to education, training and lifelong learning and should be able to acquire all basic and advanced digital skills.

We commit to:

– promoting and supporting efforts to equip all education and training institutions with digital connectivity, infrastructure, and tools;
– supporting efforts that allow learners and teachers to acquire and share all necessary digital skills and competences to take an active part in the economy, society, and in democratic processes;
– giving everyone the possibility to adjust to changes brought by the digitalisation of work through up-skilling and re-skilling.

Working conditions

Everyone has the right to fair, just, healthy, and safe working conditions and appropriate protection in the digital environment as in the physical work place, regardless of their employment status, modality or duration.

We commit to:

– ensuring that everyone shall be able to disconnect and benefit from safeguards for work-life balance in a digital environment.

Digital public services online

Everyone should have access to all key public services online across the Union. Nobody is to be asked to provide data more often than necessary when accessing and using digital public services.

We commit to:

– ensuring that all Europeans are offered an accessible, secure and trusted digital identity that gives access to a broad range of online services;
– ensuring wide accessibility and re-use of government information;
– facilitating and supporting seamless, secure and interoperable access across the Union to digital health and care services, including health records, designed to meet people's needs.

Chapter III: Freedom of choice

Interactions with algorithms and artificial intelligence systems

Everyone should be empowered to benefit from the advantages of artificial intelligence by making their own, informed choices in the digital environment, while being protected against risks and harm to one's health, safety and fundamental rights.

We commit to:

– ensuring transparency about the use of algorithms and artificial intelligence, and that people are empowered and informed when interacting with them;
– ensuring that algorithmic systems are based on suitable datasets to avoid unlawful discrimination and enable human supervision of outcomes affecting people;
– ensuring that technologies, such as algorithms and artificial intelligence are not used to pre-determine people's choices, for

example regarding health, education, employment, and their private life;

– providing for safeguards to ensure that artificial intelligence and digital systems are safe and used in full respect of people's fundamental rights.

A fair online environment

Everyone should be able to effectively choose which online services to use, based on objective, transparent and reliable information. Everyone should have the possibility to compete fairly and innovate in the digital environment.

We commit to:

– ensuring a safe, secure and fair online environment where fundamental rights are protected, and responsibilities of platforms, especially large players and gatekeepers, are well defined.

Chapter IV: Participation in the digital public space

Everyone should have access to a trustworthy, diverse and multilingual online environment. Access to diverse content contributes to a pluralistic public debate and should allow everyone to participate in democracy.

Everyone has the right to freedom of expression in the online environment, without fear of being censored or intimidated.

Everyone should have the means to know who owns or controls the media services they are using.

Very large online platforms should support free democratic debate online, given the role of their services in shaping public opinion and discourse. They should mitigate the risks stemming from the functioning and use of their services, including for disinformation campaigns and protect freedom of expression.

We commit to:

– supporting the development and best use of digital technologies to stimulate citizen engagement and democratic participation.

– continuing safeguarding fundamental rights online, notably the freedom of expression and information.

– taking measures to tackle all forms of illegal content in proportion to the harm they can cause, and in full respect of the right to

freedom of expression and information, and without establishing any general monitoring obligations;

– creating an online environment where people are protected against disinformation and other forms of harmful content.

Chapter V: Safety, security, and empowerment

A protected, safe and secure online environment

Everyone should have access to digital technologies, products and services that are safe, secure, and privacy-protective by design.

We commit to:

– protecting the interests of people, businesses and public institutions against cybercrime, including data breaches and cyberattacks. This includes protecting digital identity from identity theft or manipulation;

– countering and holding accountable those that seek to undermine security online and the integrity of the Europeans' online environment or that promote violence and hatred through digital means.

Privacy and individual control over data

Everyone has the right to the protection of their personal data online. That right includes the control on how the data are used and with whom they are shared.

Everyone has the right to the confidentiality of their communications and the information on their electronic devices, and no one shall be subjected to unlawful online surveillance or interception measures.

Everyone should be able to determine their digital legacy, and decide what happens with the publicly available information that concerns them, after their death.

We commit to:

– ensuring the possibility to easily move personal data between different digital services.

Children and young people should be protected and empowered online

Children and young people should be empowered to make safe and informed choices and express their creativity in the online environment.

Age-appropriate materials should improve children's experiences, well-being and participation in the digital environment.

Children have the right to be protected from all crimes, committed via or facilitated through digital technologies.

We commit to:

- promoting a positive, age-appropriate and safe digital environment for children and young people;
- providing opportunities to all children to acquire the necessary skills and competences to navigate the online environment actively, safely and make informed choices when online;
- protecting all children against harmful and illegal content, exploitation, manipulation and abuse online, and preventing the digital space from being used to commit or facilitate crimes

Chapter VI: Sustainability

To avoid significant harm to the environment, and to promote a circular economy, digital products and services should be designed, produced, used, disposed of and recycled in a way that minimises their negative environmental and social impact.

Everyone should have access to accurate, easy-to-understand information on the environmental impact and energy consumption of digital products and services, allowing them to make responsible choices.

We commit to:

- supporting the development and use of sustainable digital technologies that have minimal environmental and social impact;
- developing and deploying digital solutions with positive impact on the environment and climate.

[Halaman ini sengaja dikosongkan]

PROFIL PENULIS

Dr. Sayid Muhammad Rifqi Noval, S.H., M.H., lahir di Bandung tahun 1987. Pendidikan tinggi Hukum ditempuh pada Fakultas Hukum Universitas Islam Indonesia (2004). Gelar Magister Hukum (2010) diraihnya pada Program Pascasarjana Universitas Padjadjaran Bandung. Penulis mendapat Beasiswa Pascasarjana dari Direktorat Jenderal Pendidikan Tinggi (Dikti) untuk Program Doktor Ilmu Hukum yang ditempuh pada Program Pascasarjana Universitas Padjadjaran Bandung, yang diselesaikan pada tahun 2016.

Sejak 2008, penulis bekerja pada Yayasan Assalaam Bandung. Penulis juga berprofesi sebagai Advokat (Peradi). Sejak tahun 2011, penulis tercatat sebagai dosen di Fakultas Hukum Universitas Islam Nusantara.

Penulis aktif dalam kegiatan seminar pada tingkat nasional dan beberapa di antaranya mendapatkan penghargaan *paper* terbaik serta presenter terbaik. Dalam seminar internasional, tidak hanya berpartisipasi sebagai pemakalah, di antaranya yang berlangsung di Belgia (2019) serta Republik Ceko (2019), namun juga sebagai *Keynote Speaker* dalam seminar internasional mengenai *cyber security* di Thailand

(2018). Sejumlah karya telah ditulis dalam bentuk buku di antaranya, *Pendidikan di Mata Peserta Didik* (2016), *Hukum Ketenagakerjaan: Hakikat Cita Keadilan dalam Sistem Hukum Ketenagakerjaan* (2017), *Cyber Bullying,* Hak-Hak Digital: *Right on Online Safet* (2020), dalam jurnal terakreditasi nasional maupun internasional, serta prosiding nasional maupun internasional. Penulis juga aktif menjadi pembicara. Atau narasumber di berbagai pertemuan ilmiah. Penulis turut menjadi *reviewer* jurnal nasional terakreditasi maupun jurnal bereputasi Scopus.

Penulis melakukan kunjungan dalam rangka penelitian ke berbagai negara, di antaranya Singapura, Malaysia, Jepang, Turki, Tiongkok, Filipina, Thailand, New South Wales, Queensland, Tasmania, Victoria, Selandia Baru, Inggris, Belanda, Swiss, Skotlandia, Prancis, Italia, Republik Ceko, Belgia, Luksemburg, Monako, dan lainnya. Untuk berkomunikasi dengan penulis, dapat melalui alamat email: rifqi@assaalaam.id.

Soecipto, S.T., M.H., lahir di Tegal tahun 1974. Pendidikan Sarjana Teknik Informatika di STT Mandala lulus tahun 1998. Gelar Magister Hukum pada tahun 2015 diraihnya pada Program Pascasarjana Universitas Islam Nusantara. Penulis pernah mendapat beasiswa dari Supersemar dan Gubernur Jawa Barat.

Pada tahun 1997 dan 1998 pernah membantu membangun Sistem Informasi Geografis (GIS) Panasbumi di Indonesia. Pernah bekerja pada bagian IT di Perusahaan Listrik Negara (PLN) APJ Majalaya - Jawa Barat, penulis juga menjadi TIM IT Program Kemahasiswaan di Kemdikbudristek sejak tahun 2015 di Program Kreativitas Mahasiswa, Sindikker, KBMI, ASMI, PHP2D, Wiradesa, P3D, PPK Ormawa, P2MD, Pilmapres, KNMIPA. Penulis tercatat sebagai dosen di Teknik Informatika Fakultas Teknik Universitas Islam Nusantara sejak 2001 pernah menjadi Sekprodi, Kaprodi, Wakil Dekan III, Kepala Pusat Komputer, membina tim Volley Ball, UNINUS Football (UFC), HIPMI UNINUS, Iqramul Qur'an, Pramuka di Universitas Islam Nusantara.

Sejumlah karya telah ditulis dalam bentuk buku panduan, di antaranya *Panduan Program Penguatan Kapasitas Organisasi Kemahasiswaan (PPK Ormawa) 2022*, *Panduan PKMI 2021, Modul Pembelajaran Sistem Multimedia Menggunakan Teknik Animasi 2 Dimensi dan 3 Dimensi* (ISBN: 978-623-338-582-4). Untuk berkomunikasi dengan penulis, dapat melalui alamat email: cipto.bdg@gmail.com.

Ahmad Jamaludin, S.H., M.H., lahir di Pandeglang tahun 1992. Pendidikan tinggi Hukum ditempuh pada Fakultas Syariah dan Hukum Universitas Islam Negeri Sunan Gunung Djati Bandung (2010). Gelar Magister Hukum (2016) diraihnya pada Program Pascasarjana Universitas Islam Negeri Sunan Gunung Djati Bandung. Pada tahun 2019 penulis mendapat Beasiswa Pascasarjana dari Kementerian Riset dan Perguruan Tinggi (Kemenristek) untuk Program Doktor Ilmu Hukum yang ditempuh pada Program Pascasarjana Universitas Padjadjaran Bandung.

Penulis tercatat sebagai dosen di Fakultas Hukum Universitas Islam Nusantara sejak tahun 2017 dan saat ini menjabat sebagai Wakil Dekan Fakultas Hukum UNINUS. Penulis juga berprofesi sebagai Advokat (Peradi) sejak tahun 2014.

Penulis aktif dalam kegiatan seminar pada tingkat nasional dan sejumlah karya telah ditulis dalam bentuk buku, di antaranya dalam jurnal terakreditasi nasional maupun internasional, serta prosiding nasional maupun internasional. Penulis juga aktif menjadi pembicara atau narasumber di berbagai pertemuan ilmiah. Untuk berkomunikasi dengan penulis, dapat melalui alamat email: jamaludinumam@gmail.com.

PERLINDUNGAN HAK DIGITAL

Ancaman Privasi di Tengah Serangan *Social Engineering*

Di balik manfaat besar yang diberikan oleh teknologi internet saat ini, tersisip masalah besar yang sesungguhnya membayangi setiap penggunanya. Kebocoran data Kartu Tanda Penduduk (KTP) warga Indonesia, data nasabah bank, konsumen *market place,* hingga kebocoran data yang menimpa Badan Siber dan Sandi Negara (BSSN), menjadi contoh rentannya keamanan data pribadi di Indonesia saat ini.

Serangan siber telah menjadi persoalan yang membutuhkan perhatian khusus, mengingat perlunya upaya pelurusan terhadap pandangan umum yang menilai jika serangan siber yang menjadi penyebab kebocoran data hanya dapat dilakukan oleh seseorang dengan latar belakang kemampuan Informasi dan Teknologi (IT) serta dukungan peralatan mutakhir. Faktanya, serangan tersebut dapat dilakukan oleh kalangan umum, bahkan tanpa membutuhkan dukungan peralatan khusus yang dikenal dengan istilah serangan *social engineering*.

Bagi para penstudi hukum di Indonesia, kata *social engineering* mengandung relasi yang kuat dengan dua teori besar yang dikenalkan oleh Roscoe Pound serta Mochtar Kusumaatmadja. Namun, *social engineering* dalam buku ini akan diuraikan dalam optik yang berbeda, yakni sebagai jenis serangan yang bertujuan mengeksploitasi kerentanan manusia dengan cara memengaruhi, persuasi, penipuan, manipulasi, dan membujuk guna melanggar tujuan keamanan dunia maya.

Buku ini berusaha untuk memberikan penjelasan perihal serangan *social engineering* secara historis, penelusuran kasus hingga ragam potensi masalahnya. Ragam bentuk *social engineering*, seperti *phising*, *Nigerian scam*, *baiting*, *quid pro quo, dumpster diving, shoulder surfing,* dan *femme fatale* akan diuraikan, hingga potensi masalah dan langkah antisipasinya.

Sebagai penutup, penulis memanfaatkan *QR Code* dalam buku ini guna meringkas ulasan materi serta memudahkan para pembaca dalam menelusuri lebih lanjut persoalan tersebut dengan melihat pada peraturan perundang-undang, putusan pengadilan, video, maupun artikel yang terkait dengan topik pembahasan.

RajaGrafindo Persada
PT RAJAGRAFINDO PERSADA
Jl. Raya Leuwinanggung No. 112
Kel. Leuwinanggung, Kec. Tapos, Kota Depok 16456
Telp 021-84311162
Email: rajapers@rajagrafindo.co.id
www.rajagrafindo.co.id

RAJAWALI PERS
DIVISI BUKU PERGURUAN TINGGI
9 786233 725934