Technology and Economics Law Journal

Volume 2
Number 2 *Technology and Economics Law Journal Vol 2 No.2*

Article 3

8-24-2023

Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya

Russel Butarbutar
Universitas Bung Karno, russelbutar@gmail.com

Recommended Citation

Butarbutar, Russel (2023) "Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya," *Technology and Economics Law Journal*: Vol. 2: No. 2, Article 3.
DOI: 10.21143/TELJ.vol2.no2.1043
Available at: https://scholarhub.ui.ac.id/telj/vol2/iss2/3

TELJ
Technology And Economics Law Journal
Vol.2 No.2

Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya

Russel Butarbutar
Fakultas Hukum Universitas Bung Karno
korespondensi russelbutar@gmail.com

kata Kunci : Kejahatan; Siber; Individu; Jenis; Analisis.

Naskah diterima

23-06-2023

Naskah direvisi dan dipublis

24-08-2023

ABSTRAK
Penelitian ini membahas kejahatan siber terhadap individu, jenis kejahatan siber, analisis, dan perkembangannya. Penelitian ini menggunakan penelitian interdispliner dengan pendekatan metode kualitatif. Ditemukan berbagai jenis kejahatan tethadap individu, diantaranya: (1) Rekayasa Sosial dan tipu daya; (2) Pelecehan Daring; (3) Kejahatan terkait Identitas; (4) Peretasan; dan (5) Penolakan Layanan dan Informasi. Penting bagi individu untuk memahami taktik yang digunakan oleh penjahat siber dan untuk mengadopsi praktik keamanan yang kuat dalam penggunaan teknologi. Menjaga kerahasiaan informasi pribadi, menggunakan kata sandi yang kuat, memperbarui perangkat lunak secara teratur, dan menjadi sadar akan tanda-tanda serangan dan penipuan online dapat membantu melindungi diri dari ancaman kejahatan siber. Secara umum kita banyak mengenal kejahatan siber seperti phishing, malware, kejahatan identitas, penipuan online, dan pelecehan online dapat memiliki dampak serius terhadap keamanan, privasi, dan kesejahteraan individu. Penting bagi individu untuk memahami taktik yang digunakan oleh penjahat siber dan untuk mengadopsi praktik keamanan yang kuat dalam penggunaan teknologi. Menjaga kerahasiaan informasi pribadi, menggunakan kata sandi yang kuat, memperbarui perangkat lunak secara teratur, dan menjadi sadar akan tanda-tanda serangan dan penipuan online dapat membantu melindungi diri dari ancaman kejahatan siber.

I. Pendahuluan

Perkembangan dunia dan masyarakat selalu digerakkan atau diikuti dengan perkembangan teknologi yang dinamakan revolusi industri. *Revolusi Industri Pertama* menggunakan tenaga air dan uap untuk memekanisasi produksi. *Revolusi Industri Kedua* menggunakan tenaga listrik untuk menciptakan produksi massal. *Revolusi Industri Ketiga* menggunakan elektronik dan teknologi informasi untuk mengotomatisasi produksi. Sekarang *Revolusi Industri Keempat* sedang membangun ketiga revolusi digital yang telah terjadi sejak pertengahan abad lalu. Ini ditandai dengan perpaduan teknologi yang mengaburkan batas antara bidang fisik, digital, dan biologis.[1]

Teknologi dari hasil revolusi industri tersebut telah menggerakkan masyarakat modern dan mempengaruhi segalanya termasuk pemerintah dan pasar ekonomi, perdagangan global, perjalanan, dan komunikasi. Teknologi digital memiliki lebih jauh merevolusi dunia kita, dan sejak munculnya Internet dan *World Wide Web*, masyarakat telah menjadi lebih efisien dan maju.[2] Adopsi teknologi *Internet of Things* (IoT), komputasi awan (*Cloud Computing*), kecerdasan buatan (AI), dan kemampuan penginderaan dan aktuasi yang semakin luas telah menghasilkan rumah pintar yang lebih praktis, tetapi juga target yang benar-

[1] Klaus Schwab, "The Fourth Industrial Revolution: What It Means, How to Respond," *Currency* (2017), https://jmss.vic.edu.au/wp-content/uploads/2021/06/The_Fourth_Industrial_Revolution.pdf.

[2] David Thorns and Michael Nuth, "Beyond The Hype: Intellectual Property and The Knowledge Society/Knowledge Economy," *Journal of Economic Surveys* 20, no. 4 (2006): 633–690.

benar menarik untuk serangan dunia maya.[3]

Kejahatan Siber (*Cybercrime*) atau kejahatan dunia maya merupakan tantangan serius bagi masyarakat dan berbahaya bagi individu atau organisasi yang menjadi korban.[4] Kejahatan dunia maya juga dapat merugikan pribadi, organisasi, dan pemerintah, walaupun di satu sisi memberikan manfaat besar dalam hal efisiensi dan efektifitas, tetapi di satu sisi kejahatan dunia maya juga semakin meningkat.[5] Organisasi juga telah berbenah untuk menghadapi ancaman kejahatan siber dengan mengintensifkan tingkat keamanan informasi mereka, karena keamanan informasi telah menjadi elemen penting dalam manajemen bisnis.[6] Namun bagaimana dengan individu atau perorangan atau pribadi yang menghadapi kejahatan siber atau korban kejahatan siber? Perlu untuk memahami dan meliti bagaimana jenis, analisis dan perkembangan kejahatan siber yang menyerang individu atau perorangan.[7]

Untuk mencegah kejahatan sibers, individu dan pemerintah perlu memahami dengan jelas skema kejahatan di dunia maya dan tren serta perilaku Internet kontemporer dan berkelanjutan dari para penjahat ini.[8] Saat ini, pencurian kartu kredit dan kasus pencucian uang *online* kejahatan dunia maya semakin meningkat. Pelecehan dan pencemaran nama baik melalui media sosial juga menjadi perhatian individu. *Cyber*-terorisme merupakan aspek yang paling menonjol dari kejahatan dunia maya di seluruh negara.[9] Dengan demikian keamanan dan keselamatan informasi telah menjadi tantangan utama saat ini. Dengan pertumbuhan pengguna yang pesat, kasus kejahatan dunia maya juga meningkat dan tidak dibatasi oleh batasan geografis atau batas negara di dunia. Ini merupakan masalah yang sangat memprihatinkan karena berdampak negatif langsung pada kehidupan ekonomi dan sosial masyarakat.[10]

Lebih lanjut, dalam ranah pelanggaran *privacy*, akan muncul pertanyaan, bagaimana kepastian hukum untuk melindungi privasi seseorang termasuk data pribadinya.[11] Fakta bahwa privasi memiliki hubungan yang sangat erat dengan martabat manusia, kebebasan dan kemerdekaan individu, dan itu semakin ditantang di era teknologi yang cepat perkembangan masyarakat informasi.[12] Termasuk mengenai isu *big data* yang berhubungan dengan mekanisme pelestarian privasi yang dikembangkan untuk perlindungan privasi pada berbagai tahap (misalnya, pembuatan data, penyimpanan data, dan pemrosesan data) dari siklus hidup *big data*.[13] Isu lainnya juga terkait dengan prinsip transparansi yang menjadi prinsip dasar untuk pemrosesan data di bawah Undang-undang Pelindungan Data Pribadi.[14] Begitu juga dengan persyaratan transparansi untuk

[3] Ryan Heartfield (et al), "A Taxonomy of Cyber-Physical Threats and Impact in the Smart Home," *Computers & Security* 78 (2018): 398–428.

[4] Raj Singh Deora and Dhaval Chudasama, "Brief Study of Cybercrime on an Internet," *Journal of Communication Engineering & Systems* 11, no. 1 (2021): 1–6.

[5] Jesse Abulencia, "The Cost of Cybercrime in the US Healthcare Sector," *Computer Fraud & Security* 11, no. 8–13 (2021).

[6] Chunghun Lee, Choong C. Lee, and Suhyun Kim, "Understanding Information Security Stress: Focusing on the Type of Information Security Compliance Activity," *Computers & Security* 59 (2016): 60–70.

[7] Jason R. C. Nurse, "Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit," *arXiv preprint arXiv:1811.06624* (2018), https://arxiv.org/abs/1811.06624.

[8] Bhavna Arora, "Exploring and Analyzing Internet Crimes and Their Behaviours," *Perspectives in Science* 8 (2016): 540–542.

[9] *Ibid.*

[10] Y Karali, S. Panda, and C. S. Panda, "Cyber Crime: An Analytical Study of Cyber Crime Cases at the Most Vulnerable States and Cities in India," *al Journal of Engineering and Management Research (IJEMR)* 5, no. 2 (2015): 43–48.

[11] Kobbi Nissim and Alexandra Wood, "Is Privacy Privacy?," *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376, no. 2128 (2018), https://royalsocietypublishing.org/doi/pdf/10.1098/rsta.2017.0358.

[12] Alessandro Acquisti, Leslie K. John, and George Loewenstein, "What Is Privacy Worth?," *The Journal of Legal Studies* 42, no. 2 (2013): 249–274.

[13] A. Mehmood et al., "Protection of Big Data Privacy," *IEEE Access* 4, no. 1821–1834 (2016), https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7460114.

[14] Heike Felzmann, Eduard Fosch Villaronga, and Aurelia Tamò-Larrieux, "Transparency You Can Trust: Transparency Re-

kecerdasan buatan dan sistem pengambilan keputusan otomatis. Demikian juga halnya tentang isu atau risiko kerugian secara ekonomi yang diakibatkan oleh pelanggaran privasi dimaksud.[15]

Namun bagaimana dengan individu atau perorangan atau pribadi yang menghadapi kejahatan siber atau korban kejahatan siber? Bagaimana jenis, analisis dan perkembangan kejahatan siber yang menyerang individu atau perorangan.[16] Penelitian ini sangat diperlukan untuk membahas masalah tersebut.

II. Metode Penelitian

Penelitian ini merupakan penelitian interdispliner dengan pendekatan metode kualitatif.[17] Penelitian interdisipliner adalah jenis penelitian yang melibatkan integrasi berbagai disiplin ilmu yang berbeda untuk mempelajari suatu topik atau fenomena.[18] Penelitian interdisipliner mengacu kepada ilmu sosial berkolaborasi dengan ilmuwan komputasi atau data dalam proyek penelitian interdisipliner untuk mengandalkan keterampilan satu sama lain dan untuk mengembangkan prinsip etika yang diterima bersama.[19] Pendekatan metode kualitatif dalam konteks kejahatan siber digunakan dalam penelitian ini untuk mendapatkan pemahaman yang lebih mendalam tentang motif, perilaku, dan dinamika di balik kejahatan tersebut.[20]

III. Pembahasan

a. Prevalansi Kejahatan Siber

Penyebaran kejahatan dunia maya atau disebut juga kejahatan komputer atau kejahatan siber telah meningkat secara signifikan dalam beberapa tahun terakhir seiring dengan perkembangan teknologi informasi dan internet. Kejahatan siber mencakup banyak jenis kegiatan yang menggunakan komputer atau jaringan komputer untuk melakukan kegiatan ilegal.[21]

Sulit untuk secara akurat mengukur prevalensi kejahatan dunia maya karena banyak kejahatan tidak dilaporkan atau tidak diketahui. Namun, ada beberapa tren umum yang menunjukkan peningkatan kejahatan dunia maya. Prevalensi kejahatan dunia maya dapat bervariasi dari satu negara ke negara lain dan juga bergantung pada tingkat kesadaran keamanan dan perlindungan yang ada. Penting untuk memahami risiko kejahatan dunia maya dan mengambil langkah-langkah untuk melindungi diri Anda sendiri, seperti: amankan kata sandi, jangan buka lampiran atau tautan yang mencurigakan, dan gunakan perangkat lunak keamanan terbaru. Organisasi dan pemerintah juga harus menginvestasikan sumber daya untuk meningkatkan keamanan dunia maya, melatih karyawan, dan menerapkan kebijakan yang sesuai untuk mengurangi risiko kejahatan

quirements for Artificial Intelligence between Legal Norms and Contextual Concerns," *Big Data & Society* (2019): 1–14, https://journals.sagepub.com/doi/epub/10.1177/2053951719860542.

[15] Alessandro Acquisti, Curtis Taylor, and Liad Wagman, "The Economics of Privacy," • *Journal of Economic Literature* 54, no. 2 (2016): 442–492.

[16] Jason R. C. Nurse, "Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit," *arXiv preprint arXiv:1811.06624* (2018), https://arxiv.org/abs/1811.06624.

[17] Monique Hennink, Inge Hutter, and Ajay Baliley, *Qualitative Research Methods*, Second Edi. (London: Sage Publications Ltd., 2020).

[18] Alana B. Siegner, "Experiential Climate Change Education: Challenges of Conducting Mixed-Methods, Interdisciplinary Research in San Juan Islands, WA and Oakland, CA," *Energy Research & Social Science* 45 (2018): 374–384.

[19] Katalin Parti, Akos Szigeti, and Sandro Serpa, "The Future of Interdisciplinary Research in the Digital Era: Obstacles and Perspectives of Collaboration in Social and Data Sciences - An Empirical Study," *Cogent Social Sciences* 7, no. 1 (2021), https://www.tandfonline.com/doi/full/10.1080/23311886.2021.1970880.

[20] B. Dupont and T Holt, "The Human Factor of Cybercrime," *Social Science Computer Review* 40, no. 4 (2022): 860–864, https://doi.org/10.1177/08944393211011584.

[21] Nurse, "Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit.", *Loc. Cit.*

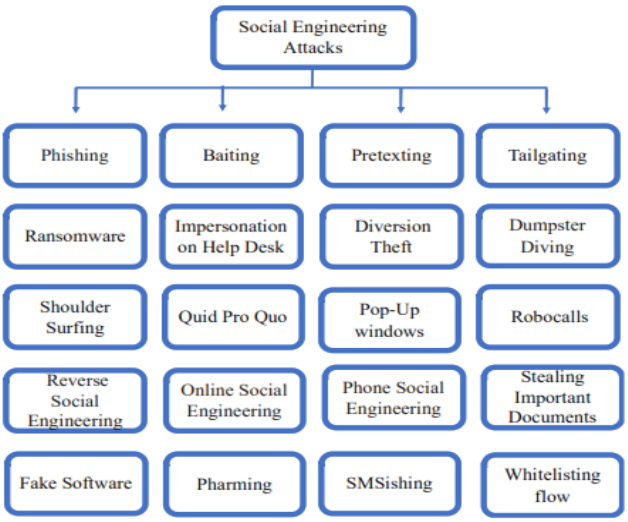
siber atau kejahatan dunia maya.[22]

b. Jenis Kejahatan Siber Terhadap Perorangan (Individu)

Kejahatan Siber adalah setiap kegiatan kriminal yang dilakukan dengan menggunakan komputer, jaringan komputer atau internet. Ini berarti menggunakan teknologi untuk melakukan aktivitas ilegal, menargetkan korban, atau mengeksploitasi kerentanan dalam sistem digital. Lanskap kejahatan dunia maya sangat luas, begitu pula berbagai cara yang dapat dicoba oleh penjahat dunia maya untuk menargetkan individu.[23] Kejahatan Siber seringkali merupakan kejahatan klasik (misalnya penipuan, pencurian identitas, pornografi anak), meskipun dilakukan dengan cepat dan terhadap sejumlah besar calon korban, seperti penggunaan yang tidak sah, kerusakan, dan gangguan sistem komputer. Yang paling berbahaya adalah kode berbahaya dan eksploitasi yang mengganggu pengoperasian komputer di seluruh dunia, serta kejahatan dunia maya lainnya yang mengancam bisnis online atau *e-commerce*.[24] Kejahatan siber terhadap perorangan mencakup berbagai jenis serangan dan ancaman yang ditujukan secara khusus kepada individu (Lihat Tabel 1.1 dan Gambar 1.1).

Tabel 1.1 Kejahatan Siber Terhadap Individu[25]

Kejahatan Siber Terhadap Individu				
Rekayasa Sosial dan tipu daya (*social engineering and trickery*)	Pelecehan Daring (*Online Harassment*)	Kejahatan terkait Identitas (*Identify-related crimes*)	Peretasan (*Hacking*)	Penolakan Layanan dan Informasi (*Denial of Service and Information*)



Gambar 1.1 Serangan Social Engineering[26]

Jenis kejahatan siber diantaranya: (1) Rekayasa Sosial dan Tipu Daya (*social engineering and trickery*), yang melibatkan penerapan metode curang untuk memaksa individu agar berperilaku dengan cara tertentu atau

[22] AAG, "The Latest 2023 Cyber Crime Statistics (Updated June 2023)," last modified 2023, accessed March 26, 2023, https://aag-it.com/the-latest-cyber-crime-statistics/#:~:text=Headline Cyber Crime Statistics&text=1 in 2 American internet,the first half of 2022.

[23] Mike McGuire and (Samantha Dowling, "Cyber Crime: A Review of the Evidence Research Report 75," last modified 2013, accessed June 27, 2023, https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=5e089b9bac3cdba577724cf0cd-23f648a4f952d9.

[24] Roderic Broadhurst, "Developments in the Global Law Enforcement of Cyber-crime," *Policing: An International Journal of Police Strategies & Management* 29, no. 3 (2006): 408–433.

[25] Nurse, "Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit."

[26] Fatima Salahdine and Naima Kaabouch, "Social Engineering Attacks: A Survey," *Future Internet,* 11 (2019): 89.

melakukan beberapa tugas.[27] (2) Pelecehan Daring serupa dengan jenis, yang lain dan menjelaskan contoh di mana orang yang daring merasa terganggu/dilecehkan dan disiksa oleh orang lain. (3) Kejahatan Terkait Identitas adalah kejahatan yang dilakukan oleh seorang individu identitasnya dicuri atau disalahgunakan oleh orang lain untuk hal yang jahat atau tidak sah tujuan tertentu (misalnya, penipuan). Meskipun secara tradisional tidak dianggap sebagai kejahatan pribadi yang signifikan. (4) Kejahatan Peretasan adalah kegiatan di mana seseorang (yaitu peretas) mengeksploitasi kelemahan dan kerentanan dalam suatu sistem untuk keuntungan atau kepuasan diri sendiri. Dengan semakin berkembangnya pergerakan dunia dari budaya *offline* ke *online* seperti aktivitas belanja, perbankan, berbagi informasi akses ke informasi sensitif melalui aplikasi *web* telah meningkat.[28] (5) Penolakan mengakomodasi Informasi merupakan tren baru *ransomware* yang serupa dengan menolak akses individu ke informasi mereka sendiri. Bagian selanjutnya menganalisis taksonomi dan masing-masing jenis kejahatannya secara rinci.[29]

c. Rekayasa Sosial dan tipu daya (*social engineering and trickery*)

Rekayasa sosial adalah bentuk penipuan yang digunakan peretas untuk mendapatkan informasi sensitif dan mendapatkan akses ke infrastruktur dan fasilitas yang tidak sah. Ada dua kategori utama di mana semua rekayasa sosial dapat diklasifikasikan sebagai penipuan berbasis teknologi atau penipuan berbasis manusia.[30] Rekayasa sosial telah menimbulkan ancaman keamanan yang serius terhadap infrastruktur, pengguna, data, dan operasi dunia maya.[31] Sejumlah besar serangan *Facebook* yang dilaporkan telah diamati dalam beberapa tahun terakhir. Penelitian ini menyajikan model baru untuk mendeteksi dan mencegah SEBPA (*Social Engineering Based Phishing Attacks*) di *Facebook*.[32] Rekayasa sosial dan tipu daya, atau dalam bahasa Inggris disebut sebagai *social engineering and trickery*,[33] merujuk pada serangkaian teknik yang digunakan untuk memanipulasi orang secara psikologis agar mengungkapkan informasi sensitif atau melakukan tindakan yang merugikan.[34]

Serangan rekayasa sosial sering dilakukan dalam konteks kejahatan dunia maya, di mana penyerang mencoba mengeksploitasi kemanusiaan dan kepercayaan orang untuk mencuri informasi, mendapatkan akses tidak sah, atau meretas sistem.[35] Faktor manusia telah terbukti menjadi sumber beberapa serangan dunia maya terburuk setiap hari di organisasi mana pun. Bagian yang paling sulit untuk dihadapi adalah metode menggunakan manusia, sering disebut sebagai "rekayasa sosial". [36] Karena rekayasa sosial sangat bergantung pada perilaku manusia, tidak ada perangkat keras atau alat yang dapat dikembangkan untuk mencegah bahaya interaksi manusia. Oleh karena itu, praktik-praktik baik tertentu disarankan. Selain itu, tujuannya adalah untuk

[27] Showkat Ahmad, "Social Engineering Techniques Contrast Study," *International Journal of Engineering Studies.* 9, no. 1 (2017): 105–110.

[28] Shivanshi Sinha and Dr Yojna Arora, "Ethical Hacking: The Story of a White Hat Hacker," *International Journal of Innovative Research in Computer Science & Technology (IJIRCST)* ISSN (2020 (2020): 131–136.

[29] Nurse, "Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit.", *Loc. Cit.*

[30] Nabie Y Conteh, "The Dynamics of Social Engineering and Cybercrime in the Digital Age," *IGI Global* (2021): 144–149.

[31] Zuoguang Wang, Limin Sun, and Hongsong Zhu, "Defining Social Engineering in Cybersecurity," *IEEE Access* 8 (2020): 85094–85115.

[32] Abid Jamil (et al), "MPMPA: A Mitigation and Prevention Model for Social Engineering Based Phishing Attacks on Facebook," *2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA,.2018.8622505.* doi: 10.11 (2018): 5040–5048.

[33] Hussain Aldawood and Geoffrey Skinner, "A Taxonomy for Social Engineering Attacks via Personal Devices," *International Journal of Computer Applications (0975 – 8887)* 178, no. 50 (2019): 19–26.

[34] I. Ghafir et al., "Social Engineering Attack Strategies and Defense Approaches," (2016): 45–149.

[35] Anshul Kumar, Mansi Chaudhary, and Nagresh Kumar, "Social Engineering Threats and Awareness: A Survey," *European Journal of Advances in Engineering and Technology* 2, no. 11 (2015): 15–19.

[36] Bandar S. Almutairi and Abdurahman Alghamdi, "The Role of Social Engineering in Cybersecurity and Its Impact," *Journal of Information Security* 13, no. 4 (2022).

menciptakan kesadaran dan mempelajari dampak rekayasa sosial di masyarakat.

Berikut ini adalah beberapa teknik rekayasa sosial yang umum digunakan:

1. *Phishing*: Ini melibatkan pengiriman email atau pesan palsu yang menyamar sebagai lembaga atau organisasi terpercaya, dengan tujuan membuat penerima tergoda untuk mengklik tautan yang mencurigakan atau mengungkapkan informasi pribadi, seperti kata sandi atau nomor kartu kredit.[37]

2. *Spear Phishing*: Ini adalah versi skema *phishing* yang lebih fokus karena penyerang memilih orang atau perusahaan tertentu. Teknik *phishing* tombak membutuhkan lebih banyak upaya dari pihak penyerang dan mungkin perlu waktu yang lama untuk menarik skema ini. Skema ini dilakukan dengan ahli sehingga membuat mereka sebagian besar tidak terdeteksi. Dalam hal ini, penyerang menyesuaikan pesan yang ditetapkan pada fitur, posisi pekerjaan, dan kepemilikan kontak dari orang yang ditargetkan agar serangan tersebut tidak terlalu terlihat atau dapat diamati.[38]

3. *Vishing*: Serangan *vishing* menggunakan panggilan telepon untuk memperoleh informasi sensitif dari korban. Penyerang berpura-pura menjadi petugas layanan pelanggan, bank, atau lembaga lainnya, dan meminta korban untuk memberikan informasi seperti nomor rekening, kata sandi, atau kode keamanan.[39] Pengelabuan suara (*vishing*) adalah jenis serangan pengelabuan di mana teknisi sosial memanipulasi individu selama percakapan telepon untuk membocorkan informasi sensitif. Pengguna ponsel menjadi sasaran sebagian besar penjahat, melalui ponsel, pengguna dapat melakukan semua layanan bank seperti penarikan tunai, transfer dan setoran, ponsel menawarkan layanan pembayaran dan melalui ponsel, seseorang dapat memproses pinjaman.[40]

4. *Tailgating*: merupakan praktik rekayasa sosial yang melibatkan pemalsuan identitas atau pemakaian metode yang menipu untuk mendapatkan akses tidak sah ke informasi sensitif atau sistem komputer. Dalam hal ini, pelaku *cyber crime* "mengikuti" atau mengekor korban mereka secara dekat dengan mengambil keuntungan dari kepercayaan atau ketidaktahuan mereka. Contoh konkret dari "tailgating" dalam konteks *cyber crime* dapat berupa seseorang yang memanfaatkan keramahan seseorang secara pribadi untuk mendapatkan akses ke jaringan komputer atau informasi rahasia. Misalnya, seorang penyerang mungkin berpura-pura menjadi staf IT dan meminta korban untuk memberikan kata sandi atau menginstal perangkat lunak berbahaya.[41]

5. *Ramsomware*: merupakan jenis perangkat lunak berbahaya (*malware*) yang dirancang untuk memblokir atau mengenkripsi data pada sistem komputer korban.[42] Penyerang kemudian menuntut pembayaran tebusan (*ransom*) kepada korban agar data mereka dapat dibuka atau dikembalikan. *Ransomware* biasanya menyebar melalui tautan atau lampiran yang meragukan dalam *email phishing*, situs

[37] Neetu Bansla, Swati Kunwar, and Khushboo Gupta, "Social Engineering: A Technique for Managing Human Behavior," *Journal of Information Technology and Sciences* 5, no. 1 (2019): 18–22.

[38] *Ibid.*

[39] Keith S Jones et al., "How Social Engineers Use Persuasion Principles during Vishing Attacks," *Information & Computer Security* 29, no. 2 (2021): 314–331.

[40] Elijah M Maseno, "Vishing Attack Detection Model For Mobile Users.," *KCA University* (2017), http://41.89.49.13:8080/xmlui/bitstream/handle/123456789/1276/Maseno-Vishing Attack Detection Model For Mobile Users..pdf?sequence=1&isAllowed=y."type":"article-journal"},"uris":["http://www.mendeley.com/documents/?uuid=5a295006-5aba-429f-8e70-00b435cc9aba"]}],"mendeley":{"formattedCitation":"Elijah M Maseno, "Vishing Attack Detection Model For Mobile Users.," KCA University (2017

[41] Salahdine and Kaabouch, "Social Engineering Attacks: A Survey.", *Loc.. Cit*.

[42] *Ibid.*

web yang terinfeksi, atau menggunakan eksploitasi kelemahan dalam sistem komputer.[43] Setelah *ransomware* berhasil menginfeksi sistem komputer, ia akan mengenkripsi *file* dan memberikan peringatan kepada korban dengan instruksi tentang bagaimana cara membayar tebusan agar mendapatkan kunci dekripsi atau pemulihan data.[44] Biasanya, pembayaran ini harus dilakukan dalam bentuk mata uang digital seperti *Bitcoin* agar sulit dilacak. Beberapa *ransomware* terkenal yang pernah muncul adalah *WannaCry*, *Petya*/*NotPetya*, dan *Ryuk*.[45]

6. *Pretexting*: Metode ini melibatkan penyerang menciptakan skenario atau alasan palsu untuk mendapatkan informasi yang diinginkan. Mereka bisa berpura-pura menjadi pegawai perusahaan, anggota staf IT, atau pihak berwenang, dan meminta korban untuk memberikan informasi rahasia atau akses ke sistem.[46]

7. *Baiting*: Dalam serangan *baiting*, penyerang menjanjikan imbalan atau hadiah menarik kepada korban sebagai daya tarik untuk membuat mereka melakukan tindakan yang merugikan. Misalnya, penyerang dapat meninggalkan USB drive yang terinfeksi dengan *malware* di tempat umum, dengan harapan bahwa seseorang akan menghubungkannya ke komputer dan menginfeksinya.[47]

8. *Quid pro quo*: Dalam serangan *quid pro quo*, penyerang menawarkan sesuatu yang diinginkan oleh korban sebagai imbalan atas informasi atau akses yang diminta. Misalnya, penyerang dapat berpura-pura menjadi teknisi IT dan menawarkan bantuan teknis kepada korban, tetapi dalam prosesnya meminta korban untuk mengungkapkan kata sandi atau memberikan akses ke sistem.[48]

Teknik rekayasa sosial ini efektif karena mengandalkan kelemahan manusia, seperti ketidaktahuan, keinginan untuk membantu, atau kurangnya kesadaran akan ancaman keamanan. Oleh karena itu, penting bagi individu dan organisasi untuk meningkatkan kesadaran tentang serangan rekayasa sosial, mengenali tanda-tanda peringatan, dan menjaga kehati-hatian dalam berbagi informasi atau melakukan tindakan online. Selain itu, edukasi, kebijakan keamanan yang ketat, dan pelatihan keamanan yang berkala juga dapat membantu mengurangi risiko serangan rekayasa sosial.[49]

d. Pelecehan Daring (*Online Harassment*)

Pelecehan daring, juga dikenal sebagai pelecehan online atau serangan siber, merujuk pada tindakan tidak pantas, ancaman, intimidasi, atau penindasan yang dilakukan melalui platform digital atau internet. Ini adalah bentuk kejahatan siber yang dapat berdampak negatif secara emosional, psikologis, dan sosial pada korban.[50] Ada tiga platform media sosial yang sering terjadi praktik pelecehan daring diantarany: *Facebook*,

[43] M. Ö. Başeskioğlu and A. Tepeci, "Cybersecurity, Computer Networks Phishing, Malware, Ransomware, and Social Engineering Anti-Piracy Reviews," *3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 2021* (2021): 1–5.

[44] Craig Beaman (et al), "Ransomware: Recent Advances, Analysis, Challenges and Future Research Directions," *Computers & Security* 111 (2021): 102490.

[45] Hesham Alshaikh, Nagy Ramadan, and Hesham Ahmed Hefny, "Ransomware Prevention and Mitigation Techniques," *International Journal of Computer Applications (0975 – 8887)* 177, no. 40 (2020): 31–39.

[46] Shivam Lohani, "Social Engineering: Hacking into Humans," *International Journal of Advanced Studies of Scientific Research* 4, no. 1 (2019).

[47] *Ibid.*

[48] *Ibid.*

[49] Jamil (et al), "MPMPA: A Mitigation and Prevention Model for Social Engineering Based Phishing Attacks on Facebook.", *Loc. Cit*.

[50] E. Jhaver, S., Ghoshal, S., Bruckman, A. and Gilbert, "Online Harassment and Content Moderation: The Case of Blocklists," *ACM Transactions on Computer-Human Interaction (TOCHI)* 25, no. 2 (2018): 1–33.

Twitter, dan *Instagram*.[51]

Berikut ini beberapa bentuk umum dari pelecehan daring:

1. *Pelecehan verbal*: Ini melibatkan penggunaan kata-kata kasar, ancaman, penghinaan, atau ejekan yang ditujukan kepada seseorang melalui pesan teks, email, komentar di media sosial, atau platform komunikasi online lainnya.[52]
2. *Pelecehan seksual*: Ini mencakup tindakan atau komunikasi yang tidak diinginkan atau tidak pantas dengan unsur seksual. Ini bisa termasuk penyalahgunaan, pemerasan, penyebaran gambar atau video pribadi tanpa izin (*revenge porn*), atau teks dan percakapan eksplisit yang tidak diinginkan.[53]
3. *Pencemaran nama baik*: Ini terjadi ketika seseorang menyebarluaskan informasi palsu atau merusak reputasi seseorang melalui media sosial, blog, forum, atau *platform online* lainnya dengan tujuan merugikan atau mencemarkan nama baik seseorang.[54]
4. *Pelecehan cyberbullying*: Ini adalah bentuk pelecehan yang berulang dan bertujuan untuk merendahkan, mengintimidasi, atau menyakiti seseorang secara emosional[55] melalui pesan teks, komentar, atau konten yang diunggah di media sosial atau platform online lainnya.[56]
5. *Stalking daring*: Ini melibatkan penelusuran, pengawasan, atau pengikutan yang tidak diinginkan terhadap seseorang secara online. Ini bisa mencakup pengawasan aktivitas media sosial, pengiriman pesan yang berlebihan, atau pembuatan akun palsu untuk mengamati dan mengganggu kehidupan pribadi korban.[57]

Pelecehan daring memiliki dampak serius pada kesejahteraan korban, termasuk stres, kecemasan, depresi, isolasi sosial, dan bahkan potensi dampak fisik. Penting bagi individu untuk melindungi diri mereka sendiri dengan mengamankan akun media sosial mereka, membatasi akses ke informasi pribadi, dan melaporkan kejahatan siber kepada penyedia platform atau otoritas yang berwenang.[58]

Selain itu, diperlukan upaya kolektif dari masyarakat, penyedia layanan online, dan pemerintah untuk memerangi pelecehan daring. Ini melibatkan penerapan kebijakan dan hukum yang memadai, pendidikan tentang kesadaran *cyberbullying* dan pelecehan daring, serta penyediaan sumber daya dan dukungan bagi korban. Semua orang memiliki peran dalam menciptakan lingkungan online yang aman, inklusif, dan bebas dari pelecehan.[59]

---

[51] Jessica Vitak, Linda Steiner, and Zahra Ashktorab, "Identifying Women's Experiences With and Strategies for Mitigating Negative Effects of Online Harassment," *In Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computingx* (2017): 1231–1245.

[52] *Ibid.*

[53] Atika Khurana et al., "The Protective Effects of Parental Monitoring and Internet Restriction on Adolescents' Risk of Online Harassment," *Journal of Youth and Adolescence* 44 (2015): 1039–1047.

[54] Vitak, Steiner, and Ashktorab, "Identifying Women's Experiences With and Strategies for Mitigating Negative Effects of Online Harassment.", *Loc. Cit.*

[55] Lynette K. Watts (et al), "Cyberbullying in Higher Education: A Literature Review," *Computers in Human Behavior* 69 (2017): 268–274.

[56] R.M. Whittaker, E. and Kowalski, "Cyberbullying Via Social Media," *Journal of school violence* 14, no. 1 (2015): 11–29.

[57] Emily A. Vogels, "The State of Online Harassment," *Pew Research Center* 13 (2021), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2021/01/PI_2021.01.13_Online-Harassment_FINAL-1.pdf.

[58] Elizabeth Englander et al., "Defining Cyberbullying," *Pediatrics 140* 140, no. 2 (2017): S148–S151.

[59] Whittaker, E. and Kowalski, "Cyberbullying Via Social Media.", *Loc. Cit.*

e. Kejahatan terkait Identitas (*Identify-related crimes*)

Kejahatan terkait identitas, juga dikenal sebagai kejahatan identitas atau pencurian identitas, merujuk pada tindakan yang melibatkan penggunaan identitas seseorang secara tidak sah untuk tujuan penipuan atau keuntungan pribadi. Dalam kejahatan ini, pelaku mencuri atau menggunakan informasi pribadi seseorang, seperti nama, nomor identitas, kartu kredit, atau informasi keuangan lainnya, dengan maksud menipu, melakukan penipuan, atau melakukan kegiatan ilegal lainnya.[60]

Berikut ini beberapa bentuk umum dari kejahatan terkait identitas:

1. *Pencurian identitas*: Ini terjadi ketika seseorang mengambil informasi pribadi seseorang tanpa izin, biasanya melalui pencurian fisik atau serangan siber, dan menggunakannya untuk tujuan ilegal. Informasi yang dicuri dapat digunakan untuk membuka rekening palsu, mengajukan pinjaman, melakukan transaksi finansial, atau melakukan tindakan ilegal lainnya atas nama korban.[61]

2. *Penipuan kartu kredit*: Pelaku menggunakan informasi kartu kredit yang dicuri untuk membuat pembelian *online* atau *offline* tanpa izin pemilik kartu. Mereka dapat membeli barang, makanan, atau layanan dengan menggunakan informasi kartu kredit yang sah namun tanpa pengetahuan pemilik kartu.

3. *Pembobolan data*: Ini terjadi ketika pelaku berhasil memperoleh akses tidak sah ke basis data yang berisi informasi pribadi, seperti data pelanggan atau data keuangan perusahaan. Informasi yang dicuri kemudian dapat digunakan untuk melakukan penipuan atau dijual ke pasar gelap.[62]

4. *Pemalsuan identitas*: Pelaku menciptakan atau menggunakan dokumen palsu, seperti paspor, SIM, atau kartu identitas palsu, yang memiliki informasi identitas orang lain untuk tujuan penipuan atau kegiatan ilegal lainnya.[63]

5. *Penipuan pajak*: Pelaku menggunakan informasi pribadi orang lain untuk mengajukan pengembalian pajak palsu atau menghindari pembayaran pajak. Mereka dapat menggunakan informasi tersebut untuk memalsukan penghasilan atau klaim deduksi palsu dalam deklarasi pajak.[64]

6. *Pencurian identitas anak-anak*: Kejahatan ini melibatkan penggunaan identitas anak-anak, yang sering kali memiliki catatan kredit yang bersih, untuk membuka rekening baru, mengajukan pinjaman, atau melakukan tindakan penipuan lainnya.[65]

Kejahatan terkait identitas dapat menyebabkan kerugian finansial dan kerugian reputasi yang serius bagi korban. Untuk melindungi diri dari kejahatan ini, penting untuk menjaga kerahasiaan informasi pribadi, mengamankan dokumen-dokumen identitas, menghindari memberikan informasi pribadi yang sensitif secara online atau kepada pihak yang tidak dikenal, serta memantau secara teratur laporan kredit dan transaksi

[60] Ali Hussain, "What Is Identity Theft? Definition, Types, and Examples," last modified 2022, accessed March 27, 2023, https://www.investopedia.com/terms/i/identitytheft.asp.

[61] E.W.' Lubua and P.D Pretorius, "Ranking Cybercrimes Based on Their Impact to Organisations' Welfare," *HREAT Conference Proceedings* (2019): 1–11.

[62] M.H. Rumlus and H Hartadi, "Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik," *Jurnal HAM* 11, no. 2 (2020): 285–299.

[63] Adik Nur Luthiya, Benny Irawan, and Rena Yulia, "Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi," *urnal Hukum Pidana dan Kriminologi* 2, no. 2 (2021): 14–29.

[64] Ross Anderson et al., "Easuring the Changing Cost of Cybercrime," last modified 2019, accessed June 27, 2023, https://orca.cardiff.ac.uk/id/eprint/122684/1/Levi_Measuring the Changing Cost of Cybercrime.pdf.

[65] Hussain, "What Is Identity Theft? Definition, Types, and Examples.", *Loc. Cit.*

keuangan.[66]

f. Peretasan (*Hacking*)

Peretasan, juga dikenal sebagai *hacking*, adalah tindakan yang melibatkan mendapatkan akses tidak sah ke sistem komputer, jaringan, atau perangkat elektronik dengan tujuan mengubah, mencuri, atau merusak data atau mengambil kendali atas sistem tersebut. Aktivitas ini mencakup mengidentifikasi kerentanan dalam sistem atau jaringan komputer, dan memeriksa serta memanipulasi data dengan niat jahat atau inisiatif sendiri. Peretasan dapat dilakukan oleh individu yang memiliki pengetahuan teknis dan keahlian dalam bidang keamanan komputer.[67]

Berikut ini beberapa bentuk umum dari peretasan:

1. *Peretasan sistem komputer*: Ini melibatkan penetrasi ilegal ke dalam sistem komputer dengan mengidentifikasi celah keamanan, mencari cara untuk menghindari pengamanan, dan mendapatkan akses ke informasi sensitif atau mengendalikan sistem.[68]
2. *Peretasan jaringan*: Pelaku mencoba memasuki jaringan komputer, baik itu jaringan perusahaan, lembaga pemerintah, atau jaringan individu, dengan tujuan mengakses informasi penting atau merusak operasi jaringan.[69]
3. *Peretasan situs web*: Ini melibatkan pengambilalihan situs web dengan mendapatkan akses ke server,[70] mengubah konten, menghapus atau mencuri data, atau membuat deface pada halaman depan situs.[71]
4. *Peretasan sandi*: Pelaku menggunakan berbagai teknik, seperti *brute-force attack* atau pencurian *password*, untuk mendapatkan akses ke akun pengguna dengan tujuan mengambil alih akun tersebut.[72]
5. *Peretasan perangkat mobile*: Pelaku mencoba mendapatkan akses tidak sah ke perangkat mobile, seperti ponsel pintar atau tablet, untuk mencuri data pribadi, menginstal perangkat lunak berbahaya, atau melakukan tindakan yang merugikan.[73]
6. *Peretasan sosial*: Ini melibatkan penggunaan manipulasi psikologis dan rekayasa sosial untuk memperoleh informasi sensitif atau akses ke sistem. Pelaku mungkin menggunakan teknik seperti *phising*, *vishing*, atau *pretexting* untuk memperdaya pengguna agar memberikan informasi pribadi atau akses ke sistem.[74]

Peretasan dapat memiliki dampak serius, termasuk pencurian identitas, kerugian finansial, kerugian reputasi, penyalahgunaan informasi pribadi, atau kerugian operasional bagi perusahaan atau organisasi. Untuk

[66] *Ibid.*

[67] Kaspersky, "What Is Hacking? And How to Prevent It," last modified 2023, accessed March 27, 2023, https://www.kaspersky.com/resource-center/definitions/what-is-hacking.

[68] Sinha and Arora, "Ethical Hacking: The Story of a White Hat Hacker." *Loc.. Cit*

[69] Samuel Chng et al., "Hacker Types, Motivations and Strategies: A Comprehensive Framework," *Computers in Human Behavior Reports* 5, no. 100167 (2022).

[70] T.H. Lenhard, "Website Hacking," *Data Security. Springer, Wiesbaden* (2022).

[71] R. S. Devi and M. M. Kumar, "Testing for Security Weakness of Web Applications Using Ethical Hacking," *4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)* 354–361, d (2020).

[72] Richard Beno and Ron Poet, "Hacking Passwords That Satisfy Common Password Policies: Hacking Passwords," *In 13th International Conference on Security of Information and Networks* (2020): 1–3.

[73] C. Bermejo, H. Flores, and P. Hui, "Notice of Retraction: Steal Your Life Using 5 Cents: Hacking Android Smartphones with NFC Tags," *Journal of Network and Computer Applications* (2020): 1–6.

[74] Kaspersky, "What Is Hacking? And How to Prevent It."

melindungi diri dari peretasan, penting untuk menggunakan praktik keamanan yang kuat, seperti menggunakan kata sandi yang kuat, memperbarui perangkat lunak dengan *patch* keamanan terbaru, menghindari mengklik tautan atau lampiran yang mencurigakan, dan mengamankan jaringan dan sistem dengan *firewall* dan keamanan yang tepat.[75]

Penting juga untuk memiliki kesadaran tentang risiko peretasan dan memperoleh pengetahuan dasar tentang keamanan komputer. Jika Anda menjadi korban peretasan, penting untuk segera melaporkan kejadian tersebut kepada penyedia layanan atau otoritas yang berwenang dan mengambil langkah-langkah untuk memulihkan keamanan sistem dan melindungi informasi pribadi.

g. Penolakan Layanan dan Informasi (*Denial of Service and Information*)

Penolakan layanan (*Denial of Service*, DoS) dan penolakan informasi (*Denial of Information*, DoI) adalah serangan yang bertujuan untuk mengganggu aksesibilitas atau ketersediaan sistem komputer, jaringan, atau layanan, sehingga mengakibatkan ketidakmampuan pengguna yang sah untuk mengakses atau menggunakan layanan tersebut.[76]

1. Penolakan Layanan (*Denial of Service, DoS*):

Serangan DoS bertujuan untuk menghambat atau menghancurkan ketersediaan sumber daya komputer atau jaringan dengan cara melimpahkan lalu lintas atau membanjiri sumber daya tersebut. Hal ini dapat dilakukan dengan mengirimkan sejumlah besar permintaan palsu ke sistem target, membanjiri jaringan dengan lalu lintas yang tidak sah, atau memanfaatkan kerentanan pada sistem atau protokol jaringan.[77]

Beberapa jenis serangan DoS meliputi:[78]

a. *Serangan Flooding*: Mengirimkan lalu lintas berlebih ke sistem target untuk menghabiskan sumber daya yang ada, sehingga sistem menjadi tidak responsif.[79]

b. *Serangan Ping of Death*: Mengirimkan paket ping yang sengaja dimodifikasi dengan ukuran yang

---

[75] Jonas Borchgrevink, "Hacking and Its Legal Consequences," last modified 2023, accessed June 23, 2023, https://hacked.com/hacking-and-its-legal-consequences/."accessed":{"date-parts":[["2023","6","23"]]},"author":[{"dropping-particle":"","family":"Borchgrevink","given":"Jonas","non-dropping-particle":"","parse-names":false,"suffix":""}],"id":"ITEM-1","issued":{"date-parts":[["2023"]]},"title":"Hacking and its Legal Consequences","type":"webpage"},"uris":["http://www.mendeley.com/documents/?uuid=38d8eda1-972e-4ab4-ba10-a8d38a0de6e3"]}],"mendeley":{"formattedCitation":"Jonas Borchgrevink, "Hacking and Its Legal Consequences," last modified 2023, accessed June 23, 2023, https://hacked.com/hacking-and-its-legal-consequences/.","plainTextFormattedCitation":"Jonas Borchgrevink, "Hacking and Its Legal Consequences," last modified 2023, accessed June 23, 2023, https://hacked.com/hacking-and-its-legal-consequences/.","previouslyFormattedCitation":"Jonas Borchgrevink, "Hacking and Its Legal Consequences," last modified 2023, accessed June 23, 2023, https://hacked.com/hacking-and-its-legal-consequences/."},"properties":{"noteIndex":75},"schema":"https://github.com/citation-style-language/schema/raw/master/csl-citation.json"}

[76] National Cyber Security Centre, "Denial of Service (DoS) Guidance," last modified 2023, accessed March 26, 2023, https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection#:~:text=%22Denial of service%22 or %22,frequently reported by the media."3","26"]]},"author":[{"dropping-particle":"","family":"National Cyber Security Centre","given":"","non-dropping-particle":"","parse-names":false,"suffix":""}],"id":"ITEM-1","issued":{"date-parts":[["2023"]]},"title":"Denial of Service (DoS

[77] *Ibid.*"3","26"]]},"author":[{"dropping-particle":"","family":"National Cyber Security Centre","given":"","non-dropping-particle":"","parse-names":false,"suffix":""}],"id":"ITEM-1","issued":{"date-parts":[["2023"]]},"title":"Denial of Service (DoS

[78] Konstantinos Pelechrinis, Marios Iliofotou, and Srikanth V. Krishnamurthy, "Denial of Service Attacks in Wireless Networks: The Case of Jammers," *IEEE Communications surveys & tutorials* 13, no. 2 (2010): 245–257.

[79] Raihan ur Rasool (et al), "A Survey of Link Flooding Attacks in Software Defined Network Ecosystems," *Journal of Network and Computer Applications* (2020).

melebihi batas yang diizinkan, sehingga menyebabkan crash atau kegagalan sistem.[80]

c. *Serangan SYN Flood*: Membanjiri sistem target dengan permintaan koneksi TCP yang tidak lengkap (SYN) untuk menghabiskan sumber daya sistem dan mencegah akses pengguna yang sah.[81]

d. *Serangan Distribusi Penolakan Layanan* (*Distributed Denial of Service*, *DDoS*): Melibatkan penggunaan botnet, yaitu jaringan komputer yang terinfeksi malware dan dikendalikan oleh penyerang, untuk meluncurkan serangan DoS dari berbagai sumber yang terdistribusi, sehingga meningkatkan kemampuan serangan dan sulit dilacak.[82]

2. Penolakan Informasi (Denial of Information, DoI):

Serangan DoI[83] bertujuan untuk menghambat aksesibilitas atau ketersediaan informasi yang sah pada sistem atau situs web. Hal ini dapat dilakukan dengan memodifikasi atau menghapus data penting, merusak atau menghapus file, atau dengan cara lain mengganggu aliran informasi yang diinginkan.[84]

Beberapa jenis serangan DoI meliputi:[85]

a. *Serangan deface*: mengubah tampilan situs web dengan tujuan mengirimkan pesan atau menyebabkan kerugian reputasi bagi pemilik situs.[86]

b. *Serangan injeksi SQL*: memanfaatkan celah keamanan pada aplikasi web yang menggunakan database dengan menyisipkan perintah SQL berbahaya untuk mengambil, memodifikasi, atau menghapus data dari database.[87]

c. *Serangan penghancuran data* (*data destruction*): menghapus, merusak, atau mengenkripsi data yang penting pada sistem komputer atau jaringan.[88]

Serangan DoS dan DoI dapat menyebabkan gangguan layanan, kerugian finansial, kerugian reputasi, atau bahkan mengancam keberlangsungan bisnis atau operasional sebuah organisasi.[89]

3. Analisis Kejahatan Siber Terhadap Individu

Analisis kejahatan siber terhadap individu melibatkan pemahaman tentang jenis kejahatan siber yang paling umum menargetkan individu, serta dampak dan strategi perlindungan yang dapat digunakan. Berikut adalah beberapa aspek penting yang perlu dianalisis:

---

[80] Sagar Pande (et al)., "DDOS Detection Using Machine Learning Technique," *In Recent Studies on Computational Intelligence: Doctoral Symposium on Computational Intelligence (DoSCI 2020), Springer Singapore.* (2020): 59–68.

[81] *Ibid.*

[82] Felix Lau et al., "Distributed Denial of Service Attacks.," *IEEE* 3 (2000): 2275–2280.

[83] Adaoma Ezenwe, Eoghan Furey, and Kevin Curran, "Mitigating Denial of Service Attacks with Load Balancing," *Journal of Robotics and Control (JRC)* 1, no. 4 (2020): 129–135.

[84] Yuchong Li and Qinghui Liu, "A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments," *Energy Reports* 7 (2021): 8176–8186.

[85] Gregory Conti and Mustaque Ahamad, "A Framework for Countering Denial-of-Information Attacks," *IEEE security & privacy* 6, no. 3 (2005): 50–56.

[86] Mariam Albalawi (et al), "Website Defacement Detection and Monitoring Methods: A ReviewNo Title," *Electronics 2022, 3573.* 11 (2022): 1–20, https://doi.org/10.3390/electronics11213573.

[87] Maha Alghawazi, Daniyal Alghazzawi, and Suaad Alarifi, "Detection of SQL Injection Attack Using Machine Learning Techniques: A Systematic Literature Review," *Journal of Cybersecurity and Privacy* 2, no. 4 (2022): 764–777.

[88] Lei Cui (et al), "Detecting False Data Attacks Using Machine Learning Techniques in Smart Grid: A Surv," *Journal of Network and Computer Applications* 170, no. 102808 (2020).

[89] Ezenwe, Furey, and Curran, "Mitigating Denial of Service Attacks with Load Balancing.", *Loc. Cit.*

1. *Phishing*: Serangan *phishing* melibatkan upaya memperoleh informasi sensitif seperti kata sandi, nomor kartu kredit, atau data pribadi dengan menyamar sebagai entitas tepercaya melalui email, pesan teks, atau situs web palsu. Analisis kejahatan siber harus melibatkan identifikasi taktik phishing yang umum, seperti tautan yang mencurigakan atau email yang meminta informasi pribadi.

2. *Malware*: *Malware* adalah perangkat lunak berbahaya yang dapat diinstal tanpa izin pengguna dan merusak sistem, mencuri informasi pribadi, atau memberikan akses ke penyerang. Analisis kejahatan siber perlu mencakup pemahaman tentang jenis-jenis malware, seperti virus, *worm*, *Trojan*, atau *ransomware*, serta cara mereka menyebar dan merusak data atau perangkat.

3. *Kejahatan identitas*: Kejahatan identitas melibatkan pencurian atau penyalahgunaan informasi pribadi seseorang, seperti nomor identitas, kartu kredit, atau informasi keuangan lainnya. Analisis kejahatan siber perlu memahami taktik yang digunakan oleh penjahat identitas, seperti pencurian data, phising, atau pencurian identitas anak-anak.

4. *Penipuan online*: Penipuan *online* melibatkan praktik penipuan untuk mengelabui individu agar memberikan informasi pribadi atau melakukan tindakan finansial yang merugikan. Analisis kejahatan siber harus memahami jenis penipuan *online* yang umum, seperti penipuan lotere, penipuan cinta, atau penipuan investasi, serta taktik yang digunakan oleh penipu untuk mengecoh korban.

5. *Pelecehan online*: Pelecehan *online* mencakup tindakan seperti pelecehan verbal, pelecehan seksual, atau cyberbullying yang dilakukan melalui platform digital. Analisis kejahatan siber perlu memahami dampak psikologis dan sosial dari pelecehan online, serta cara melindungi diri dari serangan tersebut.

6. *Keamanan data dan privasi*: Analisis kejahatan siber juga harus melibatkan pemahaman tentang perlindungan data dan privasi individu. Ini termasuk penggunaan kata sandi yang kuat, enkripsi data, pengaturan privasi media sosial, atau kebijakan penggunaan data pribadi oleh perusahaan atau *platform online*.

Secara tradisional, telah diusulkan agar rekayasa sosial dapat dicegah melalui penggunaan kebijakan keamanan; pendidikan, pelatihan dan kesadaran karyawan; dan mendirikan budaya keamanan dalam organisasi.[90] Dalam menghadapi kejahatan siber terhadap individu, penting untuk mengadopsi praktik keamanan yang kuat, seperti menjaga kerahasiaan informasi pribadi, waspada terhadap taktik penipuan, menggunakan perangkat lunak keamanan yang terbaru, dan memperbarui sistem secara teratur. Edukasi dan kesadaran terhadap kejahatan siber juga sangat penting untuk mengenali dan melindungi diri dari serangan tersebut.[91]

IV. Simpulan

Berdasarkan analisis kejahatan siber terhadap individu, dapat disimpulkan bahwa individu rentan terhadap berbagai jenis serangan dan penipuan dalam ekosistem digital. Jenis Kejahatan Siber terdiri dari: (1) Rekayasa Sosial dan tipu daya (*social engineering and trickery*); (2) Pelecehan Daring (*Online Harassment*); (3) Kejahatan terkait Identitas (*Identify-related crimes*); (4) Peretasan (*Hacking*); dan (5) Penolakan Layanan dan Informasi (*Denial of Service and Information*). Secara umum kita banyak mengenal kejahatan siber seperti *phishing*, *malware*,

[90] Ahmad Uways Zulkurnain (et al), "Social Engineering Attack Mitigation," *International Journal of Mathematics and Computational Science* 1, no. 4 (2015): 188–198.

[91] Yusuf Perwej (et al), "A Systematic Literature Review on the Cyber Security," *tional Journal of scientific research and managemen* 9, no. 12 (2021): 669–710.

kejahatan identitas, penipuan *online*, dan pelecehan *online* dapat memiliki dampak serius terhadap keamanan, privasi, dan kesejahteraan individu.

Penting bagi individu untuk memahami taktik yang digunakan oleh penjahat siber dan untuk mengadopsi praktik keamanan yang kuat dalam penggunaan teknologi. Menjaga kerahasiaan informasi pribadi, menggunakan kata sandi yang kuat, memperbarui perangkat lunak secara teratur, dan menjadi sadar akan tanda-tanda serangan dan penipuan *online* dapat membantu melindungi diri dari ancaman kejahatan siber. Selain itu, penting juga untuk memperhatikan kebijakan privasi dan keamanan data yang diterapkan oleh perusahaan dan *platform online*. Menggunakan pengaturan privasi yang tepat dan mempertimbangkan kebijakan penggunaan data pribadi dapat membantu individu menjaga privasi dan mengurangi risiko penyalahgunaan data. Edukasi dan kesadaran tentang kejahatan siber juga merupakan faktor penting. Dengan meningkatkan pemahaman tentang risiko kejahatan siber dan cara melindungi diri, individu dapat mengurangi kemungkinan menjadi korban serangan dan dapat bertindak dengan bijak saat berinteraksi dalam lingkungan digital.

Dalam upaya melawan kejahatan siber, kolaborasi antara individu, lembaga penegak hukum, dan industri teknologi juga penting. Pengembangan solusi keamanan yang kuat, peningkatan hukum yang relevan, dan kerjasama dalam mengatasi ancaman kejahatan siber dapat membantu melindungi individu dan menciptakan lingkungan digital yang lebih aman dan andal.

Daftar Referensi

Jurnal/Artkel:

AAG. "The Latest 2023 Cyber Crime Statistics (Updated June 2023)." Last modified 2023. Accessed March 26, 2023. https://aag-it.com/the-latest-cyber-crime-statistics/#:~:text=Headline Cyber Crime Statistics&text=1 in 2 American internet,the first half of 2022.

Abulencia, Jesse. "The Cost of Cybercrime in the US Healthcare Sector." *Computer Fraud & Security* 11, no. 8–13 (2021).

Acquisti, Alessandro, Leslie K. John, and George Loewenstein. "What Is Privacy Worth?" *The Journal of Legal Studies* 42, no. 2 (2013): 249–274.

Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. "The Economics of Privacy." • *Journal of Economic Literature* 54, no. 2 (2016): 442–492.

Ahmad, Showkat. "Social Engineering Techniques Contrast Study." *International Journal of Engineering Studies.* 9, no. 1 (2017): 105–110.

Albalawi (et al), Mariam. "Website Defacement Detection and Monitoring Methods: A ReviewNo Title." *Electronics 2022, 3573.* 11 (2022): 1–20. https://doi.org/10.3390/electronics11213573.

Aldawood, Hussain, and Geoffrey Skinner. "A Taxonomy for Social Engineering Attacks via Personal Devices." *International Journal of Computer Applications (0975 – 8887)* 178, no. 50 (2019): 19–26.

Alghawazi, Maha, Daniyal Alghazzawi, and Suaad Alarifi. "Detection of SQL Injection Attack Using Machine Learning Techniques: A Systematic Literature Review." *Journal of Cybersecurity and Privacy* 2, no. 4 (2022): 764–777.

Almutairi, Bandar S., and Abdurahman Alghamdi. "The Role of Social Engineering in Cybersecurity and Its Impact." *Journal of Information Security* 13, no. 4 (2022).

Alshaikh, Hesham, Nagy Ramadan, and Hesham Ahmed Hefny. "Ransomware Prevention and Mitigation Techniques." *International Journal of Computer Applications (0975 – 8887)* 177, no. 40 (2020): 31–39.

Anderson, Ross, Chris Barton, Rainer Bölme, Richard Clayton, Carlos Ganán, Tom Grasso, Michael Levi, Tyler Moore, and Marie Vasek. "Easuring the Changing Cost of Cybercrime." Last modified 2019. Accessed June 27, 2023. https://orca.cardiff.ac.uk/id/eprint/122684/1/Levi_Measuring the Changing Cost of Cybercrime.pdf.

Arora, Bhavna. "Exploring and Analyzing Internet Crimes and Their Behaviours." *Perspectives in Science* 8 (2016): 540–542.

Bansla, Neetu, Swati Kunwar, and Khushboo Gupta. "Social Engineering: A Technique for Managing Human Behavior." *Journal of Information Technology and Sciences* 5, no. 1 (2019): 18–22.

Başeskioğlu, M. Ö., and A. Tepeci. "Cybersecurity, Computer Networks Phishing, Malware, Ransomware, and Social Engineering Anti-Piracy Reviews." *3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 2021* (2021): 1–5.

Beaman (et al), Craig. "Ransomware: Recent Advances, Analysis, Challenges and Future Research Directions." *Computers & Security* 111 (2021): 102490.

Beno, Richard, and Ron Poet. "Hacking Passwords That Satisfy Common Password Policies: Hacking Passwords." *In 13th International Conference on Security of Information and Networks* (2020): 1–3.

Bermejo, C., H. Flores, and P. Hui. "Notice of Retraction: Steal Your Life Using 5 Cents: Hacking Android Smartphones with NFC Tags." *Journal of Network and Computer Applications* (2020): 1–6.

Borchgrevink, Jonas. “Hacking and Its Legal Consequences.” Last modified 2023. Accessed June 23, 2023. https://hacked.com/hacking-and-its-legal-consequences/.

Broadhurst, Roderic. “Developments in the Global Law Enforcement of Cyber-crime.” *Policing: An International Journal of Police Strategies & Management* 29, no. 3 (2006): 408–433.

Chng, Samuel, Han Yu Lu, Ayush Kumar, and David Yau. “Hacker Types, Motivations and Strategies: A Comprehensive Framework.” *Computers in Human Behavior Reports* 5, no. 100167 (2022).

Conteh, Nabie Y. “The Dynamics of Social Engineering and Cybercrime in the Digital Age.” *IGI Global* (2021): 144–149.

Conti, Gregory, and Mustaque Ahamad. “A Framework for Countering Denial-of-Information Attacks.” *IEEE security & privacy* 6, no. 3 (2005): 50–56.

Cui (et al), Lei. “Detecting False Data Attacks Using Machine Learning Techniques in Smart Grid: A Surv.” *Journal of Network and Computer Applications* 170, no. 102808 (2020).

Deora, Raj Singh, and Dhaval Chudasama. “Brief Study of Cybercrime on an Internet.” *Journal of Communication Engineering & Systems* 11, no. 1 (2021): 1–6.

Devi, R. S., and M. M. Kumar. “Testing for Security Weakness of Web Applications Using Ethical Hacking.” *4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)* 354–361, d (2020).

Dupont, B., and T Holt. “The Human Factor of Cybercrime.” *Social Science Computer Review* 40, no. 4 (2022): 860–864. https://doi.org/10.1177/08944393211011584.

Englander, Elizabeth, Edward Donnerstein, Robini Kowalsk, Carolyn A. Lin, and Katalin Parti. “Defining Cyberbullying.” *Pediatrics 140* 140, no. 2 (2017): S148–S151.

Ezenwe, Adaoma, Eoghan Furey, and Kevin Curran. “Mitigating Denial of Service Attacks with Load Balancing.” *Journal of Robotics and Control (JRC)* 1, no. 4 (2020): 129–135.

Felzmann, Heike, Eduard Fosch Villaronga, and Aurelia Tamò-Larrieux. “Transparency You Can Trust: Transparency Requirements for Artificial Intelligence between Legal Norms and Contextual Concerns.” *Big Data & Society* (2019): 1–14. https://journals.sagepub.com/doi/epub/10.1177/2053951719860542.

Ghafir, I., V. Prenosil, A. Alhejailan, and M. Hammoudeh. “Social Engineering Attack Strategies and Defense Approaches,” (2016): 45–149.

Heartfield (et al), Ryan. “A Taxonomy of Cyber-Physical Threats and Impact in the Smart Home.” *Computers & Security* 78 (2018): 398–428.

Hennink, Monique, Inge Hutter, and Ajay Baliley. *Qualitative Research Methods*. Second Edi. London: Sage Publications Ltd., 2020.

Hussain, Ali. “What Is Identity Theft? Definition, Types, and Examples.” Last modified 2022. Accessed March 27, 2023. https://www.investopedia.com/terms/i/identitytheft.asp.

Jamil (et al), Abid. “MPMPA: A Mitigation and Prevention Model for Social Engineering Based Phishing Attacks on Facebook.” *2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA,.2018.8622505.* doi: 10.11 (2018): 5040–5048.

Jhaver, S., Ghoshal, S., Bruckman, A. and Gilbert, E. “Online Harassment and Content Moderation: The Case of Blocklists.” *ACM Transactions on Computer-Human Interaction (TOCHI)* 25, no. 2 (2018): 1–33.

Jones, Keith S, Miriam E. Armstrong, McKenna K. Tornblad, and Akbar Siami Namin. “How Social Engi-

neers Use Persuasion Principles during Vishing Attacks." *Information & Computer Security* 29, no. 2 (2021): 314–331.

Karali, Y, S. Panda, and C. S. Panda. "Cyber Crime: An Analytical Study of Cyber Crime Cases at the Most Vulnerable States and Cities in India." *al Journal of Engineering and Management Research (IJEMR)* 5, no. 2 (2015): 43–48.

Kaspersky. "What Is Hacking? And How to Prevent It." Last modified 2023. Accessed March 27, 2023. https://www.kaspersky.com/resource-center/definitions/what-is-hacking.

Khurana, Atika, Amy Bleakley, Amy B. Jordan, and Daniel Romer. "The Protective Effects of Parental Monitoring and Internet Restriction on Adolescents' Risk of Online Harassment." *Journal of Youth and Adolescence* 44 (2015): 1039–1047.

Kumar, Anshul, Mansi Chaudhary, and Nagresh Kumar. "Social Engineering Threats and Awareness: A Survey." *European Journal of Advances in Engineering and Technology* 2, no. 11 (2015): 15–19.

Lau, Felix, Stuart H. Rubin, Michael H. Smith, and Ljiljana Trajkovic. "Distributed Denial of Service Attacks." *IEEE* 3 (2000): 2275–2280.

Lee, Chunghun, Choong C. Lee, and Suhyun Kim. "Understanding Information Security Stress: Focusing on the Type of Information Security Compliance Activity." *Computers & Security* 59 (2016): 60–70.

Lenhard, T.H. "Website Hacking." *Data Security. Springer, Wiesbaden* (2022).

Li, Yuchong, and Qinghui Liu. "A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments." *Energy Reports* 7 (2021): 8176–8186.

Lohani, Shivam. "Social Engineering: Hacking into Humans." *International Journal of Advanced Studies of Scientific Research* 4, no. 1 (2019).

Lubua, E.W.', and P.D Pretorius. "Ranking Cybercrimes Based on Their Impact to Organisations' Welfare." *HREAT Conference Proceedings* (2019): 1–11.

Luthiya, Adik Nur, Benny Irawan, and Rena Yulia. "Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi." *urnal Hukum Pidana dan Kriminologi* 2, no. 2 (2021): 14–29.

Mandalla, Achmad Zaki. "Deteksi Penipuan Pada Transaksi Kartu Kredit Menggunakan Metode Stochastic Gradient Descent Dengan Momentum." Institut Teknologi Sepuluh Nopember, 2023.

Maseno, Elijah M. "Vishing Attack Detection Model For Mobile Users." *KCA University* (2017). http://41.89.49.13:8080/xmlui/bitstream/handle/123456789/1276/Maseno-Vishing Attack Detection Model For Mobile Users..pdf?sequence=1&isAllowed=y.

McGuire, Mike, and (Samantha Dowling. "Cyber Crime: A Review of the Evidence Research Report 75." Last modified 2013. Accessed June 27, 2023. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=5e089b9bac3cdba577724cf0cd23f648a4f952d9.

Mehmood, A., I. Natgunanathan, Y. Xiang, G. Hua, and S. Guo. "Protection of Big Data Privacy." *IEEE Access* 4, no. 1821–1834 (2016). https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7460114.

National Cyber Security Centre. "Denial of Service (DoS) Guidance." Last modified 2023. Accessed March 26, 2023. https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection#:~:text=%22Denial of service%22 or %22,frequently reported by the media.

Nissim, Kobbi, and Alexandra Wood. "Is Privacy Privacy?" *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376, no. 2128 (2018). https://royalsocietypublishing.org/doi/pdf/10.1098/rsta.2017.0358.

Nurse, Jason R. C. "Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit." *arXiv preprint arXiv:1811.06624* (2018). https://arxiv.org/abs/1811.06624.

Pande, Sagar, Aditya Khamparia, Deepak Gupta, and Dang N. H. Thanh. "DDOS Detection Using Machine Learning Technique." *In Recent Studies on Computational Intelligence: Doctoral Symposium on Computational Intelligence (DoSCI 2020), Springer Singapore.* (2020): 59–68.

Parti, Katalin, Akos Szigeti, and Sandro Serpa. "The Future of Interdisciplinary Research in the Digital Era: Obstacles and Perspectives of Collaboration in Social and Data Sciences - An Empirical Study." *Cogent Social Sciences* 7, no. 1 (2021). https://www.tandfonline.com/doi/full/10.1080/23311886.2021.1970880

Pelechrinis, Konstantinos, Marios Iliofotou, and Srikanth V. Krishnamurthy. "Denial of Service Attacks in Wireless Networks: The Case of Jammers." *IEEE Communications surveys & tutorials* 13, no. 2 (2010): 245–257.

Perwej (et al), Yusuf. "A Systematic Literature Review on the Cyber Security." *tional Journal of scientific research and managemen* 9, no. 12 (2021): 669–710.

Rasool (et al), Raihan ur. "A Survey of Link Flooding Attacks in Software Defined Network Ecosystems." *Journal of Network and Computer Applications* (2020).

Rumlus, M.H., and H Hartadi. "Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik." *Jurnal HAM* 11, no. 2 (2020): 285–299.

Salahdine, Fatima, and Naima Kaabouch. "Social Engineering Attacks: A Survey." *Future Internet,* 11 (2019): 89.

Schwab, Klaus. "The Fourth Industrial Revolution: What It Means, How to Respond." *Currency* (2017). https://jmss.vic.edu.au/wp-content/uploads/2021/06/The_Fourth_Industrial_Revolution.pdf.

Siegner, Alana B. "Experiential Climate Change Education: Challenges of Conducting Mixed-Methods, Interdisciplinary Research in San Juan Islands, WA and Oakland, CA." *Energy Research & Social Science* 45 (2018): 374–384.

Sinha, Shivanshi, and Dr Yojna Arora. "Ethical Hacking: The Story of a White Hat Hacker." *International Journal of Innovative Research in Computer Science & Technology (IJIRCST)* ISSN (2020 (2020): 131–136.

Thorns, David, and Michael Nuth. "Beyond The Hype: Intellectual Property and The Knowledge Society/ Knowledge Economy." *Journal of Economic Surveys* 20, no. 4 (2006): 633–690.

Vitak, Jessica, Linda Steiner, and Zahra Ashktorab. "Identifying Women's Experiences With and Strategies for Mitigating Negative Effects of Online Harassment." *In Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computingx* (2017): 1231–1245.

Vogels, Emily A. "The State of Online Harassment." *Pew Research Center* 13 (2021). https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2021/01/PI_2021.01.13_Online-Harassment_FINAL-1.pdf.

Wang, Zuoguang, Limin Sun, and Hongsong Zhu. "Defining Social Engineering in Cybersecurity." *IEEE Access* 8 (2020): 85094–85115.

Watts (et al), Lynette K. "Cyberbullying in Higher Education: A Literature Review." *Computers in Human Behavior* 69 (2017): 268–274.

Whittaker, E. and Kowalski, R.M. "Cyberbullying Via Social Media." *Journal of school violence* 14, no. 1 (2015): 11–29.

Zulkurnain (et al), Ahmad Uways. "Social Engineering Attack Mitigation." *International Journal of Mathe-*

matics and Computational Science 1, no. 4 (2015): 188–198.