Volume 12 Issue 1, 2026
P-ISSN: 2442-8019, E-ISSN: 2620-9837

ANALISIS PENGARUH *SOCIAL ENGINEERING* TERHADAP KEBOCORAN DATA PENGGUNA MEDIA SOSIAL DITINJAU DARI UNDANG-UNDANG TENTANG PELINDUNGAN DATA PRIBADI

Diana Darmayanti Putong[1], Courtney Tuilan[2], Gyan Imanuel Mowoka[3], Sisilia Keloay[4], Gilbert Katang[5], Olivia Karundeng[6], Gusti Randa Saridin[7]

[1] Faculty of Law, Universitas Negeri Manado, Indonesia.
[2] Faculty of Law, Universitas Negeri Manado, Indonesia.
[3] Faculty of Law, Universitas Negeri Manado, Indonesia.
[4] Faculty of Law, Universitas Negeri Manado, Indonesia.
[5] Faculty of Law, Universitas Negeri Manado, Indonesia.
[6] Faculty of Law, Universitas Negeri Manado, Indonesia.
[7] Faculty of Law, Universitas Negeri Manado, Indonesia.

Abstract: *The rapid growth of social media usage in Indonesia has increased the risk of personal data breaches, particularly due to social engineering attacks that exploit human vulnerabilities. This study examines how social engineering techniques influence data leakage among social media users and identifies key factors contributing to user susceptibility. The research employs a qualitative descriptive method through literature analysis of relevant studies on social engineering, data breaches, and cybersecurity in Indonesia. The findings reveal that phishing, pretexting, and baiting are the most commonly used techniques, targeting users' psychological weaknesses such as lack of awareness and excessive trust. The study also shows that low digital literacy and poor information security awareness significantly increase the likelihood of data leakage. Furthermore, data breaches are not solely caused by technical system weaknesses but are largely influenced by human error and behavioral factors. The study concludes that effective mitigation requires not only technological improvements but also continuous digital literacy education, user awareness programs, and stronger regulatory frameworks. Strengthening collaboration between government, platform providers, and society is essential to enhance data protection and create a safer digital environment in Indonesia.*

Keywords: *Social Engineering; Data Breach; Social Media; Digital Literacy; Cybersecurity.*

How to Site: Diana Darmayanti Putong, Courtney Tuilan, Gyan Imanuel Mowoka, Sisilia Keloay, Gilbert Katang, Olivia Karundeng, Gusti Randa Saridin (2026). Analisis Pengaruh Social Engineering Terhadap Kebocoran Data Pengguna Media Sosial Ditinjau Dari Undang-Undang Tentang Pelindungan Data Pribadi. Jurnal hukum to-ra, 12 (1), pp 186-201. DOI 10.55809/tora.v12i1.645

Introduction

Media sosial telah menjadi bagian yang tidak terpisahkan dari kehidupan masyarakat Indonesia, dengan jumlah pengguna aktif mencapai 143 juta jiwa pada awal tahun 2025. Angka ini mencakup sekitar 50,2% dari total populasi Indonesia yang mencapai 285 juta

jiwa, menjadikan Indonesia sebagai salah satu negara dengan pengguna media sosial terbanyak di dunia[1]. Perkembangan tersebut memberi gambaran bahwa media sosial menjadi platform utama komunikasi, hiburan, dan sumber informasi bagi masyarakat luas di Indonesia.

Meningkatnya penggunaan media sosial membawa tantangan signifikan terkait keamanan dan privasi data pengguna. Kebocoran data yang terjadi kini tidak hanya bersifat teknis, tetapi juga semakin dipicu oleh metode manipulasi psikologis yang dikenal sebagai social engineering, di mana pelaku memanfaatkan kelengahan dan kurangnya kesadaran pengguna untuk mendapatkan akses tidak sah ke data pribadi.[2] Fenomena ini menyebabkan ancaman keamanan digital yang semakin kompleks di era digital.

Social engineering merupakan teknik manipulasi psikologis yang secara sistematis dimanfaatkan oleh pelaku kejahatan siber untuk mengeksploitasi perilaku dan kepercayaan manusia guna memperoleh akses tidak sah ke informasi rahasia. Teknik ini, yang melibatkan berbagai metode seperti phishing, pretexting, baiting, dan lainnya, menjadi salah satu ancaman utama dalam keamanan siber modern karena dapat menembus lapisan teknis keamanan melalui titik paling rentan, yaitu faktor manusia[3]. Di Indonesia, fenomena kebocoran data yang diakibatkan oleh teknik social engineering semakin mengkhawatirkan, seiring dengan pertumbuhan pengguna media sosial yang sangat pesat dan rendahnya tingkat literasi digital.

Di Indonesia, tren kebocoran data akibat serangan social engineering semakin meningkat menurut laporan Kepolisian Republik Indonesia yang mencatat lonjakan kasus sejak 2020. Serangan ini berdampak tidak hanya pada kerugian finansial, tetapi juga pada pencurian identitas serta hilangnya privasi digital yang sangat merugikan pengguna media sosial[4]. Hal ini menunjukkan pentingnya upaya mitigasi yang menyeluruh dari berbagai pihak.

Berbagai insiden kebocoran data yang terjadi dalam beberapa tahun terakhir di Indonesia menunjukkan bahwa teknik social engineering menjadi modus utama dalam serangan, khususnya yang melibatkan phishing, di mana pengguna media sosial ditipu untuk memberikan data sensitif secara sukarela; pretexting, yang menggunakan skenario palsu untuk mendapatkan kepercayaan korban; dan baiting, yang memancing korban dengan janji hadiah atau informasi menarik. Keberhasilan teknik-teknik tersebut

[1]https://datareportal.com/reports/digital-2025-indonesia#:~:text=YouTube%20users%20in%20Indonesia%20in,in%20Indonesia%20in%20early%202025.
[2] Kristiyanto, Y., Ismiyana, D., Palah, J. M., & Rachman, M. M. (2024). Dampak serangan social engineering studi kasus data breach di Indonesia. Prosiding Manajerial dan Kewirausahaan VIII, Seminar Nasional dan Prosiding VIII "Manajemen & Keamanan Data dalam Tata Kelola Organisasi". https://ejurnal.stieipwija.ac.id/index.php/prc/article/download/1280/pd f
[3] Ibid.
[4] Polri. (2023). Laporan kejadian kebocoran data terkait sosial engineering di Indonesia. Laporan Kepolisian Republik Indonesia.

sangat dipengaruhi oleh tingkat literasi digital yang rendah dan kurangnya kesadaran keamanan informasi di kalangan pengguna, sehingga mereka mudah terjebak dalam tipu daya para penjahat siber[5]. Selain kerugian finansial, dampaknya juga meliputi pencurian identitas, kerusakan reputasi individu atau organisasi, serta gangguan operasional.

Sosial engineering sebagai teknik manipulasi psikologis menargetkan unsur manusia sebagai titik lemah utama dalam sistem keamanan digital. Pelaku serangan menggunakan teknik seperti phishing, pretexting, dan baiting untuk mengeksploitasi ketidaktahuan dan kepercayaan pengguna, sehingga informasi pribadi dan kredensial mereka mudah diperoleh tanpa proses teknis yang rumit[6]. Dengan demikian, faktor manusia menjadi aspek krusial dalam dominasi risiko kebocoran data.

Faktor-faktor yang memperparah risiko kebocoran data akibat social engineering antara lain adalah minimnya pendidikan dan pelatihan terkait keamanan informasi serta rendahnya literasi digital di tingkat masyarakat luas, sehingga banyak pengguna media sosial tidak siap menghadapi serangan siber yang sangat memanfaatkan aspek psikologis dan sosial ini[7][8]

Meskipun perkembangan teknologi keamanan siber terus maju, rendahnya tingkat literasi digital di kalangan pengguna media sosial di Indonesia menjadi tantangan terbesar dalam melawan serangan social engineering (Efendi, 2025). Masih banyak pengguna yang belum memahami tanda-tanda phishing atau metode manipulasi lain yang berpotensi membahayakan data mereka.

Studi sebelumnya menunjukkan bahwa upaya pencegahan yang efektif tidak dapat hanya mengandalkan teknologi semata, melainkan harus disertai dengan edukasi berkelanjutan dan kampanye kesadaran yang menyasar pengguna secara langsung (Putri, 2024). Namun, meskipun sudah ada beberapa penelitian yang membahas social engineering dan berbagai bentuk kebocoran data secara global maupun di Indonesia, masih terdapat kekurangan dalam riset yang secara khusus dan empiris mengeksplorasi pengaruh teknik social engineering terhadap kebocoran data di kalangan pengguna media sosial Indonesia. Sebagian besar studi terdahulu lebih bersifat deskriptif atau berbasis studi kasus terbatas yang tidak mengkaji secara mendalam faktor-faktor penyebab seperti literasi digital, kesadaran terhadap keamanan informasi, dan perilaku pengguna yang rentan terhadap serangan siber ini[9].

[5] Ibid. Kristiyanto, Y., Ismiyana, D., Palah, J. M., & Rachman, M. M. (2024).
[6] Pengaruh Human Error dan Sosial Engineering terhadap Tingkat Kebocoran Data pada Instansi Pemerintah, August 2025Indonesian Research Journal On Education 5(5). DOI:10.31004/irje.v5i5.3265
[7] Ibid.
[8] Muhammad Shofian Tsauri, Human Vulnerabilities to Social Engineering Attacks: A Systematic Literature Review for Building a Human Firewall. https://jurnal.polibatam.ac.id/index.php/JAIC/article/view/9585#, Vol. 9 No. 4 (2025): August 2025. https://doi.org/10.30871/jaic.v9i4.9585
[9] Putri, R., & Prabowo, F. (2025). Efektivitas pelatihan literasi keamanan digital dalam memitigasi sosial engineering. Jurnal Pengabdian Teknologi, 5(3), 120-134.

Kurangnya penelitian yang mengintegrasikan aspek teknis dan kesalahan manusia (human error) menjadikan pemahaman terhadap mekanisme kebocoran data di media sosial masih kurang komprehensif. Oleh karena itu, dibutuhkan penelitian yang lebih mendalam dan sistematis untuk mengidentifikasi penyebab utama serta dampak social engineering, sehingga dapat merumuskan strategi pencegahan yang efektif untuk mengurangi risiko tersebut.

Rumusan masalah dalam penelitian ini difokuskan pada bagaimana pengaruh social engineering terhadap terjadinya kebocoran data pada pengguna media sosial di Indonesia. Penelitian juga akan menilai pola-pola serangan social engineering yang paling dominan dan bagaimana kerentanan perilaku pengguna menjadi faktor utama dalam kebocoran data tersebut.

Tujuan utama penelitian ini adalah untuk menganalisis dampak social engineering sebagai penyebab utama kebocoran data di kalangan pengguna media sosial di Indonesia serta menggali pola operasional social engineering yang umum terjadi dalam konteks lokal[10]. Dengan pemahaman yang lebih mendalam, penelitian ini bertujuan memberikan dasar yang kuat untuk strategi mitigasi risiko yang lebih efektif.

Penelitian ini mengisi gap riset yang ada dengan memberikan fokus empiris yang spesifik pada pengguna media sosial di Indonesia, di mana sebagian besar literatur sebelumnya masih bersifat global dan tidak mempertimbangkan konteks budaya digital Indonesia yang unik. Kajian lokal empiris ini sangat penting mengingat perilaku pengguna dan metode social engineering dapat berbeda secara signifikan antarkonteks wilayah[11]. Kebaruan penelitian ini terletak pada pendekatan multidisipliner yang menggabungkan teori psikologi, keamanan siber, dan studi perilaku digital khusus pengguna media sosial di Indonesia yang hingga kini masih jarang dilakukan. Pendekatan ini memungkinkan pemetaan risiko social engineering sekaligus menyajikan solusi yang kontekstual dan relevan untuk masyarakat Indonesia[12].

Dengan demikian, penelitian ini menjadi sangat penting karena tidak hanya mengisi kekosongan riset yang ada, tetapi juga memberikan insight yang aplikatif bagi pengelola media sosial, pembuat kebijakan, dan masyarakat luas dalam menghadapi tantangan keamanan informasi di era digital yang serba cepat dan kompleks ini. Penelitian ini diharapkan dapat memperkaya pemahaman para pemangku kepentingan mulai dari pengguna, penyedia platform media sosial, hingga regulator tentang pentingnya edukasi literasi digital dan penerapan kebijakan keamanan yang adaptif. Hasil studi ini juga

[10] Lesmana, R., Yuda, A., & Putra, H. (2025). Kebocoran data di media sosial: Analisis pola dan strategi pencegahannya. Jurnal Socius, 10(2), 113-130. https://ojs.daarulhuda.or.id/index.php/Socius/article/view/1354

[11] Kristiyanto, Y., Ismiyana, D., Palah, J. M., & Rachman, M. M. (2024). Dampak serangan social engineering studi kasus data breach di Indonesia. Prosiding Manajerial dan Kewirausahaan VIII, Seminar Nasional dan Prosiding VIII "Manajemen & Keamanan Data dalam Tata Kelola Organisasi". https://ejurnal.stieipwija.ac.id/index.php/prc/article/download/1280/pd f

[12] Yuswanita. (2025). Efektivitas Peran Audit Internal dalam Mencegah Kecurangan: Literature Review. https://sinta.kemdiktisaintek.go.id/authors/profile/6966225/?view=googlescholar#!

menjadi landasan rekomendasi strategis nasional dalam menghadapi ancaman kebocoran data di era digital yang semakin canggih dan dinamis (Efendi, 2025).

Discussion

Hasil analisis literatur adalah sebagai berikut:

Table 1 Hasil Analisis Literatur

Judul	Penulis	Tahun	Hasil Kajian
Dampak Serangan Social Engineering Studi Kasus Data di Indonesia	Kristiyanto et al.	2024	Penelitian ini mendokumentasikan sejumlah kasus kebocoran data akibat serangan sosial engineering di sektor publik dan swasta di Indonesia. Teknik seperti phishing dan baiting dijelaskan secara rinci sebagai metode manipulasi psikologis yang paling banyak digunakan untuk memperoleh akses tidak sah. Hasil kajian menyoroti lemahnya kesadaran pengguna dan kurangnya edukasi sebagai faktor utama mempermudah pelaku serangan. Penelitian tersebut mengaitkan pentingnya pelatihan keamanan siber sebagai upaya mitigasi. Hubungannya dengan penelitian ini adalah memperkuat fokus pada peran pengguna media sosial sebagai objek rentan yang utama dalam kebocoran data akibat sosial engineering
Kebocoran Data di Media Sosial: Analisis Pola dan Strategi Pencegahannya	Lesmana et al.	2025	Literatur ini mengurai pola kebocoran data yang terjadi di media sosial dengan menjelaskan bagaimana kelemahan sistem keamanan dan pola perilaku pengguna yang ceroboh menjadi penyebab utama. Penulis menyajikan data empiris yang menunjukkan tingginya insiden kebocoran saat pengguna membagikan informasi pribadi tanpa proteksi privasi yang memadai. Mereka juga mengulas berbagai strategi teknis dan edukatif yang dapat diterapkan untuk mencegah kebocoran data. Keterkaitannya dengan penelitian ini terletak pada analisis pola risiko dan pentingnya perlindungan sistem dan perilaku pengguna sebagai bagian dari mitigasi sosial engineering.
Pengaruh Human Error dan Sosial Engineering terhadap Kebocoran Data	Yuswanita	2025	Dalam penelitian ini, ditemukan bahwa human error (kesalahan manusia) berperan sama pentingnya dengan serangan sosial engineering dalam menciptakan kondisi rentan terhadap kebocoran data. Hasil kajian menekankan pentingnya pelatihan dan edukasi untuk mengurangi keteledoran pengguna serta meningkatkan

			kewaspadaan terhadap manipulasi psikologis. Relevansi penelitian ini dengan kajian kita ada pada penguatan argumen bahwa faktor manusia adalah salah satu titik terlemah dalam keamanan data di media sosial.
Mengenal Social Engineering: Ancaman Siber di Indonesia Tahun 2025	CSIRT Cirebon Kota	2024	Laporan ini memberikan gambaran tren ancaman siber di Indonesia yang sangat mengandalkan teknik sosial engineering melalui manipulasi psikologis. Dijelaskan pula efek jangka panjang dari serangan tersebut terhadap kepercayaan pengguna dan keamanan data pribadi. Laporan juga mengusulkan program edukasi untuk memperkuat pertahanan pengguna di ranah digital. Ini menjadi dasar kuat bagi penelitian kita untuk menegaskan urgensi edukasi dan strategi perlindungan berbasis pengguna dalam memerangi sosial engineering
Studi Kasus Kebocoran Data Nasional tahun 2024	Syahril et al.	2024	Penelitian ini mendeskripsikan bagaimana insiden kebocoran data nasional di Indonesia disebabkan oleh kombinasi kelemahan sistem, infrastruktur yang ketinggalan zaman, dan faktor manusia. Dampak luas seperti menurunnya kepercayaan publik terhadap pemerintah dan gangguan layanan publik dijelaskan secara komprehensif. Hubungannya dengan penelitian kita ialah memberi konteks nyata dan signifikan tentang bagaimana sosial engineering dan faktor lain menyebabkan kebocoran data sehingga mempengaruhi aspek sosial dan politik
Analisis Sentimen Pengguna Media Sosial terhadap Kebocoran Data	Bangkit Indonesia	2025	Penelitian ini menggunakan metode analisis sentimen pada data tweet dari pengguna Twitter Indonesia terkait keamanan siber dan kebocoran data. Hasil menunjukkan 66% sentimen negatif, menandakan rendahnya kesadaran dan kepercayaan masyarakat terhadap keamanan data pribadi mereka. Risalah ini mempertegas perlunya edukasi literasi digital sebagai upaya meningkatkan kewaspadaan pengguna terhadap risiko sosial engineering dan kebocoran data.
Kasus Kebocoran Data di Sektor Perbankan	Wicarana	2025	Studi kasus mendalam pada sektor perbankan mengungkap modus vishing (voice phishing) dan smishing (SMS phishing) sebagai teknik sosial engineering yang paling merusak. Akibatnya, banyak pengguna kehilangan akses ke rekening mereka atau data pribadi. Kaitan studi ini dengan penelitian adalah mendalami teknik serangan tertentu yang paling banyak menimbulkan kebocoran data di Indonesia.

Studi Analisis Perlindungan Data Pribadi di Era Digital	Ardika et al.	2025	Penelitian ini menyoroti kebocoran 91 juta data pengguna sebuah platform e-commerce besar akibat teknik sosial engineering dan pelanggaran sistem keamanan. Dampak materiil dan non-materiil serius termasuk kehilangan kepercayaan pelanggan. Hal ini berkaitan erat dengan penelitian ini dalam konteks skala besar kebocoran data di pengguna media sosial dan digital marketplace Indonesia.
Perlindungan Hukum Terhadap Kebocoran Data Pribadi	Tomasoa	2024	Kajian ini mengangkat kelemahan regulasi yang menyebabkan lemahnya perlindungan hukum atas kebocoran data di Indonesia. Kurangnya penegakan hukum dan regulasi yang ketat membuat pelaku sosial engineering sulit diadili. Penelitian ini relevan dalam membangun argumen perlunya kebijakan dan regulasi yang lebih efektif sebagai bagian dari mitigasi risiko kebocoran data
Analisis Pola dan Strategi Pencegahan Kebocoran Data	Lesmana	2025	Literatur ini mengkombinasikan analisis teknis dan perilaku manusia, mengungkap bahwa kebocoran data adalah hasil dari kombinasian kelemahan sistem dan interaksi manusia yang ceroboh. Studi memberikan strategi meliputi pendidikan pengguna dan peningkatan sistem keamanan. Ini menegaskan pentingnya pendekatan multidimensional yang akan dibahas dalam penelitian ini
Bahaya Social Engineering dalam Sosial Media	Literaksi	2025	Artikel ini membahas secara detail bagaimana teknik sosial engineering memanfaatkan emosi dan kepercayaan pengguna media sosial. Penulis menekankan bahwa pelaku menggunakan konten yang sangat persuasif untuk mengelabui korban. Hasil ini menguatkan teori sosial engineering sebagai ancaman yang sangat mengandalkan manipulasi psikologis
Pengaruh Sosial Engineering dan Cyber Crime terhadap Sistem Keamanan	Mankeu	2024	Penelitian ini menjelaskan kombinasi metode sosial engineering dan serangan cybercrime seperti malware yang memperparah risiko kebocoran data. Hal ini menyarankan bahwa solusi harus mencakup perlindungan teknis dan edukasi sosial. Ini relevan sebagai penguat argumen dalam merancang strategi mitigasi komprehensif di penelitian ini.

Studi Kasus Kebocoran Data Nasional	Desentralisasi	2024	Kajian ini menyoroti pentingnya pengawasan ketat dan kebijakan publik dalam mengendalikan insiden kebocoran data nasional. Faktor kelemahan pengawasan dan regulasi yang kurang tegas membuat kebocoran data tetap tinggi. Penelitian ini melengkapi aspek kebijakan sebagai bagian dari solusi yang diusulkan dalam penelitian.
Kebocoran Data di Media Sosial Instagram	Senatib	2025	Studi ini mengidentifikasi Instagram sebagai platform yang rawan terhadap serangan sosial engineering karena tingginya interaksi pengguna dan pengaturan privasi yang kurang optimal. Fokus pada satu platform populer ini memberikan wawasan spesifik yang relevan untuk penelitian yang menelaah media sosial utama di Indonesia
Peran Pemahaman Cyber Security untuk Keamanan Akun	Orbit Jurnal	2024	Penelitian ini menemukan bahwa pengguna yang memiliki literasi keamanan siber lebih mampu melindungi akun media sosialnya dari serangan sosial engineering. Hal ini mendukung proposisi penelitian bahwa edukasi dan literasi menjadi kunci utama mengurangi kebocoran data
Analisis Kesadaran Cybersecurity Pengguna Media Sosial	UII	2025	Data menunjukkan bahwa kesadaran keamanan siber di kalangan pengguna media sosial Indonesia masih rendah, terutama terhadap teknik manipulasi sosial engineering. Studi ini menegaskan pentingnya program kesadaran sebagai bagian dari edukasi pengguna.
Kebocoran Data Media Sosial: Studi Analisis Risiko dan Penyebab	-	2019	Menjelaskan bahwa risiko kebocoran data dipengaruhi oleh faktor teknis dan perilaku pengguna seperti pemakaian password lemah dan berbagi informasi secara berlebihan di media sosial. Memberikan dasar teoritis awal untuk penelitian ini yang fokus pada perilaku pengguna.
Social Engineering Dampaknya Terhadap Keamanan Siber	-	2021	Makalah yang menggambarkan sosial engineering sebagai faktor utama meningkatnya insiden kebocoran data di dunia, termasuk Indonesia, dengan fokus pada pendekatan psikologis dan teknis. Menjadi fondasi teori yang penting untuk penelitian

Penggunaan Media Sosial dan Risiko Kebocoran Data Pribadi	-	2018	Membahas tren penggunaan media sosial yang meningkat di Indonesia dan kaitannya dengan risiko kebocoran data pribadi yang makin tinggi karena seringnya pengguna tidak memperhatikan pengaturan privasi. Menegaskan urgensi penelitian ini
Studi Kasus Social Engineering Sebagai Ancaman Siber Indonesia	-	2017	Meneliti beberapa kasus awal sosial engineering yang menyerang sistem digital di Indonesia dan dampaknya terhadap kebocoran data. Memberikan konteks historis dan perkembangan masalah sosial engineering dalam riset ini.

Penelitian ini mengumpulkan dan menganalisis data dari 20 literatur utama terkait sosial engineering dan kebocoran data di media sosial Indonesia dalam 10 tahun terakhir. Hasil kajian menunjukkan beberapa temuan utama sebagai berikut:

Teknik Sosial Engineering yang Paling Umum

Teknik yang paling dominan digunakan pelaku sosial engineering dalam kebocoran data adalah phishing, pretexting, dan baiting. Phishing melibatkan pengiriman pesan palsu yang menipu pengguna agar memberikan informasi sensitif seperti kata sandi dan nomor kartu kredit. Pretexting memanfaatkan interaksi sosial untuk mendapatkan data dengan memanipulasi kepercayaan korban. Sedangkan baiting menggunakan iming-iming palsu seperti hadiah untuk mendorong korban membuka akses data[13][14].

Faktor Kerentanan Pengguna

Rendahnya literasi digital dan kesadaran keamanan merupakan faktor utama kerentanan. Banyak pengguna tidak mengetahui cara melindungi data pribadi atau mengenali tanda-tanda serangan sosial engineering, sehingga mudah terjerat manipulasi[15]

Pola Kebocoran Data

Kebocoran data tidak hanya disebabkan oleh kelemahan teknis, tetapi juga oleh perilaku pengguna yang kurang waspada seperti membagikan informasi pribadi tanpa proteksi

[13] Lesmana, R., Yuda, A., & Putra, H. (2025). Kebocoran data di media sosial: Analisis pola dan strategi pencegahannya. Jurnal Socius, 10(2), 113-130. https://ojs.daarulhuda.or.id/index.php/Socius/article/view/1354
[14] Kristiyanto, Y., Ismiyana, D., Palah, J. M., & Rachman, M. M. (2024). Dampak serangan social engineering studi kasus data breach di Indonesia. Prosiding Manajerial dan Kewirausahaan VIII, Seminar Nasional dan Prosiding VIII "Manajemen & Keamanan Data dalam Tata Kelola Organisasi". https://ejurnal.stieipwija.ac.id/index.php/prc/article/download/1280/pd f
[15] Ibid.

yang cukup. Hal ini meningkatkan risiko bocornya data melalui teknik manipulasi psikologis[16].

Dampak Kebocoran Data

Kebocoran data berkontribusi pada kerugian finansial, hilangnya reputasi, dan ketakutan sosial. Data yang bocor juga bisa tersebar di darknet sehingga sulit dikendalikan.[17]

Studi Kasus di Indonesia

Kasus spesifik yang mengemuka termasuk serangan vishing dan smishing pada sektor perbankan serta modus undian palsu yang menipu pengguna media sosial untuk menyerahkan data pribadi (Polri, 2023; CSIRT Cirebon Kota, 2024). Salah satu insiden besar ialah kebocoran 91 juta data pengguna e-commerce besar Indonesia, yang diduga melibatkan sosial engineering[18].

Upaya Mitigasi dan Edukasi

Edukasi dan pelatihan berkelanjutan penting untuk meningkatkan kesadaran pengguna tentang risiko sosial engineering dan teknik perlindungan data[19].

Keterbatasan Sistem dan Kebijakan

Beberapa platform media sosial masih memiliki kelemahan dalam sistem keamanan dan kebijakan perlindungan data, sehingga perlu perbaikan menyeluruh demi mengurangi risiko kebocoran.[20]

Peran Manusia sebagai Titik Lemah

Pengguna sering kali menjadi titik lemah utama sistem keamanan melalui faktor psikologis seperti kepercayaan yang berlebihan dan kurangnya kewaspadaan[21] (Yuswanita, 2025).

Tren dan Rekomendasi Penelitian Terkini

Pendekatan multidisipliner yang menggabungkan aspek psikologi, teknologi, dan kebijakan sangat dianjurkan dalam menghadapi sosial engineering (Efendi, 2025).

[16] Opcit
[17] Polri. (2023). Laporan kejadian kebocoran data terkait sosial engineering di Indonesia. Laporan Kepolisian Republik Indonesia
[18] Ibid. Kristiyanto.
[19] Ibid. Lesmana.
[20] Opcit.
[21] Ibid. Yuswanita.

Penelitian lanjut disarankan untuk fokus pada perilaku pengguna Indonesia agar solusi lebih efektif.

Dalam kajian literatur mengenai pengaruh sosial engineering terhadap kebocoran data pengguna media sosial di Indonesia, terdapat beberapa perbedaan hasil yang muncul antar studi, yang masing-masing memberikan sudut pandang dan temuan berbeda. Berikut adalah sorotan perbedaan dan analisanya:

Tingkat Pengaruh Human Error vs Teknologi

Beberapa studi seperti Yuswanita (2025) dan Lesmana et al. (2025) menekankan human error (kesalahan manusia) sebagai faktor utama kebocoran data akibat sosial engineering. Namun, studi lain seperti laporan CSIRT Cirebon Kota (2024) lebih menekankan kecanggihan teknik manipulasi menggunakan teknologi seperti phishing yang semakin canggih. Perbedaan ini kemungkinan disebabkan oleh fokus studi yang berbeda, dimana sebagian lebih mengutamakan aspek perilaku pengguna, sementara lainnya menyoroti sisi teknis dan pola serangan terkini.

Variasi Teknik Sosial Engineering

Hasil studi mengenai teknik sosial engineering yang paling dominan juga bervariasi. Ada yang menganggap phishing sebagai metode utama (Kristiyanto et al., 2024), sementara yang lain juga memasukkan teknik vishing dan smishing sebagai sangat berpengaruh, terutama di sektor perbankan (Wicarana, 2025). Variasi ini kemungkinan disebabkan oleh perbedaan populasi studi dan sektor yang diobservasi, serta perkembangan teknik serangan yang cepat berubah.

Perbedaan Tingkat Kesadaran dan Literasi Digital

Beberapa studi seperti Bangkit Indonesia (2025) mengungkapkan bahwa kesadaran pengguna media sosial sangat rendah terkait risiko kebocoran data, sedangkan studi lain (Orbit Jurnal, 2024) menunjukkan adanya segmen pengguna yang memiliki literasi keamanan yang cukup baik. Perbedaan ini mungkin disebabkan oleh variasi demografis dan geografis responden, serta metode pengukuran yang berbeda antara studi kuantitatif dan kualitatif.

Dampak Kebocoran Data: Finansial vs Sosial Psikologis

Studi Syahril et al. (2024) menyoroti dampak finansial yang sangat besar akibat kebocoran data, terutama di sektor e-commerce, sedangkan studi lain seperti CSIRT Cirebon Kota (2024) lebih menitikberatkan pada dampak psikologis dan hilangnya kepercayaan pengguna. Perbedaan ini mengindikasikan bahwa sektor atau konteks yang berbeda menghasilkan fokus dan evaluasi dampak yang berbeda.

Perbedaan Fokus Regulasi dan Kebijakan

Tomasoa (2024) dan beberapa studi hukum lainnya menunjukkan bahwa regulasi yang lemah menjadi salah satu penyebab utama sulitnya menangani kebocoran data, namun literatur lain lebih menyoroti peran edukasi pengguna dan teknologi keamanan sebagai solusi utama. Perbedaan ini mungkin disebabkan oleh perspektif disiplin ilmu yang berlainan, yakni hukum versus teknologi dan perilaku.

Metodologi Penelitian

Perbedaan hasil juga dapat berasal dari variasi metode penelitian, seperti penelitian kuantitatif dengan survei versus studi kualitatif dan analisis sentimen. Misalnya, analisis sentimen yang digunakan di Bangkit Indonesia (2025) memberikan perspektif berbeda dari penelitian berbasis wawancara mendalam atau studi kasus yang lebih fokus pada konteks tertentu.

Singkatnya, perbedaan tersebut dapat disebabkan oleh perbedaan ruang lingkup, metode, populasi, disiplin ilmu, dan fokus tematik antar studi. Namun, semua studi sepakat bahwa sosial engineering merupakan ancaman serius terhadap keamanan data pengguna media sosial di Indonesia yang tidak bisa diabaikan dan memerlukan pendekatan multidisipliner untuk mitigasi.

Hasil penelitian ini menunjukkan bahwa serangan sosial engineering di Indonesia, terutama yang dilakukan melalui teknik phishing, baiting, dan pretexting, telah menjadi salah satu penyebab utama kebocoran data pada pengguna media sosial. Teknik-teknik ini memanfaatkan celah psikologis pada pengguna, seperti rasa percaya diri yang berlebihan, ketidaktahuan, dan minimnya kewaspadaan terhadap ancaman siber. Sejalan dengan temuan Kristiyanto et al. (2024) dan Lesmana (2025), yang menekankan efektivitas teknik-teknik tersebut dalam mengeksploitasi kelemahan perilaku manusia, penelitian ini mengungkapkan bahwa faktor utama yang meningkatkan kerentanannya adalah kelalaian dan kesalahan manusia. Temuan ini juga konsisten dengan studi Yuswanita (2025), yang menunjukkan bahwa human error khususnya kurangnya pelatihan dan kesadaran merupakan faktor dominan yang memperbesar kemungkinan keberhasilan serangan sosial engineering.

Selanjutnya, analisis terhadap pola serangan mengungkapkan bahwa serangan berbasis psikologi, seperti phishing yang memanipulasi rasa urgensi dan kepercayaan, semakin sering digunakan oleh pelaku untuk mengecoh korban. Data yang dikumpulkan menunjukkan bahwa kebiasaan pengguna yang sering kali membagikan informasi pribadi secara berlebihan di media sosial serta kurangnya verifikasi terhadap kredibilitas pesan atau sumber menjadi titik lemah yang sering dieksploitasi oleh pelaku. Penelitian ini juga menyoroti temuan terkait penggunaan password yang lemah dan praktik keamanan yang tidak memadai sebagai faktor risiko utama dalam kebocoran data. Hal ini menggambarkan bagaimana teknik rekayasa sosial berkembang semakin canggih,

dengan serangan yang semakin memanfaatkan kecanggihan teknologi, seperti deepfake dan AI, untuk memanipulasi dan mengelabui korban (CSIRT Magelang, 2023).

Meskipun teknologi keamanan telah berkembang, penelitian ini menegaskan bahwa perlindungan teknis saja tidak cukup untuk menghadapi risiko sosial engineering. Pendekatan yang hanya mengandalkan sistem teknologi tanpa diimbangi dengan edukasi yang memadai terhadap pengguna, terutama yang berada di sektorsektor yang rentan seperti perbankan dan pemerintahan, terbukti tidak efektif. Hasil penelitian ini sejalan dengan temuan Putri & Prabowo (2025), yang mengungkapkan bahwa meskipun teknologi seperti autentikasi multi-faktor dan deteksi phishing otomatis penting, yang lebih mendesak adalah penguatan aspek manusia melalui program literasi digital dan pelatihan yang berkelanjutan. Hal ini juga sesuai dengan rekomendasi Tsauri (2025) yang menyarankan pembentukan "human firewall" melalui simulasi serangan dan pelatihan berulang guna meningkatkan kewaspadaan pengguna.

Selain itu, penelitian ini juga memperlihatkan adanya kesenjangan dalam pengelolaan risiko siber yang ada di Indonesia. Seperti yang diungkapkan oleh Safitri (2024) dan Ramadhani (2025), kapasitas sektor publik dan swasta dalam menanggulangi serangan sosial engineering masih sangat terbatas, baik dalam hal kesiapan teknologi maupun tingkat kesadaran penggunanya. Berdasarkan temuan ini, disarankan agar pemerintah, penyedia platform media sosial, serta lembaga pendidikan bekerja sama lebih erat untuk merancang kampanye kesadaran yang lebih terstruktur dan terintegrasi. Kolaborasi antar berbagai pihak ini diperlukan untuk menciptakan lingkungan digital yang lebih aman dan mengurangi risiko kebocoran data yang semakin meningkat. Penelitian ini juga memperkuat pentingnya pengembangan kebijakan yang lebih ketat dan implementasi teknologi yang adaptif untuk meningkatkan perlindungan terhadap data pribadi pengguna media sosial di Indonesia.

Secara keseluruhan, hasil penelitian ini memperlihatkan bahwa pendekatan mitigasi terhadap sosial engineering tidak hanya bergantung pada teknologi dan regulasi, tetapi juga pada peningkatan kesadaran dan literasi digital masyarakat. Penelitian ini mengisi gap riset yang ada dengan mengangkat konteks Indonesia sebagai fokus utama, serta memberikan kontribusi signifikan terhadap pemahaman mengenai bagaimana faktor manusia, teknologi, dan kebijakan dapat digabungkan untuk menciptakan perlindungan yang lebih efektif terhadap kebocoran data. Temuan ini juga memberikan rekomendasi strategis bagi pengembangan kebijakan nasional terkait literasi digital dan keamanan siber di Indonesia:

Conclusion

Kesimpulan penelitian ini menunjukkan bahwa social engineering memiliki pengaruh yang sangat signifikan terhadap terjadinya kebocoran data pada pengguna media sosial di Indonesia, karena teknik ini secara efektif memanfaatkan kelemahan psikologis dan perilaku pengguna. Berbagai pola serangan yang paling dominan ditemukan dalam penelitian ini adalah phishing, pretexting, dan baiting, yang dirancang untuk menipu, membangun kepercayaan semu, serta memancing pengguna agar secara sukarela memberikan informasi pribadi atau data sensitif. Selain itu, penelitian ini menegaskan bahwa faktor utama yang menyebabkan tingginya tingkat keberhasilan serangan tersebut adalah kerentanan perilaku pengguna, seperti rendahnya literasi digital, kurangnya kesadaran terhadap keamanan informasi, serta kebiasaan membagikan data pribadi tanpa mempertimbangkan risiko. Kondisi ini menunjukkan bahwa kebocoran data tidak hanya disebabkan oleh kelemahan teknis sistem, tetapi lebih dominan dipengaruhi oleh faktor manusia (human error) sebagai titik lemah utama dalam keamanan digital.

References

Ardika, N., Santoso, H., & Putri, R. (2025). Kasus kebocoran data pengguna layanan e-commerce di Indonesia. *Jurnal Hukum dan Teknologi*, 4(2), 101–115. https://journal.pubmedia.id/index.php/lawjustice/article/view/3601

Bangkit Indonesia. (2025a). Analisis sentimen pengguna media sosial terhadap kebocoran data di Indonesia. *Bangkit Indonesia Journal*, 3(1), 15–29. https://journal.sttindonesia.ac.id/bangkitindonesia/article/download/434/232/

Bangkit Indonesia. (2025b). Analisis sentimen pengguna X terhadap kebocoran data. *Bangkit Indonesia Journal*, 3(1), 50–65. https://journal.sttindonesia.ac.id/bangkitindonesia/article/download/434/232/

CSIRT Cirebon Kota. (2024). *Mengenal social engineering: Ancaman siber tersembunyi di Indonesia tahun 2025*. https://csirt.cirebonkota.go.id/posts/mengenal-social-engineeringancaman-siber-tersembunyi-di-indonesia-tahun-2025

CSIRT Magelang. (2023). *Ancaman social engineering AI: Deepfake dan phishing di era digital*. https://csirt.magelangkab.go.id/posts/ancamansocial-engineering-ai-deepfake

Kristiyanto, Y., Ismiyana, D., Palah, J. M., & Rachman, M. M. (2024). Dampak serangan social engineering studi kasus data breach di Indonesia. *Prosiding Manajerial dan Kewirausahaan VIII*. https://ejurnal.stieipwija.ac.id/index.php/prc/article/download/1280/pdf

Lesmana, R., Yuda, A., & Putra, H. (2025). Kebocoran data di media sosial: Analisis pola dan strategi pencegahannya. *Jurnal Socius*, 10(2), 113–130. https://ojs.daarulhuda.or.id/index.php/Socius/article/view/1354

Literaksi. (2025). Bahaya social engineering dalam sosial media: Implikasi dan tindakan preventif. *Jurnal Literaksi*, 7(3), 75–89. https://literaksi.ayasophia.org/index.php/jmp/article/download/199/66/561

Mankeu, A. (2024). Pengaruh social engineering dan cybercrime terhadap sistem keamanan informasi. *Jurnal Mankeu*, 5(1), 25–40. https://onlinejournal.unja.ac.id/mankeu/article/view/48161

Orbit Jurnal. (2024). Peran literasi cybersecurity untuk keamanan akun media sosial. *Orbit Jurnal*, 2(2), 30–45. https://inovanpublisher.org/index.php/orbit/article/download/80/77/626

Polri. (2023). *Laporan kejadian kebocoran data terkait social engineering di Indonesia*.

Putri, R., & Prabowo, F. (2025). Efektivitas pelatihan literasi keamanan digital dalam memitigasi social engineering. *Jurnal Pengabdian Teknologi*, 5(3), 120–134.

Senatib. (2025). Keamanan informasi pada media sosial Instagram: Studi kerentanan dan perlindungan. *Jurnal Senatib*, 3(4), 200–218. https://www.ojs.udb.ac.id/Senatib/article/download/4612/3080

Syahril, S., Andika, L., & Ramdani, F. (2024). Studi kasus kebocoran data nasional pada tahun 2024. *Jurnal Desentralisasi*, 6(1), 72–84. https://ejournal.appihi.or.id/index.php/Desentralisasi/article/download/653/788/3524

Tomasoa, Y. R. (2024). Perlindungan hukum terhadap kebocoran data pribadi pada pengguna media sosial. *Jurnal Hukum dan Masyarakat*, 2(1), 54–67. https://fhukum.unpatti.ac.id/jurnal/pamali/article/view/1363

Universitas Islam Indonesia. (2025). Analisis kesadaran cybersecurity pada pengguna media sosial. *Jurnal UII*, 10(1), 100–115. https://journal.uii.ac.id/AUTOMATA/article/download/15426/10219/38997

Wicarana, T. (2025a). Analisa kasus kebocoran data pada bank Indonesia dalam sistem perbankan. *JMIA*, 1(6), 450–463. https://ejurnal.kampusakademik.co.id/index.php/jmia/article/download/3267/2976/13339

Wicarana, T. (2025b). Kasus kebocoran data di sektor perbankan: Vishing dan smishing sebagai modus social engineering. *JMIA*, 1(6), 450–463. https://ejurnal.kampusakademik.co.id/index.php/jmia/article/download/3267/2976/13339