Jurnal Multidisiplin Teknik, Sains, Pendidikan dan Teknologi

E-ISSN: 3064-6103
Volume 2, **Number** 2, Juli 2025
https://doi.org/10.62671/suliwa.v2i2.67

VISHING SEBAGAI ANCAMAN REKAYASA SOSIAL: ANALISIS TEKNIK, DAMPAK, DAN UPAYA PERLINDUNGAN PENGGUNA

Ist'na Rizqi Alamsyah[1], Arief Rahman Yusuf[2]
[1]Prodi Sistem Informasi, Universitas Terbuka,
[2]Prodi Teknik Informatika – Universitas Muhammadiyah Ponorogo
[1]i.rizqialamsyah@gmail.com , [2]yusuf@umpo.ac.id

ABSTRACT

Di era digital yang semakin maju, ancaman terhadap sistem informasi tidak hanya berasal dari aspek teknis, tetapi juga dari sisi manusia yang rentan terhadap manipulasi psikologis. Salah satu bentuk serangan yang mengeksploitasi kerentanan ini adalah voice phishing atau vishing, yaitu serangan rekayasa sosial yang memanfaatkan media suara untuk mengelabui korban agar menyerahkan informasi sensitif. Kejahatan ini semakin marak seiring meningkatnya ketergantungan masyarakat terhadap teknologi komunikasi. Penelitian ini bertujuan untuk menganalisis teknik-teknik yang digunakan dalam vishing, dampak yang ditimbulkan terhadap pengguna, serta strategi perlindungan yang dapat diterapkan. Dengan menggunakan pendekatan kualitatif melalui metode studi literatur, penelitian ini mengkaji 22 sumber pustaka yang terdiri atas artikel ilmiah, buku, dan modul edukasi terkini yang relevan dengan topik vishing dan rekayasa sosial. Hasil kajian menunjukkan bahwa keberhasilan vishing sangat bergantung pada aspek psikologis korban, seperti rasa percaya, tekanan waktu, dan kepanikan. Di samping itu, keterbatasan literasi digital juga menjadi faktor utama yang meningkatkan kerentanan masyarakat. Penelitian ini merekomendasikan pendekatan edukatif berbasis komunitas dan peningkatan kesadaran digital sebagai strategi utama pencegahan. Kajian ini diharapkan dapat memberikan kontribusi nyata dalam memperkuat perlindungan pengguna terhadap ancaman rekayasa sosial berbasis suara.

Kata Kunci/ Keywords:
Keamanan Informasi, Kejahatan Siber, Phishing , Rekayasa Sosial, Voice Phishing

PENDAHULUAN

Di era digital yang semakin maju, ancaman terhadap sistem informasi tidak hanya berasal dari aspek teknis seperti malware atau eksploitasi jaringan, tetapi juga dari sisi manusia yang lebih rentan terhadap manipulasi psikologis. Salah satu bentuk serangan yang mengeksploitasi kerentanan ini adalah vishing (voice phishing), yakni teknik penipuan berbasis suara melalui komunikasi telepon untuk mengecoh korban agar menyerahkan informasi sensitif seperti kata sandi, data perbankan, atau kredensial sistem organisasi (Agustina, 2025; Hanafi, 2022; John, 2024; Rahmawati et al., 2024; Salahdine & Kaabouch, 2019). Berbeda dari phishing berbasis teks, vishing mengandalkan kekuatan persuasi vokal seperti intonasi, nada suara, dan emosi dalam skenario yang tampak sah (Hadnagy, 2014; I Gede Putu Krisna Juliharta et al., 2024; Khadka et al., 2023; Nyassi et al., 2024; Salahdine & Kaabouch, 2019).

Dengan memanfaatkan teknologi seperti spoofing nomor telepon, dan penggunaan AI generatif yang dapat menciptakan AI voice synthesis dan automated scripts, serangan vishing kini bersifat otomatis, sangat terpersonalisasi, dan memiliki efektivitas tinggi (Toapanta et al., 2024; Wang et al., 2021). Kondisi ini diperparah oleh rendahnya literasi digital di kalangan masyarakat Indonesia, yang cenderung menganggap komunikasi suara sebagai bentuk komunikasi yang sukar dipalsukan (Rahmawati et al., 2021; Teteki et al., 2023).

Penelitian mengenai social engineering sebagai fondasi vishing telah dilakukan sejak dekade 1980-an. (Wang et al., 2021) mencatat lebih dari 450 publikasi yang membahas teknik manipulasi psikologis dalam sistem keamanan informasi. (Salahdine & Kaabouch, 2019) melaporkan bahwa 84% serangan siber berakar pada rekayasa sosial. Di Indonesia (Rahmawati et al., 2024) melaporkan bahwa Kominfo mencatat 26.675 kasus vishing dalam satu kuartal. (Teteki et al., 2023) menunjukkan bahwa jurnalis, aktivis, dan pengguna awam merupakan kelompok paling rentan terhadap manipulasi vokal. Studi-studi seperti (Alshammari et al., 2025; Moegiono, 2020; Syed, 2021) telah mendokumentasikan teknik impersonasi, intimidasi, dan tekanan psikologis yang digunakan pelaku. Selain itu, (Febrika Ardy et al., 2024) mengamati pergeseran vishing ke ranah media sosial dan aplikasi suara. Meski demikian, (Hanafi, 2022; Hayati, 2020) menunjukkan bahwa sebagian besar pendekatan pertahanan digital masih bersifat umum dan belum secara spesifik membahas vishing.

Walaupun dokumentasi mengenai vishing telah berkembang, masih terdapat celah besar dalam pemahaman publik terhadap cara mengenali dan menghindarinya. Seperti dicatat oleh (Schmitt & Flechais, 2024; Toapanta et al., 2024), teknologi *voice cloning* memperumit deteksi karena suara palsu nyaris tidak terbedakan dari suara asli. Bahkan, dalam studi (Figueiredo et al., 2024) sebanyak 33% responden tetap membocorkan data meskipun telah diperingatkan.

Jurnal Multidisiplin Teknik, Sains, Pendidikan dan Teknologi

E-ISSN: 3064-6103
Volume 2, **Number** 2, Juli 2025
https://doi.org/10.62671/suliwa.v2i2.67

Di sisi lain, solusi yang ditawarkan masih terbatas. (John, 2024) m menekankan pelatihan sebagai mekanisme utama perlindungan, namun pendekatan ini belum mencakup serangan berbasis AI. (Hanafi, 2022; I Gede Putu Krisna Juliharta et al., 2024) hanya mengedepankan pendidikan umum, tanpa pendekatan teknis yang memadai. Upaya deteksi otomatis seperti yang dikembangkan oleh (Chichwadia & Mpekoa, 2024) masih membutuhkan validasi lebih lanjut. (John, 2024) juga menyebutkan bahwa pelatihan yang tidak bersifat simulatif gagal membentuk kesadaran perilaku jangka panjang.

Selain aspek teknis dan psikologis, dimensi hukum juga menjadi perhatian. Menurut (Saputra Gulo et al., 2020), Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) belum secara eksplisit mengatur bentuk kejahatan rekayasa sosial digital seperti phishing dan vishing. Kekosongan norma dalam Pasal 28, 35, dan 45A menyebabkan ketidakjelasan dalam penegakan hukum terhadap pelaku. Mereka menekankan pentingnya reformulasi kebijakan hukum pidana dengan memasukkan unsur penipuan digital secara eksplisit agar sejalan dengan dinamika teknologi. Hal serupa disuarakan oleh (I Gede Putu Krisna Juliharta et al., 2024), yang menyarankan penguatan kerangka hukum dan perlindungan data pribadi.

Penelitian ini menyatukan temuan-temuan dari studi sebelumnya dalam satu kerangka terpadu dengan pendekatan lintas-disiplin. Kontribusi utama terletak pada penggabungan perspektif teoritis seperti dalam catatan (Hadnagy, 2014), teknis dalam catatan (Toapanta et al., 2024), edukatif dalam catatan (Rahmawati et al., 2021), dimensi yuridis/hukum dalam catatan (Saputra Gulo et al., 2020) dan regulative dalam catatan (Schmitt & Flechais, 2024) untuk membangun pemahaman komprehensif terhadap ancaman vishing modern. Di samping itu, ditambahkan pula aspek hukum nasional berdasarkan analisis Gulo, Lasmadi, dan Nawawi (2020), yang menekankan perlunya reformulasi UU ITE karena kekosongan norma terhadap jenis kejahatan rekayasa sosial seperti vishing.

Penelitian ini bertujuan untuk menganalisis teknik, dampak, profil target, serta strategi perlindungan terhadap serangan vishing, khususnya yang berbasis AI dan rekayasa suara. Dengan menelaah 22 sumber literatur akademik dan praktis, penelitian ini menyatukan pendekatan teoritis, teknis, edukatif, psikologis, serta regulatif dalam satu kerangka terpadu.

Berbeda dari studi sebelumnya yang cenderung terfokus pada satu dimensi, penelitian ini menghadirkan pendekatan integratif yang menempatkan vishing sebagai persoalan multidimensi. Dengan demikian, hasil penelitian ini diharapkan dapat berkontribusi strategis dalam penyusunan kebijakan keamanan informasi yang adaptif dan kontekstual terhadap perkembangan teknologi komunikasi dan AI.

METODE

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur (library research) sebagai dasar analisis. Pemilihan metode ini didasarkan pada karakteristik vishing sebagai bentuk rekayasa sosial yang melibatkan dimensi psikologis, sosial, teknis, dan hukum, sehingga lebih tepat dianalisis melalui pemahaman mendalam daripada pendekatan kuantitatif berbasis pengukuran statistik. Selain itu, keterbatasan akses terhadap data primer seperti rekaman percakapan vishing yang autentik serta pertimbangan etis dalam memperoleh data tersebut menjadikan studi literatur sebagai metode yang paling relevan dan aman secara metodologis.

Tujuan dari penelitian ini bukan untuk mengukur frekuensi atau prevalensi serangan, melainkan untuk mengonstruksi pemahaman konseptual mengenai teknik dan dampak vishing dalam konteks sistem informasi, serta mengevaluasi efektivitas dan keterbatasan pendekatan penanggulangan yang telah ada dalam literatur.

Sumber literatur yang dikaji terdiri dari 22 dokumen ilmiah dan praktis yang dipilih secara purposif berdasarkan relevansi terhadap topik vishing, rekayasa sosial, keamanan siber, serta integrasi teknologi kecerdasan buatan. Referensi tersebut mencakup jurnal ilmiah, buku akademik, laporan teknis, serta modul pelatihan yang mewakili pendekatan konseptual, praktis, dan eksperimental.

Kriteria seleksi literatur meliputi:

1. keterkaitan langsung dengan isu vishing atau social engineering,
2. keberagaman perspektif (teknis, psikologis, edukatif, hukum),
3. kemutakhiran publikasi,
4. relevansi konteks terhadap situasi di Indonesia, dan
5. keberadaan data empiris atau temuan analitis yang dapat mendukung sintesis komparatif.

Proses pengumpulan data dilakukan melalui ekstraksi isi dari masing-masing referensi, yang difokuskan pada lima aspek utama, yaitu:

1. Teknik vishing yang digunakan,
2. Dampak terhadap individu dan organisasi,

Jurnal Multidisiplin Teknik, Sains, Pendidikan dan Teknologi

E-ISSN: 3064-6103
Volume 2, **Number** 2, Juli 2025
https://doi.org/10.62671/suliwa.v2i2.67

3. Karakteristik target yang rentan,
4. Strategi perlindungan dan deteksi,
5. Kerangka regulasi atau kebijakan yang relevan.

Data dianalisis menggunakan analisis isi tematik, yaitu dengan mengelompokkan informasi berdasarkan lima fokus tersebut. Hasilnya kemudian disusun dalam bentuk tabel matriks perbandingan yang menampilkan fokus, kelebihan, kelemahan, serta posisi kontribusi dari masing-masing referensi terhadap arah penelitian ini. Teknik ini memungkinkan peneliti mengidentifikasi pola umum, kesenjangan antarstudi, serta kontribusi sintesis yang khas dari penelitian ini.

Sebagai instrumen bantu, digunakan coding manual terhadap kutipan dan temuan utama dari masing-masing dokumen untuk memastikan konsistensi proses kategorisasi dan sintesis. Tidak dilakukan pengumpulan data primer seperti survei atau wawancara karena fokus penelitian sepenuhnya berada pada analisis konseptual dan komparatif atas literatur yang tersedia.

Studi literatur ini dipilih karena dinilai paling tepat untuk mengkaji fenomena kompleks dan multidimensi seperti vishing, terutama di tengah kemajuan teknologi komunikasi dan kecerdasan buatan yang memperluas lanskap serangan berbasis rekayasa sosial suara.

HASIL DAN PEMBAHASAN

Penelitian ini bertujuan untuk menjawab tantangan konseptual dan praktis terkait vishing sebagaimana telah diuraikan dalam Pendahuluan, yaitu dengan mengkaji teknik, dampak, karakteristik target, serta strategi perlindungan dan kebijakan yang relevan. Pendekatan yang digunakan adalah studi literatur terhadap 22 referensi ilmiah dan praktis yang telah diklasifikasikan melalui proses coding manual berdasarkan lima fokus tematik.

Hasil sintesis menunjukkan bahwa teknik vishing telah berkembang dari metode klasik ke serangan berbasis AI. (Moegiono, 2020; Salahdine & Kaabouch, 2019; Syed, 2021) menggambarkan teknik klasik seperti impersonasi dan tekanan psikologis. Sementara itu, (Nyassi et al., 2024; Toapanta et al., 2024; Wang et al., 2021) menjelaskan penggunaan voice cloning, scripting otomatis, serta deteksi emosi yang mengindikasikan kemajuan pesat dalam pola serangan.

Dampak vishing tidak hanya bersifat material, tetapi juga psikologis dan sosial. (Figueiredo et al., 2024) mengungkapkan bahwa sepertiga korban tetap membocorkan informasi meskipun diberi peringatan. (Nyassi et al., 2024) menambahkan bahwa serangan ini berdampak sistemik terhadap organisasi. Temuan ini menunjukkan bahwa serangan vishing bukan hanya ancaman personal, tetapi juga terhadap keberlangsungan sistem informasi.

Karakteristik korban yang rentan menjadi faktor penting. (I Gede Putu Krisna Juliharta et al., 2024; Teteki et al., 2023) menyoroti bahwa jurnalis, aktivis, dan pengguna awam dengan literasi digital rendah adalah kelompok paling berisiko. Hal ini menggarisbawahi pentingnya pelatihan yang disesuaikan dengan konteks sosial dan teknologi.

Strategi perlindungan yang ada seperti pelatihan tradisional dinilai belum memadai untuk menghadapi serangan vishing berbasis AI. (John, 2024) menyarankan pelatihan, namun tanpa pendekatan berbasis simulasi dan teknologi mutakhir. Pendekatan berbasis machine learning dari (Chichwadia & Mpekoa, 2024; Nyassi et al., 2024) menjanjikan, namun masih memerlukan validasi di dunia nyata.

Secara regulatif, (Saputra Gulo et al., 2020) menunjukkan bahwa UU ITE di Indonesia belum mengatur vishing secara eksplisit, menciptakan kekosongan norma. (I Gede Putu Krisna Juliharta et al., 2024; Schmitt & Flechais, 2024) menekankan perlunya pembaruan kebijakan untuk mengatur penyalahgunaan voice cloning dan teknologi generatif lainnya. sintesis

Dari sintesis diatas, berikut ini adalah tabel perbandingan dari 22 referensi utama yang digunakan dalam penelitian ini antara fokus penelitian, kelebihan, kekurangan, serta posisi kontribusi penelitian ini:

Tabel 1. Perbandingan penelitian terdahulu

No	Penulis	Fokus Penelitian	Kelebihan	Kelemahan	Posisi Penelitian Ini
1	Salahdine & Kaabouch (2019)	Peran social engineering dalam serangan siber	Menyediakan klasifikasi teknik manipulasi	Belum membahas AI voice-based vishing	Melanjutkan dan memperluas cakupan dengan menyertakan teknik AI voice cloning
2	Moegiono (2020)	Studi teknik manipulasi klasik pada rekayasa social	Memberikan contoh konkret	Tidak menyoroti teknologi	Melengkapi dengan aspek otomatisasi dan AI
3	Syed (2021)	Teknik intimidasi dan impersonasi	Mengungkap dinamika psikologis korban	Kurang analisis sistematis	Memperluasnya melalui integrasi aspek sistemik dan hukum

Jurnal Multidisiplin Teknik, Sains, Pendidikan dan Teknologi

E-ISSN: 3064-6103
Volume 2, **Number** 2, Juli 2025
https://doi.org/10.62671/suliwa.v2i2.67

4	Toapanta et al. (2024)	Otomatisasi vishing menggunakan AI	Memberikan deskripsi teknis mutakhir	Minim pembahasan dampak social	Menggabungkan perspektif teknis dengan dampak psikososial
5	Wang et al. (2021)	Survei publikasi terkait rekayasa social	Data bibliometrik kuat	Tidak fokus pada vishing	Menyempurnakan dengan fokus khusus pada vishing berbasis suara
6	Hadnagy (2014)	Psikologi social engineering	Teori manipulasi vokal mendalam	Belum menyentuh konteks digital AI	Mengontekstualisasikan teori Hadnagy dalam dunia digital modern
7	John (2024)	Efektivitas pelatihan antiphishing	Penekanan pada edukasi	Tidak membahas AI dan vishing	Mengkritisi dan memperluas efektivitas pelatihan dengan mempertimbangkan teknologi
8	Chichwadia & Mpekoa (2024)	Deteksi otomatis panggilan scam	Penggunaan ML & klasifikasi akustik	Belum diuji lapangan	Mengaitkan potensi teknis dengan kebutuhan kebijakan local
9	Figueiredo et al. (2024	Uji perilaku korban terhadap vishing	Desain eksperimental kuat	Skala terbatas	Menyintesis temuan perilaku dengan kerangka edukatif dan regulative
10	Teteki et al. (2023)	Target vishing di negara berkembang	Konteks lokal & kelompok rentan	Minim solusi praktis	Menanggapi dengan solusi berbasis pendidikan dan kebijakan local
11	I Gede Putu Krisna Juliharta et al. (2024)	Regulasi hukum dan data pribadi	Komprehensif dalam kerangka hukum	Kurang teknis	Mengintegrasikan kerangka hukum dengan aspek teknis dan psikologis
12	Schmitt & Flechais (2024)	Ancaman voice cloning dan kebijakan	Analisis kebijakan digital Eropa	Kurang relevan untuk Indonesia	Mengadaptasi dan menyesuaikan kerangka tersebut untuk konteks Indonesia
13	Saputra Gulo et al. (2020)	Kelemahan hukum dalam UU ITE	Penekanan reformasi pasal-pasal	Tidak mencakup teknologi AI	Melanjutkan rekomendasinya dengan aspek rekayasa sosial suara modern
14	Rahmawati et al. (2021)	Literasi digital dan dampaknya	Fokus pada konteks Indonesia	Tidak menyasar vishing secara spesifik	Menyambungkan literasi digital dengan kerentanan terhadap vishing
15	Hayati (2020)	Sosialisasi pencegahan umum	Praktis dan aplikatif	Terlalu umum, tanpa konteks AI	Menyempurnakan pendekatan dengan simulasi vishing berbasis AI
16	Hanafi (2022)	Edukasi anti rekayasa social	Memberi rekomendasi pelatihan	Tidak fokus vishing	Mengintegrasikan rekomendasi edukatif dengan analisis teknologis
17	Alshammari et al. (2025)	Teknik impersonasi pada telekomunikasi	Analisis eksplisit teknik intimidasi	Tidak mencakup AI atau kebijakan	Memperkaya dengan dimensi AI dan legal
18	Khadka et al. (2023)	Efek persuasi dalam suara	Bukti eksperimental kuat	Tidak membahas strategi proteksi	Menambahkan strategi pelindung dan pelatihan yang responsif
19	Febrika Ardy et al. (2024)	Vishing di media social	Fokus baru pada platform social	Minim analisis psikologis	Menyatukan teknik vishing daring dengan kerangka edukatif dan hukum
20	Nyassi et al. (2024)	AI dan ancaman organisasi	Pendekatan sistemik	Kurang fokus pada individu	Menyelaraskan risiko organisasi dan individu secara simultan
21	Agustina (2025)	Laporan investigasi vishing	Kontekstual lokal & empiris	Tidak teoritis	Menyintesis data lapangan dengan kerangka teoretis dan regulatif
22	Rahmawati et al. (2024)	Statistik nasional kasus vishing	Bukti aktual di Indonesia	Tidak menjelaskan akar penyebab	Melengkapi dengan analisis psikologis dan strategi protektif

Jurnal Multidisiplin Teknik, Sains, Pendidikan dan Teknologi

E-ISSN: 3064-6103
Volume 2, **Number** 2, Juli 2025
https://doi.org/10.62671/suliwa.v2i2.67

Hasil studi ini menunjukkan bahwa vishing telah berkembang dari metode manipulatif berbasis suara ke teknik yang menggunakan AI, menjadikannya lebih sulit dideteksi dan dicegah. Sumber-sumber seperti Digital Deception dan AI-Driven Vishing Attacks mengindikasikan perlunya pendekatan baru yang menyatukan teknologi dan kesadaran pengguna. Penelitian ini berada pada posisi strategis untuk menyatukan ragam pendekatan tersebut menjadi fondasi pemahaman baru terhadap ancaman vishing berbasis AI. Langkah selanjutnya adalah mengintegrasikan model pembelajaran mesin, pelatihan berbasis skenario, serta pendekatan hukum dan etika untuk menghasilkan strategi perlindungan yang adaptif dan berkelanjutan.

Secara keseluruhan, sintesis ini menunjukkan bahwa tidak ada satu pendekatan tunggal yang cukup untuk menjelaskan dan mengatasi ancaman vishing. Penelitian ini mencoba menjembatani berbagai sudut pandang tersebut, mulai dari aspek teknis, edukatif, psikologis, hingga hukum, untuk memberikan gambaran yang lebih menyeluruh tentang bagaimana vishing berkembang dan bagaimana pengguna dapat lebih terlindungi.

SIMPULAN DAN SARAN

Vishing merupakan salah satu bentuk ancaman rekayasa sosial yang berkembang pesat, baik dari segi teknik maupun jangkauan serangannya. Penelitian ini menemukan bahwa teknik vishing telah berevolusi dari model tradisional berbasis telepon ke bentuk serangan canggih berbasis AI seperti voice cloning dan automasi melalui sistem kecerdasan buatan. Dampak yang ditimbulkan pun semakin luas, tidak hanya bersifat finansial, tetapi juga menyasar aspek psikologis, sosial, serta kepercayaan publik terhadap teknologi komunikasi. Hal ini diperparah dengan tingginya kerentanan kelompok pengguna awam yang belum dibekali dengan literasi keamanan digital yang memadai.

Hasil studi literatur menunjukkan bahwa sebagian besar penelitian sebelumnya belum mengintegrasikan pendekatan multidisipliner dalam merespons eskalasi vishing. Oleh karena itu, penelitian ini menutup celah tersebut dengan menyatukan perspektif teknis, psikologis, edukatif, serta kebijakan dalam satu kerangka analisis terpadu. Diharapkan hasil ini dapat memberikan kontribusi nyata dalam pengembangan strategi pertahanan terhadap vishing, baik di tingkat individu, organisasi, maupun kebijakan publik.

Sebagai saran, perlindungan terhadap vishing memerlukan pendekatan kolaboratif antara pemerintah, institusi pendidikan, dan sektor teknologi. Literasi digital harus diperkuat melalui pelatihan berbasis simulasi, sementara inovasi teknologi deteksi suara dan kecerdasan buatan perlu didorong melalui regulasi dan riset berkelanjutan. Selain itu, penting untuk membangun budaya sadar keamanan informasi sebagai bagian integral dari sistem informasi modern.

REFERENSI

Agustina, D. (2025). *Phishing : Mengapa Ancaman Ini Terus Mengintai di Era Digital?* https://www.researchgate.net/publication/390299981

Alshammari, S. S., Soh, B., & Li, A. (2025). Understanding Social Engineering Victimisation on Social Networking Sites: A Comprehensive Review of Factors Influencing User Susceptibility to Cyber-Attacks. In *Information (Switzerland)* (Vol. 16, Issue 2). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/info16020153

Chichwadia, A. E., & Mpekoa, N. (2024). Detecting Smishing and Vishing Attacks using Machine Learning. *International Journal of Intelligent Computing Research*, *15*(1), 1234–1241. https://doi.org/10.20533/ijicr.2042.4655.2024.0151

Febrika Ardy, L. A., Istiqomah, I., Ezer, A. E., & Neyman, S. N. (2024). Phishing di Era Media Sosial: Identifikasi dan Pencegahan Ancaman di Platform Sosial. *Journal of Internet and Software Engineering*, *1*(4), 11. https://doi.org/10.47134/pjise.v1i4.2753

Figueiredo, J., Carvalho, A., Castro, D., Gonçalves, D., & Santos, N. (2024). *On the Feasibility of Fully AI-automated Vishing Attacks*. http://arxiv.org/abs/2409.13793

Hadnagy, C. (2014). *Social Engineering: The Science of Human Hacking*. https://archive.org/details/SocialEngineeringTheScienceOfHumanHacking2ndEdition

Hanafi. (2022). *DASAR CYBER SECURITY DAN FORENSIC*. https://eprints.amikom.ac.id/id/eprint/18330/1/Dasar%20Cyber%20Security.pdf

Hayati, N. (2020). *Buku Ajar: Sistem Keamanan*. https://tif.unusida.ac.id/wp-content/uploads/2022/11/BUKU-AJAR-Sistem-Keamanan.pdf

I Gede Putu Krisna Juliharta, Adrian, & Ayu Pradnyandari Dananjaya Erawan. (2024). *buku keamanan siber esensi keamanan sistem informasi*. EUREKA MEDIA AKSARA. https://repository.penerbiteureka.com/media/publications/569697-buku-keamanan-siber-esensi-keamanan-sist-46e50bfd.pdf

John, J. (2024). *DEFENDING AGAINST PHISHING ATTACKS: EFFECTIVE PREVENTION AND RESPONSE*

Jurnal Multidisiplin Teknik, Sains, Pendidikan dan Teknologi

E-ISSN: 3064-6103
Volume 2, **Number** 2, Juli 2025
https://doi.org/10.62671/suliwa.v2i2.67

TACTICS. https://www.researchgate.net/publication/387105573

Khadka, K., Ullah, A. B., Ma, W., Marroquin, E. M., & Alem, Y. (2023). *A Survey on the Principles of Persuasion as a Social Engineering Strategy in Phishing*. https://arxiv.org/pdf/2412.18488

Moegiono, R. (2020). *MODUS OPERANDI PHISHING*. https://medantalk.com/modus-penipuan-pesan-

Nyassi, V. S., Tchakounté, F., Yenké, B. O., Danga, D. E. H., Ngoran, M. D., & Fendji, J. L. K. E. (2024). Emoti-Shing: Detecting Vishing Attacks by Learning Emotion Dynamics through Hidden Markov Models. *Journal of Intelligent Learning Systems and Applications*, *16*(03), 274–315. https://doi.org/10.4236/jilsa.2024.163015

Rahmawati, D., Viendyasari, M., Ameliah, R., Negara, R. A., Rahmawati, I., & Lumakto, G. (2021). *MODUL KEAMANAN DIGITAL*. https://infohoax.bondowosokab.go.id/uploads/pdf/Modul%20Keamanan%20Digital%20Revisi.pdf

Rahmawati, D., Viendyasari, M., Giri Lumakto, Rienzy Kholifatur, Anindhita, W., Rizki Ameliah, Syavia Bachna, & Adienda, A. (2024). *WASPADA KEJAHATAN PHISHING ATTACK!* https://repository-penerbitlitnus.co.id/id/eprint/248/1/WASPADA%20KEJAHATAN%20PHISHING%20ATTACK!.pdf

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. In *Future Internet* (Vol. 11, Issue 4). MDPI AG. https://doi.org/10.3390/FI11040089

Saputra Gulo, A., Lasmadi, S., & Nawawi, K. (2020). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal Of Criminal*, *1*, 2020. https://online-journal.unja.ac.id/Pampas/article/view/9574/6399

Schmitt, M., & Flechais, I. (2024). *Digital Deception: Generative Artificial Intelligence in Social Engineering and Phishing*. https://arxiv.org/pdf/2310.13715

Syed, A. M. (2021). *Social engineering: Concepts, Techniques and Security Countermeasures*. https://www.scamwatch.gov.au/get-help/real-

Teteki, A., Muryanto, B., & Adikara, G. (2023). *HANDBOOK DIGITAL SAFETY*. https://ykpindonesia.org/wp-content/uploads/2023/11/BUKU-DIGITAL-SAFETY-2.pdf

Toapanta, F., Rivadeneira, B., Tipantuña, C., & Guamán, D. (2024). AI-Driven Vishing Attacks: A Practical Approach †. *Engineering Proceedings*, *77*(1). https://doi.org/10.3390/engproc2024077015

Wang, Z., Zhu, H., Liu, P., & Sun, L. (2021). Social engineering in cybersecurity: a domain ontology and knowledge graph application examples. *Cybersecurity*, *4*(1). https://doi.org/10.1186/s42400-021-00094-6