

Memetakan Konsep Dan Faktor-Faktor Psikologis Yang Mempengaruhi Kerentanan Individu Sebagai Korban Phishing: A Scoping Review

Mapping the Concepts and Psychological Factors Influencing Individual Vulnerability to Phishing: A Scoping Review

Rafif Salsabila¹, Alfiza Fakhriya Haq², Dian Putriana³

Fakultas Psikologi, Universitas Muhammadiyah Kalimantan Timur^{1 2}

e-mail: raffsalsabila033@gmail.com¹ afh467@umkt.ac.id² dp958@umkt.ac.id³

ABSTRAK

Serangan phishing meningkat dan menyebabkan kerugian yang diproyeksikan mencapai \$10,5 triliun pada 2025 dan \$15,63 triliun pada 2029, dengan biaya pemulihan rata-rata mencapai \$4,88 juta per perusahaan. Di Indonesia sendiri laporan IDADX mencatatkan 26.675 serangan phishing pada Q1 2023 yang menargetkan domain seperti .id, biz.id, dan my.id. dengan kasus seperti penipuan pada situs BCA dan DJKN yang pernah terjadi di Indonesia. Tinjauan ini bertujuan untuk memetakan konsep dan faktor-faktor psikologis yang mempengaruhi kerentanan individu sebagai korban kejahatan phishing. Metode yang digunakan adalah scoping review untuk memetakan konsep dan faktor psikologis yang mempengaruhi individu sebagai korban dari kejahatan phishing yang dijadikan panduan dalam studi ini. Peneliti memasukkan studi kualitatif dan kuantitatif yang diterbitkan dari tahun 2016 hingga 2025 dalam berbagai data base seperti ScienceDirect, Pubmed, dan Google Scholar. Hasil penelitian memetakan faktor psikologis yang terjadi pada korban kejahatan phishing seperti faktor kognitif, faktor emosional, dan faktor sosial teknologi yang saling terkait dan membentuk respons individu terhadap ancaman phishing. Penelitian ini menyoroti peran dari faktor psikologis pada kerentanan phishing dengan implikasinya untuk penelitian selanjutnya dan pengembangan pelatihan Cyber Awareness. Diperlukannya penelitian lebih lanjut untuk melihat faktor atau aspek-aspek apa saja yang muncul pada korban kejahatan phishing dan penelitian longitudinal di Indonesia guna mendapatkan strategi pencegahan yang efektif sesuai sosial-kultur Indonesia.

Kata kunci :

Cyber; Kejahatan Cyber; Korban Phishing; Phishing; Psikologi Forensik

ABSTRACT

Phishing attacks are on the rise and are projected to cause losses of \$10.5 trillion by 2025 and \$15.63 trillion by 2029, with average recovery costs reaching \$4.88 million per company. In Indonesia alone, an IDADX report recorded 26,675 phishing attacks in Q1 2023 targeting domains such as .id, biz.id, and my.id, with cases including scams on the BCA and DJKN websites that have occurred in Indonesia. This review aims to map the concepts and psychological factors influencing an individual's vulnerability as a victim of phishing crimes. The method used is a scoping review to map the concepts and psychological factors influencing individuals as victims of phishing crimes, which serves as a guide for this study. The researcher included qualitative and quantitative studies published from 2016 to 2025 in various databases such as ScienceDirect, PubMed, and Google Scholar. The results of the study mapped the psychological factors experienced by victims of phishing crimes, such as cognitive factors, emotional factors, and socio-technological factors, which are interrelated and shape individuals' responses to phishing threats. This study highlights the role of psychological factors in phishing vulnerability, with implications for future research and the development of cyber awareness training. Further research is needed to identify the factors or aspects that affect victims of phishing, as well as longitudinal studies in Indonesia to develop effective prevention strategies tailored to the country's sociocultural context.

Keywords :

Cyber; Cybercrime; Forensic Psychology; Phishing; Phishing Victims

Copyright © 2025 JPFI: Jurnal Psikologi Forensik Indonesia



This is an open article under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License

PENDAHULUAN

Kejahatan di dunia cyber, khususnya serangan phishing, terus meningkat dan menimbulkan kerugian. Berdasarkan situs vikingcloud.com kerugian mencapai \$10,5 triliun pada tahun 2025 dan diprediksi akan terus meningkat hingga menyentuh \$15,63 triliun pada tahun 2029. Selain itu juga biaya yang harus dikeluarkan sebuah perusahaan untuk memperbaiki diri setelah serangan phishing rata-rata di angka \$4,88 juta. Data dari situs getastra.com juga memaparkan hampir 1,2% dari total email yang dikirim setiap harinya adalah email phishing yang berbahaya atau sekitar 3,4 miliar email phishing yang tersebar setiap harinya. Selain itu diperkirakan lebih dari 33 juta data menjadi sasaran pemerasan melalui serangan ransomware dan phishing pada tahun 2023, dengan frekuensi serangan setiap 11 detik. Merek-merek ternama seperti Amazon dan Google menjadi target tiruan terbanyak sebesar 13%, diikuti oleh Facebook dan WhatsApp dengan 9%, serta Netflix dan Apple sebesar 2%, yang menunjukkan bagaimana pelaku kejahatan di dunia cyber memanfaatkan nama besar untuk menjebak atau menipu korbannya.

Selain itu, laporan tahunan dari Internet Crime Complaint Center (IC3) pada tahun 2024 menunjukkan phishing dan spoofing menjadi jenis kejahatan siber yang paling banyak dilaporkan sebanyak 193.407 kasus. Sedangkan jenis kejahatan cyber lainnya seperti pemerasan dilaporkan sebanyak 86.415 kasus. Federal Bureau of Investigation (FBI) juga mengungkapkan lebih dari 42.000 nama domain unik yang terhubung ke LabHost, salah satu platform phishing-as-a-service (PhaaS) terbesar yang berhasil ditutup pada April 2024. Domain itu digunakan untuk menipu korban dan didaftarkan mulai November 2021 hingga April 2024. Hal ini menunjukkan besarnya serangan phishing yang tidak hanya merugikan secara finansial tetapi juga mengancam keamanan data pribadi (cybernews.com). Pada laporan Global Cybersecurity Outlook 2025 juga mencatat pada tahun 2024 terjadi peningkatan dalam serangan phishing dan social engineering dengan 42% laporan. Phishing tetap menjadi faktor serangan cyber yang paling umum dan terus berkembang dengan kemajuan teknologi sehingga menjadi ancaman utama yang harus diwaspadai setiap individu.

Pada penelitiannya Malunsenge et al., (2022) terdapat sebuah kasus pada tahun 2001 yang menimpa Bank Central Asia (BCA), pada saat itu layanan internet banking sebagai bentuk

layanan elektronik dalam bidang perbankan baru mulai dijalankan oleh bank-bank di Indonesia. Pelaku membeli 6 domain mirip www.klikbca.com untuk menipu nasabah. Saat nasabah memasukkan user ID dan PIN di situs palsu tersebut sehingga data terekam dan tersimpan di komputer pelaku. Kasus ini menunjukkan kerentanan transaksi elektronik di Indonesia, terutama karena minimnya pemahaman masyarakat tentang kejahatan siber seperti phishing, yang mengandalkan tipu muslihat sehingga tidak semua orang dapat menyadarinya. berdasarkan dari situs detik.com bahwa seperti lembaga pemerintahan sebesar 68% sebagai target untuk serangan phishing disusul oleh e-commerce atau ritel sebesar 17% sebagai target dari serangan phishing.

Salah satu contoh berikutnya berdasarkan situs djkn.kemenkeu.go.id terdapat kasus pada situs lelang, pada saat itu muncul situs bernama lelanginternal.com yang mirip dengan situs resmi milik Direktorat Jenderal Kekayaan Negara (DJKN) yaitu lelang.go.id, hal ini dimanfaatkan oleh pelaku phishing dengan menggunakan nama kementerian keuangan untuk menipu korbannya. selanjutnya berdasarkan situs bpkn.go.id ada 5.579 serangan phishing yang terjadi di Indonesia pada kuartal II tahun 2022 dan meningkat sekitar sebesar 41,52% dari kuartal I tahun 2022 dari produk yang paling rentan seperti e-wallet, rekening bank, internet banking, mobile banking, hingga ATM Bank. dari sisi peraturan OJK terdapat POJK nomor 6/POJK.07/2022 yang berisi aturan tentang perlindungan konsumen dan masyarakat di sektor jasa keuangan. Selanjutnya berdasarkan laporan Indonesia Anti-Phishing Data Exchange (IDADX) total pengaduan serangan phishing di Indonesia Tercatat sebanyak 26.675 laporan pada periode kuartal I 2023. IDADX juga menyebutkan terdapat beberapa SLD (Second Level Domain) yang menjadi target serangan phishing pada Q1 2023, yakni id, biz.id, dan my.id. Sementara, total serangan phishing pada SLD id merupakan yang terbanyak sebesar 26.485 laporan.

Phishing merupakan bentuk serangan cyber yang di mana pelaku menyamar sebagai pihak terpercaya untuk mencuri informasi sensitive seperti kata sandi dan nomor kartu kredit dengan melalui email, SMS, atau situs web palsu, yang berpotensi menyebabkan kerugian finansial dan pencurian identitas bagi korban, sehingga memerlukan peningkatan kesadaran dan edukasi sebagai upaya pencegahannya (Dewanto et al., 2024). Perkembangan pesatnya

teknologi memang telah menciptakan dunia tanpa batas yang mengubah tatanan sosial, namun juga dimanfaatkan untuk kejahatan atau cybercrime (Lokapala et al., 2024). Berdasarkan penelitiannya (Oyadeyi et al., 2024) dampak finansial dari serangan cyber pada kasus phishing dan kebocoran data di kawasan APAC Persemakmuran, seperti serangan terhadap Departemen Pendidikan Tasmania yang membocorkan 30.000 dokumen pribadi siswa, insiden di Latitude Financial Australia yang memengaruhi 14 juta pelanggan, serta kebocoran lebih dari 14 juta data di Bangladesh melalui Kantor Pendaftaran umum dan semua bertujuan untuk memperoleh keuntungan finansial, mengganggu layanan vital, dan mengeksploitasi data pribadi seseorang. Bahkan dalam penelitiannya (Prawiyogi & Alwiyah, 2023) menunjukkan negara dengan tingkat penguasaan teknologi tinggi seperti Singapura tidak luput juga dari ancaman ini; Pada 2018, data kartu kredit 19.000 pelanggan Singapura bocor dan diperdagangkan secara ilegal (Tech Collective). Singapura dan Vietnam juga mengalami kebocoran data dari 410.000 pengguna Vietnam Airlines, sementara Malaysia kehilangan data ribuan pengguna Jobstreet.com akibat serangan hacker. Laporan Asia Pacific Risk Center menyatakan kerugian akibat ancaman siber mencapai US\$ 2,1 triliun pada 2019.

Pada penelitiannya Hanifah et al., (2025) yang menunjukkan dampak psikologis dan sosial yang dialami korban cybercrime menunjukkan betapa pentingnya Pembangunan Berkelanjutan (SDGs), kesehatan mental sebagai isu holistic, kegagalan dalam memenuhinya dapat berdampak pada konsekuensi sosial, pendidikan, dan ekonomi yang besar dalam jangka waktu panjang. Di sisi lain, kejahatan cyber juga memberikan tekanan karena tindakan pencurian identitas, penipuan tidak hanya menyebabkan kerugian finansial namun dapat berakibat kerusakan reputasi yang dapat memicu emosional negatif (Hapsari & Pambayun, 2023). Hal ini menunjukkan bahwa stigma sosial yang didapat korban kejahatan cyber dapat menghambat proses pemulihannya.

Negara-negara di Asia Tenggara sendiri menunjukkan kerentanan terhadap serangan cyber akibat digitalisasi ekonomi yang begitu cepat salah satunya inisiatif kota pintar dan Internet of Things (IoT) yang telah memperluas permukaan potensial cybercrime, oleh karena itu para peretas terus menyempurnakan metode mereka dengan memanfaatkan kelemahan sistem, terutama di negara-negara yang langkah keamanan cyber nya masih kurang berkembang (B. T. F. Lee et al., 2025). Di tingkat organisasi global, phishing menjadi ancaman yang menurut

laporan Proofpoint's 2024 State of the Phish dalam penelitiannya (Weinz et al., 2025) bahwa 4 dari 5 serangan paling umum berkaitan dengan phishing, termasuk lebih dari 66 juta serangan pencurian email bisnis setiap bulan pada 2023 yang dikaitkan dengan kemajuan AI generatif, sementara hanya 23% perusahaan yang memberikan edukasi tentang keamanan AI generatif dan hanya 53% yang melatih seluruh karyawannya untuk tidak menciptakan celah yang dapat dieksploitasi peretas. Upaya mitigasi seperti daftar blokir server-side, meskipun akurat dalam mengidentifikasi situs phishing dengan sedikit kesalahan, tetap juga memiliki keterbatasan karena keterlambatan pembaruan yang memungkinkan 75% korban mengakses halaman phishing sebelum diblokir, serta ketidakmampuannya terhadap serangan yang sangat ditargetkan seperti spear phishing (Pourmohamad et al., 2024). Oleh karena itu, paradigma keamanan cyber perlu bergeser dari "melindungi sistem" ke "melindungi pengguna atau pelanggan".

Oleh karena itu, pendekatan psikologi diperlukan untuk memungkinkan identifikasi kerentanan individu berdasarkan pola dan kebiasaan digital mereka. Pemetaan faktor-faktor psikologis ini menjadi dasar dalam merancang edukasi berbasis bukti yang dapat dimanfaatkan oleh peneliti selanjutnya. Penelitian ini bertujuan memetakan konsep dan faktor psikologis yang memengaruhi kerentanan individu terhadap serangan phishing melalui metode scoping review yang diperkenalkan oleh (Arksey & O'Malley, 2005). Kontribusi utama dari penelitian ini adalah mensintesis faktor-faktor psikologi yang ditemukan dari berbagai disiplin ilmu guna memberikan gambaran komprehensif. Selain itu, artikel ini diharapkan dapat memperkaya pemahaman dalam konteks Indonesia, di mana literasi digital yang masih dalam tahap perkembangan dan belum merata di seluruh lapisan masyarakat. Dengan demikian, hasil penelitian ini dapat menjadi dasar bagi pengembangan strategi pencegahan phishing yang lebih baik dan kontekstual bagi masyarakat di Indonesia.

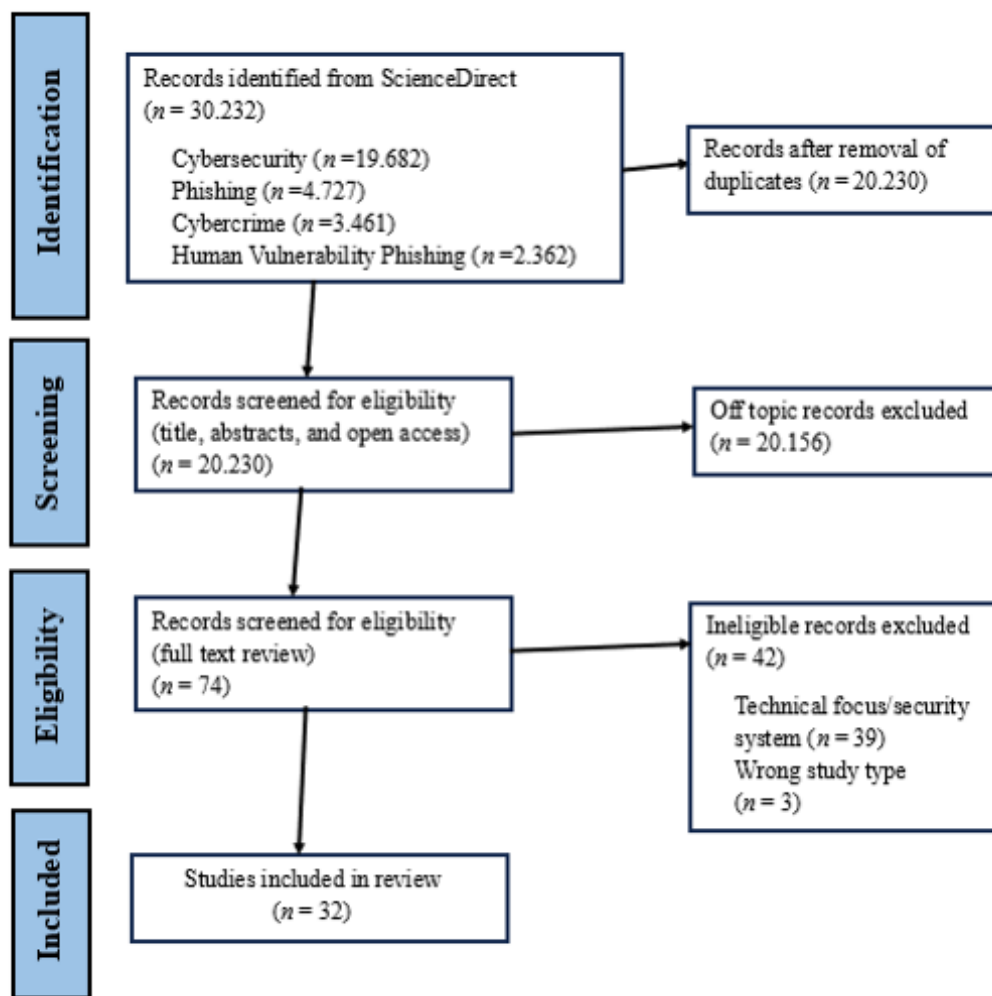
METODE PENELITIAN

Penelitian ini menggunakan desain scoping review yang dimana Pendekatan ini dipilih karena tujuannya adalah untuk memetakan cakupan luas sebuah topik berdasar literatur. Review ini memungkinkan identifikasi konsep dan celah pengetahuan dalam bidang yang berkembang pesat seperti keamanan cyber. Pendekatan ini dinilai sesuai untuk menjawab pertanyaan penelitian yang bersifat eksploratif. Tidak ada meta analisis statistik yang dilakukan

karena fokusnya pada pemetaan konsep dan seluruh proses mengikuti pedoman PRISMA-ScR. Penelitian ini menggunakan kerangka PCC Framework (Population, Concept, Context) untuk merumuskan pertanyaan penelitian. Pertanyaan penelitian dirumuskan sebagai: "Apa konsep dan faktor-faktor psikologis yang mempengaruhi kerentanan (Concept) individu (Population) sebagai korban phishing dalam konteks digital/email (Context)?". Konteks penelitian bersifat global, dengan implikasi khusus untuk Indonesia. Pertanyaan ini memandu seluruh proses pencarian dan seleksi literatur.

Pencarian literatur dilakukan di database ScienceDirect, dan google scholar. Kata kunci yang di pergunakan seperti "cybersecurity", "phishing", "cybercrime", dan "human vulnerability phishing". Operator Boolean (AND, OR) di pergunakan juga untuk memperluas cakupan pencarian. Filter tahun publikasi diterapkan dari 2016 hingga 2025. setelah literatur ditemukan, pemilihan artikel dilakukan berdasarkan tahapan dan proses memilah yang terdapat pada PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). Studi yang dikumpulkan sendiri membahas tentang kerentanan phishing. Screening dilakukan baik dari judul, abstrak lalu artikel yang dapat di akses isinya. Dilanjut pada tahap eligibility dimana dilakukannya penilaian keseluruhan isi artikel sehingga didapatkan artikel dan Seluruh alasan pengecualian ini dicatat untuk meningkatkan transparansi proses seleksi dan menjamin keterulangan (replicability) penelitian.

Pada penelitian ini juga mempergunakan bantuan Software berupa Mendeley dalam prosesnya karena menyediakan fitur untuk mengumpulkan dan mengelola referensi secara efisien. Dengan bantuan Mendeley peneliti dapat dengan mudah menyimpan dan mengorganisir artikel yang telah dikutip dalam satu tempat yang terintegrasi. Berawal dengan terkumpulnya 30.232 artikel dengan penggunaan 4 kata kunci seperti "Cybersecurity", "Phishing", "Cybercrime", dan "Human Vulnerability Phishing". Lalu dilanjutkan dengan tahap menghapus duplicates didapat kan 20.230 artikel yang kemudian akan dilanjutkan pada pengecekan kesesuaian judul, abstrak, dan open access yang bertujuan agar nantinya full teks dapat dinilai kesesuaiannya. Pada tahap itu didapatkan 74 artikel yang kemudian di seleksi lagi didapati 32 artikel yang akhirnya dipergunakan nantinya.



Gambar 1. Model PRISMA

HASIL DAN PEMBAHASAN

Sebagai bagian dari tahap sintesis, sejumlah artikel yang memenuhi kriteria inklusi dianalisis. Artikel-artikel tersebut diperoleh dari jurnal yang didapat dari berbagai database ilmiah, serta artikel tersebut juga menggunakan pendekatan metodologis yang beragam, seperti tinjauan sistematis, meta-analisis, analisis

konseptual, hingga sintesis kualitatif. Setiap artikel ditelaah berdasarkan tujuan penelitian, metode yang digunakan, hasil utama yang diperoleh. Dan juga artikel-artikel ini telah melalui tahap PRISMA dan juga tersusun dengan kerangka PCC Framework (Population, Concept, Context) untuk merumuskan pertanyaan penelitian pada artikel yang dibuat ini

Tabel 1. Hasil Review Artikel Literature

Penulis. Tahun. Judul	Tujuan Penelitian	Metode Penelitian	Hasil Penelitian
(Mirtaheeri et al., 2025) Cybersecurity in the age of generative AI: A systematic taxonomy of AI-powered vulnerability assessment and risk management	Mengembangkan taksonomi komprehensif yang mengklasifikasikan aplikasi ganda GenAI (ofensif dan defensif) dalam VA dan RM di cybersecurity melalui tinjauan sistematis, sambil menjawab RQ1-RQ5 tentang transformasi proses VA/RM, klarifikasi dual use, pengatasi tantangan prioritas dan remediasi, standar explainability untuk trustworthiness, dan fokus jenis cyberattack.	Systematic review, Keyword search dan filtering; Basis data: ACM, IEEE, ScienceDirect, Springer; Kriteria inklusi/eksklusi: Targeted keyword combinations (e.g., "Generative AI," "Vulnerability Assessments"), filtered to high quality papers focusing on security domain intersections; Jumlah studi	GenAI mentransformasi VA/RM melalui lifecycle empat tahap (discovery, assessment, risk prioritization, remediation) dengan aplikasi dual-use; taksonomi mengklasifikasikan teknik dominan seperti LLMs dan GANs, menyoroti tantangan seperti security, explainability, dan trustworthiness; GenAI mengatasi tantangan tradisional VA/RM, menyediakan peluang riset untuk deteksi vulnerabilitas, prioritas risiko, dan remediasi adaptif.

(Colabianchi et al., 2025) Transforming threats into opportunities: The role of human factors in enhancing cybersecurity	Mengidentifikasi tindakan manajerial yang meningkatkan cybersecurity dengan memanfaatkan peran faktor manusia melalui pencapaian konsensus ahli.	akhir: Over 100; Rentang tahun: 2020–2025. Kualitatif, Desain: Delphi study, Teknik pengumpulan/analisis data: Kompilasi tindakan dari literatur, putaran survei dengan panel ahli untuk konsensus, analisis tematik.	Studi menyajikan 16 tindakan manajerial kunci yang menggeser pandangan manusia dari sumber kerentanan menjadi komponen esensial solusi cybersecurity, menekankan pengembangan budaya organisasi yang menghargai cybersecurity, definisi peran dan tanggung jawab yang jelas, serta promosi pembelajaran berkelanjutan.
(Sarker et al., 2025) Understanding practitioners' challenges and requirements in the design, implementation, and evaluation of anti-phishing interventions	(1) Menginvestigasi tantangan praktisi dalam desain, implementasi, dan evaluasi intervensi anti-phishing di pengaturan dunia nyata; (2) Memahami perspektif praktisi terhadap panduan mereka dan bagaimana membuatnya mudah diakses bagi praktisi.	Kualitatif, Desain: Wawancara semi-struktural, Teknik pengumpulan/analisis data: Wawancara, analisis tematik, Jumlah partisipan: 18 praktisi dari 18 organisasi, Lokasi: 6 negara.	Mengidentifikasi 8 tantangan dalam desain konten pelatihan, dataset anti-phishing, penilaian pengetahuan pasca-pelatihan, dan sebagainya; membandingkan tantangan ini dengan yang dari MLR untuk menunjukkan validitas ekologis dan memperoleh wawasan untuk mengatasinya; melaporkan umpan balik praktisi terhadap panduan; mengumpulkan fitur yang dapat ditindaklanjuti untuk alat yang divisualisasikan guna membuat panduan mudah diakses.
(Greco et al., 2025) Enhancing Phishing Defenses: The Impact of Timing and Explanations in Warnings for Email Clients	Menyelidiki dampak timing aktivasi peringatan (sebelum atau setelah membuka email) dan kehadiran pesan penjelasan pada efektivitas peringatan dalam mencegah phishing, serta persepsi pengguna dan dampak karakteristik demografis (RQ1-RQ4).	Kuantitatif, Eksperimen terkontrol, Eksperimen, analisis statistik, Jumlah partisipan: 900	Peringatan yang ditampilkan setelah pengguna membaca konten email secara signifikan mengurangi tingkat klik, menunjukkan efektivitas lebih besar dalam mencegah phishing; kehadiran penjelasan juga menurunkan tingkat klik; namun, peringatan tanpa penjelasan dan peringatan sederhana untuk email false positive mungkin diperlukan; temuan disajikan sebagai lessons learned untuk mendesain sistem peringatan yang lebih efektif.
(Sarker et al., 2024) A Multi-vocal Literature Review on challenges and critical success factors of phishing education, training and awareness	Menyajikan pandangan komprehensif dan terstruktur tentang tantangan dan faktor keberhasilan kritis dalam desain, implementasi, dan evaluasi tahap phishing education, training, and awareness (PETA).	Multi-vocal Literature Review (MLR), Desain: Systematic review, Jumlah studi akhir: 53 studi akademik dan 16 studi grey.	Mengidentifikasi 20 tantangan dan 23 faktor keberhasilan kritis, termasuk faktor manusia dan socio-technical dalam PETA; menyoroti kebutuhan untuk sistem anti-phishing yang explainable, alat otomatis untuk studi phishing dunia nyata, mengatasi kesenjangan pengetahuan pengguna, dan pendekatan personalisasi.
(Beu et al., 2023) Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation	Mengidentifikasi apakah faktor-faktor seperti kemampuan deteksi phishing, kepercayaan pada keputusan identifikasi phishing, sikap umum terhadap tanggung jawab dan efikasi, serta kepuasan dan loyalitas karyawan dapat memprediksi perilaku dalam simulasi phishing naturalistik di pengaturan pekerjaan.	Kuantitatif, Survei dengan tugas deteksi phishing, Teknik pengumpulan/analisis data: Survei pasca-simulasi, analisis statistik, Lokasi: Organisasi besar.	Tahun kerja yang lebih sedikit di organisasi dan kepuasan serta loyalitas karyawan yang lebih rendah memprediksi perilaku tidak aman dalam simulasi.
(Naqvi et al., 2023) Mitigation strategies against the phishing attacks: A systematic literature review	Mengidentifikasi strategi mitigasi yang ada terhadap serangan phishing dan teknologi yang mendasarinya; vektor phishing yang paling dipertimbangkan dalam pengembangan strategi mitigasi; panduan dan rekomendasi anti-phishing	Systematic literature review, Basis data: Main digital libraries, Kriteria Jumlah studi akhir: 248, Rentang tahun: 2018 hingga Maret 2023.	Advokasi kebutuhan mempertimbangkan kemampuan pengguna manusia selama desain dan pengembangan strategi mitigasi karena solusi berpusat teknologi saja tidak cukup untuk mengatasi tantangan yang ditimbulkan oleh serangan phishing.

	untuk organisasi dan end-user; serta celah dan isu terbuka dalam state of the art.		
(Gallo et al., 2024) The human factor in phishing: Collecting and analyzing user behavior when reading emails	Mengumpulkan dan menganalisis data perilaku pengguna saat membaca email phishing dengan berbagai fitur dan strategi serangan melalui sistem Spamley, sambil menyebarkan kesadaran dan menganalisis literatur tentang phishing untuk mengidentifikasi pergeseran fokus dari aspek teknis ke aspek manusia.	Mixed methods, Tinjauan literatur dan pengembangan sistem empiris, Analisis literatur, survei, simulasi email phishing, analisis data; Jumlah partisipan: 500 pengguna.	Analisis literatur menunjukkan pergeseran fokus studi phishing dari aspek teknis ke aspek berorientasi manusia; sistem Spamley memungkinkan pengumpulan data yang digunakan untuk analisis seperti karakteristik email yang relevan dengan kerentanan kognitif kelompok pengguna tertentu; data tersedia untuk komunitas ilmiah.
(Chrysanthou et al., 2024) The anatomy of deception: Measuring technical and human factors of a large-scale phishing campaign	Memberikan perspektif ganda tentang mekanik teknis dan elemen manusia dalam kampanye phishing besar yang menargetkan pengguna Meta melalui analisis data korban nyata untuk memahami pendorong, fasilitator, dan faktor manusia.	Kuantitatif dan kualitatif, Analisis data empiris, Analisis data dari kampanye phishing nyata, pemrosesan bahasa alami, machine learning, metode berbasis transformer, Jumlah partisipan: Lebih dari 25.000 korban, Lokasi: Seluruh dunia.	Pilihan password korban buruk (30.27% kompleksitas rendah, 58.23% reuse password bocor); lebih dari 10% menunjukkan persistensi re-victimisation; korelasi demografi dan waktu rentan selama hari; analisis sentimen, emosi, dan nada dari respons teks menunjukkan keyakinan korban terhadap scam.
(Baltutis & Teubner, 2024) Effects of visual risk indicators on phishing detection behavior: An eye-tracking experiment	Menyelidiki bagaimana indikator risiko visual mempengaruhi pemrosesan informasi manusia dalam mendeteksi upaya phishing, khususnya pengaruhnya terhadap kepercayaan dan perilaku respons, tanpa menghilangkan isyarat phishing implisit. Ketersediaan indikator risiko visual secara signifikan mempengaruhi kepercayaan dan perilaku respons, tanpa menghilangkan isyarat phishing implisit; kalibrasi indikator risiko visual merupakan trade-off yang tergantung pada lingkungan organisasi.	Kuantitatif, Eksperimen lab eye-tracking, Teknik pengumpulan/analisis data: Penilaian kepercayaan email, eye-tracking.	
(Sturman et al., 2025) Security awareness, decision style, knowledge, and phishing email detection: Moderated mediation analyses	Memeriksa apakah hubungan negatif antara kesadaran keamanan informasi email dan kerentanan email phishing dimediasi oleh pengambilan keputusan intuitif yang lebih sedikit saat menilai email, dan apakah hubungan ini dimoderasi oleh pengetahuan email phishing.	Kuantitatif, Desain: Survei dan tugas pengurutan email, Teknik pengumpulan/analisis data: Tugas pengurutan email online, ukuran kesadaran keamanan informasi, pengambilan keputusan intuitif, pengetahuan phishing, analisis mediasi dimoderasi, Jumlah partisipan: 291.	Kesadaran keamanan informasi memprediksi niat perilaku positif secara langsung dan tidak langsung melalui preferensi pengambilan keputusan intuitif yang lebih rendah, dengan hubungan lebih kuat ketika pengetahuan phishing rendah; hubungan langsung dan tidak langsung antara kesadaran dan sensitivitas melalui gaya keputusan intuitif dimoderasi oleh pengetahuan phishing, dengan kesadaran memprediksi kemampuan diskriminasi phishing ketika pengetahuan rata-rata atau tinggi tetapi tidak rendah; pengetahuan phishing diperlukan sebelum perilaku dan proses pengambilan keputusan membantu deteksi phishing.
(Paul et al., 2024) Potential smart grid vulnerabilities to cyber attacks: Current threats and existing mitigation strategies	Memberikan analisis komprehensif tentang kerentanan smart grid, klasifikasi serangan umum dan dampaknya, strategi mitigasi dan deteksi menggunakan	Narrative review, Review article, Analisis literatur.	Smart grid mewarisi kerentanan dari teknologi komunikasi yang ada; eksploitasi dapat menyebabkan pelanggaran privasi, kegagalan beruntun, atau blackout sistem; menekankan hubungan rumit

	algoritma yang sesuai, serta tantangan penelitian saat ini dan inisiatif masa depan untuk meningkatkan keamanan siber smart grid.		antara kerentanan teknologi dan tantangan keamanan siber dalam kerangka smart grid, dengan area spesifik yang memerlukan perhatian lebih untuk pertahanan efektif dan kuat terhadap ancaman potensial.
(López-Aguilar et al., 2025) Phishing vulnerability and personality traits: Insights from a systematic review	Mengonsentrasikan pada sifat kepribadian dan efeknya terhadap kerentanan serangan phishing melalui tinjauan sistematis untuk meningkatkan strategi pertahanan keamanan siber dengan mempertimbangkan sifat kepribadian individu.	Systematic review, Pencarian literatur dan PRISMA, Basis data: Web of Science, Scopus, IEEE Xplore, ACM Digital Library, PubMed, Jumlah studi akhir: 26; Rentang tahun: 1900 hingga Januari 2025.	Extraversion, agreeableness, dan neuroticism umumnya menunjukkan asosiasi positif dengan kerentanan phishing, sedangkan conscientiousness muncul sebagai faktor protektif; terdapat kesenjangan signifikan dalam metodologi pengukuran kerentanan phishing saat ini, termasuk kurangnya alat pengukuran standar untuk eksperimen phishing.
(Yasin et al., 2024) Can serious gaming tactics bolster spear-phishing and phishing resilience? : Securing the human hacking in Information Security	Memberikan pelatihan dan konten edukasi kepada peserta tentang serangan phishing melalui serious game. Meningkatkan kesadaran peserta mengenai bahaya pengungkapan informasi berlebih secara online.	Mixed methods, Tinjauan literatur dan evaluasi empiris, Tinjauan literatur komprehensif, desain game hybrid dengan QR code, survei, observasi, diskusi, penilaian URL.	Data kuantitatif dan observasi kualitatif menunjukkan game "PhishDefend Quest" berhasil meningkatkan pemahaman pemain tentang ancaman phishing dan cara mendeteksi melalui pengalaman belajar interaktif; pembelajaran berbasis game merupakan pendekatan viable untuk mendidik tentang kesadaran phishing dan risiko pengungkapan informasi sensitif online.
(Sushma et al., 2023) Healthcare 4.0: A Review of Phishing Attacks in Cyber Security	Meninjau serangan phishing dalam konteks Healthcare 4.0, membahas motivasi cyberattack, tantangan yang terlibat, dan langkah-langkah preventif untuk mengatasi ancaman tersebut.	Narrative review, Review article, Analisis literatur.	Healthcare 4.0 rentan terhadap serangan phishing karena data bernilai tinggi, perangkat medis tidak dirancang untuk keamanan, akses jarak jauh, anggaran terbatas, teknologi usang, dan kurangnya kesadaran staf; tantangan utama meliputi email phishing, ransomware, pencurian perangkat, kebocoran insider, dan serangan pada perangkat terhubung yang memengaruhi keselamatan pasien.
(Le-Nye et al., 2024) Evaluating Phishing Awareness Strategies: A Comparative Study of Education-based approaches and Game-based learning	Menyelidiki efektivitas metode kesadaran phishing di tengah peningkatan serangan siber melalui analisis kuantitatif kerentanan individu dan evaluasi dampak strategi kesadaran berbasis pendidikan dan pembelajaran berbasis game.	Kuantitatif, Survei komparatif, Statistik deskriptif dan inferensial, model machine learning (Logistic Regression, Random Forest); Jumlah partisipan: 115.	Kursus tradisional dan game interaktif bermanfaat tetapi memerlukan evaluasi ulang berkelanjutan; usia dan bidang aktivitas penting dalam memprediksi kerentanan, sementara gender memiliki dampak kurang signifikan.
(Alraddadi et al., 2025) Towards Understanding the Critical Role of Human Behavior in Smart and Cognitive City Cybersecurity	Memeriksa peran faktor manusia dalam lanskap keamanan siber kota pintar dan kognitif melalui tinjauan literatur untuk menyelidiki bagaimana interaksi manusia dengan infrastruktur digital mempengaruhi keamanan dan privasi.	Narrative review, Literature review, Analisis literatur.	Integrasi data perilaku manusia ke dalam sistem AI meningkatkan deteksi dan respons ancaman; alat deteksi AI berpusat manusia mengurangi risiko kesalahan manusia dan kegagalan laten serta meningkatkan perlindungan populasi rentan; perbedaan infrastruktur, kecerdasan, dan peran warga antara kota pintar dan kognitif membentuk pengelolaan kerentanan berpusat manusia.
(Skinner et al., 2025) Cultivating Cybersecurity Awareness Among Seafarers	Memperkenalkan kerangka kerja untuk mengembangkan kesadaran keamanan siber di kalangan pelaut dengan mengintegrasikan konteks spesifik lingkungan maritim ke dalam program kesadaran.	Narrative review, Pengembangan kerangka kerja, Analisis literatur.	Pendekatan kesadaran saat ini kurang efektif karena mengabaikan aspek unik pelayaran; serangan siber maritim meningkat tujuh kali lipat antara 2010-2020 dengan faktor manusia sebagai penyebab utama melalui kurangnya

(Stylianou et al., 2025) Suspicious minds: Psychological techniques correlated with online phishing attacks	Mengembangkan taksonomi komprehensif teknik psikologis dalam serangan phishing, Menerapkan metrik baru (ACR, RCR, CCR) untuk mengukur dan membandingkan efektivitas Teknik, Menganalisis implementasi teknik dalam serangan dunia nyata berprofil tinggi.	Systematic review, Desain: Tinjauan literatur dan analisis empiris, Tinjauan sistematis literatur, data eksperimen psikologis.	kesadaran terhadap teknik social engineering seperti phishing. Teknik Majority Size paling kuat (CCR) pada tingkat kepatuhan awal rendah; Authority, Commitment & Consistency, dan Reciprocity juga sangat efektif; teknik memanfaatkan proses nonconscious untuk memanipulasi persepsi dan keputusan.
(Mouncey & Ciobotaru, 2025) Phishing scams on social media: An evaluation of cyber awareness education on impact and effectiveness	Menilai dampak dan efektivitas pendidikan kesadaran phishing terhadap pengguna Instagram melalui survei kesadaran dan faktor keterlibatan.	Kuantitatif dan kualitatif, Survei pengguna, Kuesioner, statistik deskriptif, regresi linier, analisis konten, Jumlah partisipan: 73.	Pendidikan phishing meningkatkan literasi digital dan dirasakan bermanfaat untuk keamanan Instagram terlepas dari waktu pelatihan; hambatan termasuk keterbatasan waktu dan persepsi pelatihan membosankan atau tidak relevan.
(Alanazi, 2024) ML-SPAs: Fortifying Healthcare Cybersecurity Leveraging Varied Machine Learning Approaches against Spear Phishing Attacks	Menguatkan pertahanan keamanan siber sektor kesehatan terhadap serangan spear phishing menggunakan berbagai pendekatan machine learning.	Kuantitatif, Desain: Eksperimen model ML, Analisis fitur email (konten, perilaku pengirim, lampiran), pengujian model ML.	Model CNN mencapai akurasi tertinggi 99.99%, diikuti BiLSTM 99.94%, dan MLP 98.46%; model sequential dan hierarchical unggul dibandingkan pendekatan tradisional dalam mendeteksi spear phishing.
(Sarkki et al., 2025) Fear of cybercrime victimisation: Examining the relationship between fear and victimisation	Menyelidiki hubungan temporal antara ketakutan terhadap cybercrime dan viktimisasi, termasuk apakah viktimisasi memengaruhi ketakutan dan sebaliknya, serta prediksi ketakutan dan viktimisasi sebelumnya terhadap yang berikutnya.	Kuantitatif, Desain: Longitudinal, Teknik pengumpulan/analisis data: Survei dua gelombang, regresi linier dan logistic, Jumlah partisipan: 1886, Lokasi: Belanda, Durasi: 2019–2020.	Viktimisasi baru-baru ini dan ketakutan sebelumnya meningkatkan ketakutan cybercrime saat ini (ketakutan sebelumnya prediktor terkuat); ketakutan tidak memengaruhi risiko viktimisasi tahun berikutnya; viktimisasi sebelumnya memprediksi risiko viktimisasi hampir lima kali lebih tinggi tahun berikutnya.
(Ruohonen et al., 2025) From cyber security incident management to cyber security crisis management in the European Union	Menganalisis persiapan Uni Eropa untuk mengelola krisis keamanan siber, termasuk hubungan antara insiden dan krisis, berdasarkan undang-undang keamanan siber baru dan dokumen kebijakan terkait.	Kualitatif, Desain: Analisis kebijakan, Teknik pengumpulan/analisis data: Analisis dokumen hukum dan kebijakan.	Krisis keamanan siber didefinisikan sebagai insiden berskala besar yang melebihi kapasitas satu negara anggota atau memengaruhi minimal dua negara; undang-undang baru meningkatkan pelaporan wajib insiden; pengelolaan krisis keamanan siber aktual di tingkat EU tetap tidak jelas meskipun adanya undang-undang dan badan tata kelola baru.
(Fang et al., 2025) A flight-to-safety from Bitcoin to stock markets: Evidence from cyber attacks	Menemukan dan menguji efek flight-to-safety dari pasar kripto ke pasar saham yang dipicu serangan hacking pada exchange kripto, serta mekanisme transmisinya melalui ketidakpastian dan persepsi risiko investor.	Kuantitatif, Desain: Analisis event study, Analisis data global 39 negara, sentimen media sosial, aliran dana mutual fund, Lokasi: Global.	Serangan hacking memicu FTS dari kripto ke saham karena ketidakpastian meningkatkan kesadaran risiko; efek diperkuat serangan berulang; sentimen media sosial sebagai indikator peringatan dan tekanan FTS; aliran dana abnormal ke mutual fund AS mengonfirmasi hipotesis FTS.
(Klütsch et al., 2025) InstaTrust or InstaTrap: How relationships and developmental tasks affect young adults' phishing susceptibility on Instagram	Memeriksa kerentanan phishing di Instagram pada dewasa muda dengan mengintegrasikan perspektif perkembangan, khususnya pengaruh hubungan dengan pengirim dan peluang pemenuhan tugas perkembangan usia.	Kuantitatif, Desain: Eksperimen vignette online, Teknik pengumpulan/analisis data: Skenario chat Instagram, analisis regresi, Jumlah partisipan: 500, Usia: 16–29 tahun.	Pesan dari follower yang menawarkan peluang sosial (acara) untuk pemenuhan tugas perkembangan bergabung dengan kelompok sebaya menghasilkan kerentanan tertinggi; hubungan dengan phisher dan peluang sosial sebagai prediktor signifikan kerentanan.
(Runturambi & Arifin, 2025) New patterns and trends of	Memeriksa pola baru perdagangan manusia dan cybercrime di kalangan pekerja	Kualitatif, Desain: Analisis kebijakan dan literatur, Teknik	Munculnya kejahatan transnasional campuran (human trafficking + cybercrime) dengan potensi bentuk

migration: Hybrid-crimes among indonesian migrant workers in Southeast Asia	migran Indonesia di Asia Tenggara pasca-pandemi, termasuk integrasi cybercrime dengan metode trafficking tradisional.	pengumpulan/analisis data: Analisis dokumen dan kasus.	hybrid lebih kompleks; kegagalan harmonisasi penegakan hukum perbatasan dengan kebijakan migrasi, mengabaikan keamanan perbatasan, cyberspace, hak asasi manusia, dan kesejahteraan pekerja migran.
(Huynh et al., 2025) From Programming Bugs to Multimillion-Dollar Scams: An Analysis of Trapdoor Tokens on Uniswap	Menyelidiki Trapdoor tokens pada Uniswap, menyusun klasifikasi sistematis teknik Trapdoor, mengembangkan tool deteksi TrapdoorAnalyser, membangun dataset Trapdoor, melatih model machine learning untuk deteksi, dan menganalisis karakteristik serta dampak finansial scam.	mixed methods, Desain: analisis data blockchain dengan inspeksi manual, pengembangan tool, dan machine learning, pengumpulan data dari Ethereum menggunakan web3 library dan Etherscan APIs, inspeksi manual 2,723 token untuk klasifikasi teknik, pengembangan TrapdoorAnalyser (uji buy-and-sell dengan error-log dan pemeriksaan semantik kontrak), ekstraksi fitur dari transaksi dan opcode untuk ML (algoritma seperti random forest), (data dari 131,172 token unik, 137,454 pool), Lokasi: UniswapV2 pada Ethereum, Durasi: Mei 2020 hingga Januari 2023.	Ditemukan 1,859 sampel Trapdoor dari inspeksi manual, diklasifikasikan menjadi lima teknik Trapdoor (exchange permission, fee manipulation, numerical exception, exchange suspension, transfer amount manipulation) dan enam maneuver penyembunyian; TrapdoorAnalyser menggunakan GoPlus dalam akurasi dan menyediakan penjelasan kode malicious; Dataset ground-truth: 11,943 Trapdoor dan 18,548 non-Trapdoor token; Model ML mendeteksi Trapdoor dengan F1 score sangat tinggi (hingga 0.99); Trapdoor scams menyebabkan kerugian satu miliar USD bagi 267,000 investor dari 2020-2023, dengan taktik scammer termasuk token palsu mirip nama terkenal dan klon token.
(Mirzania et al., 2025) Improved convenience or a cyber security threat? Public acceptance of mobility-as-a-service in Great Britain	Memeriksa persepsi publik terhadap Mobility-as-a-Service (MaaS), faktor-faktor yang memengaruhi kesediaan mengadopsi, termasuk kekhawatiran praktis dan kepercayaan digital, dengan penekanan pada risiko keamanan siber dalam membentuk penerimaan, di konteks urban dan rural di Great Britain.	kualitatif, focus group, semi-structured online focus groups dengan presentasi PowerPoint dan skenario hipotetis, thematic coding menggunakan NVivo dengan pendekatan bottom-up diikuti pemetaan ke TAM, Jumlah partisipan: 24, Lokasi: Great Britain (London, Greater Manchester, rural Exeter, rural Norwich), Durasi: Januari 2024, setiap sesi 120 menit.	Adopsi MaaS dipengaruhi oleh lokasi, keakraban teknologi, biaya, dan faktor sosio-demografis seperti usia; partisipan rural mempertanyakan kelayakan MaaS di konteks mereka; kekhawatiran privasi data dan keamanan siber tidak muncul secara inisiatif tetapi menjadi faktor penting dalam membentuk kepercayaan dan adopsi setelah dipicu.
(Qollakaj et al., 2025) Cybersecurity of remote work migration: A study on the VPN security landscape post Covid-19 outbreak	Mensintesis temuan dari 106 studi (2020–2023) untuk menganalisis evolusi serangan siber yang menargetkan VPN, taktik yang digunakan oleh aktor ancaman, dan strategi mitigasi yang efektif.	tinjauan literatur, Desain: sintesis literatur, pencarian dan analisis laporan, makalah akademik, dan temuan dari organisasi cybersecurity; sintesis data dan laporan insiden untuk mengidentifikasi pola dan tren, Kriteria inklusi/eksklusi: fokus pada insiden yang melibatkan penggunaan atau eksploitasi VPN, Jumlah studi akhir: 106, Rentang tahun: 2020–2023.	Adopsi kerja remote yang luas memicu lonjakan 238% serangan yang menargetkan VPN antara 2020 dan 2022; aktor ancaman, termasuk penjahat siber independen dan aktor yang didukung negara, menggunakan phishing, ransomware, dan advanced persistent threats untuk mengakses jaringan; organisasi menghadapi kerentanan seperti protokol VPN usang, autentikasi lemah, dan segmentasi jaringan tidak memadai; mengusulkan Kerangka Pengerasan VPN yang mencakup autentikasi kuat, enkripsi kuat, konfigurasi aman, dan pemantauan berkelanjutan; menyoroti tren seperti arsitektur zero-trust, enkripsi tahan kuantum, dan deteksi intrusi berbasis AI.
(Chiang et al., 2025) Fighting fraud: Corpus-assisted approaches to understanding and disrupting fraud activity on the dark web	Menunjukkan aplikasi metode corpus untuk memahami interaksi komunitas fraud di dark web guna mendukung infiltrasi oleh polisi undercover dan menginformasikan tools monitoring komersial untuk aktivitas fraud terkait produk.	empiris (corpus-assisted discourse studies/CADS), Desain: analisis corpus dengan demonstrasi aplikasi, Teknik pengumpulan/analisis data: pengumpulan data dari dark-web fraud fora, analisis	Situs dark-web berfungsi sebagai ruang efisien dan dinamis untuk upskilling dalam aktivitas fraud; Praktik diskursif mencakup mencari dan memberikan informasi, serta merekrut kolaborator; Terdapat tujuan komunitas luas untuk

(Suzuki et al., 2025) Patterns and predictors of cyber fraud victimization: Testing routine activity theory and general theory of crime in Japan	Menentukan apakah karakteristik korban cyber fraud di negara maju lain berlaku di Jepang, dengan fokus pada routine activity theory dan general theory of crime, serta bagaimana perilaku korban berikutnya berubah setelah viktimisasi.	corpus menggunakan metode linguistik dan modifikasi tools corpus untuk audiens non-linguist. kuantitatif, survei nasional, Teknik pengumpulan/analisis data: dua gelombang survei online dengan pertanyaan skrining, analisis regresi least squares biasa, Lokasi: Jepang, Durasi: Agustus 2024.	berbagi expertise; Terdapat barrier rendah untuk masuk anggota baru. Analisis regresi least squares biasa menunjukkan applicability dari routine activity theory dan general theory of crime dalam menjelaskan prediktor viktimisasi cyber fraud di Jepang; hanya sedikit korban cyber fraud yang mengubah perilaku mereka setelah viktimisasi.
(Ewoh et al., 2025) Sociotechnical Cybersecurity Framework for Securing Health Care From Vulnerabilities and Cyberattacks: Scoping Review	Memeriksa dinamika faktor kerentanan dan serangan siber dalam konteks teori sistem sosioteknis yang mendasari hubungan antara manusia, teknologi, dan proses; mengembangkan kerangka konseptual cybersecurity sosioteknis untuk mencegah kerentanan dan merespons serangan siber dan ancaman dalam sistem perawatan kesehatan.	scoping review, Teknik pengumpulan/analisis data: pencarian literatur dan thematic analysis, Basis data: Web of Science, PubMed (MEDLINE), Scopus, Kriteria inklusi/eksklusi: penelitian asli dan review, bahasa Inggris, domain perawatan kesehatan dan cybersecurity, Jumlah studi akhir: 76, Rentang tahun: 2012-2024.	Dari 1375 makalah, 76 memenuhi kriteria; faktor kerentanan terhadap serangan siber terdiri dari 12 subfaktor; faktor teknologi: desain sistem kompleks dan kegunaan (21%), integrasi teknologi baru (20%); faktor manusia: kekurangan profesional terampil dan anggaran terbatas; proses melibatkan teknologi dan manusia; terdapat interaksi sosioteknis antar faktor; konsep cybersecurity sosioteknis menawarkan perspektif komprehensif pada dasar sosioteknis dan optimalisasi bersama.

Penjahat atau pelaku kriminal di dunia cyber kini semakin cerdas dan canggih dalam memanfaatkan media sosial sebagai sarana melancarkan serangan phishing yang sering kali dengan menyamar sebagai institusi atau individu tepercaya. Pada penelitiannya (Syah, 2023) menggaris bawahi kurangnya kesadaran dan pemahaman pengguna atau user tentang risiko serangan phishing serta diperlukannya pendidikan tentang tanda-tanda serangan cyber yang umum dilakukan oleh pelaku kriminal dan cara melindungi diri untuk memastikan tidak termakan tipu muslihat dari penjahat cyber. Di Indonesia, ancaman phishing menjadi persoalan yang terbilang serius yang dapat mengganggu keamanan transaksi elektronik dan hal yang lainnya berkaitan dengan identitas korban ataupun celah yang dapat dimanfaatkan pelaku kejahatan yang bersumber dan didapatkan melalui perangkat digital. Pengguna internet yang berasal dari berbagai latar belakang sosial, ekonomi, dan pendidikan, sehingga tidak semua memiliki kesadaran yang memadai terhadap modus operandi atau cara menipu dalam kasus kejahatan cyber (Malunsenge et al., 2022). Lebih dari sekadar masalah teknis atau system error semata, phishing sendiri juga memanfaatkan faktor psikologis seperti rasa urgensi, kepercayaan berlebihan, atau ketidaktahuan, yang menegaskan perlunya pendekatan psikologi pada dunia cyber yang holistik dan kolaboratif dengan melibatkan otoritas penegak hukum, platform media sosial, para tokoh public, serta partisipasi aktif dari masyarakat sebagai garda

terdepan dalam mengenali dan melaporkan upaya penipuan yang menggunakan modus menyerupai organisasi atau Lembaga bahkan sampai pada yang mengincar seorang individu melalui SMS, WA, bahkan EMAIL (Syah, 2023). Dalam konteks ini, edukasi publik yang berkelanjutan diperkuat dengan pemanfaatan teknologi atau platform untuk meningkatkan literasi digital menjadi langkah strategis untuk membangun ketahanan kolektif terhadap serangan phishing dan menciptakan ekosistem cyber yang lebih aman.

Faktor kognitif yang muncul pada korban phishing ternyata beraneka ragam dan salah satunya adalah dipengaruhi akan rendahnya literasi digital masyarakat, di mana banyak individu masih kurang memahami bahaya dan modus operandi atau cara penipu di dunia cyber sehingga membuat mereka menjadi target yang rentan terhadap phishing yang berujung pada kerugian material maupun non-material (Lubis et al., 2025). Secara spesifik, faktor kognitif seperti tingkat kepercayaan diri yang tinggi maupun rendah juga dapat mempengaruhi peluang seseorang menjadi korban dari serangan phishing melalui pesan instan (SMS, WA, EMAIL, DLL) di mana tingkat kepercayaan diri yang lebih tinggi justru menjadi target yang rentan karena memicu kemudahan dari pelaku kejahatan untuk mengakases informasi-informasi mengenai korban, sehingga peluang untuk phishing meningkat (Y. Y. Lee et al., 2023). Modus operandi phishing sendiri seperti penggunaan halaman website palsu atau surel palsu untuk

mengelabui korban atau user guna mencuri data pribadi, karena phishing sendiri memiliki penguasaan sistem komputer yang jauh lebih tinggi daripada masyarakat umum yang berakibat mampunya pelaku kejahatan untuk mengakses dan mengeksploitasi celah keamanan untuk mengambil alih akun, melakukan transaksi keuangan, atau menyebabkan kerugian finansial lainnya pada korban (Wiranata et al., 2024).

Pada penelitiannya Andri & Somawati, (2025) menunjukkan ketika jumlah pengguna media sosial terus meningkat secara pesat di seluruh belahan dunia, para penjahat cyber pun bertambah dan aktif mencari berbagai cara atau modus untuk mengambil keuntungan dari pengguna yang merasa nyaman dan percaya diri beraktivitas di medsos. Phishing sendiri dapat dijelaskan secara sederhana dan singkat sebagai sebuah jebakan digital atau perangkap yang sengaja dibuat untuk 'memancing' korban agar mau menyerahkan data pribadi mereka atau membuka akses untuk seorang penjahat masuk kedalam perangkatnya. Para penipu ini membuat pesan atau laman yang tampak sangat resmi dan meyakinkan, sehingga korban merasa aman tanpa curiga. Akibatnya, korban sering kali secara tidak sadar memasukkan informasi penting seperti kata sandi, nomor rekening bank, atau data pribadi lainnya ke dalam situs atau pesan palsu tersebut. Kondisi ini sangat berbahaya karena informasi yang berhasil dicuri bisa digunakan penjahat siber untuk melakukan penipuan lebih lanjut dan merugikan korban dalam berbagai aspek, baik finansial maupun privasinya sendiri.

Faktor-faktor yang muncul pada korban serangan phishing semakin diperburuk oleh modus operandi atau cara menipunya seorang pelaku kriminal yang terstruktur dan dinamis, pelaku memanfaatkan kemajuan teknologi informasi melalui situs palsu, media sosial, aplikasi jual beli online, dompet digital, serta manipulasi psikologis untuk menjerat korban yang rentan dengan konten-konten atau pesan-pesan yang masuk kedalam perangkat korban (Oktaviana & Rinaldi, 2025). Pada penelitiannya Kim et al., (2023) ditemukan bahwa rendahnya literasi digital di kawasan ASEAN, sebagaimana ditunjukkan oleh peringkat Indeks Keamanan Siber Global ITU 2020 dan Indeks Keamanan Siber Nasional Estonia, bahwa Singapura dan Malaysia di atas 70% sementara rata-rata negara lain 28% dan Myanmar hanya 36,41% yang menciptakan peningkatan kerentanan terhadap ancaman cyber di tengah pertumbuhan ekonomi, populasi, dan konektivitas ICT lintas batas. Revolusi digital dalam dunia bisnis juga menawarkan kemudahan, biaya rendah, serta kepraktisan yang justru dimanfaatkan secara

tidak bertanggung jawab oleh pihak tertentu untuk menyusup ke situs web instansi guna mencuri atau mengubah informasi seseorang atau kelompok, sehingga kejahatan phishing menjadi bentuk kejahatan utama dengan mengelabui atau menipu korban agar secara sukarela memberikan data pribadi (Wibowo & Hidayat, 2024). Sebagai serangan rekayasa sosial paling umum di dunia digital, phishing termasuk (smishing/penipuan melalui pesan dan pharming/penipuan dengan mengalihkan dari situs web asli ke situs web palsu) sehingga memicu kebocoran informasi keuangan melalui pesan atau situs web palsu, dengan frekuensi yang meningkat 2 kali lipat pada 2020 menurut laporan Internet Crime Complaint Center FBI yang dikutip dalam penelitiannya (Park et al., 2023). Akibatnya, korban mengalami kerugian finansial besar disertai kerusakan reputasi dan kepercayaan diri, yang semakin sulit dideteksi karena perkembangan AI dan big data memungkinkan serangan phishing yang lebih meyakinkan serta dipersonalisasi ke pada seorang yang dinilai berpengaruh (Putra et al., 2024).

Penelitiannya W. Lee et al., (2024) menunjukkan banyaknya penelitian tentang kit phishing, masih terdapat berbagai hal yang menyulitkan upaya dalam pengurangan serangan phishing. Studi umumnya hanya memfokuskan pada kit phishing tertentu, misalnya merek keuangan, cara melewati otentikasi dua faktor yang dimana hanya menganalisis beberapa kit phishing man-in-the-middle (MITM). Lebih lanjutnya strategi yang berjalan di server belum dianalisis secara mendalam. Sebagai contoh, sebuah penelitian terbaru hanya memeriksa keberadaan halaman tambahan pada situs palsu, sehingga gagal menggali proses rinci dan data yang terekspos selama serangan. Penelitian ini menekankan bahwa sedikitnya studi yang menguji interaksi multidimensi ini secara empiris, interaksi seorang korban yang mudah terkena serangan phishing, serta minimnya studi longitudinal untuk memahami perubahan kerentanan seiring waktunya.

Temuan ini juga memberikan masukan untuk implikasi langsung bagi praktisi keamanan cyber dalam berbagai tingkatan dengan menyarankan edukasi yang disesuaikan dengan profil psikologi kelompok yang akan menerima edukasi. Selanjutnya merekomendasikan pentingnya menciptakan budaya organisasi yang mudah dan aman secara psikologi untuk pelaporan kejadian. Pada intinya, temuan ini menyarankan pada satu kesimpulan praktis yaitu pencegahan phishing yang efektif memerlukan strategi untuk menangani aspek psikologi yang dapat diterapkan dengan teknologi dan kebijakan yang mendukung.

Penilaian terhadap kasus-kasus phishing juga di Indonesia dalam era kemajuan teknologi informasi dan komunikasi yang pesat ini keamanan digital menjadi aspek yang cukup krusial. Diperlukannya strategi edukasi keamanan digital untuk meningkatkan kewaspadaan masyarakat secara aktif guna membentuk lapisan pertahanan kuat dan meminimalkan dari dampak serangan phishing (Nugroho et al., 2023). Pada tahun 2021, BSSN Indonesia dalam penelitiannya Febrika Ardy et al., (2024) mencatat setidaknya 264 kasus phishing yang terbagi menjadi 5 jenis yaitu Email Phishing, Spear Phishing, Whaling, Vishing/penipuan melalui telpon atau suara, dan Smishing, di mana kejahatan ini menyebabkan kerugian nyata karena data korban disalahgunakan untuk pencurian identitas, peretasan sistem komputer, serta tindakan merugikan lainnya. Pada penelitiannya Cahyaningsih et al., (2025) tentang pendekatan melalui UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) serta di Malaysia melalui Personal Data Protection Act (PDPA) 2010 (Act 709) dan Akta A1727 tahun 2024 yang menunjukkan kebijakan penanggulangan phishing ke depannya perlu menekankan kelembagaan, kerjasama internasional penegakan hukum, serta mekanisme ganti rugi bagi korban. Oleh karena itu juga, respons keamanan cyber di Indonesia yang masih didominasi pendekatan teknis dan hukum perlu dilengkapi dengan eksplorasi mendalam terhadap dimensi psikologis korban sebagai salah satu sudut pandang dalam menetapkan hukum.

Secara keseluruhan, scoping review ini bertujuan untuk memetakan empat domain utama seperti faktor psikologis yaitu: kognitif, emosional, sosial-teknologis, dan pengetahuan/demografis. penekanan pada sintesis dan juga deskripsi pada bagian ini menegaskan bahwa keamanan cyber yang efektif harus berpusat atau berdasar pada manusia itu sendiri (human-centered cybersecurity). Psikologi sendiri dalam keamanan cyber masih cukup kurang terleih terhadap pada penelitian-penelitian yang longitudinal fokus terhadap keamanan seorang manusia mengenai kejahatan cyber / cybercrime. Kontribusi utama penelitian ini adalah upaya untuk menjembatani atau memberikan tambahan wawasan keilmuan terhadap cybercrime terutama pada kasus phishing. Artikel ini diharapkan menjadi referensi bagi peneliti, praktisi, dan pembuat kebijakan untuk membangun ekosistem digital yang lebih aman dan inklusif dengan pendekatan berbasis bukti dan mengutamakan kenyamanan manusia sebagai sosok penggunanya atau user.

Kedepannya diharapkan muncul modul-modul, teknik intervensi, atau game yang dapat menyentuh atau memberikan pemahaman yang lebih baik terhadap bijak dalam menggunakan digital atau bahkan meningkatnya literasi digital pada berbagai kelompok kalangan. Namun juga masih dan perlunya validitas eksternal, studi empiris di berbagai konteks budaya, termasuk masyarakat multi etnis dan multi bahasa seperti Indonesia pasti perlunya penyesuaian didalamnya.

SIMPULAN

Penelitian ini bertujuan untuk memetakan konsep dan faktor-faktor psikologis yang memengaruhi kerentanan individu sebagai korban kejahatan phishing melalui pendekatan scoping review terhadap literatur ilmiah yang diterbitkan antara tahun 2016 hingga 2025. Melalui proses seleksi sistematis berbasis kerangka PRISMA-ScR dan analisis tematik terhadap 32 artikel yang memenuhi kriteria inklusi, penelitian ini mengidentifikasi empat kategori utama faktor psikologis yang saling terkait dan membentuk respons individu terhadap ancaman phishing itu sendiri seperti faktor kognitif, faktor emosional, faktor sosial-teknologis, serta faktor demografis dan pengetahuan. Faktor kognitif mencakup rendahnya literasi digital, kepercayaan diri berlebihan (overconfidence), serta pengambilan keputusan yang kurang kritis. Pada faktor emosional meliputi rasa urgensi dan ketakutan yang sering dimanipulasi penjahat melalui pesan yang memunculkan tekanan psikologi. Selanjutnya faktor sosial-teknologi seperti manipulasi identitas melalui media sosial dengan pemanfaatan nama besar institusi (seperti BCA, DJKN, atau platform global) digunakan untuk membangun ilusi keabsahan untuk menipu korban. Sementara itu, faktor demografis dan pengetahuan seperti usia, latar belakang pendidikan, pengalaman digital, dan tingkat kesadaran keamanan cyber turut menjadi bagian dari menentukan sejauh mana seseorang mampu mengenali dan merespons upaya phishing itu akan terjadi pada dirinya atau orang lain.

Temuan ini menegaskan bahwa kerentanan terhadap phishing bukan semata-mata disebabkan oleh ketidaktahuan teknis atau kelemahan sistem, melainkan hasil dari berbagai aspek seperti kognitif, emosional, sosial, dan demografis yang membentuk cara individu memproses informasi, menilai risiko, dan mengambil keputusan dalam lingkungan digital. Pendekatan keamanan cyber yang efektif harus bergeser dari paradigma “melindungi sistem” menuju “melindungi pengguna”, dengan menempatkan manusia sebagai pusat strategi

pencegahan. Hal ini selaras dengan temuan dalam pembahasan bahwa upaya mitigasi berbasis teknologi seperti daftar blokir atau deteksi otomatis masih memiliki keterbatasan, terutama dalam menghadapi serangan yang sangat dipersonalisasi dikarenakan power atau tingkat berpengaruhnya individu tersebut seperti spear phishing atau manipulasi berbasis rekayasa sosial.

Peta konsep yang dihasilkan ini diharapkan memberikan landasan empiris yang kuat bagi pengembangan intervensi berbasis bukti, baik di tingkat kebijakan, edukasi, maupun desain teknologi. Di Indonesia sendiri dimana literasi digital masih belum merata dan serangan phishing terus meningkat seperti yang terlihat dari 26.675 laporan pada kuartal I 2023 menurut IDADX, serta kasus-kasus nyata pada BCA dan DJKN memberikan pemahaman mendalam tentang dimensi psikologi ini. Edukasi keamanan cyber tidak cukup hanya menyampaikan aturan teknis, melainkan perlu dirancang secara kontekstual, budaya, dan psikologi, sehingga mampu menyentuh cara berpikir, perasaan, dan kebiasaan digital masyarakat guna edukasi yang tepat guna dan berdampak.

Untuk penelitian mendatang diperlukannya studi empiris dan longitudinal yang dilakukan secara terkhusus di konteks Indonesia, dengan melibatkan populasi yang lebih beragam tidak hanya mahasiswa atau pekerja perkotaan, tetapi juga masyarakat pedesaan, lansia, pelaku usaha mikro, serta kelompok-kelompok dengan akses terbatas terhadap teknologi. Hal ini penting mengingat karakteristik sosial-budaya, tingkat pendidikan, dan pola penggunaan internet di Indonesia sangat heterogen atau beraneka ragam. Selain itu juga masih minim eksplorasi terhadap dampak psikologi jangka panjang korban kejahatan phishing, seperti trauma digital, kehilangan kepercayaan terhadap institusi, atau stigma sosial yang dapat menghambat pemulihan korban kejahatan.

DAFTAR PUSTAKA

- Alanazi, S. A. (2024). ML-SPAs: Fortifying Healthcare Cybersecurity Leveraging Varied Machine Learning Approaches against Spear Phishing Attacks. *Computers, Materials and Continua*, 81(3), 4049–4080. <https://doi.org/10.32604/cmc.2024.057211>
- Alraddadi, R., Alshayeb, M., Mahmood, S., & Niazi, M. (2025). Towards Understanding the Critical Role of Human Behavior in Smart and Cognitive City Cybersecurity. *Procedia Computer Science*, 257, 1039–1046. <https://doi.org/10.1016/j.procs.2025.03.135>
- Andri, & Somawati. (2025). Ancaman dan Pencegahan Phishing Pengguna Media Sosial untuk Siswa di SMK Wisata Indonesia. *Jurnal Kemitraan Masyarakat*, 2. <https://doi.org/https://doi.org/10.62383/jkm.v2i2.1596>
- Arksey, H., & O'Malley, L. (2005). Scoping studies: towards a methodological framework. *International Journal of Social Research Methodology* ISSN:, 8(1), 19–32. <https://doi.org/10.1080/1364557032000119616>
- Badan Perlindungan Konsumen Nasional (BPKN). (2023). Kasus phising makin marak, BPKN RI bahas strategi pencegahan bareng Pemprov Sulsel. <https://bpkn.go.id/beritaterkini/detail/kasus-phising-makin-marak-bpknri-bahas-strategi-pencegahan-bareng-pemprov-sulsel>
- Baltutis, D., & Teubner, T. (2024). Effects of visual risk indicators on phishing detection behavior: An eye-tracking experiment. *Computers and Security*, 144(0167–4048), 103940. <https://doi.org/10.1016/j.cose.2024.103940>
- Beu, N., Jayatilaka, A., Zahedi, M., Babar, A., Hartley, L., Lewinsmith, W., & Baetu, I. (2023). Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation. *Computers and Security*, 131, 103313. <https://doi.org/10.1016/j.cose.2023.103313>
- Cahyaningsih, R. D., Fauzan, A., Hasbi, S., & Winanti, A. (2025). Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Phising Dengan Undang-Undang Perlindungan Data Pribadi: Studi Perbandingan Indonesia dan Malaysia. *Abdurrauf Science and Society*, 1(4), 800–811. <https://doi.org/10.70742/asoc.v1i4.283>
- Chiang, E., Kredens, K., & Thornton, J. (2025). Fighting fraud: Corpus-assisted approaches to understanding and disrupting fraud activity on the dark web. *Applied Corpus Linguistics*, 100159. <https://doi.org/10.1016/j.acorp.2025.100159>
- Chrysanthou, A., Pantis, Y., & Patsakis, C. (2024). The anatomy of deception: Measuring technical and human factors

- of a large-scale phishing campaign. *Computers and Security*, 140, 103780. <https://doi.org/10.1016/j.cose.2024.103780>
- Colabianchi, S., Costantino, F., Nonino, F., & Palombi, G. (2025). Transforming threats into opportunities: The role of human factors in enhancing cybersecurity. *Journal of Innovation and Knowledge*, 10(3), 100695. <https://doi.org/10.1016/j.jik.2025.100695>
- Cybernews. (2025, Mei 10). FBI shares 42,000 phishing domains linked to LabHost takedown. <https://cybernews.com/cybercrime/fbi-shares-42000-phishing-domains/>
- Dewanto, M. A. B., Fathurrahman, M., Firdaus, D. R., & Setiawan, A. (2024). Penipuan Penambah Followers Instagram: Analisis Serangan Phising dan Dampaknya pada Keamanan Data. *Journal of Internet and Software Engineering*, 1(4), 11. <https://doi.org/10.47134/pjise.v1i4.2672>
- Direktorat Jenderal Kekayaan Negara (DJKN), Kementerian Keuangan Republik Indonesia. (2023). Waspada kejahatan phising mengintai Anda. <https://www.djkn.kemenkeu.go.id/artikel/baca/14851/Waspada-Kehajatan-Phising-Mengintai-Anda.html>
- Ewoh, P., Vartiainen, T., & Mantere, T. (2025). Sociotechnical Cybersecurity Framework for Securing Health Care from Vulnerabilities and Cyberattacks: Scoping Review. *Journal of Medical Internet Research*, 27. <https://doi.org/10.2196/75584>
- Fang, Y., Chen, C. Y. H., & Jiang, C. (2025). A flight-to-safety from Bitcoin to stock markets: Evidence from cyber attacks. *International Review of Financial Analysis*, 103, 104093. <https://doi.org/10.1016/j.irfa.2025.104093>
- 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>
- Federal Bureau of Investigation (FBI). (2023). Internet Crime Report 2022. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
- Gallo, L., Gentile, D., Ruggiero, S., Botta, A., & Ventre, G. (2024). The human factor in phishing: Collecting and analyzing user behavior when reading emails. *Computers and Security*, 139, 103671. <https://doi.org/10.1016/j.cose.2023.103671>
- GetAstra. (2025). 18 Phishing attack statistics 2025: The Ultimate Insight. <https://www.getastra.com/blog/security-audit/phishing-attack-statistics/>
- Greco, F., Desolda, G., Buono, P., & Piccinno, A. (2025). Enhancing Phishing Defenses: The Impact of Timing and Explanations in Warnings for Email Clients. *Computer Standards and Interfaces*, 93, 103982. <https://doi.org/10.1016/j.csi.2025.103982>
- Hanifah, L., Sab'ngatun, Setyorini, C., Putri, A. P., & Fitriani, E. A. (2025). Skrining kesehatan mental pada anak: scoping review. 16(1), 180–197. <https://doi.org/10.36419/jki.v16i1.1319>
- Hapsari, R. D., & Pambayun, K. G. (2023). ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Konstituen*, 5(1), 1–17. <https://doi.org/10.33701/jk.v5i1.3208>
- Huynh, P. D., Dau, S. H., Li, X., Gondal, I., De Silva, T., & Viterbo, E. (2025). From Programming Bugs to Multimillion-Dollar Scams: An Analysis of Trapdoor Tokens on Uniswap. *Blockchain: Research and Applications*, 100370. <https://doi.org/10.1016/j.bcr.2025.100370>
- Kim, Y. K., Go, M. H., Kim, S., Lee, J., & Lee, K. (2023). Evaluating Cybersecurity Capacity Building of ASEAN Plus Three through Social Network Analysis. *Journal of Internet Technology*, 24(2), 495–505. <https://doi.org/10.53106/160792642023032402031>
- Klütsch, J., Haehn, L., Kreuder, A., Böffel, C., Frick, U., & Schlittmeier, S. J. (2025). InstaTrust or InstaTrap: How relationships and developmental tasks affect young adults' phishing susceptibility on Instagram. *International Journal of Human Computer Studies*, 197. <https://doi.org/10.1016/j.ijhcs.2025.103456>
- Le-Nye, E. N. M., Yaacoub, C., & Possik, J. (2024). Evaluating Phishing Awareness Strategies: A Comparative Study of Education-based approaches and Game-based learning. *Procedia Computer Science*, 251, 666–671. <https://doi.org/10.1016/j.procs.2024.11.166>
- Lee, B. T. F., Kornphetcharat, K., Sims, J. P., Linh Dieu, D., & Salman Ali, B. (2025). ASEAN Cybersecurity Cooperation Strategy:

- Combating Cyber Terrorism and Hackers Through CERT Coordination. *International Journal of Law and Public Policy (IJLAPP)*, 7(1), 20–30. <https://doi.org/10.36079/lamintang.ijlapp-0701.788>
- Lee, W., Hur, J., & Kim, D. (2024). Beneath the Phishing Scripts: A Script-Level Analysis of Phishing Kits and Their Impact on Real-World Phishing Websites. *ACM AsiaCCS 2024 - Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, 1214–1230. <https://doi.org/10.1145/3634737.3657013>
- Lee, Y. Y., Gan, C. L., & Liew, T. W. (2023). Thwarting Instant Messaging Phishing Attacks: The Role of Self-Efficacy and the Mediating Effect of Attitude towards Online Sharing of Personal Information. *International Journal of Environmental Research and Public Health*, 20(4). <https://doi.org/10.3390/ijerph20043514>
- Lokapala, Y. H., Nurfauzi, F. J., & Widowaty, Y. (2024). Aspek Yuridis Kejahatan Phishing dalam Ketentuan Hukum di Indonesia. *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, 5(1), 19–24. <https://doi.org/10.18196/ijclc.v5i1.19853>
- López-Aguilar, P., Urruela, C., Batista, E., Machin, J., & Solanas, A. (2025). Phishing vulnerability and personality traits: Insights from a systematic review. *Computers in Human Behavior Reports*, 20, 100784. <https://doi.org/10.1016/j.chbr.2025.100784>
- Lubis, H., Awaludin, D. T., Sari, D. P., Milasari, L. A., & Sofyan. (2025). Edukasi Keamanan Siber: Pelatihan Dasar Mengenali Phishing dan Proteksi Data Pribadi di Dunia Digital. *JIPITl: Jurnal Pengabdian Kepada Masyarakat*, 2(2), 101–105. <https://jipiti.technolabs.co.id/index.php/pkm/index>
- Malunsenge, L. M., Massie, C. D., & Rorie, R. E. (2022). Penegakan Hukum Terhadap Pelaku Dan Korban Tindak Pidana Cyber Crime Berbentuk Phising Di Indonesia. *Lex Crimen*, 11(3), 1–10. <https://ejournal.unsrat.ac.id/index.php/lexcrimen/article/view/40797>
- Mirtaheri, S. L., Movahed, N., Shahbazian, R., Pascucci, V., & Pugliese, A. (2025). Cybersecurity in the age of generative AI: A systematic taxonomy of AI-powered vulnerability assessment and risk management. *Future Generation Computer Systems*, 175, 108107. <https://doi.org/10.1016/j.future.2025.108107>
- Mirzania, P., Balta-Ozkan, N., & Whitmarsh, L. (2025). Improved convenience or a cyber security threat? Public acceptance of mobility-as-a-service in Great Britain. *Energy Research and Social Science*, 127(June 2024), 104309. <https://doi.org/10.1016/j.erss.2025.104309>
- Mouncey, E., & Ciobotaru, S. (2025). Phishing scams on social media: An evaluation of cyber awareness education on impact and effectiveness. *Journal of Economic Criminology*, 7(October 2024), 100125. <https://doi.org/10.1016/j.jeconc.2025.100125>
- Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., & Porras, J. (2023). Mitigation strategies against the phishing attacks: A systematic literature review. *Computers and Security*, 132, 103387. <https://doi.org/10.1016/j.cose.2023.103387>
- Nugroho, H., Nur Ihsan, M., Haryoko, A., Ma`arif, F., & Alifah, F. (2023). Edukasi Keamanan Digital Untuk Meningkatkan Kewaspadaan Masyarakat Terhadap Link Phising. *Alahyan Jurnal Pengabdian Masyarakat Multidisiplin*, 1(2), 104–111. <https://doi.org/10.61492/ecospreneurs.v1i2.60>
- Oktaviana, H., & Rinaldi, K. (2025). Modus Operandi Phisher dalam Kejahatan Phishing (Studi Kasus Ditreskrimsus Polda Riau). *Journal of Knowledge and Collaboration*, 2(5), 655–658. <https://doi.org/https://doi.org/10.59613/xb36sv81>
- Oyadeyi, O. O., Oyadeyi, O. A., & Bello, R. O. (2024). Cybercrime in the Asia-Pacific Region: A Case Study of Commonwealth APAC Countries. *Commonwealth Cyber Journal*, 3018, 130–160. <https://www.researchgate.net/publication/381430723%0ACybercrime>
- Park, H., Lim, K., Kim, D., Yu, D., & Koo, H. (2023). Demystifying the Regional Phishing Landscape in South Korea. *IEEE Access*, 11(November), 130131–130143. <https://doi.org/10.1109/ACCESS.2023.333883>
- Paul, B., Sarker, A., Abhi, S. H., Das, S. K., Ali, M. F., Islam, M. M., Islam, M. R., Moyeen, S. I., Rahman Badal, M. F., Ahamed, M. H., Sarker, S. K., Das, P., Hasan, M. M., & Saqib, N. (2024). Potential smart grid

- vulnerabilities to cyber attacks: Current threats and existing mitigation strategies. *Heliyon*, 10(19), e37980. <https://doi.org/10.1016/j.heliyon.2024.e37980>
- Pourmohamad, R., Wirsz, S., Oest, A., Bao, T., Shoshitaishvili, Y., Wang, R., Doupé, A., & Bazzi, R. A. (2024). Deep Dive into Client-Side Anti-Phishing: A Longitudinal Study Bridging Academia and Industry. *ACM AsiaCCS 2024 - Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, 1(1), 638–653. <https://doi.org/10.1145/3634737.3657027>
- Prawiyogi, A. G., & Alwiyah. (2023). Southeast Asia's Cyber Security Strategy: Multilateralism or Self-help. *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, 4(2), 119–127. <https://doi.org/10.34306/itsdi.v4i2.581>
- Putra, F. P. E., Ubaidi, U., Zulfikri, A., Arifin, G., & Ilhamsyah, R. M. (2024). Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study. *Brilliance: Research of Artificial Intelligence*, 4(1), 413–421. <https://doi.org/10.47709/brilliance.v4i1.4357>
- Qollakaj, K., Larsson, L. E., & Memeti, S. (2025). Cybersecurity of remote work migration: A study on the VPN security landscape post Covid-19 outbreak. *Array*, 27, 100437. <https://doi.org/10.1016/j.array.2025.100437>
- Runturambi, A. J. S., & Arifin, R. (2025). New patterns and trends of migration: Hybrid-crimes among indonesian migrant workers in Southeast Asia. *Regional Science Policy and Practice*, 17(10), 100215. <https://doi.org/10.1016/j.rspp.2025.100215>
- Ruohonen, J., Rindell, K., & Buseti, S. (2025). From cyber security incident management to cyber security crisis management in the European Union. *Computers & Security*, 159, 104689. <https://doi.org/10.1016/j.cose.2025.104689>
- Sarker, O., Jayatilaka, A., Haggag, S., Liu, C., & Babar, M. A. (2024). A Multi-vocal Literature Review on challenges and critical success factors of phishing education, training and awareness. *Journal of Systems and Software*, 208, 111899. <https://doi.org/10.1016/j.jss.2023.111899>
- Sarker, O., Jayatilaka, A., Haggag, S., Liu, C., & Babar, M. A. (2025). Understanding practitioners' challenges and requirements in the design, implementation, and evaluation of anti-phishing interventions. *Journal of Systems and Software*, 225, 112356. <https://doi.org/10.1016/j.jss.2025.112356>
- Sarkki, P. A. H., van 't Hoff-de Goede, M. S., van Leuken, M. A. G., van de Weijer, S. G. A., & Leukfeldt, E. R. (2025). Fear of cybercrime victimisation: Examining the relationship between fear and victimisation. *Journal of Criminal Justice*, 101(April), 102531. <https://doi.org/10.1016/j.jcrimjus.2025.102531>
- Skinner, S. S., Solms, R. Von, van Niekerk, J., & Delport, P. M. J. (2025). Cultivating Cybersecurity Awareness Among Seafarers. *Procedia Computer Science*, 263, 242–249. <https://doi.org/10.1016/j.procs.2025.07.030>
- Sturman, D., Auton, J. C., & Morrison, B. W. (2025). Security awareness, decision style, knowledge, and phishing email detection: Moderated mediation analyses. *Computers and Security*, 148(June 2024), 104129. <https://doi.org/10.1016/j.cose.2024.104129>
- Stylianou, I., Bountakas, P., Zarras, A., & Xenakis, C. (2025). Suspicious minds: Psychological techniques correlated with online phishing attacks. *Computers in Human Behavior Reports*, 19(July 2024), 100694. <https://doi.org/10.1016/j.chbr.2025.100694>
- Sushma, K. S. N., Viji, C., Rajkumar, N., Ravi, J., Stalin, M., & Najmusher, H. (2023). Healthcare 4.0: A Review of Phishing Attacks in Cyber Security. *Procedia Computer Science*, 230, 874–878. <https://doi.org/10.1016/j.procs.2023.12.045>
- Suzuki, A., Shikata, K., & Shimada, T. (2025). Patterns and predictors of cyber fraud victimization: Testing routine activity theory and general theory of crime in Japan. *Journal of Economic Criminology*, 9(April), 100186. <https://doi.org/10.1016/j.jeconc.2025.100186>
- Syah, R. (2023). Strategi Kepolisian Dalam Pencegahan Kejahatan Phising Melalui

- Media Sosial Di Ruang Siber. *Jurnal Impresi Indonesia*, 2(9), 864–870. <https://doi.org/10.58344/jii.v2i9.3594>
- VikingCloud. (2025). 207 Cybersecurity Stats And Facts For 2025. <https://www.vikingcloud.com/blog/cybersecurity-statistics>
- Weinz, M., Zannone, N., Allodi, L., & Apruzzese, G. (2025). The Impact of Emerging Phishing Threats: Assessing Quishing and LLM-generated Phishing Emails against Organizations. In *Proceedings of the ACM Conference on Computer and Communications Security* (Vol. 1, Issue 1). arXiv. <https://doi.org/10.1145/3708821.3736195>
- Wibowo, B., & Hidayat, T. (2024). Strategi Efektif dalam Meningkatkan Kesadaran Keamanan Siber terhadap Ancaman Phishing di Lingkungan Perusahaan PT. XYZ. *Jurnal Pengabdian Masyarakat Sultan Indonesia*, 2(1), 1–9. <https://doi.org/10.58291/abdisultan.v2i1.294>
- Wiranata, G. A., Ucu, Y., Subekti, & Sidarta, D. D. (2024). Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Phishing. *COURT REVIEW: Jurnal Penelitian Hukum* (e-ISSN: 2776-1916), 4(02), 13–25. <https://doi.org/10.69957/cr.v4i02.1503>
- Yasin, A., Fatima, R., JiangBin, Z., Afzal, W., & Raza, S. (2024). Can serious gaming tactics bolster spear-phishing and phishing resilience?: Securing the human hacking in Information Security. *Information and Software Technology*, 170(November 2023), 107426. <https://doi.org/10.1016/j.infsof.2024.107426>