INOMATEC: Jurnal Inovasi dan Kajian Multidisipliner Kontemporer
Vol. 01, No. 07, Tahun 2026, Hal. 482-488, ISSN: 3123-5573 (Online)

Analisis Serangan *Phishing* terhadap Keamanan Transaksi Digital di Indonesia: *Systematic Literature Review*

Evy Nurmiati[1], Dinda Zeinitta Quratuaini Putri[2]
[1,2]Program Studi Sistem Informasi, Universitas Islam Negeri Syarif Hidayatullah Jakarta
E-mail: evy.nurmiati@uinjkt.ac.id[1], dinda.zeinitta24@mhs.uinjkt.ac.id[2]

Article Info

Article history:

Received May 02, 2026
Revised May 04, 2026
Accepted May 06, 2026

Keywords:

Phishing,
Digital Transaction Security,
Social Engineering,
Machine Learning Detection,
Systematic Literature Review

ABSTRACT

Digital transactions in Indonesia grew rapidly, yet phishing attacks continue to pose a serious threat to financial security and personal data. This Systematic Literature Review (SLR) was conducted following the PRISMA protocol, selecting 15 national peer-reviewed journal articles from 100 identified sources across Google Scholar, Semantic Scholar, and Garuda databases. Three research questions were examined: (RQ1) what detection methods are most widely used; (RQ2) what attack vectors dominate in the Indonesian digital transaction context; and (RQ3) what mitigation strategies are most effective. Findings reveal that machine learning particularly Random Forest and ensemble methods achieves detection accuracy above 94%. Phishing via fake websites, social media cloning, and WhatsApp-based links are the dominant attack vectors. Mitigation efforts combining technical detection with digital literacy programs demonstrate the best outcomes. This review provides a structured foundation for future interdisciplinary research on phishing in Indonesia's digital economy.

Article Info

Article history:

Received May 02, 2026
Revised May 04, 2026
Accepted May 06, 2026

Kata Kunci:

Phishing,
Keamanan Transaksi Digital,
Social Engineering,
Deteksi Machine Learning,
Systematic Literature Review

ABSTRACT

Transaksi digital di Indonesia berkembang pesat, namun serangan *phishing* terus menjadi ancaman serius terhadap keamanan keuangan dan data pribadi pengguna. *Systematic Literature Review* (SLR) ini dilakukan menggunakan protokol PRISMA, dengan menyeleksi 15 artikel jurnal nasional *peer-review* dari 100 sumber yang teridentifikasi di Google Scholar, Semantic Scholar, dan Garuda. Tiga pertanyaan penelitian yang dikaji adalah: (RQ1) metode deteksi phishing apa yang paling banyak digunakan; (RQ2) vektor serangan apa yang dominan dalam konteks transaksi digital Indonesia; dan (RQ3) strategi mitigasi apa yang paling efektif. Temuan menunjukkan bahwa *machine learning* khususnya *Random Forest* dan *ensemble methods* mencapai akurasi deteksi di atas 94%. *Phishing* melalui situs palsu, kloning halaman media sosial, dan tautan berbahaya via WhatsApp merupakan vektor serangan dominan. Upaya mitigasi yang menggabungkan deteksi teknis dengan program literasi digital terbukti memberikan hasil terbaik. Tinjauan ini memberikan landasan terstruktur untuk penelitian interdisipliner *phishing* di ekosistem ekonomi digital Indonesia.

INOMATEC: Jurnal Inovasi dan Kajian Multidisipliner Kontemporer
Vol. 01, No. 07, Tahun 2026, Hal. 482-488, ISSN: 3123-5573 (Online)

Corresponding Author:

Dinda Zeinitta Quratuaini Putri
Universitas Islam Negeri Syarif Hidayatullah Jakarta
Email: dinda.zeinitta24@mhs.uinjkt.ac.id

PENDAHULUAN

Pertumbuhan ekonomi digital Indonesia dalam satu dekade terakhir telah mendorong transformasi masif dalam sistem keuangan nasional. Bank Indonesia (2024) mencatat volume transaksi digital perbankan meningkat lebih dari 35% secara tahunan, dengan nilai transaksi mencapai ratusan triliun rupiah per bulan. Namun, dinamika ini juga diiringi oleh meningkatnya ancaman kejahatan siber, khususnya serangan *phishing* yang menargetkan pengguna layanan keuangan digital.

Phishing adalah teknik serangan siber yang menggunakan rekayasa sosial (*social engineering*) untuk mengelabui korban agar menyerahkan informasi sensitif seperti kata sandi, nomor rekening, atau data kartu kredit, dengan cara menyamar sebagai entitas tepercaya (Gulo et al., 2021). Badan Siber dan Sandi Negara (BSSN, 2024) melaporkan terdapat 26.771.610 serangan *phishing* di Indonesia sepanjang tahun 2024, menjadikannya salah satu ancaman siber paling dominan secara nasional. Badan Siber dan Sandi Negara (BSSN, 2023) mencatat total trafik anomali siber di Indonesia sepanjang tahun 2023 mencapai 403.990.813 anomali, dengan *phishing* masuk dalam daftar ancaman siber paling dominan bersama ransomware dan APT (*Advanced Persistent Threat*)

Seiring meningkatnya sofistikasi serangan, respons dari komunitas peneliti pun berkembang. Pendekatan teknis berbasis *machine learning* mulai diadopsi untuk mendeteksi situs dan email *phishing* secara otomatis (Mahmud & Wirawan, 2024; Pradana & Susanto, 2026), sementara penelitian *socio-legal* mengkaji efektivitas regulasi UU ITE dan UU PDP dalam perlindungan korban (Gulo et al., 2021). Namun, belum tersedia tinjauan sistematis yang mengintegrasikan seluruh dimensi penelitian *phishing* dalam konteks transaksi digital Indonesia secara menyeluruh.

Penelitian ini bertujuan mengisi kesenjangan tersebut melalui *Systematic Literature Review* (SLR) menggunakan protokol *PRISMA*. Tiga pertanyaan penelitian (*Research Questions*) yang dirumuskan adalah:

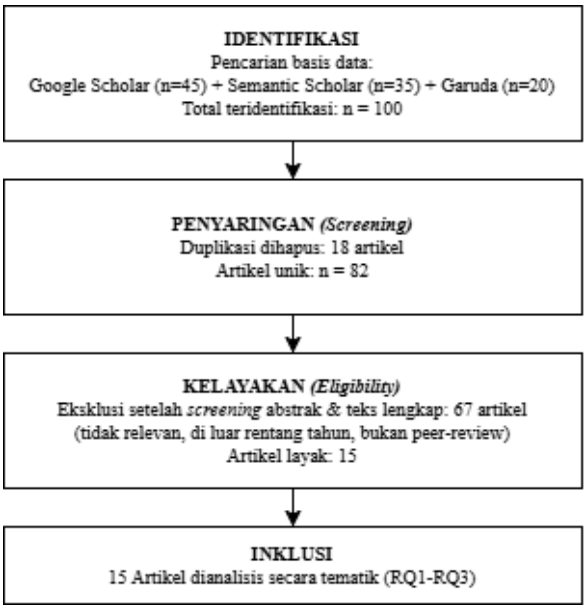
1. RQ1: Metode deteksi *phishing* apa yang paling banyak digunakan dalam literatur terkini?
2. RQ2: Vektor serangan *phishing* apa yang dominan dalam konteks transaksi digital di Indonesia?
3. RQ3: Strategi mitigasi apa yang paling efektif untuk mencegah serangan *phishing* pada transaksi digital?

METODE PENELITIAN

Penelitian ini menggunakan metode *Systematic Literature Review* (SLR) dengan protokol *PRISMA* (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*). Tahapan yang dilakukan meliputi: (1) Identifikasi pencarian literatur di Google Scholar, Semantic Scholar, dan Portal Garuda menggunakan kata kunci: "*phishing*", "*phising*", "*serangan phishing Indonesia*", "*deteksi phishing machine learning*", "*mobile banking phishing*", "*social engineering transaksi digital*"; (2) Penyaringan penghapusan duplikasi; (3) Kelayakan skrining berdasarkan kriteria inklusi/eksklusi; dan (4) Inklusi analisis tematik terhadap artikel terpilih.

Kriteria inklusi meliputi: jurnal nasional *peer-review* berbahasa Indonesia atau Inggris, diterbitkan 2021–2026, membahas *phishing* dalam konteks keamanan siber atau transaksi digital Indonesia, dan tersedia *full-text* dengan DOI valid. Kriteria eksklusi: artikel di luar rentang tahun, tidak *peer-review*, tidak relevan dengan topik, dan duplikat.

Dari total 100 artikel teridentifikasi, 18 artikel dihapus karena duplikasi sehingga menyisakan 82 artikel unik. Setelah skrining judul, abstrak, dan teks lengkap, 67 artikel dieksklusikan. Akhirnya, 15 artikel memenuhi seluruh kriteria dan dimasukkan dalam analisis. Diagram alur *PRISMA* disajikan pada Gambar 1.



Gambar 1. Diagram Alur Seleksi Artikel (PRISMA)

Sumber: Hasil Penelitian, 2026

HASIL DAN PEMBAHASAN

Proses seleksi menghasilkan 15 artikel nasional yang terverifikasi. Berdasarkan pertanyaan penelitian, distribusi artikel adalah: RQ1 (metode deteksi) sebanyak 6 artikel (40%), RQ2 (vektor serangan) sebanyak 5 artikel (33,3%), dan RQ3 (strategi mitigasi) sebanyak 4 artikel (26,7%). Keseluruhan artikel berasal dari basis data Garuda, Google Scholar, dan Semantic Scholar, diterbitkan antara tahun 2021–2026 oleh jurnal nasional terindeks. Tabel 1 menyajikan daftar lengkap artikel beserta informasi jurnal dan fokus kajiannya.

Tabel 1. Daftar Artikel Inklusif dalam SLR

No	Penulis	Tahun	Database	Fokus Kajian
1	Mahmud & Wirawan	2024	Garuda / Google Scholar	RQ1 – Membandingkan *Decision Tree, Random Forest*, dan KNN untuk deteksi URL *phishing*; akurasi terbaik RF 94,2%
2	Nugraha et al.	2022	Garuda / Google Scholar	RQ1 – *Ensemble stacking* meningkatkan akurasi deteksi *phishing* hingga 4,5% dibanding model tunggal
3	Windarni et al.	2023	Google Scholar	RQ1 – Teknik filter fitur URL berbasis ML mengurangi *false positive rate* deteksi *phishing*
4	Fitria & Mutijarsa	2023	Garuda / Google Scholar	RQ1 – Tinjauan metode AI (ML, DL, NLP) untuk deteksi ancaman siber termasuk *phishing* di Indonesia
5	Gumay et al.	2024	Garuda / Google Scholar	RQ1 & RQ2 – Analisis teknis serangan web *phishing* pada sistem informasi akademik; identifikasi kelemahan deteksi
6	Pradana & Susanto	2026	Google Scholar	RQ1 – Optimasi ekstraksi fitur URL meningkatkan presisi deteksi *phishing* model ML hingga 96,8%
7	Gulo et al.	2021	Garuda / Google Scholar	RQ2 – Memetakan modus serangan *phishing* (email, situs palsu, SMiShing) dalam konteks hukum UU ITE
8	Ansyafa et al.	2024	Google Scholar	RQ2 – Membuktikan kerentanan platform media sosial terhadap *phishing via cloning* halaman dan *email spoofing*
9	Wahyuni et al.	2022	Garuda / Google Scholar	RQ2 – Mengidentifikasi teknik *email spoofing* dan *credential harvesting* di media sosial profesional Indonesia
10	Ginting et al.	2023	Google Scholar	RQ2 – Mendokumentasikan modus phishing pada layanan *mobile banking* BRI: situs tiruan dan link berbahaya via WhatsApp
11	Ardy et al.	2024	Google Scholar	RQ2 & RQ3 – Mengidentifikasi vektor *phishing* di Instagram, Facebook, dan WhatsApp; menawarkan strategi pencegahan berbasis edukasi
12	Ramadhan & Purwandari	2023	Garuda / Google Scholar	RQ3 – Mengukur kesadaran keamanan pengguna *mobile banking* (KAB-HAISQ); merekomendasikan program *security awareness*
13	Huwaidi & Destya	2022	Garuda / Google Scholar	RQ3 – Strategi *human firewall* sebagai lapis pertahanan terhadap *social engineering* termasuk *phishing*
14	Nugroho et al.	2023	Garuda	RQ3 – Program edukasi terstruktur meningkatkan kemampuan masyarakat mengenali *link phishing* secara signifikan
15	Nur'aini & Simanjuntak	2025	Google Scholar	RQ3 – Pengetahuan anti-*phishing* dan pengalaman internet secara signifikan meningkatkan kewaspadaan pengguna *banking online* (TTAT model)

Sumber: Hasil Analisis, 2026

Pembahasan

RQ1: Metode Deteksi Phishing yang Paling Banyak Digunakan

Dari enam artikel yang menjawab RQ1, seluruhnya menggunakan pendekatan *machine learning* (ML) berbasis fitur URL sebagai metode deteksi utama. *Random Forest* merupakan algoritma yang paling banyak digunakan (4 dari 6 artikel), diikuti oleh *Decision Tree* (3 artikel) dan *K-Nearest Neighbor* (KNN) (2 artikel). Temuan ini konsisten dengan tren global yang menunjukkan dominasi *ensemble methods* dalam deteksi *phishing* (Nugraha et al., 2022).

Mahmud & Wirawan (2024) membandingkan *Decision Tree* (akurasi 83,3%), *Random Forest*, dan KNN, dengan *Random Forest* memberikan hasil terbaik pada *dataset* Indonesia. Pradana & Susanto (2026) melangkah lebih jauh dengan mengoptimalkan ekstraksi fitur URL dan berhasil mencapai presisi 96,8%. Nugraha et al. (2022) membuktikan bahwa metode *stacking ensemble* meningkatkan akurasi hingga 4,5% dibanding model tunggal. Windarni et al. (2023) menambahkan teknik *filter* untuk mengurangi dimensi fitur tanpa kehilangan akurasi. Fitria & Mutijarsa (2023) memberikan perspektif yang lebih luas dengan mensurvei berbagai metode *AI* termasuk *Deep Learning* dan *NLP* untuk deteksi ancaman siber secara umum.

Temuan penting dari RQ1: meskipun akurasi teknis tinggi, keterbatasan utama yang konsisten disebutkan lintas studi adalah kurangnya *dataset phishing* lokal Indonesia yang terstandarisasi. Hampir semua studi menggunakan *dataset* publik internasional (*PhishTank*, *UCI*), sehingga performa model pada konteks URL berbahasa Indonesia belum sepenuhnya tervalidasi.

RQ2: Vektor Serangan Phishing yang Dominan dalam Transaksi Digital Indonesia

Lima artikel yang menjawab RQ2 mengidentifikasi tiga vektor serangan dominan dalam konteks Indonesia: (1) situs web/URL palsu yang menyerupai platform resmi perbankan atau pemerintah; (2) serangan berbasis media sosial melalui kloning halaman dan *email spoofing*; dan (3) pesan instan berbahaya via WhatsApp yang menyertakan tautan *phishing*.

Gulo et al. (2021) memetakan modus *phishing* dalam kerangka hukum UU ITE, mengidentifikasi email palsu dan situs tiruan institusi keuangan sebagai vektor klasik. Ansyafa et al. (2024) dan Wahyuni et al. (2022) mendokumentasikan bahwa platform media sosial khususnya *Instagram, Facebook, dan LinkedIn* sangat rentan terhadap kloning halaman *login* menggunakan *tools* seperti *Zphisher* dan *Social Engineering Toolkit* (SET). Ginting et al. (2023) secara khusus menganalisis studi kasus Bank BRI dan menemukan bahwa WhatsApp menjadi media utama penyebaran *link phishing* ke nasabah, mengeksploitasi kepercayaan terhadap notifikasi resmi bank.

Ardy et al. (2024) memperluas temuan ini dengan mengidentifikasi evolusi vektor serangan ke arah konten visual palsu dan iklan berbayar di media sosial yang meniru merek perbankan. Secara keseluruhan, RQ2 menunjukkan bahwa *phishing* di Indonesia berevolusi dari serangan email konvensional menuju ekosistem *mobile* dan media sosial, sejalan dengan tingginya penetrasi *smartphone* dan platform digital di Indonesia (BSSN, 2024).

RQ3: Strategi Mitigasi Paling Efektif terhadap Serangan Phishing

Empat artikel yang menjawab RQ3 secara konsisten menunjukkan bahwa mitigasi paling efektif bersifat multilapis: menggabungkan solusi teknis, regulasi, dan peningkatan literasi pengguna. Tidak ada satu strategi tunggal yang mencukupi.

Ramadhan & Purwandari (2023) mengukur tingkat kesadaran keamanan informasi 299 pengguna *mobile banking* Indonesia menggunakan metode *HAIS-Q* dan mendapati skor rata-

rata 81,30% (kategori baik). Namun, dimensi perilaku hanya 78,06% (cukup), mengindikasikan celah antara pengetahuan dan tindakan nyata. Mereka merekomendasikan program *security awareness* terstruktur dan regulasi instalasi aplikasi ilegal. Huwaidi & Destya (2022) menawarkan konsep *human firewall* pelatihan berkelanjutan yang mengubah pengguna dari titik lemah menjadi lapisan pertahanan aktif terhadap *social engineering*.

Nugroho et al. (2023) mengevaluasi efektivitas program edukasi publik dan menemukan peningkatan signifikan kemampuan masyarakat mengidentifikasi *link phishing* pasca-intervensi. Nur'aini & Simanjuntak (2025) mengonfirmasi menggunakan *Technology Threat Avoidance Theory* (TTAT) bahwa pengalaman internet dan pengetahuan anti-*phishing* secara langsung meningkatkan kewaspadaan pengguna perbankan *online*. Temuan RQ3 menegaskan bahwa investasi dalam *human-centered security* bukan hanya sistem teknis adalah kunci mitigasi *phishing* yang berkelanjutan.

KESIMPULAN

Systematic Literature Review ini menganalisis 15 artikel jurnal nasional Indonesia terpilih guna menjawab tiga pertanyaan penelitian tentang serangan *phishing* dalam konteks transaksi digital di Indonesia. Berikut ringkasan jawaban atas masing-masing RQ:

1. RQ1:*Random Forest* dan *ensemble methods* merupakan metode deteksi *phishing* paling banyak digunakan dengan akurasi di atas 94%. Kebutuhan *dataset phishing* lokal Indonesia yang terstandarisasi menjadi tantangan utama ke depan.
2. RQ2: *Phishing* via situs web palsu, kloning halaman media sosial (Instagram, Facebook), dan tautan berbahaya melalui WhatsApp adalah vektor serangan yang paling dominan dalam ekosistem transaksi digital Indonesia.
3. RQ3: Strategi mitigasi paling efektif bersifat multidimensi: menggabungkan deteksi ML otomatis, program *security awareness* berbasis *human firewall*, dan penguatan regulasi UU PDP dalam perlindungan pengguna.

Penelitian ke depan direkomendasikan untuk: (1) membangun *dataset phishing* URL lokal Indonesia yang terstandarisasi untuk melatih model ML yang lebih kontekstual; (2) mengkaji efektivitas implementasi UU PDP No. 27 Tahun 2022 terhadap kasus *phishing* pasca-penerapan; dan (3) merancang intervensi edukasi keamanan siber yang terukur dan skalabel berbasis karakteristik pengguna Indonesia.

DAFTAR PUSTAKA

Ansyafa, K. Z., Fajarudin, M., Fadhil, M., & Neyman, S. N. (2024). Analisis keamanan media sosial terhadap serangan phising online menggunakan metode Zphisher dan Social Engineering Toolkit. *Journal of Internet and Software Engineering*, 1(4), 10. https://doi.org/10.47134/pjise.v1i4.2641

Ardy, L. A. F., 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

Badan Siber dan Sandi Negara (BSSN). (2023). *Lanskap Keamanan Siber Indonesia 2023*. Jakarta: BSSN. https://www.bssn.go.id/monitoring-keamanan-siber/

Badan Siber dan Sandi Negara (BSSN). (2024). *Lanskap Keamanan Siber Indonesia 2024*. Jakarta: BSSN. https://www.bssn.go.id/monitoring-keamanan-siber/

Bank Indonesia. (2024). *Laporan Perekonomian Indonesia 2024*. Jakarta: Bank Indonesia

Fitria, E. Y., & Mutijarsa, K. (2023). Survei penelitian metode kecerdasan buatan untuk mendeteksi ancaman teknologi serangan siber. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 10. https://doi.org/10.25126/jtiik.2023107341

Ginting, E., Sinaga, M. P., Nurdin, M. R., & Putra, M. D. (2023). Analisis ancaman phising terhadap layanan online perbankan (Studi Kasus Bank BRI). *UNES Journal of Scientech Research*, 8(1), 41–47. https://doi.org/10.31933/ujsr.v8i1

Gulo, A. S., Lasmadi, S., & Nawawi, K. (2021). Cyber crime dalam bentuk phising berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal of Criminal Law*, 1(2), 68–81. https://doi.org/10.22437/pampas.v1i2.9574

Gumay, B., Hendrawan, A. H., & Kusumah, F. S. F. (2024). Analisis dampak ancaman cybercrime terhadap data mahasiswa pada serangan web phising SIAK UIKA. *INFOTECH Journal*, 10(2), 297–305. https://doi.org/10.31949/infotech.v10i2.11463

Huwaidi, M. Z., & Destya, S. (2022). Mencegah serangan rekayasa sosial dengan human firewall. *Justin: Jurnal Sistem dan Teknologi Informasi*, 10(1). https://doi.org/10.26418/justin.v10i1.44280

Mahmud, A. F., & Wirawan, S. (2024). Deteksi phishing website menggunakan machine learning metode klasifikasi. *Sistemasi: Jurnal Sistem Informasi*, 13(4), 1368–1380. https://doi.org/10.32520/stmsi.v13i4.3456

Nugraha, A. F., Aziza, R. F. A., & Pristyanto, Y. (2022). Penerapan metode stacking dan random forest untuk meningkatkan kinerja klasifikasi pada proses deteksi web phishing. *Jurnal Infomedia: Teknik Informatika Multimedia Jaringan*, 7(1), 39. https://doi.org/10.30811/jim.v7i1.2959

Nugroho, H., Ihsan, M. N., 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/ecos-preneurs.v1i2.60

Nur'aini, R. J., & Simanjuntak, M. (2025). Phishing awareness and security concerns: Analyzing the role of anti-phishing knowledge and internet experience in online banking users. *Jurnal Ilmu Keluarga dan Konsumen*, 18(2). https://doi.org/10.24156/jikk.2025.18.2.121

Pradana, A., & Susanto, S. (2026). Implementasi model machine learning untuk deteksi phishing dengan pendekatan ekstraksi fitur yang dioptimalkan. *Jurnal Teknologi Informasi dan Multimedia*, 8(1), 27–40. https://doi.org/10.35746/jtim.v8i1.881

Ramadhan, T., & Purwandari, B. (2023). Analisis tingkat kesadaran keamanan informasi: Studi kasus pengguna aplikasi perbankan digital di Indonesia guna mencegah social engineering. *Syntax Idea*, 5(1), 86–98. https://doi.org/10.36418/syntax-idea.v5i1.2113

Wahyuni, S., Raazi, I. M., & Dwitawati, I. (2022). Analisis teknik penyerangan phishing pada social engineering terhadap keamanan informasi di media sosial profesional menggunakan kombinasi Black Eye dan Setoolkit. *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, 5(1), 49–55. https://doi.org/10.32672/jnkti.v5i1.3962

Windarni, V. A., Nugraha, A. F., Ramadhani, S. T. A., Istiqomah, D. A., Puri, F. M., & Setiawan, A. (2023). Deteksi website phishing menggunakan teknik filter pada model machine learning. *Information System Journal*, 6(1). https://doi.org/10.24076/infosjournal.2023v6i01.1268