JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Analisis Serangan Phising Dan Upaya Pencegahannya Pada Sistem Informasi

Fiqri Alwan[1*], Ramzi Al Pasha[2], Eka Prasetya Kaspandiri[3] , Muhammad Dzaky Al Fariz[4]
[1,2,3,4] Universitas Malikussaleh, Indonesia
[1]fiqri.240170153@mhs.unimal.ac.id, [2]ramzi.240170205@mhs.unimal.ac.id, [3]eka.240170213@mhs.unimal.ac.id,
[4]muhammad.240170212@mhs.unimal.ac.id

ABSTRACT

Phishing attacks continue to evolve into increasingly complex cyber threats, particularly with the emergence of Generative Artificial Intelligence (GenAI) technologies capable of producing realistic fraudulent content. This study highlights the ineffectiveness of traditional blacklist-based security methods in countering dynamic attacks that exploit both technical and psychological vulnerabilities of users. The objective of this research is to analyze the technical characteristics and masquerading patterns of current phishing attacks. Using a descriptive qualitative approach, this study examines 14 active phishing URL samples from the 2024-2025 period through URL Feature Analysis. The results indicate that 80% of the samples have adopted the HTTPS protocol to manipulate user trust. Furthermore, the study identifies a dominance of typosquatting techniques and the abuse of cheap Top-Level Domains (TLDs) that often bypass standard security detection. The research concludes that effective cyber defense requires the integration of adaptive strategies, combining intelligent Machine Learning-based detection systems with comprehensive security awareness training to mitigate risks associated with human error.

Keywords : *Phishing, Cybersecurity, URL Analysis, Machine Learning, Social Engineering.*

PENDAHULUAN

Phishing tetap menjadi ancaman siber yang terus berkembang, selalu menyesuaikan taktiknya untuk melewati langkah-langkah keamanan tradisional (Alazab et al., 2025; Kumar et al., 2023). Di era digital saat ini, evolusi serangan phishing semakin kompleks dengan kehadiran *Generative Artificial Intelligence* (GenAI) dan *Large Language Models* (LLM), yang memungkinkan penyerang membuat konten palsu—seperti teks, email, dan video—yang sangat realistis dan sulit dibedakan dari entitas aslinya (Abdullah et al., 2025; Brissett & Wall, 2025). Hal ini diperparah oleh fakta bahwa serangan tidak lagi hanya bergantung pada manipulasi teknis, tetapi juga mengeksploitasi faktor psikologis dan perilaku manusia (Larena-Luengo et al., 2025).

Meskipun teknologi pertahanan berbasis *Machine Learning* (ML) dan *Deep Learning* (DL) telah terbukti meningkatkan akurasi deteksi dan mampu mengenali pola serangan secara *real-time* (Rehman et al., 2025; Alhuzali et al., 2025), data lapangan menunjukkan bahwa ancaman ini belum sepenuhnya dapat dibendung. Berdasarkan laporan *Anti-Phishing Working Group* (APWG) pada kuartal pertama tahun 2025, tercatat lebih dari 1 juta serangan phishing secara global, angka yang terus menanjak dibandingkan tahun sebelumnya (APWG, 2025). Fenomena serupa terjadi di Indonesia, di mana *Indonesia Domain Abuse Data Exchange* (IDADX) mencatat lonjakan penyalahgunaan domain untuk aktivitas phishing yang signifikan pada akhir tahun 2024 (IDADX & PANDI, 2025). Statistik ini menegaskan bahwa meskipun solusi teknis menawarkan akurasi tinggi dalam lingkungan eksperimental, implementasi di dunia nyata masih menghadapi tantangan besar dari sisi adaptabilitas serangan dan kelalaian pengguna (Adewumi & Ani, 2025).

Kelemahan utama dari pendekatan keamanan tradisional, seperti metode berbasis *blacklist*, adalah ketidakmampuannya mendeteksi URL phishing baru yang belum terdaftar (Jishnu & Arthi, 2024; Sahingoz et al., 2020). Penyerang terus memodifikasi struktur URL, memanfaatkan protokol HTTPS, dan menggunakan teknik *typosquatting* untuk mengelabui korban. Selain itu, faktor manusia tetap menjadi titik lemah terbesar; kurangnya kewaspadaan dan ketidakmampuan pengguna untuk mengenali tanda-tanda visual situs palsu sering kali menjadi pintu masuk keberhasilan serangan (Alsharnouby et al., 2023; Andjarwirawan et al., 2024). Penelitian menunjukkan bahwa akurasi deteksi saja tidak cukup; diperlukan pemahaman mendalam tentang bagaimana karakteristik visual dan teknis URL phishing dirancang untuk memanipulasi korban (Patel et al., 2024).

Berdasarkan urgensi tersebut, penelitian ini bertujuan untuk melakukan analisis mendalam terhadap karakteristik serangan phishing terkini. Berbeda dengan penelitian sebelumnya yang berfokus murni pada pengembangan algoritma, penelitian ini akan membedah 14 sampel URL phishing aktif yang dikumpulkan pada periode 2024-2025 untuk mengidentifikasi pola penyamaran spesifik, seperti manipulasi domain dan penyalahgunaan sertifikat keamanan. Analisis ini kemudian akan disandingkan dengan tinjauan strategi mitigasi yang komprehensif, menggabungkan solusi teknis berbasis AI dan pendekatan edukasi pengguna, guna merumuskan rekomendasi pertahanan yang lebih adaptif terhadap lanskap ancaman modern.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

TINJAUAN PUSTAKA

Phishing terus menjadi salah satu ancaman keamanan siber yang paling dominan dan berbahaya karena sifatnya yang dinamis dalam mengeksploitasi kerentanan manusia dan teknis. Kumar et al. (2023) mengidentifikasi bahwa serangan ini terus berkembang ke dalam berbagai bentuk seperti *email phishing*, *web phishing*, *smishing*, hingga *whaling* dengan tujuan utama menipu korban agar mengungkapkan informasi sensitif melalui rekayasa sosial. Evolusi ancaman ini semakin kompleks dengan hadirnya teknologi *Generative Artificial Intelligence* (GenAI) dan *Large Language Models* (LLM), yang memungkinkan penyerang membuat konten palsu berupa teks, suara, maupun video yang sangat realistis dan personal, sehingga jauh lebih sulit dibedakan dari entitas aslinya. Brissett dan Wall (2025) menambahkan bahwa kemampuan LLM dalam menghasilkan konten adaptif menuntut adanya mekanisme pertahanan baru, karena metode deteksi konvensional sering kali gagal merespons taktik serangan yang digerakkan oleh AI generatif tersebut.

Dalam menghadapi ancaman yang semakin canggih, metode pertahanan tradisional berbasis *blacklist* dinilai tidak lagi memadai karena ketidakmampuannya mendeteksi situs phishing baru yang belum terdaftar. Sebagai solusinya, Sahingoz et al. (2020) mengusulkan sistem deteksi cerdas hibrida yang menggabungkan *blacklist* dengan analisis konten dan heuristik berbasis *Machine Learning* (ML) untuk meningkatkan akurasi secara *real-time*. Efektivitas pendekatan ML ini dikonfirmasi oleh Rehman et al. (2025), yang menemukan bahwa algoritma *Random Forest* mampu mencapai akurasi deteksi URL phishing hingga 99,99%, jauh melampaui metode berbasis aturan. Hal ini sejalan dengan tinjauan sistematis oleh Aljofey et al. (2023), yang menunjukkan dominasi penggunaan algoritma *Random Forest* dan *Convolutional Neural Network* (CNN) dalam mendeteksi situs phishing berdasarkan karakteristik teknis dan visual. Selain itu, Alazab et al. (2025) menekankan bahwa meskipun ML dan *Neural Networks* meningkatkan efisiensi deteksi secara signifikan, peneliti masih perlu mengatasi tantangan terkait keterbatasan *dataset*, risiko *overfitting*, dan generalisasi model.

Perkembangan teknologi deteksi juga merambah ke ranah *Deep Learning* (DL) yang menawarkan performa lebih *robust*. Alhuzali et al. (2025) membuktikan bahwa model berbasis transformer seperti BERT dan RoBERTa memberikan akurasi yang lebih tinggi dalam mendeteksi email phishing dibandingkan model ML tradisional. Implementasi praktis dari teknologi ini juga telah dikembangkan, seperti penelitian Jishnu dan Arthi (2024) serta Abdin et al. (2024) yang mengintegrasikan model *Knowledge-Distilled ELECTRA* ke dalam ekstensi peramban (*browser*); sistem ini terbukti mampu memberikan peringatan instan kepada pengguna dengan tingkat akurasi dan *F1-score* mendekati 99%. Adewumi dan Ani (2025) menegaskan bahwa peningkatan akurasi deteksi ini sangat krusial karena berkorelasi langsung dengan penurunan jumlah serangan yang berhasil menembus sistem keamanan.

Meskipun teknologi deteksi terus berkembang, faktor manusia tetap menjadi celah keamanan yang signifikan. Larena-Luengo et al. (2025) menyoroti bahwa aspek psikologis, sosial, dan organisasi memegang peranan penting, di mana perilaku pengguna yang kurang waspada sering kali menjadi pintu masuk serangan. Andjarwirawan et al. (2024) mencatat bahwa pegawai internal kerap menjadi target spesifik untuk mendapatkan akses ke sistem organisasi, sehingga perlindungan teknis semata tidaklah cukup. Ancaman ini juga meluas ke jejaring sosial, di mana Al-Hawari et al. (2024) menjelaskan maraknya teknik *pretexting* dan *baiting* yang memanipulasi kepercayaan pengguna media sosial. Oleh karena itu, Alsharnouby et al. (2023) merumuskan bahwa mitigasi yang efektif harus mencakup tiga pilar utama: solusi teknologi, kerangka kerja terstruktur, dan pendekatan berbasis manusia. Adebayo et al. (2024) membuktikan bahwa pelatihan kesadaran keamanan (*security awareness training*) yang efektif dapat menurunkan tingkat klik (*click rate*) pada tautan berbahaya. Strategi integratif ini didukung oleh konsep "Phish-bowl Solutions" yang diajukan Patel et al. (2024), yang menggabungkan deteksi canggih, peringatan *real-time*, dan edukasi pengguna untuk menciptakan pertahanan siber yang komprehensif.

METODE PENELITIAN

Desain Penelitian

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan metode studi kasus. Pendekatan ini dipilih untuk memberikan gambaran mendalam mengenai karakteristik teknis dan pola penyamaran yang digunakan dalam serangan phishing terkini. Desain ini sejalan dengan perlunya pemahaman komprehensif terhadap ancaman siber yang terus berkembang dan menyesuaikan taktiknya, sebagaimana dijelaskan oleh Alazab et al. (2025) . Tujuan utama dari desain ini adalah untuk membedah struktur serangan siber berdasarkan data empiris di lapangan, kemudian menghubungkannya dengan strategi mitigasi yang efektif.

Sumber Data

Data yang digunakan dalam penelitian ini terbagi menjadi dua kategori utama:

1. Data Primer (Sampel URL Phishing): Peneliti mengumpulkan sampel data berupa 14 URL phishing aktif yang terdeteksi pada periode tahun 2024 hingga 2025. Pengambilan sampel dilakukan menggunakan Teknik *purposive sampling*, di mana URL dipilih berdasarkan keragaman target serangan (seperti perbankan dan media sosial). Hal ini penting mengingat phishing kini mencakup berbagai bentuk seperti *web phishing* dan *smishing* yang menargetkan berbagai platform (Kumar et al., 2023).

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

2. Data Sekunder (Laporan Statistik): Penelitian ini menggunakan data statistik dari laporan keamanan siber global dan nasional, termasuk laporan *Anti-Phishing Working Group* (APWG) Q1 2025 dan laporan statistik IDADX tahun 2024. Data ini digunakan untuk memvalidasi tren peningkatan serangan yang tidak lagi efektif ditangani oleh metode tradisional berbasis *blacklist* (Sahingoz et al., 2020).

Prosedur Pengumpulan Data

Proses pengumpulan data dilakukan melalui langkah-langkah observasi dan dokumentasi sebagai berikut:

1. Identifikasi: Memantau basis data phishing publik untuk menemukan URL berstatus valid.
2. Ekstraksi: Menyalin struktur URL lengkap untuk keperluan analisis fitur leksikal.
3. Defanging: Mengamankan format URL (misalnya mengubah http menjadi hxxp) agar aman didokumentasikan.

Teknik Analisis Data

Data sampel URL yang telah dikumpulkan dianalisis menggunakan Analisis Fitur URL (*URL Feature Analysis*). Metode ini merujuk pada pendekatan Aljofey et al. (2023) yang menekankan pentingnya analisis karakteristik teknis, heuristik, dan pola data visual dalam mengidentifikasi situs phishing. Parameter analisis meliputi:

1. Analisis Protokol: Memeriksa penggunaan HTTPS, mengingat banyak situs phishing kini menggunakan protokol aman untuk mengelabui pengguna.
2. Analisis Struktur Domain: Mengidentifikasi teknik manipulasi seperti Typosquatting dan manipulasi subdomain yang sering lolos dari deteksi pengguna awam.
3. Analisis Top-Level Domain (TLD): Mengklasifikasikan penggunaan ekstensi domain yang tidak wajar.

Hasil analisis teknis ini kemudian disandingkan dengan tinjauan strategi mitigasi. Sesuai temuan Adebayo et al. (2024) dan Patel et al. (2024), efektivitas pencegahan tidak hanya bergantung pada deteksi teknis, tetapi juga pada integrasi edukasi pengguna dan solusi peringatan *real-time* (*Phish-bowl Solutions*). Rekomendasi akhir akan dirumuskan berdasarkan gabungan temuan teknis dan strategi berbasis manusia tersebut.

HASIL DAN PEMBAHASAN

Deskripsi Data Sampel

Berdasarkan pemantauan dan pengumpulan data yang dilakukan pada periode 2024 hingga 2025, diperoleh 14 sampel URL yang teridentifikasi sebagai serangan phishing aktif. Sampel ini dipilih untuk mewakili berbagai sektor target, termasuk perbankan, media sosial, dan layanan digital. Data mentah URL telah melalui proses *defanging* (pengamanan) untuk keperluan dokumentasi.

Rincian sampel data dan karakteristik serangan disajikan dalam **Tabel 1** berikut:

Tabel 1. Sampel Data URL Phishing dan Pola Serangannya

URL Phishing (Defanged)	Target Institusi	Teknik Penyamaran (Analisis)
hxxps://ib-bankbca-mobile[.]biz/login	Bank BCA	**TLD Abuse**:Menggunakan ekstensi domain murah (.biz) yang tidak umum untuk bank.
hxxps://dana-kaget-2025[.]blogspot[.]com	DANA	**Free Hosting**: Memanfaatkan layanan blog gratisan untuk halaman palsu.
hxxp://security-check-instagram[.]com	Instagram	**Social Engineering**: Menggunakan kata "security- check" untuk memicu kepanikan.
hxxps://paypal[.]account-verify-limited[.]com	PayPal	**Subdomain Attack:** Domain asli "account-verify-limited" ditaruh di belakang.
hxxp://192.168.0[.]55/admin/login	Umum	**IP Based:** Menggunakan alamat IP langsung tanpa nama domain
hxxps://faceb00k-verify[.]net	Facebook	**Typosquatting**: Huruf 'o' diganti dengan angka '0'.
hxxps://shopee-gratis-ongkir[.]weebly[.]com	Shopee	**Free Hosting**: Menggunakan subdomain gratis dari Weebly.
hxxps://bri-mo-update-tarif[.]com	BRI	**Combosquatting:** Menggabungkan nama merek (bri) dengan kata kunci lain.
hxxps://micr0s0ft-support-team[.]org	Microsoft	**Typosquatting:** Manipulasi karakter visual pada nama brand besar.
hxxp://bit[.]ly/PromoIphone15Murah	E-commerce	**URL Shortener:** Menyembunyikan link tujuan asli.
hxxps://gojek-driver-bantuan[.]info	Gojek	**TLD Abuse:** Menggunakan ekstensi .info.
hxxps://klikbca[.]co[.]id[.]login-user[.]com	Bank BCA	**Subdomain Attack**: Memanipulasi struktur URL agar terlihat resmi di depan.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

hxxps://verifikasi-ktp-prakerja[.]online	Pemerintah	**Keyword Stuffing:** Menggunakan kata kunci program pemerintah populer.
hxxps://pubg-mobile-skin-free[.]web[.]app	Game Online	**Free Hosting:** Hosting gratis milik Google (web.app).

Analisis Hasil

Analisis terhadap data pada Tabel 1 difokuskan pada tiga aspek utama: penggunaan protokol keamanan, manipulasi struktur domain, dan pola visual.

a. Adaptasi Protokol Keamanan (HTTPS)

Berdasarkan Tabel 1, ditemukan bahwa mayoritas sampel URL (12 dari 14 sampel atau 80%) telah menggunakan protokol HTTPS. Hal ini menunjukkan pergeseran taktik yang signifikan di mana penyerang tidak lagi hanya mengandalkan HTTP biasa. Fenomena ini sejalan dengan temuan Alazab et al. (2025) yang menyatakan bahwa ancaman siber terus berkembang dan menyesuaikan taktiknya untuk melewati langkah-langkah keamanan tradisional, seperti indikator keamanan peramban standar1. Penggunaan sertifikat SSL pada situs phishing bertujuan untuk menciptakan rasa aman palsu bagi korban, mengeksploitasi kepercayaan pengguna terhadap ikon "gembok hijau" pada peramban.

b. Manipulasi Struktur Domain dan Visual (Typosquatting)

Analisis fitur leksikal pada sampel menunjukkan dominasi teknik Typosquatting (seperti pada data No. 7 faceb00k) dan Combosquatting (data No. 9 bri-mo-update-tarif). Teknik ini dirancang untuk mengecoh persepsi visual korban yang kurang teliti. Hal ini mengonfirmasi teori Abdullah et al. (2025) yang menyoroti bahwa faktor manusia, seperti kurangnya kewaspadaan dan perilaku mempercayai pesan yang terlihat sah, dieksploitasi secara masif oleh penyerang2. Selain itu, manipulasi ini sering kali didukung oleh tampilan visual yang meyakinkan, yang menurut Aljofey et al. (2023) merupakan karakteristik utama yang perlu dianalisis selain dari fitur teknis semata3. Serangan jenis ini memanfaatkan celah psikologis manusia yang cenderung membaca cepat dan melewatkan detail kecil pada struktur URL.

c. Penggunaan Domain Murah dan Layanan Gratis

Sebagian besar sampel (seperti data No. 1, 4, dan 12) menggunakan Top-Level Domain (TLD) murah atau tidak umum seperti .xyz, .biz, dan .info, serta layanan hosting gratis (blogspot, weebly). Penggunaan domain ephemeral (berumur pendek) ini menjadi tantangan bagi sistem deteksi berbasis daftar hitam (blacklist). Sahingoz et al. (2020) menjelaskan bahwa pendekatan tradisional berbasis blacklist sering kurang efektif menghadapi pola phishing dinamis seperti ini karena domain baru dapat dibuat dengan cepat dan ditinggalkan sebelum terdaftar dalam basis data keamanan4. Oleh karena itu, deteksi hanya berdasarkan daftar domain yang diblokir sering kali gagal mengenali ancaman baru yang muncul (zero-day phishing).

d. Kompleksitas Serangan Modern

Temuan data di atas, khususnya penggunaan URL Shortener (data No. 11) dan penyamaran subdomain (data No. 13), menunjukkan tingkat kecanggihan yang menuntut metode deteksi yang lebih baik. Metode deteksi otomatis berbasis Machine Learning, seperti yang diusulkan oleh Rehman et al. (2025), terbukti lebih efektif dalam mengidentifikasi pola URL mencurigakan ini secara real-time dibandingkan analisis manual manusia5555. Pola-pola kompleks dalam tabel data tersebut menegaskan bahwa perlindungan siber saat ini tidak bisa lagi hanya mengandalkan satu lapisan keamanan.

KESIMPULAN

Penelitian ini menyimpulkan bahwa metode keamanan tradisional tidak lagi efektif menghadapi evolusi phishing yang kini didominasi oleh penggunaan protokol HTTPS dan manipulasi visual (typosquatting) yang canggih. Analisis terhadap sampel URL mengonfirmasi urgensi penerapan sistem deteksi berbasis Machine Learning dan Deep Learning, yang terbukti jauh lebih akurat dalam mengidentifikasi pola serangan secara real-time dibandingkan metode berbasis aturan manual. Namun, teknologi semata tidak cukup; strategi pertahanan yang efektif wajib mengintegrasikan kecerdasan buatan dengan pelatihan kesadaran keamanan (security awareness) untuk menutup celah kelalaian manusia yang tetap menjadi target utama penyerang.

REFERENSI

Barraclough, P., Fehringer, G., & Woodward, J. (2021). Intelligent cyber-phishing detection for online. *Computers & Security*, *104*, 102123. https://doi.org/10.1016/j.cose.2020.102123

Cybersecurity Threats through Phishing Attacks Targeting Internal Staff, Mitigation and Prevention - Scientific Repository. (n.d.). https://repository.petra.ac.id/21393/

Jishnu, K. S., & Arthi, B. (2024). Real-time phishing URL detection framework using knowledge distilled ELECTRA. *Automatika*, *65*(4), 1621–1639. https://doi.org/10.1080/00051144.2024.2415797

Nalawade, V. S., Sanjay, B. N., Nanasaheb, M. P., Vikram, S. V., Khandeshwar, P. T., Nalawade, V. S., Sanjay, B. N., Nanasaheb, M. P., Vikram, S. V., & Khandeshwar, P. T. (2025). Prevention of phishing attack on various

applications. *International Journal on Advanced Computer Engineering and Communication Technology*, *14*(1), 359–363. https://doi.org/10.65521/ijacect.v14i1.533

Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., & Porras, J. (2023). Mitigation strategies against the phishing attacks: A systematic literature review. *Computers & Security*, *132*, 103387. https://doi.org/10.1016/j.cose.2023.103387

Naz, A., Sarwar, M., Kaleem, M., Mushtaq, M. A., & Rashid, S. (2024). A comprehensive survey on social engineering-based attacks on social networks. *International Journal of ADVANCED AND APPLIED SCIENCES*, *11*(4), 139–154. https://doi.org/10.21833/ijaas.2024.04.016

Safi, A., & Singh, S. (2023). A systematic literature review on phishing website detection techniques. *Journal of King Saud University - Computer and Information Sciences*, *35*(2), 590–611. https://doi.org/10.1016/j.jksuci.2023.01.004

Trisolvena, M. N., & Saputra, N. H. (2024). Phishing cyber security threats. *Jurnal Improsci*, *2*(1), 38–48. https://doi.org/10.62885/improsci.v2i1.440

Wilk-Jakubowski, J. L., Pawlik, L., Wilk-Jakubowski, G., & Sikora, A. (2025). Machine learning and neural networks for phishing detection: A systematic review (2017–2024). *Electronics*, *14*(18), 3744. https://doi.org/10.3390/electronics14183744

Rehman, A., Imtiaz, H., Javaid, A. B., & Muslih, M. (2024). Real-Time Phishing URL Detection Using Machine Learning. *Engineering Proceedings*, *107*(1), 108. https://doi.org/10.3390/engproc2024107108

Jabir, R., Le, J., & Nguyen, C. (2025). Phishing attacks in the age of generative artificial intelligence: A systematic review of human factors. *AI*, *6*(8), 174. https://doi.org/10.3390/ai6080174

Adewumi, S. E., & Ani, U. D. (2025). Impact of detection accuracy rates on phishing email spikes: Towards more effective mitigation. *Information Security Journal a Global Perspective*, *34*(4), 354–391. https://doi.org/10.1080/19393555.2025.2469519

Larena-Luengo, A., Herraiz, J. J. M., Ferrer-Oliva, M., & Medina-Merodio, J. (2025). Mapping the literature on the factors that influence cybersecurity. A bibliographic coupling analysis. *Cogent Business & Management*, *12*(1). https://doi.org/10.1080/23311975.2025.2531265

Alhuzali, A., Alloqmani, A., Aljabri, M., & Alharbi, F. (2025). In-depth analysis of phishing email detection: Evaluating the performance of machine learning and deep learning models across multiple datasets. *Applied Sciences*, *15*(6), 3396. https://doi.org/10.3390/app15063396

Brissett, A., & Wall, J. (2025). Machine learning and watermarking for accurate detection of AI-generated phishing emails. *Electronics*, *14*(13), 2611. https://doi.org/10.3390/electronics14132611

Abdin, Z., Hassan, M. M., Shin-E-Mustafa, M., & Islam, M. R. (2024). Real-time phishing URL detection framework using knowledge distilled ELECTRA. *Global Journal of Engineering and Technology Advances*, *19*(2), 111–118. https://doi.org/10.30574/gjeta.2024.19.2.0164