ANALISIS KEMAMPUAN MASYARAKAT DALAM MENDETEKSI LINK PHISHING DENGAN METODE SPSS REGRESI LINEAR

Ayu Talenta Lumbatoruan, Nikita Aidina Hidayat, Siti Fatul Zahrani, Rahmawati
Teknik Informatika, Universitas Pamulang
Jalan Raya Puspitek, Buaran, Kec. Pamulang, Kota Tangerang Selatan, Banten 15310
dosen02394@gmail.com

ABSTRAK

Phishing merupakan salah satu bentuk kejahatan siber yang paling sering terjadi dan menargetkan masyarakat melalui manipulasi tautan berbahaya untuk memperoleh data pribadi secara ilegal. Rendahnya tingkat literasi digital menjadi faktor yang meningkatkan kerentanan masyarakat terhadap serangan tersebut. Penelitian ini bertujuan untuk menganalisis pengaruh pengetahuan masyarakat tentang phishing terhadap kemampuan mereka dalam mendeteksi tautan phishing. Metode penelitian menggunakan pendekatan kuantitatif dengan desain regresi linear sederhana. Data dikumpulkan melalui kuesioner daring yang melibatkan 106 responden dan dianalisis menggunakan perangkat lunak SPSS. Hasil penelitian menunjukkan adanya hubungan yang kuat antara pengetahuan dan kemampuan deteksi phishing dengan nilai koefisien korelasi (R) sebesar 0,797. Nilai koefisien determinasi (R^2) sebesar 0,636 menunjukkan bahwa pengetahuan berkontribusi sebesar 63,6% terhadap kemampuan responden dalam mendeteksi tautan phishing, sedangkan sisanya dipengaruhi oleh faktor lain di luar model penelitian. Uji signifikansi menghasilkan nilai $P < 0,001$ yang menandakan bahwa model regresi bersifat signifikan. Penelitian ini menyimpulkan bahwa peningkatan literasi digital berperan penting sebagai strategi preventif untuk memperkuat kemampuan masyarakat dalam menghadapi ancaman phishing dan meningkatkan keamanan siber.

***Kata kunci** : Phishing Detection, Cybersecurity, Digital Literacy, Linear Regression, SPSS*

1. PENDAHULUAN

Percepatan transformasi digital telah membawa perubahan signifikan dalam pola interaksi masyarakat, khususnya dalam pemanfaatan layanan berbasis internet dan media sosial. Di balik manfaat tersebut, muncul implikasi serius terhadap keamanan data pribadi yang menempatkan keamanan siber sebagai isu strategis. Tantangan ini menjadi semakin kompleks bagi kelompok masyarakat yang belum sepenuhnya memiliki literasi digital yang memadai, sehingga rentan terhadap berbagai bentuk kejahatan siber.

Salah satu ancaman siber yang paling dominan adalah phishing, yaitu teknik penipuan yang memanfaatkan manipulasi tautan palsu untuk memperoleh informasi sensitif seperti kredensial akun dan data keuangan. Serangan ini umumnya memanfaatkan kelengahan pengguna serta teknik *social engineering* yang menciptakan tekanan psikologis atau urgensi semu. Kondisi tersebut diperparah dengan tingginya aktivitas masyarakat di ruang digital. Berdasarkan laporan Badan Pusat Statistik pada Kuartal I-2023, tingkat penetrasi internet pada generasi Milenial dan Generasi Z mencapai 94,16%, dengan 84,37% di antaranya aktif menggunakan media sosial yang kerap menjadi medium penyebaran tautan phishing.

Berbagai penelitian terdahulu menunjukkan bahwa kesadaran dan perilaku keamanan siber masyarakat Indonesia masih tergolong rendah. Studi yang melibatkan 254 responden mengungkapkan adanya pengaruh faktor demografis terhadap kesadaran keamanan digital. Penelitian lain pada mahasiswa Universitas Jambi menemukan adanya kesenjangan antara tingkat pengetahuan yang tinggi dan praktik keamanan yang masih rendah. Sementara itu, penelitian di Universitas Islam Indonesia mengidentifikasi perbedaan kesadaran keamanan siber berdasarkan usia dan gender, di mana kelompok usia muda justru cenderung kurang peka terhadap indikasi ancaman siber. Temuan-temuan tersebut menegaskan bahwa pengetahuan saja belum tentu berbanding lurus dengan kemampuan deteksi ancaman, sehingga diperlukan analisis empiris yang lebih terukur.

Berdasarkan latar belakang tersebut, permasalahan utama dalam penelitian ini adalah masih tingginya kerentanan masyarakat terhadap serangan phishing yang diduga berkaitan dengan tingkat pemahaman mereka terhadap karakteristik dan mekanisme serangan tersebut. Hingga saat ini, masih terbatas penelitian kuantitatif yang secara spesifik mengukur seberapa besar pengaruh pengetahuan tentang phishing terhadap kemampuan masyarakat dalam mendeteksi tautan berbahaya secara empiris.

Penelitian ini bertujuan untuk menganalisis pengaruh tingkat pemahaman masyarakat mengenai phishing terhadap kemampuan mereka dalam mendeteksi tautan phishing. Secara khusus, penelitian ini bertujuan untuk mengukur kekuatan hubungan antara kedua variabel tersebut serta mengetahui besarnya kontribusi pengetahuan dalam membentuk kemampuan deteksi phishing.

Penelitian ini menggunakan pendekatan kuantitatif dengan desain analisis regresi linear sederhana. Data dikumpulkan melalui instrumen kuesioner daring yang melibatkan 106 responden dari berbagai latar belakang. Data yang diperoleh

selanjutnya dianalisis menggunakan perangkat lunak SPSS untuk menghasilkan statistik deskriptif dan inferensial, meliputi uji korelasi, koefisien determinasi, serta uji signifikansi model.

Melalui pendekatan kuantitatif dan analisis statistik yang sistematis, penelitian ini diharapkan mampu memberikan gambaran empiris mengenai hubungan antara pengetahuan phishing dan kemampuan deteksi tautan berbahaya. Hasil penelitian diharapkan dapat menjadi dasar bagi pemerintah, institusi pendidikan, dan pemangku kepentingan lainnya dalam merancang program literasi digital yang lebih efektif dan berbasis bukti. Dari sisi akademik, penelitian ini diharapkan dapat memperkaya kajian keamanan siber dengan pendekatan kuantitatif serta menjadi referensi bagi penelitian lanjutan dengan cakupan dan metode yang lebih luas.

2. TINJAUAN PUSTAKA

2.1. Konsep Phishing dan Psikologi *Social Engineering*

Phishing didefinisikan sebagai bentuk penipuan digital yang menggunakan manipulasi psikologis dan teknis untuk mengelabui pengguna agar mengungkapkan informasi sensitif. Serangan ini tidak hanya bergantung pada kecanggihan teknologi, tetapi lebih pada eksploitasi kelemahan kognitif manusia atau yang dikenal sebagai *human vulnerability*. Dalam ekosistem keamanan siber, *phishing* sering dikategorikan sebagai serangan semantik yang memanipulasi interpretasi pengguna terhadap konten digital.

Teknik ini tidak dapat dipisahkan dari konsep *Social Engineering* (rekayasa sosial). *Social engineering* bekerja dengan memanipulasi aspek psikologis korban seperti rasa takut, urgensi, rasa ingin tahu, atau kepercayaan pada otoritas agar mengambil keputusan impulsif tanpa verifikasi. Kehadiran *Generative AI* memperparah ancaman ini dengan memungkinkan penyerang membuat narasi *phishing* yang lebih personal, rapi secara tata bahasa, dan persuasif, sehingga semakin sulit dibedakan dari komunikasi yang sah. Oleh karena itu, pemahaman terhadap mekanisme psikologis ini menjadi fundamental dalam mendeteksi serangan.

2.2. Anatomi URL dan Indikator Deteksi Phishing

Kemampuan mendeteksi *phishing* sangat bergantung pada pengetahuan teknis mengenai struktur *Uniform Resource Locator* (URL). Sebuah URL *phishing* umumnya dirancang menggunakan teknik *Typosquatting* atau *Homograph Attack*, di mana penyerang mendaftarkan nama domain yang secara visual sangat mirip dengan domain asli (misalnya, mengganti huruf 'o' dengan angka '0').

Indikator utama yang harus dipahami masyarakat dalam mendeteksi tautan berbahaya meliputi:

a. Ketidaksesuaian Domain: Memeriksa apakah nama domain sesuai dengan organisasi yang diklaim.
b. Struktur Subdomain: Penyerang sering menggunakan subdomain panjang untuk menyembunyikan domain asli.
c. Protokol Keamanan: Meskipun protokol HTTPS kini juga banyak digunakan oleh situs phishing, ketiadaan enkripsi pada situs transaksi tetap menjadi indikator bahaya yang valid.
d. Urgensi Semu: Adanya elemen desain atau teks yang memaksa pengguna bertindak cepat.

Pengetahuan mendalam mengenai indikator-indikator teknis inilah yang menjadi variabel independen dalam penelitian ini, di mana tujuannya adalah menguji apakah penguasaan teori ini berkorelasi linear dengan kemampuan praktis deteksi.

2.3. Literasi Digital sebagai *Human Firewall*

Literasi digital dalam konteks keamanan siber bertransformasi dari sekadar keterampilan operasional menjadi *Security Awareness*. Konsep ini menempatkan manusia sebagai *"Human Firewall"* atau garis pertahanan terakhir ketika sistem keamanan teknis gagal memfilter ancaman.

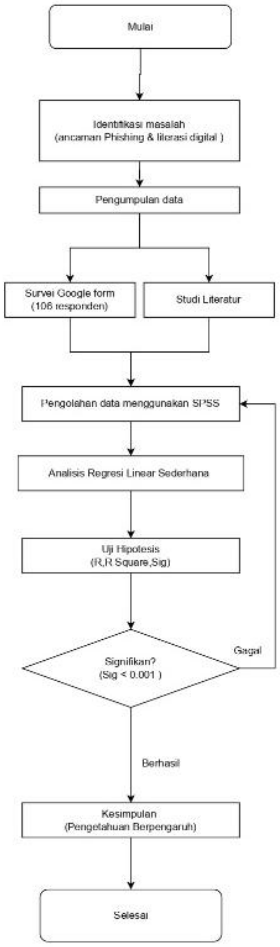
Studi menunjukkan bahwa literasi digital memiliki korelasi dengan demografi dan pengalaman pengguna. Misalnya, pengguna *e-wallet* atau layanan keuangan digital sering menjadi target utama karena dianggap memiliki aset likuid, namun sering kali memiliki tingkat kewaspadaan yang rendah. Oleh karena itu, pendekatan edukasi yang berkelanjutan, seperti gamifikasi atau simulasi serangan, dianggap lebih efektif dalam membangun memori jangka panjang terkait keamanan dibandingkan sekadar panduan tekstual. Akselerasi literasi ini krusial untuk menciptakan imunitas komunal terhadap serangan siber.

2.4. Penelitian Terdahulu dan Kebaruan Riset (State of the Art)

Peta penelitian mengenai deteksi *phishing* saat ini didominasi oleh pendekatan teknis. Sebagian besar literatur berfokus pada pengembangan sistem otomatis menggunakan algoritma *Machine Learning*, *Deep Learning*, hingga *Hybrid Framework* untuk memfilter URL jahat sebelum mencapai pengguna. Studi-studi ini berorientasi pada peningkatan akurasi mesin

Di sisi lain, penelitian yang berfokus pada faktor manusia (*human-centric*) masih terus berkembang. Beberapa studi menyoroti kerentanan spesifik pada demografi tertentu atau efektivitas metode pelatihan kesadaran. Kebaruan (*novelty*) dari penelitian ini terletak pada pendekatan kuantitatif eksplanatif menggunakan regresi linear untuk mengukur secara presisi seberapa besar kontribusi pengetahuan teoritis terhadap kompetensi praktis. Berbeda dengan pendekatan pengembangan algoritma, penelitian ini menegaskan bahwa secerdas apapun sistem deteksi dibuat, celah keamanan akan tetap terbuka jika pengguna (manusia) tidak memiliki kompetensi dasar untuk mengenali anomali pada tautan digital.

3. METODE PENELITIAN



Gambar 1. Alur Tahapan Penelitian

Penelitian ini disusun berdasarkan tahapan yang sistematis sebagaimana ditunjukkan pada Gambar 1 Alur Tahapan Penelitian, yang bertujuan untuk mengkaji kemampuan masyarakat dalam mendeteksi link phishing berdasarkan tingkat pengetahuan yang dimiliki.

3.1. Identifikasi Masalah

Tahap awal penelitian dimulai dengan proses identifikasi masalah. Masalah yang diangkat dalam penelitian ini adalah meningkatnya ancaman phishing sebagai salah satu bentuk kejahatan siber yang memanfaatkan rendahnya literasi keamanan digital masyarakat. Banyak pengguna internet masih kesulitan membedakan link asli dan link palsu, sehingga berpotensi menjadi korban penipuan digital. Oleh karena itu, penelitian ini berfokus pada hubungan antara pengetahuan phishing dan kemampuan masyarakat dalam mengenali link phishing.

3.2. Pengumpulan Data

Pada tahap ini, pengumpulan data dilakukan melalui dua pendekatan, yaitu:

a. Survei Kuesioner Online
   Data primer diperoleh melalui penyebaran kuesioner berbasis web menggunakan Google Form. Kuesioner disebarkan kepada masyarakat umum dan berhasil mengumpulkan 106 responden sebagai sampel penelitian. Responden berasal dari berbagai latar belakang usia, pendidikan, dan pengalaman penggunaan internet.
b. Studi Literatur
   Data sekunder diperoleh melalui studi literatur dari jurnal ilmiah, buku, dan sumber terpercaya yang membahas topik phishing, literasi digital, dan keamanan siber. Studi ini digunakan sebagai dasar penyusunan variabel, indikator penelitian, serta penguatan teori dalam pembahasan hasil.

3.3. Instrumen Penelitian

Instrumen penelitian berupa kuesioner tertutup yang disusun menggunakan skala Likert 1–5, dengan kategori:

1 = Sangat Tidak Setuju
2 = Tidak Setuju
3 = Netral
4 = Setuju
5 = Sangat Setuju

Variabel penelitian terdiri dari:

a. Variabel Independen (X): Pengetahuan Phishing, yang diukur melalui beberapa indikator (X1–X5) terkait pemahaman definisi phishing, ciri-ciri link palsu, dan kesadaran keamanan digital.
b. Variabel Dependen (Y): Kemampuan Mendeteksi Link Phishing, yang diukur melalui indikator (Y1–Y5) terkait kemampuan membedakan link asli dan palsu serta sikap kehati-hatian terhadap tautan mencurigakan.

Nilai masing-masing indikator kemudian dijumlahkan untuk membentuk skor total X_total dan Y_total.

3.4. Pengolahan Data Menggunakan SPSS

Data hasil kuesioner yang telah dikonversi ke bentuk numerik selanjutnya diolah menggunakan perangkat lunak SPSS. Sebelum analisis utama dilakukan, data terlebih dahulu melalui:

a. Uji Validitas, untuk memastikan setiap item pernyataan mampu mengukur variabel yang dimaksud.
b. Uji Reliabilitas, untuk menguji konsistensi instrumen penelitian dalam mengukur variabel.

Instrumen dinyatakan layak digunakan apabila memenuhi kriteria valid dan reliabel.

3.5. Analisis Regresi Linear Sederhana

Setelah data dinyatakan valid dan reliabel, dilakukan analisis regresi linear sederhana untuk mengetahui pengaruh variabel pengetahuan phishing (X) terhadap kemampuan mendeteksi link phishing (Y). Model regresi yang digunakan dirumuskan sebagai:

$$Y = \alpha + bX$$

di mana:
Y = Kemampuan mendeteksi link phishing

X = Pengetahuan phishing
α = Konstanta
b = Koefisien regresi

Analisis ini bertujuan untuk mengetahui arah hubungan, besarnya pengaruh, serta kekuatan prediksi variabel independen terhadap variabel dependen.

3.6. Pengujian Hipotesis

Pengujian hipotesis dilakukan melalui beberapa tahapan:

a. Uji Model Summary, untuk melihat kekuatan hubungan (R) dan kontribusi variabel X terhadap Y (R Square).
b. Uji ANOVA (Uji F), untuk menilai kelayakan model regresi secara keseluruhan.
c. Uji Coefficient (Uji t), untuk menguji signifikansi pengaruh variabel X terhadap Y secara parsial.

Kriteria pengambilan keputusan didasarkan pada nilai signifikansi (Sig.) dengan tingkat kepercayaan 95% (α = 0,05).

4. HASIL DAN PEMBAHASAN

Hasil penelitian menggunakan regresi linear sederhana untuk mengetahui pengaruh pengetahuan phishing (X) terhadap kemampuan masyarakat dalam mendeteksi link phishing (Y). Analisis dilakukan menggunakan SPSS dengan 106 responden. Output yang diperoleh dapat dilihat pada tabel Model Summary, ANOVA, dan Coefficients.

4.1. Model Summary

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.797[a]	.636	.632	2.44811

a. Predictors: (Constant), X_total

Gambar 2. Output Analisis Model Summary

Interpretasi

a. Berdasarkan output di atas, diperoleh koefisien korelasi (R) di angka 0,797. Data ini merefleksikan adanya hubungan linear yang sangat kuat antara variabel pengetahuan terhadap kompetensi deteksi.
b. Selanjutnya, angka 0,636 pada kolom R Square memberikan gambaran tentang besaran pengaruh efektif. Hal ini bermakna bahwa 63,6% variasi kemampuan responden dalam mengidentifikasi tautan palsu merupakan dampak langsung dari pemahaman teori mereka.
c. Adapun sisa persentase (36,4%) merupakan variabel residu atau faktor lain di luar lingkup riset ini, seperti intuisi personal atau jam terbang penggunaan internet.

4.2. Uji ANOVA (Uji F)

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1087.541	1	1087.541	181.461	<,001[b]
	Residual	623.299	104	5.993		
	Total	1710.840	105			

a. Dependent Variable: Y_total
b. Predictors: (Constant), X_total

Gambar 3. Output Analisis ANOVA (Uji F)

Interpretasi

a. Validitas model regresi terkonfirmasi melalui nilai probabilitas (Sig.) yang tercatat < 0,001.
b. Karena nilai tersebut jauh di bawah standar alpha 0,05, maka hipotesis dapat diterima. Artinya, variabel pengetahuan (X) terbukti berperan sebagai prediktor yang nyata dan simultan terhadap variabel kemampuan deteksi (Y).
c. Kesimpulannya, model ini dinyatakan fit (layak) untuk digunakan sebagai basis analisis.

4.3. Uji Coefficient (Uji t)

Coefficients[a]

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	t	Sig.
1	(Constant)	-2.205	1.577		-1.398	.165
	X_total	1.034	.077	.797	13.471	<,001

a. Dependent Variable: Y_total

Gambar 4. Output Analisis Coefficient (Uji t)

Interpretasi

a. Uji parsial menunjukkan signifikansi (Sig.) variabel X berada pada level < 0,001. Ini memvalidasi bahwa pengetahuan phishing memiliki dampak yang signifikan secara statistik.
b. Dari kolom *Unstandardized Coefficients*, didapatkan nilai B positif sebesar 1,034.
c. Angka ini merepresentasikan elastisitas hubungan: setiap terjadi kenaikan satu poin pada skor pengetahuan responden, maka skor kemampuan deteksi mereka diprediksi akan naik sebesar 1,034 poin.
d. Persamaan struktural yang terbentuk adalah Y = -2,205 + 1,034 X .
e. Konstanta negatif (-2,205) dengan status tidak signifikan (Sig. 0,165) memberikan wawasan menarik: tanpa adanya bekal pengetahuan (X=0), kemampuan deteksi seseorang secara statistik dianggap tidak ada atau tidak valid. Hal ini logis karena deteksi phishing adalah kompetensi kognitif yang harus dipelajari.

Berdasarkan pengujian hipotesis menggunakan regresi linear sederhana, terbukti bahwa variabel pengetahuan (X) memegang peranan krusial dan berpengaruh signifikan terhadap kompetensi responden dalam mengidentifikasi tautan phishing (Y). Data ini mengonfirmasi bahwa kedalaman wawasan seseorang terkait mekanisme, indikator, dan pola serangan siber berkorelasi lurus dengan ketajaman mereka dalam mengevaluasi validitas sebuah tautan.

Secara statistik, kekuatan hubungan ini tecermin dari nilai koefisien korelasi (R) sebesar 0,797, yang dalam kaidah statistik dikategorikan sebagai korelasi yang sangat kuat. Artinya, semakin tinggi literasi digital pengguna, semakin presisi pula akurasi deteksi yang mereka miliki.

Lebih lanjut, besaran pengaruh variabel independen terhadap dependen ditunjukkan oleh nilai koefisien determinasi (R2) sebesar 0,636. Angka ini mengimplikasikan bahwa 63,6% variabilitas kemampuan deteksi phishing pada masyarakat merupakan kontribusi langsung dari pemahaman kognitif mereka mengenai phishing. Sementara itu, sisa varians sebesar 36,4% dipengaruhi oleh residu atau faktor eksternal di luar cakupan model ini, seperti intuisi, pengalaman traumatis siber sebelumnya, tingkat skeptisisme individu, atau penggunaan alat bantu keamanan digital. Dominasi variabel pengetahuan ini memperkuat argumen bahwa intervensi edukasi teknis adalah strategi mitigasi yang paling berdampak.

Kelayakan model regresi ini juga telah teruji melalui analisis varians (ANOVA), di mana nilai F hitung tercatat sebesar 181,461 dengan probabilitas signifikansi (P) di bawah 0,001. Signifikansi statistik ini menegaskan bahwa pengetahuan phishing adalah prediktor yang valid dan andal untuk mengestimasi kemampuan pertahanan diri pengguna.

Pada analisis koefisien, nilai B positif sebesar 1,034 menunjukkan elastisitas hubungan yang linear; setiap eskalasi satu poin pada skor pengetahuan akan mendongkrak skor kemampuan deteksi sebesar 1,034 poin. Sebaliknya, nilai konstanta negatif (–2,205) yang tidak signifikan (Sig. 0,165) memberikan wawasan menarik: tanpa bekal pengetahuan dasar, kemampuan deteksi tautan berbahaya nyaris tidak eksis atau tidak dapat dijelaskan secara statistik. Hal ini logis, mengingat kewaspadaan terhadap phishing bukanlah insting alamiah, melainkan hasil dari proses kognitif dan pembelajaran

Riset ini menyajikan antitesis humanis terhadap pendekatan teknis murni. Jika dikomparasikan dengan literatur sebelumnya, seperti studi Daniel et al. [4] yang menitikberatkan pada pendekatan teknis *Machine Learning*, terdapat divergensi orientasi yang jelas. Ketika studi teknis tersebut mengagungkan akurasi mesin (hingga 96,29%), penelitian ini justru menempatkan kognisi manusia sebagai benteng pertahanan terakhir (*last resort*) saat filter teknologi gagal berfungsi.

Temuan ini melengkapi literatur yang ada dengan postulat bahwa teknologi canggih dan literasi manusia bukanlah substitusi, melainkan komplementer. Di tengah ekosistem digital Indonesia yang beragam, ketergantungan penuh pada deteksi otomatis tidaklah cukup. Ketika sistem keamanan gagal memfilter ancaman baik dalam bentuk tautan situs web maupun smishing (SMS phishing) pemahaman pengguna menjadi lapisan pertahanan terakhir (last line of defense). Oleh karena itu, sinergi antara pengembangan piranti lunak deteksi dan program edukasi literasi siber yang masif bagi masyarakat menjadi imperatif untuk menciptakan ekosistem digital yang tangguh.

5. KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa pengetahuan masyarakat mengenai phishing memiliki pengaruh yang sangat signifikan terhadap kemampuan mereka dalam mendeteksi tautan phishing. Hasil analisis regresi linear sederhana menggunakan SPSS membuktikan bahwa pengetahuan merupakan prediktor yang kuat, ditunjukkan oleh nilai signifikansi di bawah 0,001 yang berarti hipotesis penelitian diterima secara statistik. Hubungan antara pengetahuan dan kemampuan deteksi juga tergolong sangat kuat, dengan kontribusi sebesar 63,6%, yang mengindikasikan bahwa mayoritas kemampuan masyarakat dalam mengenali tautan berbahaya berasal dari tingkat literasi digital mereka. Persamaan regresi yang dihasilkan mempertegas bahwa tanpa pengetahuan yang memadai, kemampuan mendeteksi phishing hampir tidak terbentuk, sehingga deteksi phishing bukanlah kemampuan intuitif, melainkan kompetensi yang harus dipelajari melalui edukasi keamanan siber.

Meskipun demikian, penelitian ini juga menemukan bahwa masih terdapat 36,4% faktor lain di luar pengetahuan yang memengaruhi kemampuan deteksi phishing. Faktor-faktor tersebut diduga berkaitan dengan aspek psikologis, pengalaman penggunaan internet, tingkat kewaspadaan individu, serta pemanfaatan fitur keamanan digital. Oleh karena itu, penelitian selanjutnya disarankan untuk memasukkan variabel tambahan agar gambaran pengaruh terhadap kemampuan deteksi phishing menjadi lebih komprehensif. Selain itu, penggunaan metode analisis yang lebih kompleks seperti regresi linear berganda atau Structural Equation Modeling (SEM) juga direkomendasikan untuk melihat peran variabel demografis dan moderator lainnya.

Sebagai implikasi praktis, hasil penelitian ini menegaskan pentingnya peningkatan edukasi dan literasi keamanan siber di masyarakat, khususnya terkait ancaman phishing. Program sosialisasi dan pelatihan yang berfokus pada pengenalan ciri-ciri phishing perlu terus ditingkatkan agar masyarakat tidak hanya memiliki pengetahuan secara teoritis, tetapi juga mampu menerapkannya dalam situasi nyata. Dengan demikian, risiko menjadi korban kejahatan siber dapat diminimalkan secara lebih efektif

DAFTAR PUSTAKA

[1] M. S. Ansary, “Machine Learning-Based Detection of Spear Phishing Emails,” *Int. J. Comput. Appl.*, vol. 187, no. 24, pp. 15–20, 2025, doi: 10.5120/ijca2025925421.

[2] Yuliana, “the Importance of Cybersecurity Awareness for Children,” *Lampung J. Int. Law*,

vol. 4, no. 1, pp. 39–46, 2022, doi: 10.25041/lajil.v4i1.2526.

[3] S. E. Adewumi and U. D. Ani, "Impact of detection accuracy rates on phishing email spikes: Towards more effective mitigation," *Inf. Secur. J.*, vol. 34, no. 4, pp. 354–391, 2025, doi: 10.1080/19393555.2025.2469519.

[4] M. A. Daniel, S.-C. Chong, L.-Y. Chong, and K.-K. Wee, "Optimising Phishing Detection: A Comparative Analysis of Machine Learning Methods with Feature Selection," *J. Informatics Web Eng.*, vol. 4, no. 1, pp. 200–212, 2025, doi: 10.33093/jiwe.2025.4.1.15.

[5] A. K. Gwenhure and F. S. Rahayu, "Gamification of Cybersecurity Awareness for Non-IT Professionals: A Systematic Literature Review," *Int. J. Serious Games*, vol. 11, no. 1, pp. 83–99, 2024, doi: 10.17083/ijsg.v11i1.719.

[6] A. Safi and S. Singh, "A systematic literature review on phishing website detection techniques," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 2, pp. 590–611, 2023, doi: 10.1016/j.jksuci.2023.01.004.

[7] S. Vaithilingam and S. A. M. Shankar, "Enhancing Security in QR Code Technology Using AI: Exploration and Mitigation Strategies," *Int. J. Intell. Sci.*, vol. 14, no. 02, pp. 49–57, 2024, doi: 10.4236/ijis.2024.142003.

[8] P. Sari and T. Sutabri, "Analisis kejahatan online phising pada institusi pemerintah/pendidik sehari-hari," *J. Digit. Teknol. Inf.*, vol. 6, no. 1, p. 29, 2023, doi: 10.32502/digital.v6i1.5620.

[9] Q. E. ul Haq, M. H. Faheem, and I. Ahmad, "Detecting Phishing URLs Based on a Deep Learning Approach to Prevent Cyber-Attacks," *Appl. Sci.*, vol. 14, no. 22, 2024, doi: 10.3390/app142210086.

[10] I. A. Saputro, L. Sugiarto, and F. S. Nugraha, "Analisis Kesadaran Masyarakat Terhadap Bahaya Internet Phishing Menggunakan K-Means Clustering," *STRING (Satuan Tulisan Ris. dan Inov. Teknol.*, vol. 9, no. 2, p. 139, 2024, doi: 10.30998/string.v9i2.22404.

[11] A. Shaikh, M. Shaikh, and Srivaramangai R., "Smishing Detection: Combating SMS Phishing Attacks by Utilizing Machine-Learning Algorithms," *Int. J. Innov. Technol. Explor. Eng.*, vol. 14, no. 5, pp. 28–33, 2025, doi: 10.35940/ijitee.d1068.14050425.

[12] M. Schmitt and I. Flechais, "Digital deception: generative artificial intelligence in social engineering and phishing," *Artif. Intell. Rev.*, vol. 57, no. 12, 2024, doi: 10.1007/s10462-024-10973-2.

[13] T. M. Alotayan, "Awareness of Social Engineering Attacks and their Relation to the Ability to Persuade among users of Social Networking Sites," *J. Ecohumanism*, vol. 3, no. 7, pp. 2580–2592, 2024, doi: 10.62754/joe.v3i7.4662.

[14] N. Nelmiawati, M. Fani, H. Arif, H. Khaira, G. B. Ramadhan, and I. Afif, "Workshop Cybersecurity Awareness Meningkatkan Literasi Keamanan Digital di Wilayah Suburban Kepulauan Riau," *J. Pengabdi. Kpd. Masy. Politek. Negeri Batam*, vol. 5, no. 2, pp. 153–164, 2024, doi: 10.30871/abdimaspolibatam.v5i2.6821.

[15] R. J. van Geest, G. Cascavilla, J. Hulstijn, and N. Zannone, "The applicability of a hybrid framework for automated phishing detection," *Comput. Secur.*, vol. 139, no. February 2023, p. 103736, 2024, doi: 10.1016/j.cose.2024.103736.

[16] M. Mutlutürk, M. Wynn, and B. Metin, "Phishing and the Human Factor: Insights from a Bibliometric Analysis," *Inf.*, vol. 15, no. 10, 2024, doi: 10.3390/info15100643.

[17] M. S. Alif and A. R. Pratama, "Analisis Kesadaran Keamanan di Kalangan Pengguna E-Wallet di Indonesia," *J. Inf.*, vol. 2, no. 1, pp. 1–7, 2021, [Online]. Available: https://journal.uii.ac.id/AUTOMATA/article/view/17279