

Analisis Kesadaran dan Perilaku Mahasiswa IT Dalam Menghindari Ancaman *Phishing* Menggunakan Model TTAT

Shelly Pramudiawardani, Ghaida Syafa Azizah*, Amalia Rahmah

¹Program Studi Sistem Informasi, Sekolah Tinggi Teknologi Terpadu Nurul Fikri, Kota Depok, Indonesia

Email: ¹shelly@nurulfikri.ac.id, ^{2,*}ghai22223si@student.nurulfikri.ac.id, ³amalia.rahmah@nurulfikri.ac.id

Email Penulis Korespondensi: ghai22223si@student.nurulfikri.ac.id*

Submitted: 31/05/2026; Accepted: 09/07/2026; Published: 30/09/2026

Abstrak— *Phishing* merupakan ancaman siber berbasis rekayasa sosial yang terus menyasar mahasiswa sebagai pengguna aktif layanan digital kampus, seperti *email* akademik, *Learning Management System*, dan sistem administrasi daring. Penelitian ini bertujuan menganalisis kesadaran dan perilaku menghindari ancaman *phishing* mahasiswa IT di Kota Depok menggunakan *Technology Threat Avoidance Theory* (TTAT). Penelitian menggunakan pendekatan kuantitatif dengan desain survei *cross-sectional*. Instrumen penelitian berupa kuesioner skala Likert 1-4 yang disusun berdasarkan tujuh konstruk TTAT, yaitu *perceived severity*, *perceived susceptibility*, *safeguard effectiveness*, *safeguard cost*, *self-efficacy*, *avoidance motivation*, dan *avoidance behavior*. Data valid yang dianalisis berjumlah 307 responden dan diolah menggunakan SPSS melalui uji validitas, reliabilitas, asumsi klasik, serta regresi dua tahap. Hasil penelitian memberikan dukungan parsial terhadap model TTAT. Pengujian hipotesis dilakukan melalui dua tahap regresi, yaitu regresi tahap pertama untuk menguji faktor-faktor pembentuk *avoidance motivation* dan regresi tahap kedua untuk menguji pengaruh *avoidance motivation* terhadap *avoidance behavior*. Pada regresi tahap pertama, *self-efficacy* dan *safeguard effectiveness* berpengaruh signifikan terhadap *avoidance motivation*, sedangkan *perceived severity*, *perceived susceptibility*, dan *safeguard cost* tidak berpengaruh signifikan. Pada regresi tahap kedua, *avoidance motivation* terbukti berpengaruh signifikan terhadap *avoidance behavior*. Model regresi menunjukkan nilai R Square sebesar 0,734 pada tahap pertama dan 0,540 pada tahap kedua. Temuan ini menunjukkan bahwa upaya peningkatan perilaku menghindari *phishing* pada mahasiswa IT sebaiknya tidak hanya berfokus pada penyampaian bahaya *phishing*, tetapi juga diarahkan pada penguatan *self-efficacy* dan pemahaman terhadap efektivitas tindakan pengamanan digital.

Kata Kunci: *Phishing*; TTAT; Kesadaran Keamanan Siber; *Avoidance Motivation*; *Avoidance Behavior*

Abstract— *Phishing* is a social engineering-based cyber threat that continues to target university students as active users of campus digital services, including academic email, Learning Management Systems, and online administrative platforms. This study aims to analyze the awareness and phishing avoidance behavior of IT students in Depok City using the Technology Threat Avoidance Theory (TTAT). A quantitative approach with a cross-sectional survey design was employed. The research instrument consisted of a Likert scale questionnaire (1–4) developed based on the seven TTAT constructs: *perceived severity*, *perceived susceptibility*, *safeguard effectiveness*, *safeguard cost*, *self-efficacy*, *avoidance motivation*, and *avoidance behavior*. A total of 307 valid responses were analyzed using SPSS through validity testing, reliability testing, classical assumption testing, and two-stage regression analysis. The findings provide partial support for the TTAT model. Hypothesis testing was conducted in two regression stages: the first stage examined the factors shaping *avoidance motivation*, while the second stage assessed the effect of *avoidance motivation* on *avoidance behavior*. In the first-stage regression, *self-efficacy* and *safeguard effectiveness* were found to have a significant effect on *avoidance motivation*, whereas *perceived severity*, *perceived susceptibility*, and *safeguard cost* showed no significant effect. In the second-stage regression, *avoidance motivation* was proven to significantly influence *avoidance behavior*. The regression model yielded an R-square value of 0.734 in the first stage and 0.540 in the second stage. These findings suggest that efforts to improve phishing avoidance behavior among IT students should not solely focus on communicating the dangers of phishing, but should also be directed toward strengthening *self-efficacy* and enhancing students' understanding of the effectiveness of digital safeguarding measures.

Keywords: *Phishing*; TTAT; Cybersecurity Awareness; *Avoidance Motivation*; *Avoidance Behavior*

1. PENDAHULUAN

Transformasi digital di lingkungan pendidikan tinggi telah mengubah cara mahasiswa berinteraksi dengan layanan akademik. Aktivitas perkuliahan, administrasi, komunikasi, pengumpulan tugas, hingga akses informasi kampus semakin bergantung pada layanan digital seperti *email* institusi, *Learning Management System* (LMS), sistem informasi akademik, penyimpanan awan, dan berbagai platform komunikasi daring. Perubahan ini memberikan kemudahan dan efisiensi, tetapi sekaligus memperluas ruang paparan terhadap ancaman keamanan siber. Salah satu ancaman yang paling relevan dengan aktivitas digital mahasiswa adalah *phishing*, yaitu bentuk serangan rekayasa sosial yang menyamar sebagai pihak tepercaya untuk memperoleh informasi sensitif, seperti kredensial akun, data pribadi, atau akses ke sistem tertentu [1], [2]. Serangan ini tidak selalu bergantung pada kelemahan teknis sistem, tetapi lebih banyak memanfaatkan kelalaian, rasa percaya, urgensi, dan kebiasaan pengguna ketika memproses informasi digital [3].

Peningkatan pemanfaatan teknologi digital juga terjadi pada berbagai sektor, termasuk pendidikan tinggi, sehingga memperluas interaksi pengguna dengan berbagai layanan berbasis teknologi [4]. Seiring dengan perkembangan tersebut, ancaman *phishing* masih menjadi salah satu isu yang menonjol dalam lanskap keamanan

siber Indonesia. *Indonesia Threat Landscape Report 2024* mencatat lebih dari 4.046 kasus *phishing* dalam satu periode pemantauan [5]. Data dari *Indonesia Anti-Phishing Data Exchange* juga menunjukkan bahwa laporan *phishing* dapat mengalami lonjakan pada periode tertentu, sehingga ancaman ini bersifat dinamis dan adaptif terhadap perubahan situasi digital [6]. Selain itu, laporan BSSN menunjukkan bahwa semakin luasnya penggunaan akun dan layanan digital berpotensi meningkatkan risiko penyalahgunaan akses apabila tidak disertai dengan pengelolaan keamanan yang memadai [7].

Salah satu lingkungan yang memiliki tingkat paparan tinggi terhadap ancaman tersebut adalah pendidikan tinggi. Mahasiswa, dosen, dan tenaga kependidikan menggunakan berbagai akun digital yang terhubung dengan sistem akademik dan layanan institusional dalam aktivitas sehari-hari. Tingginya intensitas penggunaan akun tersebut menjadikan lingkungan perguruan tinggi sebagai target yang menarik bagi pelaku *phishing*. Laporan keamanan siber menunjukkan bahwa sektor pendidikan termasuk salah satu sasaran penting dalam kampanye *phishing* karena tingginya penggunaan akun institusional dan komunikasi berbasis *email* [8], [9]. Apabila akun akademik berhasil dikompromikan melalui serangan *phishing*, dampak yang ditimbulkan tidak hanya berupa kerugian bagi individu, tetapi juga berpotensi mengganggu keamanan dan keberlangsungan layanan digital kampus. Oleh karena itu, upaya mitigasi *phishing* tidak cukup dilakukan melalui penguatan teknologi keamanan semata, tetapi juga perlu didukung oleh peningkatan kesadaran dan perilaku keamanan pengguna.

Mahasiswa bidang *Information Technology* (IT) sering diasumsikan memiliki literasi digital yang lebih baik dibandingkan mahasiswa non-IT karena terbiasa menggunakan perangkat, aplikasi, jaringan, dan sistem berbasis teknologi. Namun, pengetahuan teknis tidak selalu menjamin perilaku keamanan yang konsisten. Beberapa studi menunjukkan bahwa faktor manusia tetap menjadi titik lemah dalam keamanan siber karena pengguna dapat mengambil keputusan yang tidak aman meskipun telah mengetahui risiko dasar dari sebuah ancaman [10], [11]. Dalam ancaman *phishing*, mahasiswa dengan latar belakang teknologi tetap dapat mengalami bias percaya diri berlebihan, terburu-buru membuka pesan, mengabaikan verifikasi *Uniform Resource Locator* (URL), atau merasa mampu membedakan pesan palsu tanpa pemeriksaan mendalam [12]. Artinya, penelitian mengenai mahasiswa IT tidak hanya perlu mengukur apakah mereka mengetahui *phishing*, tetapi juga perlu menjelaskan faktor apa yang membuat pengetahuan tersebut berubah menjadi motivasi dan perilaku menghindari ancaman *phishing*.

Penelitian ini tetap menggunakan istilah kesadaran karena fokus penelitian tidak hanya berada pada tindakan akhir, tetapi juga pada penilaian kognitif mahasiswa terhadap ancaman *phishing* dan cara menghadapinya. Dalam penelitian ini, kesadaran terhadap *phishing* tidak diposisikan sebagai konstruk terpisah di luar *Technology Threat Avoidance Theory* (TTAT), melainkan dipahami sebagai bagian dari penilaian mahasiswa terhadap ancaman dan tindakan perlindungan. Kesadaran tersebut direpresentasikan melalui *threat appraisal*, yaitu *perceived severity* dan *perceived susceptibility*, serta diperkuat oleh *coping appraisal*, yaitu *safeguard effectiveness*, *safeguard cost*, dan *self-efficacy*. Dengan demikian, istilah kesadaran dalam penelitian ini merujuk pada pemahaman mahasiswa terhadap risiko *phishing* sekaligus penilaian mereka terhadap kemampuan dan tindakan perlindungan yang dapat dilakukan.

Berbagai penelitian telah membahas ancaman *phishing* dari sudut pandang psikologis, perilaku, dan keamanan siber. Kerentanan terhadap *phishing* diketahui dipengaruhi oleh faktor psikologis dan perilaku pengguna, sementara faktor manusia tetap menjadi aspek dominan yang berkontribusi terhadap keberhasilan serangan *phishing* [2], [3]. Penelitian lainnya juga menunjukkan bahwa tingkat kesadaran keamanan terhadap ancaman *phishing* belum sepenuhnya merata pada pengguna internet [13]. Selain itu, penerapan *Technology Threat Avoidance Theory* (TTAT) menunjukkan bahwa *threat appraisal* dan *coping appraisal* dapat menjelaskan motivasi pengguna dalam menghadapi ancaman *phishing* [14]. Penelitian lain juga menunjukkan bahwa *self-efficacy* berperan penting dalam membentuk perilaku keamanan pengguna ketika menghadapi ancaman *phishing* melalui *email* [15].

Di Indonesia, TTAT juga telah digunakan untuk menjelaskan kesadaran perlindungan data privasi pada pengguna media sosial, sehingga menunjukkan relevansi model tersebut dalam menganalisis perilaku keamanan digital pengguna [16]. Penelitian lain menunjukkan bahwa *phishing awareness* tidak selalu berpengaruh signifikan terhadap *security concern*, sehingga memperkuat kebutuhan untuk menjelaskan mekanisme yang menghubungkan pengetahuan, motivasi, dan perilaku keamanan pengguna [17]. Meskipun demikian, sebagian kajian masih berfokus pada tingkat *awareness*, *perceived risk*, *security concern*, atau pengguna digital secara umum, sehingga kajian pada mahasiswa IT sebagai kelompok dengan tingkat paparan teknologi yang tinggi masih relatif terbatas. Oleh karena itu, masih diperlukan pengujian yang lebih spesifik mengenai bagaimana komponen *threat appraisal* dan *coping appraisal* membentuk *avoidance motivation*, serta bagaimana motivasi tersebut mendorong *avoidance behavior* pada mahasiswa IT. Dengan demikian, penelitian ini tidak berupaya mengisi kekosongan penelitian secara absolut, melainkan memberikan pengujian pada populasi yang lebih spesifik, yaitu mahasiswa IT di Kota Depok.

Technology Threat Avoidance Theory (TTAT) digunakan karena mampu menjelaskan proses kognitif pengguna dalam menghindari ancaman teknologi. TTAT memandang perilaku menghindari ancaman sebagai hasil dari dua proses utama, yaitu *threat appraisal* dan *coping appraisal* [18]. *Threat appraisal* mencakup *perceived severity* dan *perceived susceptibility*, sedangkan *coping appraisal* mencakup *safeguard effectiveness*, *safeguard cost*, dan *self-efficacy*. Kedua proses tersebut membentuk *avoidance motivation* yang kemudian mendorong

avoidance behavior [18], [19]. Dengan demikian, TTAT tidak hanya menjelaskan apakah pengguna menyadari adanya ancaman, tetapi juga bagaimana *threat appraisal* dan *coping appraisal* membentuk *avoidance motivation* yang kemudian mendorong *avoidance behavior*.

Kota Depok dipilih sebagai lokasi penelitian karena memiliki sejumlah perguruan tinggi dengan program studi Teknik Informatika dan Ilmu Komputer, seperti Universitas Indonesia, Sekolah Tinggi Teknologi Terpadu Nurul Fikri, Universitas Gunadarma, Universitas Bina Sarana Informatika, Universitas Nusa Mandiri, dan Universitas Muhammadiyah Jakarta Kampus Depok. Mahasiswa pada program studi tersebut menggunakan layanan digital kampus secara intensif, sehingga berpotensi menjadi target *phishing* melalui *email* akademik, tautan palsu, pesan administrasi, atau halaman login tiruan. Berdasarkan kondisi tersebut, penelitian ini bertujuan menganalisis kesadaran dan perilaku menghindari ancaman *phishing* mahasiswa IT di Kota Depok menggunakan model TTAT. Secara khusus, penelitian ini menguji pengaruh *perceived severity*, *perceived susceptibility*, *safeguard effectiveness*, *safeguard cost*, dan *self-efficacy* terhadap *avoidance motivation*, serta pengaruh *avoidance motivation* terhadap *avoidance behavior*. Kontribusi penelitian ini terletak pada penyediaan bukti empiris mengenai faktor-faktor yang memengaruhi perilaku menghindari ancaman *phishing* pada mahasiswa IT di Indonesia berdasarkan kerangka *Technology Threat Avoidance Theory* (TTAT), serta penyusunan rekomendasi praktis bagi perguruan tinggi dalam merancang edukasi keamanan siber yang lebih tepat sasaran.

2. METODOLOGI PENELITIAN

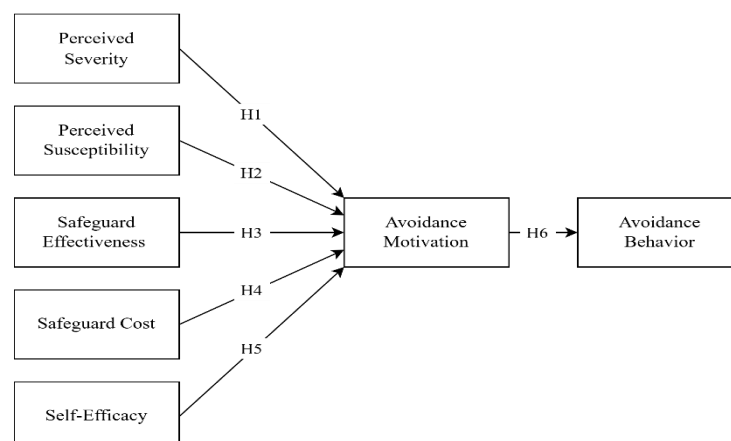
2.1 Tahapan Penelitian

Penelitian ini dilakukan melalui beberapa tahapan yang disusun secara sistematis agar proses pengumpulan dan analisis data sesuai dengan tujuan penelitian. Tahap pertama adalah identifikasi masalah, yaitu penentuan isu utama berupa risiko *phishing* pada mahasiswa IT yang aktif menggunakan layanan digital kampus. Tahap ini dilanjutkan dengan studi literatur untuk memahami konsep *phishing*, keamanan siber berbasis perilaku, dan model *Technology Threat Avoidance Theory* (TTAT). Studi literatur juga digunakan untuk mengidentifikasi *research gap*, terutama terkait keterbatasan penelitian yang hanya mengukur *awareness* tanpa menjelaskan hubungan antara persepsi ancaman, motivasi, dan perilaku menghindari ancaman.

Tahap berikutnya adalah perumusan model penelitian berbasis TTAT. Model ini menempatkan *perceived severity*, *perceived susceptibility*, *safeguard effectiveness*, *safeguard cost*, dan *self-efficacy* sebagai variabel yang memengaruhi *avoidance motivation*. Selanjutnya, *avoidance motivation* diuji pengaruhnya terhadap *avoidance behavior*. Setelah model dirumuskan, instrumen kuesioner disusun berdasarkan tujuh konstruk TTAT. Instrumen tersebut divalidasi melalui peninjauan isi agar setiap item pernyataan sesuai dengan konstruk yang diukur. Pengumpulan data dilakukan melalui survei kepada mahasiswa IT di Kota Depok. Data yang terkumpul kemudian diproses melalui tahap pembersihan data, pengkodean jawaban, dan pembentukan skor variabel komposit.

Setelah data siap, dilakukan uji validitas dan reliabilitas untuk memastikan kelayakan instrumen. Uji asumsi klasik kemudian dilakukan untuk memastikan model regresi memenuhi asumsi normalitas residual, bebas multikolinearitas, dan bebas heteroskedastisitas. Analisis utama dilakukan menggunakan regresi dua tahap. Tahap pertama menguji pengaruh lima variabel independen terhadap *avoidance motivation*, sedangkan tahap kedua menguji pengaruh *avoidance motivation* terhadap *avoidance behavior*. Hasil analisis kemudian diinterpretasikan berdasarkan kerangka TTAT dan dibandingkan dengan temuan penelitian terdahulu. Tahap akhir adalah penarikan kesimpulan, penyusunan implikasi praktis, keterbatasan penelitian, serta saran untuk penelitian selanjutnya.

2.2 Model Konseptual dan Hipotesis



Gambar 1. Model Konseptual Penelitian

Model konseptual penelitian yang ditunjukkan pada Gambar 1 mengadopsi struktur TTAT dengan penyesuaian pada ancaman *phishing* di lingkungan akademik. *Perceived severity* menggambarkan persepsi mahasiswa terhadap tingkat keseriusan dampak *phishing*, sedangkan *perceived susceptibility* menggambarkan persepsi mahasiswa mengenai kemungkinan dirinya menjadi korban *phishing*, kedua variabel tersebut merepresentasikan *threat appraisal*. *Safeguard effectiveness* menggambarkan keyakinan bahwa tindakan pengamanan seperti memeriksa URL, memverifikasi pengirim, menggunakan autentikasi dua faktor, dan memperbarui pengetahuan keamanan siber dapat mengurangi risiko *phishing*. *Safeguard cost* menggambarkan persepsi mengenai waktu, usaha, atau kerumitan dalam menerapkan tindakan keamanan. *Self-efficacy* menggambarkan keyakinan mahasiswa terhadap kemampuan diri dalam mengenali dan menghindari *phishing*, ketiga variabel tersebut merepresentasikan *coping appraisal*.

Dalam model ini, *avoidance motivation* berperan sebagai variabel mediasi yang menghubungkan *threat appraisal* dan *coping appraisal* dengan *avoidance behavior*. *Avoidance behavior* menjadi variabel dependen yang merepresentasikan tindakan mahasiswa dalam menghindari *phishing*, seperti tidak mengklik tautan mencurigakan, memeriksa alamat URL, tidak mengisi data pribadi pada situs tidak resmi, dan memverifikasi sumber pesan. Berdasarkan model tersebut, hipotesis penelitian dirumuskan sebagai berikut:

H1: *Perceived severity* berpengaruh positif terhadap *avoidance motivation*.

H2: *Perceived susceptibility* berpengaruh positif terhadap *avoidance motivation*.

H3: *Safeguard effectiveness* berpengaruh positif terhadap *avoidance motivation*.

H4: *Safeguard cost* berpengaruh negatif terhadap *avoidance motivation*.

H5: *Self-efficacy* berpengaruh positif terhadap *avoidance motivation*.

H6: *Avoidance motivation* berpengaruh positif terhadap *avoidance behavior*.

2.3 Populasi, Sampel, dan Instrumen Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan desain survei *cross-sectional*. Populasi penelitian adalah mahasiswa program studi Teknik Informatika dan Ilmu Komputer jenjang S1 pada enam perguruan tinggi di Kota Depok yang dipilih berdasarkan keberadaan program studi tersebut menurut data Pangkalan Data Pendidikan Tinggi (PDDIKTI), dengan total populasi sebanyak 2.676 mahasiswa [20]. Teknik pengambilan sampel yang digunakan adalah *purposive sampling* karena penelitian memerlukan responden dengan karakteristik tertentu, yaitu mahasiswa aktif program studi IT, menggunakan layanan digital kampus, dan pernah menerima pesan atau email mencurigakan. Jumlah sampel minimum dihitung menggunakan rumus Slovin dengan *margin of error* 6%, sehingga diperoleh kebutuhan minimum sebanyak 252 responden. Dalam pelaksanaan penelitian, data valid yang berhasil dianalisis berjumlah 307 responden.

Distribusi responden berdasarkan asal perguruan tinggi disajikan pada Tabel 1. Mayoritas responden berasal dari Sekolah Tinggi Teknologi Terpadu Nurul Fikri, sedangkan responden lainnya berasal dari Universitas Bina Sarana Informatika, Universitas Gunadarma, Universitas Indonesia, Universitas Nusa Mandiri, dan Universitas Muhammadiyah Jakarta Kampus Depok.

Tabel 1. Distribusi Responden Berdasarkan Perguruan Tinggi

Perguruan Tinggi	Jumlah	Persentase (%)
STT Terpadu Nurul Fikri	269	87,62
Universitas Bina Sarana Informatika	19	6,19
Universitas Gunadarma	7	2,28
Universitas Indonesia	4	1,30
Universitas Nusa Mandiri	4	1,30
Universitas Muhammadiyah Jakarta Kampus Depok	4	1,30
Total	307	100,00

Instrumen penelitian berupa kuesioner yang disusun berdasarkan tujuh konstruk TTAT, yaitu *perceived severity*, *perceived susceptibility*, *safeguard effectiveness*, *safeguard cost*, *self-efficacy*, *avoidance motivation*, dan *avoidance behavior*. Setiap konstruk awalnya diukur menggunakan lima item pernyataan sehingga total terdapat 35 item. Seluruh item menggunakan skala Likert 1–4, dengan skor 1 menunjukkan sangat tidak setuju dan skor 4 menunjukkan sangat setuju. Penggunaan skala tanpa opsi netral bertujuan mendorong responden memberikan sikap yang lebih tegas terhadap pernyataan yang diberikan [21].

Sebelum kuesioner disebarkan kepada responden, instrumen penelitian terlebih dahulu melalui proses validasi isi (*content validity*) oleh dosen yang memiliki kompetensi di bidang keamanan siber dan metodologi penelitian. Validasi ini bertujuan untuk memastikan bahwa setiap item pernyataan sesuai dengan definisi operasional dan mampu merepresentasikan konstruk TTAT yang diukur dalam penelitian. Hasil validasi

digunakan sebagai dasar penyempurnaan redaksi item sebelum kuesioner disebarkan kepada responden. Rincian operasionalisasi variabel yang menjadi dasar penyusunan instrumen penelitian disajikan pada Tabel 2.

Tabel 2. Operasionalisasi Variabel dan Indikator Penelitian

Variabel	Indikator	Jumlah Item
<i>Perceived Severity</i> (PS)	Persepsi terhadap tingkat keparahan dampak <i>phishing</i> , seperti kerugian data pribadi, penyalahgunaan akun, gangguan aktivitas akademik, dan risiko keamanan informasi	5
<i>Perceived Susceptibility</i> (PSS)	Persepsi mengenai kemungkinan menjadi korban <i>phishing</i> dan kerentanan terhadap serangan yang menasar pengguna layanan digital kampus	5
<i>Safeguard Effectiveness</i> (SGE)	Keyakinan terhadap efektivitas tindakan pengamanan, seperti memeriksa URL, memverifikasi pengirim, menggunakan autentikasi dua faktor, dan meningkatkan pengetahuan keamanan siber	5
<i>Safeguard Cost</i> (SC)	Persepsi mengenai biaya, waktu, usaha, dan tingkat kerumitan yang diperlukan untuk menerapkan tindakan pengamanan terhadap <i>phishing</i>	5
<i>Self-Efficacy</i> (SE)	Keyakinan terhadap kemampuan diri dalam mengenali karakteristik <i>phishing</i> , membedakan pesan asli dan palsu, serta mengambil tindakan perlindungan yang tepat	5
<i>Avoidance Motivation</i> (AM)	Motivasi atau dorongan untuk menghindari ancaman <i>phishing</i> melalui penerapan perilaku keamanan yang sesuai	5
<i>Avoidance Behavior</i> (AB)	Perilaku aktual dalam menghindari <i>phishing</i> , seperti tidak mengklik tautan mencurigakan, memverifikasi sumber pesan, dan melindungi informasi pribadi	5
Total		35

Berdasarkan Tabel 2, seluruh konstruk penelitian dioperasionalkan ke dalam 35 item pernyataan yang disusun sesuai konsep TTAT. Masing-masing konstruk awalnya terdiri atas lima item pernyataan yang diukur menggunakan skala Likert 1–4. Setelah dilakukan pengujian validitas, sebagian besar item memenuhi kriteria *Corrected Item-Total Correlation* $\geq 0,30$. Namun demikian, terdapat dua item yang tidak memenuhi kriteria validitas sehingga dikeluarkan dari analisis lanjutan. Rincian item yang dieliminasi disajikan pada Tabel 3.

Tabel 3. Item yang Dikeluarkan Berdasarkan Hasil Uji Validitas

Variabel	Item	Keputusan
<i>Safeguard Cost</i> (SC)	SC2	Dikeluarkan
<i>Self-Efficacy</i> (SE)	SE1	Dikeluarkan

Dengan dikeluarkannya item SC2 dan SE1, pembentukan skor komposit pada tahap analisis hanya menggunakan item-item yang memenuhi kriteria validitas. Langkah ini dilakukan untuk memastikan bahwa setiap konstruk diukur menggunakan indikator yang valid dan mampu merepresentasikan konsep yang diteliti secara lebih akurat.

2.4 Teknik Analisis Data

Data dianalisis menggunakan SPSS melalui beberapa tahap. Pertama, uji validitas dilakukan menggunakan *Corrected Item-Total Correlation* dengan batas nilai $\geq 0,30$. Item dinyatakan valid apabila memiliki korelasi yang memadai terhadap skor total konstruk [22]. Kedua, uji reliabilitas dilakukan menggunakan *Cronbach's Alpha* untuk melihat konsistensi internal antar item dalam setiap variabel. Secara umum, nilai *Cronbach's Alpha* $\geq 0,70$ menunjukkan reliabilitas yang baik, meskipun nilai yang mendekati batas tersebut masih dapat dipertimbangkan pada penelitian eksploratori atau perilaku [22], [23].

Setelah instrumen dinyatakan layak, dilakukan uji asumsi klasik yang meliputi normalitas residual, multikolinearitas, dan heteroskedastisitas. Normalitas residual diperiksa melalui Normal Q-Q Plot. Multikolinearitas diperiksa menggunakan nilai *Tolerance* dan *Variance Inflation Factor* (VIF), dengan kriteria *Tolerance* $> 0,10$ dan *VIF* < 10 . Heteroskedastisitas diperiksa melalui scatterplot antara nilai residual dan nilai

prediksi. Analisis regresi dilakukan dalam dua tahap. Regresi tahap pertama menguji pengaruh *perceived severity*, *perceived susceptibility*, *safeguard effectiveness*, *safeguard cost*, dan *self-efficacy* terhadap *avoidance motivation*. Regresi tahap kedua menguji pengaruh *avoidance motivation* terhadap *avoidance behavior*. Persamaan regresi yang digunakan adalah sebagai berikut:

$$AM = \alpha + \beta_1PS + \beta_2PSS + \beta_3SGE + \beta_4SC + \beta_5SE + \varepsilon$$

$$AB = \alpha + \beta_1AM + \varepsilon$$

AM adalah *avoidance motivation*, AB adalah *avoidance behavior*, PS adalah *perceived severity*, PSS adalah *perceived susceptibility*, SGE adalah *safeguard effectiveness*, SC adalah *safeguard cost*, SE adalah *self-efficacy*, α adalah konstanta, β adalah koefisien regresi, dan ε adalah *error*.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Uji Instrumen

Uji validitas dan reliabilitas dilakukan untuk memastikan bahwa instrumen penelitian layak digunakan dalam pengujian model TTAT. Hasil uji validitas menunjukkan bahwa sebagian besar item memiliki nilai *Corrected Item-Total Correlation* di atas 0,30. Namun, terdapat dua item yang tidak memenuhi kriteria, yaitu SC2 pada variabel *safeguard cost* dan SE1 pada variabel *self-efficacy*, sehingga kedua item tersebut dikeluarkan dari analisis. Item lain yang valid kemudian digunakan untuk membentuk skor variabel komposit.

Tabel 4. Hasil Uji Validitas dan Reliabilitas

Variabel	Item Valid	Cronbach's Alpha	Keterangan
<i>Perceived Severity</i>	5	0,835	Reliabel
<i>Perceived Susceptibility</i>	5	0,690	Cukup reliabel
<i>Safeguard Effectiveness</i>	5	0,844	Reliabel
<i>Safeguard Cost</i>	4	0,762	Reliabel
<i>Self-Efficacy</i>	4	0,756	Reliabel
<i>Avoidance Motivation</i>	5	0,894	Reliabel
<i>Avoidance Behavior</i>	5	0,854	Reliabel

Berdasarkan Tabel 4, mayoritas variabel memiliki nilai *Cronbach's Alpha* di atas 0,70. Hal ini menunjukkan bahwa instrumen memiliki konsistensi internal yang baik. *Perceived susceptibility* memiliki nilai *Cronbach's Alpha* sebesar 0,690. Meskipun sedikit di bawah 0,70, nilai tersebut masih dapat dikategorikan cukup reliabel karena mendekati batas reliabilitas yang disarankan. Dengan demikian, instrumen penelitian dinilai layak digunakan untuk analisis regresi. Pengeluaran item SC2 dan SE1 juga memperkuat kualitas pengukuran karena hanya item yang valid yang digunakan dalam pembentukan skor akhir.

3.2 Hasil Uji Asumsi Klasik

Uji asumsi klasik dilakukan sebelum analisis regresi untuk memastikan bahwa model memenuhi syarat dasar regresi linear. Uji normalitas residual menunjukkan nilai Kolmogorov-Smirnov sebesar 0,082 dengan signifikansi $< 0,001$ dan Shapiro-Wilk sebesar 0,965 dengan signifikansi $< 0,001$. Meskipun uji statistik formal menunjukkan nilai signifikansi di bawah 0,05, hasil Normal Q-Q Plot memperlihatkan bahwa titik-titik residual cenderung mengikuti garis diagonal. Dengan jumlah sampel yang relatif besar, penyimpangan dari normalitas yang terdeteksi melalui uji statistik formal masih dapat ditoleransi sehingga asumsi normalitas residual dianggap terpenuhi dan model dapat dilanjutkan pada tahap pengujian berikutnya.

Uji multikolinearitas menunjukkan bahwa seluruh variabel independen memiliki nilai *Tolerance* di atas 0,10 dan nilai VIF di bawah 10, sehingga tidak terdapat indikasi multikolinearitas yang mengganggu estimasi model. Hasil pengujian menunjukkan rentang *Tolerance* sebesar 0,266-0,842 dan rentang VIF sebesar 1,188-3,765. Selanjutnya, uji heteroskedastisitas melalui scatterplot menunjukkan bahwa titik-titik residual menyebar secara acak di atas dan di bawah sumbu nol serta tidak membentuk pola tertentu. Ringkasan hasil pengujian asumsi klasik dapat dilihat pada Tabel 5. Berdasarkan hasil tersebut, model regresi dinyatakan memenuhi asumsi klasik dan layak digunakan untuk pengujian hipotesis.

Tabel 5. Ringkasan Uji Asumsi Klasik

Jenis Uji	Nilai/Kriteria	Hasil	Keterangan
Normalitas residual	Kolmogorov-Smirnov = 0,082; Sig. < 0,001; Shapiro-Wilk = 0,965; Sig. < 0,001; Q-Q Plot mengikuti garis diagonal	Residual mendekati normal secara visual	Memenuhi asumsi normalitas residual
Multikolinearitas	<i>Tolerance</i> > 0,10; VIF < 10	<i>Tolerance</i> 0,266-0,842; VIF 1,188-3,765	Tidak terdapat multikolinearitas
Heteroskedastisitas	Scatterplot ZPRED-ZRESID tidak membentuk pola tertentu	Titik residual menyebar acak	Tidak terdapat indikasi heteroskedastisitas

3.3 Hasil Regresi Tahap Pertama

Regresi tahap pertama dilakukan untuk menguji pengaruh *perceived severity*, *perceived susceptibility*, *safeguard effectiveness*, *safeguard cost*, dan *self-efficacy* terhadap *avoidance motivation*. Hasil regresi tahap pertama disajikan pada Tabel 6.

Tabel 6. Hasil Regresi Tahap Pertama

Variabel	Beta	t	Sig.	Keputusan
<i>Perceived Severity</i>	0,029	0,680	0,497	H1 Ditolak
<i>Perceived Susceptibility</i>	0,040	1,127	0,261	H2 Ditolak
<i>Safeguard Effectiveness</i>	0,211	4,627	<0,001	H3 Diterima
<i>Safeguard Cost</i>	-0,059	-1,834	0,068	H4 Ditolak
<i>Self-Efficacy</i>	0,677	16,385	<0,001	H5 Diterima
R Square	0,734	-	-	
F	166,474	-	<0,001	Model signifikan

Berdasarkan Tabel 6, model regresi tahap pertama signifikan secara simultan dengan nilai $F = 166,474$ dan $p < 0,001$. Nilai *R Square* sebesar 0,734 menunjukkan bahwa *perceived severity*, *perceived susceptibility*, *safeguard effectiveness*, *safeguard cost*, dan *self-efficacy* secara bersama-sama mampu menjelaskan 73,4% variasi *avoidance motivation*. Nilai ini menunjukkan bahwa model memiliki kemampuan penjelasan yang kuat terhadap motivasi mahasiswa dalam menghindari *phishing*.

Secara parsial, hanya *safeguard effectiveness* dan *self-efficacy* yang berpengaruh signifikan terhadap *avoidance motivation*. *Safeguard effectiveness* memiliki nilai Beta 0,211, t 4,627, dan $p < 0,001$, sehingga H3 diterima. *Self-efficacy* memiliki nilai Beta 0,677, t 16,385, dan $p < 0,001$, sehingga H5 diterima. Nilai Beta *self-efficacy* merupakan yang terbesar dibandingkan variabel lain, sehingga *self-efficacy* menjadi prediktor paling dominan dalam membentuk *avoidance motivation*. Sementara itu, *perceived severity* memiliki $p = 0,497$, *perceived susceptibility* memiliki $p = 0,261$, dan *safeguard cost* memiliki $p = 0,068$. Ketiga nilai tersebut lebih besar dari 0,05, sehingga H1, H2, dan H4 ditolak.

3.4 Hasil Regresi Tahap Kedua

Regresi tahap kedua dilakukan untuk menguji pengaruh *avoidance motivation* terhadap *avoidance behavior*. Hasil regresi tahap kedua disajikan pada Tabel 7.

Tabel 7. Hasil Regresi Tahap Kedua

Variabel	Beta	t	Sig.	Keputusan
<i>Avoidance Motivation</i>	0,735	18,913	<0,001	H6 Diterima
R Square	0,540	-	-	
F	357,709	-	<0,001	Model signifikan

Berdasarkan Tabel 7, model regresi tahap kedua signifikan dengan nilai $F = 357,709$ dan $p < 0,001$. Nilai R^2 sebesar 0,540 menunjukkan bahwa *avoidance motivation* mampu menjelaskan 54% variasi *avoidance behavior*. Hasil ini menunjukkan bahwa motivasi mahasiswa untuk menghindari *phishing* memiliki kontribusi yang kuat dalam membentuk kecenderungan perilaku menghindari ancaman yang dilaporkan responden.

Secara parsial, *avoidance motivation* memiliki nilai *standardized* beta 0,735, t 18,913, dan $p < 0,001$. Dengan demikian, H_6 diterima. Artinya, semakin tinggi motivasi mahasiswa dalam menghindari *phishing*, semakin tinggi pula kecenderungan mereka untuk menunjukkan perilaku menghindari ancaman, seperti tidak mengklik tautan mencurigakan, memverifikasi sumber pesan, memperhatikan alamat URL, dan tidak mengisi data pribadi pada situs tidak resmi.

3.5 Pembahasan

Hasil penelitian menunjukkan bahwa *perceived severity* tidak berpengaruh signifikan terhadap *avoidance motivation*. Temuan ini mengindikasikan bahwa *perceived severity* yang dimiliki mahasiswa belum cukup untuk mendorong *avoidance motivation*. Dengan kata lain, meskipun responden memahami konsekuensi yang dapat ditimbulkan oleh *phishing*, seperti pencurian akun, penyalahgunaan data pribadi, atau gangguan terhadap aktivitas akademik, *perceived severity* tidak menjadi faktor yang menentukan dalam pembentukan *avoidance motivation*. Hasil ini menunjukkan bahwa pemahaman mengenai dampak ancaman belum tentu diikuti oleh dorongan yang kuat untuk menerapkan tindakan perlindungan. Temuan tersebut sejalan dengan penelitian sebelumnya yang menunjukkan bahwa persepsi ancaman yang tinggi tidak selalu berpengaruh terhadap motivasi individu dalam menghindari serangan *phishing* [17].

Variabel *perceived susceptibility* juga tidak berpengaruh signifikan terhadap *avoidance motivation*. Hasil ini menunjukkan bahwa tingkat *perceived susceptibility* yang dimiliki responden belum mampu meningkatkan *avoidance motivation*. Salah satu kemungkinan penyebabnya adalah karakteristik responden yang berasal dari program studi IT sehingga memiliki tingkat paparan teknologi dan pemahaman keamanan digital yang relatif baik. Kondisi tersebut dapat membuat responden merasa lebih mampu mengenali ancaman *phishing*, sehingga *perceived susceptibility* tidak menjadi faktor utama yang mendorong *avoidance motivation*. Temuan ini menunjukkan bahwa persepsi mengenai kemungkinan menjadi korban *phishing* belum tentu menghasilkan dorongan untuk melakukan perlindungan apabila responden merasa memiliki kemampuan yang memadai dalam menghadapi ancaman tersebut. Hasil ini mendukung penelitian sebelumnya yang menunjukkan bahwa *perceived susceptibility* tidak selalu menjadi prediktor yang kuat dalam membentuk motivasi menghadapi ancaman siber [17].

Berbeda dengan dua variabel sebelumnya, *safeguard effectiveness* terbukti berpengaruh positif dan signifikan terhadap *avoidance motivation*. Hasil ini menunjukkan bahwa semakin tinggi *safeguard effectiveness*, semakin tinggi pula *avoidance motivation* yang dimiliki mahasiswa. Temuan tersebut mengindikasikan bahwa mahasiswa memiliki kecenderungan untuk menerapkan tindakan perlindungan ketika mereka meyakini bahwa tindakan tersebut mampu memberikan manfaat yang nyata dalam mengurangi risiko *phishing*. Bentuk tindakan tersebut dapat berupa memeriksa URL sebelum mengakses suatu halaman, memverifikasi identitas pengirim, maupun menggunakan autentikasi tambahan pada akun digital. Temuan ini menunjukkan bahwa keyakinan terhadap efektivitas tindakan perlindungan merupakan faktor penting dalam mendorong motivasi penghindaran ancaman. Hasil tersebut sejalan dengan penelitian sebelumnya yang menunjukkan bahwa *safeguard effectiveness* berperan penting dalam membentuk motivasi penghindaran terhadap ancaman siber [19].

Pada penelitian ini, *safeguard cost* tidak berpengaruh signifikan terhadap *avoidance motivation*. Hasil tersebut menunjukkan bahwa *safeguard cost* yang dirasakan responden tidak menjadi hambatan utama dalam membentuk *avoidance motivation*. Kondisi ini dapat dipengaruhi oleh karakteristik mahasiswa IT yang telah terbiasa menggunakan berbagai teknologi digital sehingga langkah-langkah pengamanan dianggap sebagai bagian dari aktivitas yang wajar dan tidak memerlukan usaha yang berlebihan. Dengan demikian, waktu, tenaga, maupun tingkat kerumitan yang diperlukan untuk menerapkan tindakan perlindungan tidak menjadi pertimbangan utama dalam menghadapi ancaman *phishing*. Temuan ini mengindikasikan bahwa *safeguard cost* bukan faktor yang dominan dalam membentuk *avoidance motivation*. Hasil tersebut sejalan dengan penelitian sebelumnya yang menunjukkan bahwa ketika pengguna memiliki kemampuan teknologi yang memadai, *safeguard effectiveness* dan *self-efficacy* cenderung lebih berpengaruh dibandingkan *safeguard cost* dalam membentuk motivasi perlindungan terhadap ancaman siber [18], [19].

Variabel *self-efficacy* merupakan faktor yang memiliki pengaruh paling dominan terhadap *avoidance motivation*. Hasil ini menunjukkan bahwa semakin tinggi *self-efficacy*, semakin tinggi pula *avoidance motivation* mahasiswa dalam menghadapi ancaman *phishing*. Temuan tersebut mengindikasikan bahwa keyakinan terhadap kemampuan diri menjadi faktor yang sangat penting dalam membentuk motivasi perlindungan. Mahasiswa yang merasa mampu mengenali karakteristik *phishing*, membedakan pesan yang sah dan mencurigakan, serta mengambil tindakan yang tepat ketika menghadapi ancaman cenderung memiliki motivasi yang lebih tinggi untuk

melindungi dirinya. Besarnya pengaruh *self-efficacy* menunjukkan bahwa kemampuan yang dirasakan oleh individu memiliki peran yang lebih kuat dibandingkan persepsi terhadap ancaman itu sendiri. Temuan ini mendukung penelitian sebelumnya yang menunjukkan bahwa *self-efficacy* merupakan salah satu faktor utama yang mendorong individu untuk menerapkan perilaku keamanan informasi secara konsisten [15], [19].

Selanjutnya, *avoidance motivation* terbukti berpengaruh positif dan signifikan terhadap *avoidance behavior*. Hasil ini menunjukkan bahwa semakin tinggi *avoidance motivation*, semakin tinggi pula kecenderungan mahasiswa untuk menerapkan *avoidance behavior* dalam aktivitas digital sehari-hari. Bentuk *avoidance behavior* tersebut dapat berupa memverifikasi identitas pengirim, memeriksa URL sebelum mengakses tautan, menghindari situs yang mencurigakan, serta tidak memberikan informasi pribadi kepada pihak yang tidak dapat diverifikasi. Temuan ini mendukung konsep utama dalam *Technology Threat Avoidance Theory* (TTAT) yang menjelaskan bahwa *avoidance motivation* merupakan faktor yang secara langsung mendorong terbentuknya *avoidance behavior*. Dengan demikian, *avoidance motivation* menjadi mekanisme yang menjembatani pengaruh *threat appraisal* dan *coping appraisal* terhadap *avoidance behavior* [18], [19].

4. KESIMPULAN

Penelitian ini menerapkan *Technology Threat Avoidance Theory* (TTAT) untuk menganalisis kesadaran dan perilaku mahasiswa IT dalam menghindari ancaman *phishing* di Kota Depok. Hasil penelitian menunjukkan bahwa model TTAT memberikan dukungan parsial dalam menjelaskan pembentukan *avoidance motivation* dan *avoidance behavior*. Pada regresi tahap pertama, *safeguard effectiveness* dan *self-efficacy* terbukti berpengaruh signifikan terhadap *avoidance motivation*, sedangkan *perceived severity*, *perceived susceptibility*, dan *safeguard cost* tidak menunjukkan pengaruh signifikan. Nilai *R Square* sebesar 0,734 menunjukkan bahwa kelima variabel tersebut secara bersama-sama mampu menjelaskan 73,4% variasi *avoidance motivation*, sehingga model memiliki kemampuan penjelasan yang kuat terhadap motivasi mahasiswa dalam menghindari *phishing*. Selanjutnya, pada regresi tahap kedua, *avoidance motivation* terbukti berpengaruh signifikan terhadap *avoidance behavior* dengan nilai *R Square* sebesar 0,540, yang berarti motivasi menghindari ancaman memiliki kontribusi kuat dalam menjelaskan variasi perilaku menghindari *phishing* pada mahasiswa IT.

Temuan tersebut menunjukkan bahwa kesadaran mahasiswa terhadap ancaman *phishing* tidak hanya ditentukan oleh pemahaman mengenai tingkat keparahan dan kemungkinan terjadinya ancaman, tetapi juga oleh keyakinan terhadap kemampuan diri (*self-efficacy*) serta efektivitas tindakan pengamanan (*safeguard effectiveness*). Faktor-faktor tersebut terbukti memiliki peran yang lebih besar dalam membentuk *avoidance motivation* yang kemudian mendorong terbentuknya *avoidance behavior*. Dengan demikian, perilaku menghindari *phishing* pada mahasiswa IT lebih kuat dipengaruhi oleh konstruk *coping appraisal*, khususnya *self-efficacy* dan *safeguard effectiveness*, dibandingkan konstruk *threat appraisal*. Secara praktis, hasil penelitian ini mengindikasikan bahwa edukasi keamanan siber di perguruan tinggi tidak cukup hanya menekankan bahaya *phishing*, tetapi perlu diarahkan pada penguatan keterampilan praktis mahasiswa, peningkatan *self-efficacy*, serta pemahaman terhadap efektivitas tindakan pengamanan digital. Penelitian ini memiliki keterbatasan karena hanya berfokus pada mahasiswa IT di Kota Depok, menggunakan *purposive sampling*, dan mengandalkan data self-report, sehingga generalisasi hasil perlu dilakukan secara hati-hati dan perilaku responden dalam penelitian ini belum tentu sepenuhnya mencerminkan perilaku aktual dalam situasi *phishing* nyata. Penelitian selanjutnya dapat memperluas wilayah responden, membandingkan mahasiswa IT dan non-IT, menggunakan simulasi *phishing* atau eksperimen untuk mengukur perilaku aktual, serta mempertimbangkan pendekatan longitudinal atau *Structural Equation Modeling* (SEM) untuk menguji hubungan antarvariabel secara lebih komprehensif.

REFERENCES

- [1] National Institute of Standards and Technology, "Phishing – Glossary," CSRC Glossary – NIST. Accessed: Jan. 05, 2026. [Online]. Available: <https://csrc.nist.gov/glossary/term/phishing>
- [2] L. Ribeiro, I. S. Guedes, and C. S. Cardoso, "Which Factors Predict Susceptibility to Phishing? An Empirical Study," *Computers & Security*, vol. 136, 2024, doi: 10.1016/j.cose.2023.103558.
- [3] M. Mutlutürk, M. Wynn, and B. Metin, "Phishing and the Human Factor: Insights from a Bibliometric Analysis," *Information*, vol. 15, no. 10, 2024, doi: 10.3390/info15100643.
- [4] P. C. Verhoef *et al.*, "Digital Transformation: A Multidisciplinary Reflection and Research Agenda," *Journal of Business Research*, vol. 122, pp. 889–901, 2021, doi: 10.1016/j.jbusres.2019.09.022.
- [5] SOCRadar Cyber Intelligence Inc., "Indonesia Threat Landscape Report 2024." Accessed: Nov. 20, 2025. [Online]. Available: <https://socradar.io/resources/report/indonesia-threat-landscape-report-2024/>
- [6] Indonesia Anti-Phishing Data Exchange, "Statistik Laporan Phishing Periode 2022–2025," Indonesia Anti-Phishing Data Exchange. Accessed: Jan. 08, 2026. [Online]. Available: <https://idadx.id/>
- [7] Badan Siber dan Sandi Negara, "Lanskap Keamanan Siber Indonesia 2023," 2023. Accessed: Jan. 05, 2026. [Online]. Available: <https://educsirt.kemendikdasmen.go.id/portal/berita/197>

- [8] European Union Agency for Cybersecurity (ENISA), “Enisa Threat Landscape 2023.” Accessed: Nov. 20, 2025. [Online]. Available: [https://www.enisa.europa.eu/sites/default/files/publications/ENISA Threat Landscape 2023.pdf](https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf)
- [9] A. Pearson, R. Rath, G. Simches, B. Timberlake, R. Magaw, and J. Wilbur, “Phishing Campaigns Targeting Higher Education Institutions,” Google Cloud. Accessed: Jan. 10, 2026. [Online]. Available: <https://cloud.google.com/blog/topics/threat-intelligence/phishing-targeting-higher-education/>
- [10] M. M. Quchi, M. Hakimi, and A. W. Fazil, “Human Factors in Cybersecurity: An in Depth Analysis of User Centric Studies,” *Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)*, vol. 3, no. 01, pp. 20–33, 2024, doi: 10.58471/esaprom.v3i01.
- [11] D. Jampen, G. Gür, T. Sutter, and B. Tellenbach, “Don’t Click: Towards an Effective Anti-Phishing Training. A Comparative Literature Review,” *Human-centric Computing and Information Sciences*, vol. 10, no. 1, 2020, doi: 10.1186/s13673-020-00237-7.
- [12] S. Das, C. Nippert-Eng, and L. J. Camp, “Evaluating User Susceptibility to Phishing Attacks,” *Information and Computer Security*, vol. 30, no. 1, pp. 1–18, 2022, doi: 10.1108/ICS-12-2020-0204.
- [13] N. Vadila and A. R. Pratama, “Analisis Kesadaran Keamanan Terhadap Ancaman Phishing,” *Automata*, vol. 2, no. 2, pp. 1–4, 2023.
- [14] I. Daila Sari, D. Hariyadi, R. Sahtyawan, and N. I. Kusumaningtyas, “Analisis Tingkat Security Awareness-Personal Threat Terhadap Ancaman Phishing Dengan Metode Technology Threat Avoidance Theory (TTAT),” *Teknomatika: Jurnal Informatika dan Komputer*, vol. 16, no. 2, pp. 49–55, 2023, doi: 10.30989/teknomatika.v16i2.1250.
- [15] A. K. Gwenthure, “University Students’ Security Behavior Against Email Phishing Attacks: Insights from the Health Belief Model,” *Journal of Cybersecurity*, vol. 11, no. 1, 2025, doi: 10.1093/cybsec/tyaf034.
- [16] A. Rifai, A. Meliyani, P. Chyntia, and I. A. Sakti, “Penerapan Metode Technology Threat Avoidance Theory Terhadap Tingkat Kesadaran Data Privasi Pengguna Media Sosial,” *Journal of Information System Research (JOSH)*, vol. 4, no. 3, pp. 1026–1032, 2023, doi: 10.47065/josh.v4i3.3081.
- [17] R. J. Nur’aini and M. Simanjuntak, “Phishing Awareness and Security Concerns: Analyzing the Role of Anti-Phishing Knowledge and Internet Experience in Online Banking Users,” *Jurnal Ilmu Keluarga dan Konsumen*, vol. 18, no. 2, pp. 121–133, 2025, doi: 10.24156/jikk.2025.18.2.121.
- [18] H. Liang and Y. Xue, “Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective,” *Journal of the Association for Information Systems*, vol. 11, no. 7, pp. 394–413, 2010, doi: 10.17705/1jais.00232.
- [19] N. A. G. Arachchilage, S. Love, and K. Beznosov, “Phishing Threat Avoidance Behaviour: An Empirical Investigation,” *Computers in Human Behavior*, vol. 60, pp. 185–197, 2016, doi: 10.1016/j.chb.2016.02.065.
- [20] Kemdiktisaintek, “Pangkalan Data Pendidikan Tinggi (PDDIKTI).” Accessed: Nov. 17, 2025. [Online]. Available: <https://pddikti.kemdiktisaintek.go.id/>
- [21] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*, 3rd ed. Bandung: Alfabeta, 2021.
- [22] I. Ghazali, *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, 10th ed. Semarang: Badan Penerbit Universitas Diponegoro, 2021.
- [23] J. F. Hair Jr., W. C. Black, B. J. Babin, and R. E. Anderson, *Multivariate Data Analysis*, 8th ed. Hampshire: Cengage Learning, 2019.