Analisis Mediasi *Intuitive Decision Style* dan Moderasi *Phishing Email Knowledge* antara *Information Security Awareness* terhadap *Phising Detection Confidence* pada Karyawan Kampus XYZ

Muh. Bafadhal Kurnia Alamsyah[1], Candiwan Candiwan[2]
[1] Manajemen Bisnis Telekomunikasi & Informatika, Fakultas Ekonomi dan Bisnis, Universitas Telkom, Indonesia, alamsyahbafadhal@student.telkomuniversity.ac.id
[2] Manajemen Bisnis Telekomunikasi & Informatika, Fakultas Ekonomi dan Bisnis, Universitas Telkom, Indonesia, candiwan@telkomuniversity.ac.id

Abstrak
Perkembangan teknologi informasi telah membawa manfaat besar sekaligus tantangan yang signifikan, salah satunya adalah meningkatnya serangan phishing yang menyasar institusi pendidikan. Penelitian ini bertujuan untuk menganalisis pengaruh information security awareness terhadap phishing detection confidence pada karyawan Kampus XYZ, dengan mempertimbangkan peran mediasi intuitive decision style dan moderasi phishing email knowledge. Penelitian ini menggunakan pendekatan kuantitatif dengan metode survei terhadap 120 karyawan. Instrumen penelitian berupa kuesioner dengan skala Likert yang mengukur kesadaran keamanan informasi, gaya pengambilan keputusan intuitif, pengetahuan phishing, dan kepercayaan diri dalam mendeteksi phishing. Data dianalisis menggunakan teknik uji mediasi dan moderasi. Hasil penelitian menunjukkan bahwa information security awareness memiliki pengaruh langsung maupun tidak langsung terhadap phishing detection confidence melalui intuitive decision style, serta pengaruh tersebut diperkuat dengan tingkat pengetahuan phishing yang lebih tinggi. Temuan ini menegaskan pentingnya kombinasi antara kesadaran, intuisi, dan pengetahuan dalam meningkatkan kemampuan deteksi terhadap ancaman siber. Penelitian ini memberikan kontribusi teoretis dalam literatur keamanan informasi, serta kontribusi praktis dalam perumusan program pelatihan siber bagi institusi pendidikan. Disarankan agar institusi pendidikan memperkuat literasi keamanan siber melalui pendekatan perilaku dan peningkatan kompetensi individu terhadap ancaman phishing

Kata Kunci- kesadaran keamanan informasi, *phishing*, gaya pengambilan keputusan, keamanan siber, institusi pendidikan.

I. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat telah memberikan pengaruh besar dalam berbagai aspek kehidupan, termasuk dalam sektor pendidikan tinggi. Keamanan informasi merupakan suatu isu yang semakin penting di era industri 4.0. Terlebih lagi pasca Covid-19, penggunaan internet dalam mendukung beragam aktivitas harian manusia di Indonesia semakin meningkat (Candiwan et al., 2024). Di balik manfaatnya yang besar, transformasi digital ini juga menimbulkan berbagai risiko, salah satunya adalah meningkatnya ancaman serangan siber seperti *phishing*. *Phishing* merupakan bentuk serangan siber yang memanfaatkan teknik rekayasa sosial untuk memperoleh informasi pribadi atau sensitif melalui komunikasi elektronik, biasanya melalui email, dengan cara menyamar sebagai pihak yang sah (Okokpujie et al., 2023). Serangan *phishing* menjadi salah satu ancaman paling umum di Indonesia, dengan lebih dari satu juta aktivitas terkait yang tercatat sepanjang tahun 2023 menurut Badan Siber dan Sandi Negara.

Institusi pendidikan tinggi menjadi salah satu sektor yang rentan terhadap serangan *phishing*, karena di dalamnya tersimpan data penting mahasiswa, dosen, dan karyawan, serta sistem informasi yang kompleks dan saling terintegrasi. Gangguan terhadap sistem ini dapat berdampak langsung pada kelancaran proses akademik, administratif, dan layanan kampus. Dengan begitu, karyawan kampus memegang peran strategis, tidak hanya dalam menjalankan fungsi administratif dan pendukung pendidikan, tetapi juga sebagai penjaga keamanan informasi institusi.

Kampus XYZ merupakan salah satu perguruan tinggi yang berfokus pada inovasi dan kewirausahaan. Kampus ini telah beroperasi selama 28 tahun dan memiliki total 120 karyawan yang terdiri dari tenaga pendidik dan tenaga kependidikan yang tersebar di dua fakultas. Program studi yang ditawarkan meliputi tujuh program studi jenjang Sarjana (S1) dan tiga program studi jenjang Pascasarjana (S2). Sebagai institusi yang mengusung visi meningkatkan daya saing global, Kampus XYZ memiliki komitmen untuk membangun lingkungan kerja yang aman dan adaptif terhadap tantangan digital, termasuk ancaman phishing.

Namun, tingkat kesadaran keamanan siber di kalangan karyawan kampus masih menjadi perhatian serius. Berdasarkan laporan Badan Siber dan Sandi Negara (2023), rendahnya tingkat pengetahuan tentang *phishing* dan pengambilan keputusan yang impulsif menjadi faktor utama meningkatnya kerentanan terhadap serangan ini. Serangan *phishing* sering kali dirancang untuk memicu respons emosional atau keputusan yang cepat, sehingga

individu yang tidak memiliki kewaspadaan tinggi berisiko lebih besar menjadi korban. Menurut Sturman et al. (2024), gaya pengambilan keputusan yang reflektif dan hati-hati terbukti mampu mengurangi risiko individu menjadi korban phishing, sementara gaya yang intuitif dan impulsif justru meningkatkan kerentanannya.

Selain itu, pengetahuan tentang *phishing* juga merupakan komponen penting dalam perlindungan terhadap serangan siber. Individu yang memahami karakteristik phishing, seperti tautan mencurigakan, kesalahan penulisan, dan tampilan email yang tidak biasa, akan lebih mampu mengenali dan menghindari potensi ancaman (Uma, 2024). Pengetahuan ini, jika dikombinasikan dengan kesadaran keamanan dan gaya pengambilan keputusan yang tepat, dapat membentuk sistem pertahanan manusia *(human firewall)* yang efektif di lingkungan institusi pendidikan.

Di Kampus XYZ, berdasarkan informasi internal, permasalahan ini pernah terjadi secara nyata. Salah satu karyawan diketahui pernah menjadi korban phishing melalui akun email kerja pribadinya. Meskipun insiden tersebut tidak menimbulkan kerusakan langsung pada sistem kampus, ada kekhawatiran bahwa akun yang digunakan juga terhubung dengan perangkat dan layanan internal kampus. Hal ini menimbulkan potensi risiko keamanan yang lebih luas, khususnya terhadap sistem informasi institusi yang sensitif. Kejadian ini menunjukkan bahwa pemahaman, kewaspadaan, dan perilaku keamanan siber di kalangan karyawan masih perlu ditingkatkan.

Dengan begitu, penelitian ini berfokus pada karyawan Kampus XYZ sebagai objek kajian, dengan tujuan untuk memahami sejauh mana tingkat kesadaran keamanan, gaya pengambilan keputusan, dan pengetahuan tentang *phishing* memengaruhi kerentanan terhadap serangan *phishing*. Hasil dari penelitian ini diharapkan dapat memberikan kontribusi dalam merancang strategi pelatihan keamanan siber yang lebih efektif dan relevan di lingkungan pendidikan tinggi, khususnya bagi tenaga kerja non-teknis yang menjadi garda depan dalam menjaga keamanan informasi institusi.

II. TINJAUAN LITERATUR

Manajemen keamanan informasi merupakan proses yang dirancang untuk melindungi aset informasi dari berbagai ancaman seperti akses tidak sah, penyalahgunaan, hingga gangguan operasional. Aryanti et al. (2023) menekankan bahwa inti dari manajemen ini adalah pemeliharaan terhadap kerahasiaan, integritas, dan ketersediaan informasi, yang dikenal sebagai prinsip *CIA triad*. Ketiganya membentuk fondasi dalam upaya perlindungan informasi yang sistematis dan berkelanjutan. Pandangan ini diperkuat oleh Nagata (2024) yang memperluas pendekatan manajemen keamanan informasi secara holistik, mencakup kebijakan, kontrol teknis, serta aspek manusia dan operasional yang saling terintegrasi. Sementara itu, Iriqat (2022) menyoroti pentingnya partisipasi seluruh karyawan dalam praktik manajemen keamanan, dengan menyatakan bahwa keberhasilan sistem ini sangat bergantung pada kesadaran kolektif dalam organisasi. Dengan demikian, manajemen keamanan informasi tidak hanya menjadi tanggung jawab teknologi, tetapi juga mengandalkan kolaborasi lintas fungsi dan individu dalam menjaga ketahanan terhadap ancaman yang terus berkembang.

Kesadaran keamanan informasi *(information security awareness)* menjadi aspek krusial yang mendukung efektivitas manajemen keamanan. Menurut F. Naga et al. (2024), kesadaran ini melibatkan pemahaman risiko serta penerapan tindakan preventif yang dipengaruhi oleh karakteristik personal dan tingkat kepatuhan individu terhadap kebijakan organisasi. Fadlika et al. (2023) menyatakan bahwa pemahaman dan kepatuhan ini merupakan faktor utama dalam mengurangi risiko serangan yang berasal dari faktor manusia. Ancaman tersebut tidak hanya bersumber dari luar organisasi, tetapi juga dari dalam, seperti dijelaskan oleh (Candiwan et al., 2022). Sari et al. (2021) lebih lanjut menunjukkan pentingnya edukasi dan pelatihan keamanan untuk meningkatkan kesadaran, khususnya dalam sektor-sektor sensitif seperti layanan kesehatan. Schutz & Fertig (2023) menambahkan bahwa kesadaran ini tidak hanya bersifat pasif tetapi perlu ditingkatkan melalui pelatihan dan promosi kebijakan yang relevan, sehingga karyawan tidak hanya paham secara konseptual, tetapi juga memiliki keterampilan praktis dalam menghadapi potensi ancaman.

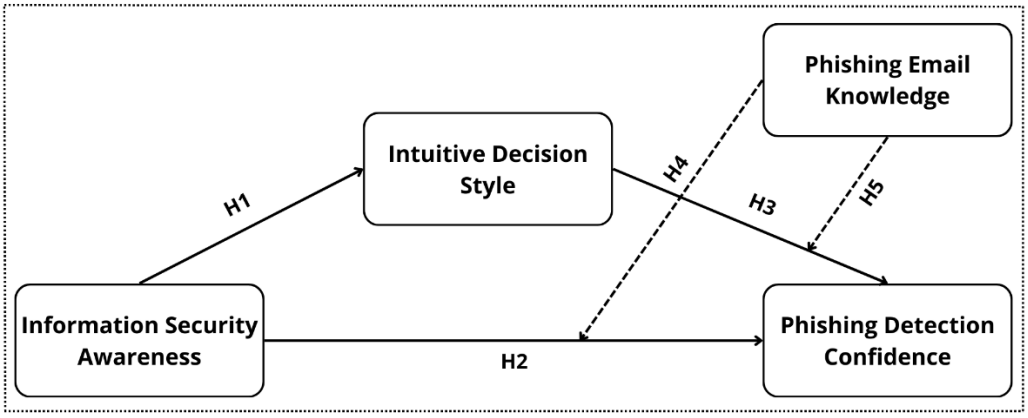
Gaya pengambilan keputusan intuitif *(intuitive decision style)* turut mempengaruhi respons individu dalam konteks keamanan informasi. Julmi (2019) menjelaskan bahwa gaya ini melibatkan pemrosesan informasi secara holistik, memungkinkan individu mengambil keputusan tanpa mengikuti prosedur eksplisit, tetapi berdasarkan pengalaman dan penilaian implisit. Pendekatan ini sangat berguna dalam kondisi tidak terstruktur. Darabos (2022) menambahkan bahwa keputusan intuitif sering kali dipengaruhi oleh narasi dan bias kognitif yang muncul dari pengalaman pribadi, menjadikan gaya ini berbeda dari pendekatan rasional. Hal ini dipertegas oleh Zulauf & Wagner (2021) yang menyebutkan bahwa intuisi memungkinkan pengambilan keputusan secara cepat dan fleksibel dengan mengandalkan rasa tahu yang muncul secara tidak sadar. Ketiganya menunjukkan bahwa intuisi, meskipun tidak berbasis logika formal, dapat menjadi mekanisme adaptif dalam menghadapi ketidakpastian dan tekanan waktu.

Dalam keamanan informasi, pengetahuan mengenai *email phishing* menjadi elemen kunci untuk menghindari serangan siber. Verma et al. (2020) menyatakan bahwa serangan *phishing* sering kali menggunakan email palsu yang terlihat sah, dengan tautan berbahaya untuk mengelabui korban agar membocorkan informasi sensitif. Tharani & Arachchilage (2020) mengidentifikasi *phishing* sebagai bagian dari rekayasa sosial di mana pelaku menyamar sebagai entitas tepercaya. Pengetahuan tentang taktik manipulasi URL dan struktur email sangat penting untuk mendeteksi

ancaman ini. Sun et al. (2021) menambahkan bahwa phishing modern menggunakan pendekatan canggih, termasuk penggunaan tampilan visual yang menyerupai institusi resmi, sehingga deteksinya memerlukan kemampuan teknis maupun edukasi pengguna. Oleh karena itu, pengetahuan tentang *phishing* menjadi prasyarat bagi setiap individu dalam organisasi untuk dapat bertindak proaktif dalam perlindungan informasi.

Selain pengetahuan, kepercayaan diri dalam mendeteksi *email phishing (phishing detection confidence)* juga berpengaruh terhadap efektivitas deteksi. Brickley (2022) menyebutkan bahwa kepercayaan diri dapat menjadi faktor yang menentukan dalam proses pengambilan keputusan terkait ancaman phishing—baik sebagai penguat kemampuan atau justru menjadi titik lemah ketika berlebihan. Pawar & Tijare (2023) menekankan pentingnya kemampuan mendeteksi sinyal bahaya dalam pesan-pesan phishing yang terus berkembang. Darmaningrat et al. (2022) menggambarkan taktik *phishing* yang kerap kali menyasar emosi korban, seperti rasa takut atau urgensi, agar mereka segera melakukan tindakan tertentu. Email semacam ini biasanya menyamar sebagai pemberitahuan penting dari instansi resmi, lengkap dengan logo dan bahasa yang meyakinkan. Oleh karena itu, perlindungan terhadap *phishing* perlu didukung tidak hanya oleh sistem teknis seperti server anti-spam dan threat intelligence platform, tetapi juga dengan edukasi yang membangun kepercayaan diri serta ketajaman pengguna dalam mengidentifikasi pesan mencurigakan.

Berdasarkan teori diatas dapat dibentuk kerangka berpikir dan hipotesis sebagai berikut:



(Sturman et al., 2024)

Gambar.1.Kerangka Pemikiran

Kerangka penelitian dalam studi ini mengintegrasikan studi dari Sturman et al. (2024) mengenai hubungan antara *Information Security Awareness*, *Intuitive Decision Style*, serta *Behavioral Intention & Phishing Detection*. Namun, studi ini memodifikasi variabel dependen dengan mengganti *Behavioral Intention & Phishing Detection* menjadi *Phishing Detection Confidence* (PDC). Perubahan ini dilakukan untuk lebih menyelaraskan fokus penelitian terhadap bagaimana individu menilai kemampuan mereka dalam mendeteksi *phishing*, bukan sekadar niat untuk bertindak.

Pergeseran ini sejalan dengan pendapat Brickley (2022), yang menekankan bahwa kepercayaan diri dalam mendeteksi *phishing* dapat memengaruhi efektivitas deteksi, baik secara positif maupun negatif. Selain itu, studi ini tetap mempertahankan *Phishing Email Knowledge* sebagai faktor moderasi, guna mengeksplorasi apakah peningkatan pengetahuan mengenai *phishing* benar-benar meningkatkan kepercayaan diri dalam mendeteksi ancaman atau justru menciptakan kepercayaan diri yang salah, yang berpotensi membuat individu lebih rentan terhadap serangan *phishing* yang lebih canggih. Dengan mengadaptasi kerangka penelitian sebelumnya, studi ini bertujuan memberikan pemahaman yang lebih mendalam mengenai mekanisme psikologis dan kognitif yang membentuk kepercayaan diri seseorang dalam mendeteksi phishing.

Berdasarkan narasi pada bagian sebelumnya, dapat diambil beberapa hipotesis yang ingin dibuktikan keabsahannya pada penelitian ini. Adapun hipotesis dalam penelitian ini adalah sebagai berikut:

- H1: *Information Security Awareness* berpengaruh positif terhadap *Intuitive Decision Style* pada karyawan kampus XYZ.
- H2: *Information Security Awareness* berpengaruh positif terhadap *Phishing Detection Confidence* pada karyawan kampus XYZ.
- H3: *Intuitive Decision Style* berpengaruh positif terhadap *Phishing Detection Confidence* pada karyawan kampus XYZ.
- H4: *Phishing Email Knowledge* memoderasi hubungan antara *Information Security Awareness* dan *Phishing Detection Confidence* pada karyawan kampus XYZ.

- H5: *Phishing Email Knowledge* memoderasi hubungan antara *Intuitive Decision Style* dan *Phishing Detection Confidence* pada karyawan kampus XYZ.

III. METODOLOGI PENELITIAN

Penelitian ini merupakan studi eksplanatori kuantitatif yang bertujuan untuk memahami hubungan kausal antara variabel kesadaran keamanan, gaya pengambilan keputusan, pengetahuan, dan kemampuan deteksi email phishing. Pendekatan eksplanatori dipilih untuk mengungkap mekanisme sebab-akibat yang kompleks, termasuk peran mediasi dan moderasi antar variabel (Huang et al., 2023). Pendekatan kuantitatif memungkinkan pengumpulan dan analisis data numerik untuk menguji hipotesis secara objektif melalui teknik statistik seperti regresi (Sekaran & Bougie, 2016); (Brahimi & Leperlier, 2023). Dengan demikian, pendekatan ini memberikan pemahaman relasional yang komprehensif sekaligus menjaga akurasi pengukuran data.

Strategi yang digunakan dalam penelitian ini adalah survei, dengan pengumpulan data melalui kuesioner yang disebarkan kepada karyawan Kampus XYZ. Survei dianggap efektif untuk menggali persepsi, sikap, dan perilaku individu secara sistematis (Sekaran & Bougie, 2016). Unit analisis dalam penelitian ini adalah individu, karena fokus utama adalah pada perilaku personal dalam mendeteksi phishing, seperti tingkat kesadaran keamanan dan gaya pengambilan keputusan. Peneliti memiliki keterlibatan minimal, hanya bertindak sebagai pengumpul data tanpa intervensi langsung terhadap responden, sesuai dengan karakteristik studi korelasional (Sekaran & Bougie, 2016).

Penelitian ini dilakukan dalam lingkungan kerja nyata tanpa manipulasi kondisi, sehingga bersifat noncontrived (Sekaran & Bougie, 2016). Hal ini memungkinkan hasil penelitian mencerminkan situasi yang sebenarnya di lingkungan Kampus XYZ. Desain penelitian yang digunakan adalah *cross-sectional*, yaitu pengumpulan data dilakukan dalam satu waktu tertentu untuk menggambarkan hubungan antar variabel pada saat itu (Sekaran & Bougie, 2016). Desain ini memberikan efisiensi dalam penggunaan waktu dan sumber daya, sekaligus menghasilkan wawasan yang relevan mengenai fenomena yang diteliti.

Penelitian ini dilakukan dalam lingkungan kerja nyata tanpa manipulasi kondisi, sehingga bersifat noncontrived (Sekaran & Bougie, 2016). Hal ini memungkinkan hasil penelitian mencerminkan situasi yang sebenarnya di lingkungan Kampus XYZ. Desain penelitian yang digunakan adalah *cross-sectional*, yaitu pengumpulan data dilakukan dalam satu waktu tertentu untuk menggambarkan hubungan antar variabel pada saat itu (Sekaran & Bougie, 2016). Desain ini memberikan efisiensi dalam penggunaan waktu dan sumber daya, sekaligus menghasilkan wawasan yang relevan mengenai fenomena yang diteliti. Indikator-indikator yang dikembangkan akan mewakili ciri-ciri atau atribut dari setiap variabel yang diteliti. Setiap indikator ini akan dijabarkan dalam bentuk pertanyaan kuesioner yang dapat diukur menggunakan skala Likert, yang mengukur sejauh mana responden setuju atau tidak setuju dengan pernyataan yang diberikan. Setiap pertanyaan dalam kuesioner akan diidentifikasi dengan nomor item yang unik, sehingga memudahkan analisis data yang terkumpul. Skala Likert yang digunakan akan mengukur intensitas sikap responden terhadap indikator-indikator yang relevan, mulai dari "Sangat Tidak Setuju" hingga "Sangat Setuju" (Andrade, 2021).

Penelitian ini melibatkan empat jenis variabel, yaitu independen, mediasi, moderasi, dan dependen. Variabel independen adalah kesadaran keamanan, yang mencerminkan pemahaman karyawan terhadap pentingnya mengenali dan mencegah phishing, diukur dengan 9 indikator. Variabel mediasi berupa gaya pengambilan keputusan intuitif, yaitu kecenderungan mengandalkan insting dalam mengambil keputusan, diukur dengan 5 indikator. Sebagai variabel moderasi, pengetahuan tentang phishing email berperan dalam memperkuat atau memperlemah hubungan antara kesadaran keamanan dan kemampuan deteksi phishing, diukur dengan 15 indikator. Adapun variabel dependen adalah kemampuan deteksi phishing, yaitu sejauh mana karyawan mampu mengenali email phishing, diukur dengan 15 indikator yang dilengkapi contoh email.

Populasi dalam penelitian ini adalah seluruh karyawan Kampus XYZ yang berjumlah 120 orang. Populasi merupakan wilayah generalisasi yang terdiri atas subjek dengan karakteristik tertentu yang ditetapkan oleh peneliti untuk kemudian dipelajari dan ditarik kesimpulannya (Darwin et al., 2021). Dalam penelitian ini, karena jumlah populasi relatif kecil dan sesuai dengan kriteria penelitian, maka digunakan teknik saturated sampling atau sensus, di mana seluruh anggota populasi dijadikan sebagai sampel (Darwin et al., 2021). Teknik ini termasuk dalam kategori non-probability sampling, yang tidak memberikan peluang yang sama bagi setiap anggota populasi untuk terpilih, berbeda dengan probability sampling (Darwin et al., 2021; Wahyudi & Damanik, 2022). Dengan demikian, seluruh karyawan Kampus XYZ dijadikan responden untuk memperoleh data yang representatif dan menyeluruh.

Analisis data dalam penelitian ini dibagi menjadi dua tahap utama, yaitu analisis deskriptif dan analisis *moderated mediation*. Menurut Darwin et al. (2021), analisis deskriptif digunakan untuk mengolah dan menyajikan data guna menggambarkan karakteristik responden dan kecenderungan jawaban mereka. Data disajikan dalam bentuk tabel, grafik, atau diagram, serta dianalisis menggunakan kriteria evaluasi berdasarkan garis kontinum (Iba & Wardhana, 2024). Interpretasi terhadap jawaban responden dilakukan melalui langkah: menghitung nilai kumulatif dan persentase, menentukan nilai maksimal dan minimal dari skala Likert, hingga memperoleh interval klasifikasi. Rentang persentase dari 20% hingga 100% dibagi ke dalam lima kategori: sangat rendah (20–36%), rendah (36–52%), cukup tinggi (52–68%), tinggi (68–84%), dan sangat tinggi (84–100%) (Iba & Wardhana, 2023).

Untuk menguji hubungan antar variabel secara simultan, digunakan analisis moderated mediation dengan bantuan perangkat lunak PROCESS Macro versi 4.3 pada SPSS (Hayes, 2015). Model yang digunakan adalah Model 15, yang

menguji efek mediasi dari variabel independen (X) terhadap variabel dependen (Y) melalui mediator (M), dengan efek yang dimoderasi oleh variabel moderator (W). Analisis ini mencakup penghitungan efek langsung, tidak langsung, serta efek interaksi, yang semuanya dievaluasi menggunakan metode bootstrapping sebanyak 5000 sampel untuk meningkatkan akurasi estimasi (Alfons et al., 2022). Adapun struktur variabel dalam model ini adalah Information Security Awareness (X), Intuitive Decision Style (M), Phishing Email Knowledge (W), Phishing Detection Confidence (Y).

Sebelum analisis, data X, M, dan W ditransformasi menjadi z-score. Nilai moderator diklasifikasikan ke dalam tiga kondisi (rendah, sedang, tinggi). Uji signifikansi dilakukan dengan p-value < 0,05 (Darwin et al., 2021), serta efek moderasi dan mediasi dianggap signifikan jika interval kepercayaan tidak mencakup nol (Hayes, 2015).

IV. HASIL DAN PEMBAHASAN

A. Analisis Deskriptif

Analisis deskriptif dilakukan untuk menggambarkan hasil tanggapan responden. Untuk mempermudah interpretasi hasil penelitian, maka dilakukan kategorisasi skor sebagaimana perhitungan yang disajikan pada tabel 1.

Tabel 1. Kriteria Interpretasi

No.	Interval Persentase	Kategori
1.	20% - 36%	Sangat tidak baik
2.	> 36% - 52%	Tidak baik
3.	> 52% - 68%	Cukup baik
4.	> 68% - 84%	Baik
5.	> 84% - 100%	Sangat baik

Sumber: Iba & Wardhana (2023)

Berikut disajikan hasil analisis deskriptif terhadap empat variabel utama dalam penelitian ini, yaitu *Information Security Awareness* (X), *Intuitive Decision Style* (M), *Phishing Email Knowledge* (W), dan *Phishing Detection Confidence* (Y). Setiap variabel diukur berdasarkan sejumlah pernyataan yang dijawab oleh responden menggunakan skala Likert 5 poin, mulai dari "Sangat Tidak Setuju" hingga "Sangat Setuju". Analisis ini bertujuan untuk memberikan gambaran umum mengenai tingkat kesadaran, gaya pengambilan keputusan, pengetahuan, serta keyakinan responden dalam mendeteksi phishing email, yang menjadi fokus utama dalam konteks keamanan informasi pribadi melalui media email. Rangkuman skor, skor ideal, serta persentase untuk masing-masing item dapat dilihat pada tabel 2.

Tabel 2. Analisis Deskriptif

No.	Variabel	Jumlah Item	Skor Total	Skor Ideal	Presentase (%)	Kategori	Item Tertinggi (Kode - %)	Item Terendah (Kode - %
1	*Information Security Awareness* (X)	9	4.149	6.000	76,8%	Baik	ISA2 – 80,8% ("Tidak mengklik tautan dari pengirim tidak dikenal")	ISA1 – 71,2% ("Tautan dari orang dikenal tidak selalu aman")
2	*Intuitive Decision Style* (M)	5	1.945	3.000	64,8%	Cukup Baik	IDS4 – 71,7% ("Mengandalkan kesan pertama")	IDS5 – 55,8% ("Lebih mengandalkan perasaan daripada analisis")
3	*Phishing Email Knowledge* (W)	15	6.803	9.000	75,6%	Baik	PEK1 – 85,2% ("Lembaga keuangan tidak minta kata sandi lewat email")	PEK13 – 64,5% ("Email dari perusahaan afiliasi bisa phishing")
4	*Phishing Detection Confidence* (Y)	15	6.709	9.000	74,5%	Baik	PDC1 – 85,0% ("Merasa aman mengklik tautan email ini")	PDC13 – 63,7% ("Merasa aman mengklik tautan email ini")

Sumber: Olahan Data Penulis (2025)

Information Security Awareness (X) memiliki rata-rata persentase sebesar 76,8%, tergolong dalam kategori Baik. Responden secara umum memiliki kesadaran yang cukup baik terkait risiko keamanan informasi, khususnya dalam konteks interaksi melalui email. Nilai tertinggi terdapat pada pernyataan terkait penghindaran klik pada tautan dari pengirim tidak dikenal, sedangkan nilai terendah mengindikasikan adanya rasa aman yang berlebihan terhadap pengirim yang dikenal.

Intuitive Decision Style (M) menunjukkan rata-rata 64,8%, dalam kategori Cukup Baik. Hal ini menunjukkan

bahwa meskipun intuisi digunakan, responden cenderung tidak sepenuhnya mengandalkannya dalam pengambilan keputusan. Nilai tertinggi terkait kesan pertama, sementara nilai terendah menunjukkan ketergantungan terhadap perasaan daripada analisis yang masih cukup rendah.

Phishing Email Knowledge (W) memiliki rata-rata 75,6%, termasuk kategori Baik. Ini mencerminkan bahwa responden memiliki pengetahuan yang relatif kuat dalam mengenali ciri-ciri email phishing, dengan skor tertinggi terkait pemahaman bahwa kata sandi tidak seharusnya diminta via email oleh lembaga keuangan, dan skor terendah menunjukkan adanya keraguan terhadap email dari pihak yang tampak berafiliasi.

Phishing Detection Confidence (Y) mencapai 74,5%, juga dalam kategori Baik, menunjukkan tingkat kepercayaan diri responden yang cukup tinggi dalam mendeteksi phishing. Meskipun demikian, masih terdapat beberapa item dengan skor rendah yang menunjukkan ketidakyakinan dalam situasi tertentu, khususnya pada email yang tampak sah namun berpotensi mencurigakan.

B. Moderated Mediation Analysis

1. Analisis Korelasi

Tabel 3. menyajikan hasil analisis regresi yang menguji pengaruh variabel X terhadap variabel mediastor yaitu *Intuitive Decision Style* (IDS). Berdasarkan hasil tersebut, *Information Security Awareness* (ISA) menunjukkan hubungan yang positif dan signifikan dengan *Intuitive Decision Style* (IDS). Nilai koefisien korelasi sebesar r = 0.637 dengan tingkat signifikansi $p < 0.01$ menunjukkan adanya asosiasi yang cukup kuat antara kedua variabel tersebut.

Tabel 3. Model Regresi untuk Prediktor IDS

Variabel	Koefisien	SE (HC4)	t	p-value	LLCI	ULCI
Constant	0.441	0.196	2.249	0.026	0.053	0.830
ISA → IDS	0.637	0.065	9.772	0.000	0.508	0.766
COV	-0.148	0.069	-2.145	0.034	-0.284	-0.011

Sumber: Olahan Data Penulis (2025)

Hasil regresi menunjukkan bahwa ISA memiliki koefisien regresi sebesar 0.637 dengan nilai p = 0.000, yang mengindikasikan bahwa kontribusi ISA terhadap peningkatan IDS sangat signifikan secara statistik. Hal ini berarti bahwa semakin tinggi tingkat kesadaran keamanan informasi seseorang, maka cenderung semakin tinggi pula kemampuannya dalam mengambil keputusan secara intuitif.

Koefisien ini dapat diartikan bahwa setiap peningkatan satu satuan pada nilai ISA akan diikuti oleh peningkatan sebesar 0.637 pada skor IDS, dengan asumsi variabel lain konstan. Rentang nilai Confidence Interval (CI) antara 0.508 hingga 0.766 memberikan keyakinan bahwa pengaruh tersebut tidak hanya signifikan, tetapi juga stabil dalam rentang prediksi yang sempit.

2. Analisis Mediasi

Tabel 4. menyajikan hasil regresi yang menguji peran variabel *Intuitive Decision Style* (IDS) sebagai mediator dalam hubungan antara *Information Security Awareness* (ISA) dan *Phishing Detection Confidence* (PDC). Hasil menunjukkan adanya hubungan negatif dan signifikan antara IDS dan PDC dengan koefisien $\beta = -0.300$, SE = 0.066, dan $p < 0.001$. Interval kepercayaan 95% yang tidak melintasi angka nol ([-0.431, -0.169]) memperkuat signifikansi statistik hubungan tersebut.

Tabel 4. Model Regresi untuk Prediktor PDC

Variabel	Koefisien	SE (HC4)	t	p-value	LLCI	ULCI
Constant	3.604	0.211	17.093	0.000	3.186	4.022
ISA → PDC	0.266	0.099	2.688	0.008	0.070	0.462
IDS → PDC	-0.300	0.066	-4.540	0.000	-0.431	-0.169
PEK → PDC	0.250	0.134	1.860	0.065	-0.016	0.516
ISA × PEK	0.185	0.153	1.212	0.228	-0.117	0.487
IDS × PEK	-0.305	0.155	-1.971	0.051	-0.612	-0.002
COV	0.051	0.062	0.833	0.407	-0.071	0.174

Sumber: Olahan Data Penulis (2025)

Temuan ini mengindikasikan bahwa kecenderungan individu untuk menggunakan gaya pengambilan keputusan intuitif justru menurunkan tingkat kepercayaan diri mereka dalam mendeteksi serangan *phishing*. Hal ini bisa dijelaskan dengan pemahaman bahwa pendekatan intuitif dalam pengambilan keputusan, yang mengandalkan

penilaian cepat dan pengalaman subjektif, kurang efektif dalam konteks yang memerlukan pemrosesan informasi yang cermat dan analitis seperti deteksi *phishing*.

Sebaliknya, pengaruh langsung antara ISA dan PDC menunjukkan hubungan yang positif dan signifikan, dengan β = 0.266, SE = 0.099, dan p = 0.008. Rentang interval kepercayaan 95% [0.070, 0.462] mengindikasikan bahwa semakin tinggi kesadaran individu terhadap keamanan informasi, semakin besar pula kepercayaan dirinya dalam mengidentifikasi upaya phishing. Ini menggarisbawahi pentingnya literasi dan pemahaman keamanan sebagai fondasi kepercayaan dalam menghadapi ancaman siber.

3. Analisis Moderasi

Untuk menguji lebih lanjut pengaruh interaksi antara *Intuitive Decision Style* (IDS) dan *Phishing Email Knowledge* (PEK) terhadap Phishing Detection Confidence (PDC), digunakan analisis Johnson-Neyman. Teknik ini memungkinkan identifikasi titik potong di mana efek prediktor (IDS) terhadap variabel dependen (PDC) berubah dari tidak signifikan menjadi signifikan, tergantung pada nilai variabel moderator (PEK) (Hayes, 2015).

Tabel 5. Johnson-Neyman: Rentang Signifikan Moderasi PEK

PEK Level	Effect of IDS → PDC	SE (HC4)	t	p-value	LLCI	ULCI
-0.720	-0.081	0.138	-0.585	0.560	-0.353	0.192
0.000	-0.300	0.066	-4.540	0.000	-0.431	-0.169
0.720	-0.520	0.121	-4.298	0.000	-0.759	-0.

Sumber: Olahan Data Penulis (2025)

Hasil analisis yang ditampilkan pada Tabel 5. menunjukkan bahwa pengaruh negatif IDS terhadap PDC bersifat signifikan pada tingkat PEK sedang hingga tinggi, namun tidak signifikan pada tingkat PEK yang rendah. Sebagai contoh:

- Pada tingkat PEK rendah (misalnya PEK = -0.720), pengaruh IDS terhadap PDC sebesar β = -0.081, namun tidak signifikan (p = 0.560, dengan interval kepercayaan [-0.353, 0.192]).
- Pada tingkat PEK sedang (PEK = 0.000), pengaruh IDS terhadap PDC sebesar β = -0.300, yang signifikan secara statistik (p = 0.000, CI: [-0.431, -0.169]).
- Pada tingkat PEK tinggi (PEK = 0.720), efek negatif IDS terhadap PDC menjadi lebih kuat, yakni β = -0.520, juga signifikan (p = 0.000, CI: [-0.759, -0.280]).

Interpretasi dari temuan ini menunjukkan bahwa pengetahuan tentang phishing (PEK) memperkuat efek negatif dari gaya pengambilan keputusan intuitif (IDS) terhadap kepercayaan diri dalam mendeteksi phishing (PDC). Dengan kata lain, semakin tinggi pengetahuan individu tentang phishing, semakin kuat pula efek merugikan dari penggunaan intuisi terhadap kepercayaan mendeteksi phishing.

Hal ini dapat dijelaskan melalui kemungkinan adanya konflik kognitif. Individu dengan PEK tinggi cenderung memiliki pengetahuan eksplisit tentang tanda-tanda phishing, sehingga saat mereka mengandalkan intuisi (yang mungkin bertentangan dengan informasi yang telah mereka pelajari), mereka menjadi lebih tidak yakin dalam penilaian mereka. Ini dapat menurunkan kepercayaan diri mereka terhadap keputusan yang diambil. Sebaliknya, individu dengan PEK rendah mungkin tidak memiliki cukup informasi untuk mengalami konflik tersebut, sehingga pengaruh IDS terhadap PDC tidak signifikan.

4. Analisis Mediasi Termoderasi

Untuk menguji hubungan yang lebih kompleks antara *Information Security Awareness* (ISA), *Intuitive Decision Style* (IDS), *Phishing Detection Confidence* (PDC), dan peran moderasi *Phishing Email Knowledge* (PEK), digunakan analisis mediasi termoderasi dengan menggunakan Model 15 dari PROCESS. Model ini memungkinkan analisis simultan dari pengaruh tidak langsung (mediasi) yang dipengaruhi oleh variabel moderator (moderasi), dengan fokus khusus pada apakah PEK memoderasi efek mediasi dari ISA terhadap PDC melalui IDS.

Tabel 6. Efek Langsung Kondisional ISA terhadap PDC pada Level PEK yang Berbeda

PEK Level	Direct Effect of IDS → PDC	SE (HC4)	t	p-value	95% CI (LLCI, ULCI)
-0.720	0.133	0.128	1.037	0.302	[-0.121, 0.387]
0.000	0.266	0.099	2.688	0.008	[0.070, 0.462]
0.720	0.399	0.165	2.416	0.017	[0.072, 0.726]

Sumber: Olahan Data Penulis (2025)

Hasil analisis menunjukkan bahwa efek langsung ISA terhadap PDC bersifat kondisional, bergantung pada tingkat PEK. Tabel 6. menunjukkan:

- Pada PEK rendah (-0.720), efek langsung ISA terhadap PDC tidak signifikan (β = 0.133, p = 0.302, CI [-

0.121, 0.387]).

- Pada PEK sedang (0.000), efek menjadi signifikan (β = 0.266, p = 0.008, CI [0.070, 0.462]).
- Pada PEK tinggi (0.720), efek semakin kuat (β = 0.399, p = 0.017, CI [0.072, 0.726]).

Interpretasi dari temuan ini adalah bahwa peningkatan pengetahuan phishing memperkuat hubungan langsung antara ISA dan PDC. Artinya, kesadaran keamanan informasi akan berdampak lebih besar terhadap keyakinan dalam mendeteksi phishing pada individu dengan tingkat pengetahuan yang lebih tinggi. Hal ini mengindikasikan sinergi antara pengetahuan deklaratif (PEK) dan kesadaran konseptual (ISA) dalam meningkatkan kepercayaan diri karyawan dalam menghadapi serangan phishing.

Tabel 7. Efek Tidak Langsung ISA terhadap PDC melalui IDS pada Level PEK yang Berbeda

PEK Level	Indirect Effect of IDS → PDC	BootSE	95% CI (BootLLCI, BootULCI)
-0.720	-0.051	0.090	[-0.247, 0.112]
0.000	-0.191	0.052	[-0.304, -0.103]
0.720	-0.331	0.084	[-0.516, -0.188]

Sumber: Olahan Data Penulis (2025)

Selanjutnya, efek tidak langsung dari ISA terhadap PDC melalui IDS juga ditemukan sebagai termoderasi oleh PEK. Tabel 7. menunjukkan bahwa:

- Pada PEK rendah, efek tidak langsung tidak signifikan (β = -0.051, CI [-0.247, 0.112]).
- Pada PEK sedang, efek menjadi signifikan dan negatif (β = -0.191, CI [-0.304, -0.103]).
- Pada PEK tinggi, efek menjadi semakin kuat secara negatif (β = -0.331, CI [-0.516, -0.188]).

Temuan ini menunjukkan bahwa semakin tinggi PEK, semakin kuat pengaruh negatif yang dimediasi oleh IDS terhadap PDC. Dengan kata lain, walaupun ISA secara langsung meningkatkan PDC, sebagian dari pengaruh tersebut justru terhambat ketika individu lebih mengandalkan intuisi (IDS), dan efek hambatan ini semakin jelas pada individu yang memiliki PEK tinggi.

C. Hasil Pengujian Hipotesis

Dalam penelitian ini terdapat 5 hipotesis yang diuji. Berikut hasil rekapitulasi uji hipotesis:

Tabel 8. Pengujian Hipotesis

Hipotesis	Hasil Uji Statistik	Keterangan
H1: Information Security Awareness berpengaruh positif terhadap Intuitive Decision Style pada karyawan kampus XYZ.	Koefisien = 0.637, p = 0.000 (signifikan).	Diterima
H2: Information Security Awareness berpengaruh positif terhadap Phishing Detection Confidence pada karyawan kampus XYZ.	Koefisien = 0.266, p = 0.008 (signifikan).	DIterima
H3: Intuitive Decision Style berpengaruh positif terhadap Phishing Detection Confidence pada karyawan kampus XYZ.	Koefisien = -0.300, p = 0.000 (signifikan namun arah negatif).	Ditolak
H4: Phishing Email Knowledge memoderasi hubungan antara Information Security Awareness dan Phishing Detection Confidence pada karyawan kampus XYZ.	Indeks mediasi termoderasi signifikan, efek meningkat pada PEK tinggi (p = 0.017).	Diterima
H5: Phishing Email Knowledge memoderasi hubungan antara Intuitive Decision Style dan Phishing Detection Confidence pada karyawan kampus XYZ.	Efek interaksi signifikan (p = 0.051), efek negatif IDS terhadap PDC menguat saat PEK tinggi.	Diterima

Sumber: Olahan Data Penulis (2025)

Berdasarkan Tabel 8, dapat disimpulkan bahwa dari lima hipotesis yang diajukan dalam penelitian ini, empat hipotesis dinyatakan diterima, sementara satu hipotesis ditolak. Hipotesis pertama (H1) yang menyatakan bahwa *Information Security Awareness* (ISA) berpengaruh positif terhadap *Intuitive Decision Style* (IDS) terbukti signifikan dengan arah hubungan positif, sehingga hipotesis ini diterima. Hipotesis kedua (H2) juga didukung oleh hasil analisis, di mana ISA terbukti berpengaruh positif dan signifikan terhadap *Phishing Detection Confidence* (PDC).

Namun, hipotesis ketiga (H3) yang menyatakan bahwa IDS berpengaruh positif terhadap PDC tidak didukung oleh data. Meskipun hubungan antara kedua variabel signifikan, arah koefisien menunjukkan hubungan negatif, sehingga hipotesis ini ditolak karena tidak sesuai dengan arah prediksi awal.

Selanjutnya, hipotesis keempat (H4) yang menguji peran moderasi dari *Phishing Email Knowledge* (PEK) dalam hubungan antara ISA dan PDC menunjukkan hasil signifikan. Artinya, pengaruh tidak langsung ISA terhadap PDC melalui IDS dipengaruhi oleh tingkat PEK, terutama pada tingkat sedang dan tinggi. Hal serupa juga terjadi pada hipotesis kelima (H5), di mana PEK terbukti memoderasi pengaruh IDS terhadap PDC. Efek negatif IDS terhadap PDC menjadi semakin kuat pada tingkat PEK yang lebih tinggi. Oleh karena itu, H4 dan H5 keduanya diterima karena moderasi yang signifikan ditemukan dalam model.

D. Pembahasan Hasil Penelitian

Hasil penelitian ini menunjukkan bahwa *Information Security Awareness* (ISA) memiliki peran yang signifikan dalam memengaruhi *Intuitive Decision Style* (IDS) serta tingkat kepercayaan diri dalam mendeteksi phishing (Phishing Detection Confidence/PDC). Pengaruh positif dan signifikan antara ISA terhadap IDS menunjukkan bahwa ketika karyawan memiliki tingkat kesadaran yang tinggi terhadap keamanan informasi, mereka cenderung mengandalkan intuisi dalam proses pengambilan keputusan yang berkaitan dengan ancaman siber. Temuan ini sejalan dengan teori dual-process, di mana individu yang memiliki pemahaman memadai terhadap suatu isu lebih mampu membuat keputusan intuitif yang cepat dan tepat.

Lebih lanjut, ISA juga terbukti berpengaruh secara positif terhadap PDC. Artinya, karyawan yang lebih sadar akan pentingnya keamanan informasi menunjukkan tingkat keyakinan yang lebih tinggi dalam mengenali dan mendeteksi potensi serangan phishing. Hasil ini menguatkan temuan sebelumnya yang menyatakan bahwa awareness adalah salah satu elemen penting dalam membentuk perilaku keamanan informasi yang efektif. Pengetahuan dan perhatian terhadap risiko keamanan tampaknya memberikan dasar yang kuat bagi individu untuk merasa lebih percaya diri dalam mengambil keputusan yang berkaitan dengan keamanan, terutama dalam menghadapi email mencurigakan.

Namun, hasil yang cukup menarik ditemukan pada pengaruh IDS terhadap PDC. Secara statistik, hubungan ini signifikan namun menunjukkan arah negatif. Ini berarti bahwa semakin tinggi ketergantungan seseorang pada intuisi, justru semakin rendah tingkat keyakinan mereka dalam mendeteksi phishing. Temuan ini bertolak belakang dengan hipotesis awal, dan menunjukkan bahwa pengambilan keputusan yang terlalu mengandalkan intuisi tanpa penalaran analitis justru dapat menurunkan efektivitas dalam mendeteksi ancaman. Dalam konteks phishing, ancaman yang bersifat manipulatif dan kompleks tampaknya lebih tepat direspon melalui proses berpikir yang analitis daripada hanya mengandalkan insting.

Aspek menarik lainnya dari hasil penelitian ini adalah ditemukannya peran moderasi dari *Phishing Email Knowledge* (PEK). Pengetahuan tentang phishing terbukti memoderasi hubungan antara ISA dan PDC melalui IDS, serta hubungan langsung antara IDS dan PDC. Hasil moderated mediation menunjukkan bahwa pada tingkat PEK yang sedang dan tinggi, pengaruh tidak langsung dari ISA terhadap PDC melalui IDS menjadi signifikan. Ini berarti bahwa semakin tinggi pengetahuan seseorang tentang phishing, semakin besar pengaruh ISA terhadap keyakinan mereka dalam mendeteksi phishing, meskipun jalur pengaruh melalui IDS bersifat negatif.

Demikian pula, interaksi antara IDS dan PEK juga signifikan. Pada individu dengan PEK tinggi, pengaruh negatif IDS terhadap PDC menjadi semakin kuat. Ini menunjukkan bahwa meskipun seseorang memiliki pengetahuan tentang *phishing*, gaya pengambilan keputusan yang terlalu intuitif dapat tetap menurunkan kepercayaan diri dalam mendeteksi *phishing*, kemungkinan karena munculnya konflik antara insting dan fakta yang diketahui.

Secara keseluruhan, hasil penelitian ini menegaskan pentingnya kesadaran keamanan informasi dan pengetahuan *phishing* sebagai dua pilar utama dalam membentuk perilaku karyawan terhadap ancaman siber. Sementara intuisi berperan dalam pengambilan keputusan cepat, hasil ini menunjukkan bahwa kepercayaan diri dalam mendeteksi *phishing* memerlukan keseimbangan antara intuisi dan pengetahuan faktual. Dengan demikian, upaya peningkatan awareness dan pelatihan tentang phishing email menjadi sangat penting, terutama untuk membentuk pola pikir yang adaptif dan responsif terhadap risiko siber di lingkungan organisasi.

V. KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa *Information Security Awareness* (ISA) memiliki pengaruh positif terhadap *Intuitive Decision Style* (IDS) dan *Phishing Detection Confidence* (PDC), yang mengindikasikan bahwa peningkatan kesadaran keamanan dapat mendorong penggunaan intuisi sekaligus memperkuat keyakinan dalam mendeteksi *phishing*. Namun, IDS justru memiliki pengaruh negatif terhadap PDC, yang berarti kecenderungan untuk mengambil keputusan secara intuitif dapat menurunkan kepercayaan diri dalam mengenali serangan phishing, kemungkinan karena kurangnya evaluasi rasional terhadap informasi. Selain itu, *Phishing Email Knowledge* (PEK) terbukti memoderasi hubungan antara ISA dan PDC melalui IDS, serta memoderasi langsung hubungan antara IDS dan PDC. Efek moderasi ini menunjukkan bahwa pengetahuan tentang *phishing* memperkuat pengaruh awareness, namun tetap diperlukan kemampuan berpikir yang seimbang antara analitis dan intuitif untuk meningkatkan efektivitas deteksi *phishing*.

Berdasarkan temuan ini, pihak manajemen kampus disarankan untuk menyusun program pelatihan keamanan informasi yang tidak hanya membangun kesadaran dan pengetahuan tentang *phishing*, tetapi juga melatih karyawan untuk mengembangkan gaya pengambilan keputusan yang seimbang dalam mengintegrasikan respons intuitif dengan evaluasi analitis. Pelatihan berbasis simulasi dapat membantu karyawan mengenali skenario serangan *phishing* secara nyata dan memperkuat kepercayaan diri mereka dalam meresponsnya. Selain itu, institusi perlu menumbuhkan budaya pengambilan keputusan yang mendukung pemrosesan informasi secara rasional namun tetap responsif terhadap situasi, sehingga terbentuk pola pikir yang adaptif terhadap ancaman digital. Untuk pengembangan ilmu lebih lanjut, studi ke depan dapat memperluas cakupan dengan pendekatan longitudinal dan mengeksplorasi interaksi antara gaya berpikir, pengetahuan, dan efikasi diri dalam konteks keamanan informasi.

REFERENSI

Alfons, A., Ateş, N. Y., & Groenen, P. J. F. (2022). A Robust Bootstrap Test for Mediation Analysis. *Organizational*

Research Methods, *25*(3), 591–617. https://doi.org/10.1177/1094428121999096

Andrade, C. (2021). A Student's Guide to the Classification and Operationalization of Variables in the Conceptualization and Design of a Clinical Study: Part 1. *Indian Journal of Psychological Medicine*, *43*(2), 177–179. https://doi.org/10.1177/0253717621994334

Aryanti, U., Taufan Anwar, M., & Rahmawati, T. (2023). Information Security Risk Management Using OCTAVE Allegro Method at University. In *International Journal of Ethno-Sciences and Education Research* (Vol. 3, Issue 4).

Badan Siber dan Sandi Negara. (2023). *LANSKAP KEAMANAN SIBER INDONESIA*.

Brahimi, M. A., & Leperlier, T. (2023). *Quantitative Methods in Intellectual History*. 9781003093046. https://doi.org/10.4324/9781003093046-8ï

Brickley, J. (2022). *What Drives User Retrospective Confidence Levels Towards Phishing Detection Behavior*. https://doi.org/10.13140/RG.2.2.31741.44002

Candiwan, C., Azmi, M., & Alamsyah, A. (2022). Analysis of Behavioral and Information Security Awareness among Users of Zoom Application in COVID-19 Era. *International Journal of Safety and Security Engineering*, *12*(2), 229–237. https://doi.org/10.18280/ijsse.120212

Candiwan, C., Sidiq, F., Prabowo, A., & Hidayatulloh, D. S. (2024). Sosialisasi Awareness Keamanan Informasi Untuk Guru Yayasan Fitrah Insani. *Jurnal Pengabdian Masyarakat Akademisi*, *3*(2). https://doi.org/10.54099/jpma.v3i2.97

Darabos, K. (2022). INTUITIVE DECISION: WHEN TO BEGIN THE SUCCESSION PROCESS. *Corvinus Journal of Sociology and Social Policy*, *13*(2), 79–105. https://doi.org/10.14267/CJSSP.2022.2.4

Darmaningrat, E. W. T., Ali, A. H. N., Herdiyanti, A., Subriadi, A. P., Muqtadiroh, F. A., Astuti, H. M., & Susanto, T. D. (2022). Sosialisasi Bahaya dan Upaya Pencegahan Social Engineering untuk Meningkatkan Kesadaran Masyarakat tentang Keamanan Informasi. *Sewagati*, *6*(2). https://doi.org/10.12962/j26139960.v6i2.92

Darwin, M., Mamondol, M. R., Sormin, S. A., Nurhayati, Y., Tambunan, H., Sylvia, D., Adnyana, I. M. D. M., Prasetiyo, B., Gebang, A. A., & Vianitati, P. (2021). *Metode penelitian pendekatan kuantitatif*. https://www.researchgate.net/publication/354059356

F. Naga, J., Amor C. Tinam-isan, M., Mae O. Maluya, M., Antonnette D. Panal, K., & Tanya A. Tupac, Ma. (2024). Investigating the Relationship Between Personality Traits and Information Security Awareness. *International Journal of Computing and Digital Systems*, *15*(1), 1233–1246. https://doi.org/10.12785/ijcds/160191

Fadlika, R., Ruldeviyani, Y., Tuah Butarbutar, Z., Istiqomah, R. A., & Fariz, A. A. (2023). Employee Information Security Awareness in the Power Generation Sector of PT ABC. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 14, Issue 4). www.ijacsa.thesai.org

Hayes, A. F. (2015). An Index and Test of Linear Moderated Mediation. *Multivariate Behavioral Research*, *50*(1), 1–22. https://doi.org/10.1080/00273171.2014.962683

Huang, J.-H., Yang, C.-H. H., Chen, P.-Y., Chen, M.-H., & Worring, M. (2023). *Causalainer: Causal Explainer for Automatic Video Summarization*. http://arxiv.org/abs/2305.00455

Iba, Z., & Wardhana, A. (2023). *METODE PENELITIAN* (M. Pradana, A. A. Hayuwaskita, & H. Sukma, Eds.). https://www.researchgate.net/publication/382060598

Iba, Z., & Wardhana, A. (2024). *ANALISIS REGRESI DAN ANALISIS JALUR UNTUK RISET BISNIS MENGGUNAKAN SPSS 29.0 & SMART-PLS 4.0* (M. Pradana, A. A. Hayuwaskita, & N. C. Nisa, Eds.). EUREKA MEDIA AKSARA.

Iriqat, Y. M. (2022). Investigating Benefits Realization of Information Security Policies for Palestine Higher Education: An SEM-ANN Approach. *International Journal on Engineering*, *4*(4).

Julmi, C. (2019). When rational decision-making becomes irrational: a critical assessment and re-conceptualization of intuition effectiveness. *Business Research*, *12*(1), 291–314. https://doi.org/10.1007/s40685-019-0096-4

Nagata, K. (2024). *Establishing Information Security Policy as an Organizational Risk Management*. www.intechopen.com

Okokpujie, K., Kennedy, C. G., Nnodu, K., & Noma-Osagha, E. (2023). Cybersecurity Awareness: Investigating Students' Susceptibility to Phishing Attacks for Sustainable Safe Email Usage in Academic Environment (A Case Study of a Nigerian Leading University). *International Journal of Sustainable Development and Planning*, *18*(1), 255–263. https://doi.org/10.18280/ijsdp.180127

Pawar, N., & Tijare, P. A. (2023). A Review on Phishing Website Detection Using Machine Learning Approach. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 267–272. https://doi.org/10.32628/cseit2390227

Sari, P. K., Prasetio, A., Candiwan, Handayani, P. W., Hidayanto, A. N., Syauqina, S., Astuti, E. F., & Tallei, F. P. (2021). Information security cultural differences among health care facilities in Indonesia. *Heliyon*, *7*(6). https://doi.org/10.1016/j.heliyon.2021.e07248

Schutz, A. E., & Fertig, T. (2023). *The Forgotten Model – Validating the Integrated Behavioral Model in Context of*

Information Security Awareness.
Sekaran, U., & Bougie, R. (2016). *Research Methods for Business*. www.wileypluslearningspace.com
Sturman, D., Auton, J. C., & Morrison, B. W. (2024). Security awareness, decision style, knowledge, and phishing email detection: Moderated mediation analyses. *Computers and Security*, *148*. https://doi.org/10.1016/j.cose.2024.104129
Sun, Y., Chong, N., & Ochiai, H. (2021). *Federated Phish Bowl: LSTM-Based Decentralized Phishing Email Detection*. http://arxiv.org/abs/2110.06025
Tharani, J. S., & Arachchilage, N. A. G. (2020). *Understanding Phishers' Strategies of Mimicking URLs to Leverage Phishing Attacks: A Machine Learning Approach*. http://www.g0og1e.com
Uma. (2024). *7 Ciri-ciri E-mail Phising, Hati-hati !* https://p2ti.uma.ac.id/7-ciri-ciri-e-mail-phising-hati-hati/
Verma, P., Goyal, A., & Gigras, Y. (2020). Email phishing: text classification using natural language processing. *Computer Science and Information Technologies*, *1*(1), 1–12. https://doi.org/10.11591/csit.v1i1.p1-12
Wahyudi, I., & Damanik, D. (2022). *METODOLOGI PENELITIAN MANAJEMEN*. https://www.researchgate.net/publication/365038890
Zulauf, K., & Wagner, R. (2021). Intuitive and Deliberative Decision-Making in Negotiations. *Management Dynamics in the Knowledge Economy*, *9*(3), 293–306. https://doi.org/10.2478/mdke-2021-0020