DARI PESAN MENCURIGAKAN MENUJU RESPONS AMAN: EDUKASI KEAMANAN SIBER BERBASIS KASUS BAGI PEGAWAI KCP BANK MANDIRI PERAK TIMUR SURABAYA

***Elly Yuniar Nitawati[1], Fitriyah Kusuma Devi[2], Amas Raka Darmawan[3]**
[1] [3]Program Studi Manajemen, Fakultas Ekonomi dan Bisnis, Universitas Bhayangkara Surabaya
[2] Program Studi Akuntansi, Fakultas Ekonomi dan Bisnis, Universitas Bhayangkara Surabaya

**Corresponding Author: ellyyuniar@ubhara.ac.id*

ABSTRACT

Bank employees make security decisions while processing digital communications, transactions, and sensitive information. A preliminary survey and semi-structured interview with the management of Bank Mandiri Perak Timur Sub-Branch, Surabaya, identified the need for contextual learning on phishing, social engineering, credential protection, personal data, and incident reporting. This community engagement program was implemented from 25 May to 5 June 2026, with the main webinars held on 3-4 June. The intervention combined needs assessment, role-relevant case design, concise explanation, interactive discussion, and qualitative reflection. The evaluation drew on process observation, scenario discussion, and participant feedback without collecting customer data or internal security information. The learning process centered on five safe decisions: pause before acting, inspect message indicators, verify through official channels, protect data and access, and report suspected incidents. Case discussion also positioned cybersecurity as a shared organizational responsibility rather than an issue assigned solely to information-technology personnel. The program produced an initial five-step response framework and a needs-to-response matrix for future role-based training. These outputs are meaningful because they translate technical and legal information into practical decisions relevant to daily banking work. Further evaluation is required to assess retention and behavioral application.
Keywords: *case-based education; cybersecurity awareness; phishing; banking employees; social engineering*

ABSTRAK

Pegawai perbankan mengambil keputusan keamanan ketika memproses komunikasi digital, transaksi, dan informasi sensitif. Survei serta wawancara semi-terstruktur dengan pimpinan KCP Bank Mandiri Perak Timur Surabaya mengidentifikasi kebutuhan pembelajaran kontekstual mengenai phishing, rekayasa sosial, perlindungan kredensial, data pribadi, dan pelaporan insiden. Program pengabdian dilaksanakan pada 25 Mei-5 Juni 2026 dengan rangkaian webinar utama pada 3-4 Juni. Intervensi memadukan asesmen kebutuhan, perancangan kasus yang relevan dengan peran pegawai, penjelasan ringkas, diskusi interaktif, dan refleksi kualitatif. Evaluasi menggunakan observasi proses, pembahasan skenario, serta umpan balik peserta tanpa menghimpun data nasabah atau informasi keamanan internal. Proses pembelajaran dipusatkan pada lima keputusan aman: berhenti sebelum bertindak, memeriksa indikator pesan, memverifikasi melalui saluran resmi, melindungi data dan akses, serta melaporkan indikasi insiden. Diskusi kasus juga menempatkan keamanan siber sebagai tanggung jawab bersama dalam organisasi, bukan hanya urusan unit teknologi informasi. Program menghasilkan kerangka awal respons lima langkah dan matriks kebutuhan-respons untuk pengembangan pelatihan berbasis peran. Luaran tersebut bermakna karena menerjemahkan informasi teknis dan hukum menjadi keputusan yang dekat dengan pekerjaan perbankan. Evaluasi lanjutan diperlukan untuk menilai retensi dan penerapannya dalam perilaku kerja.
Kata kunci: edukasi berbasis kasus; kesadaran keamanan siber; phishing; pegawai perbankan; rekayasa sosial

1. PENDAHULUAN

Transformasi layanan perbankan memperluas penggunaan komunikasi digital, sistem transaksi, dan pertukaran informasi. Perubahan tersebut meningkatkan efisiensi, tetapi juga memperbanyak titik keputusan yang dapat dimanfaatkan melalui phishing, rekayasa sosial, pencurian identitas, tautan berbahaya, dan permintaan data yang tampak mendesak. Risiko tidak hanya muncul dari kelemahan perangkat. Cara pengguna membaca pesan, menilai urgensi, memverifikasi identitas, dan melaporkan kejanggalan ikut menentukan

kemampuan organisasi menghentikan rantai serangan. Oleh karena itu, pengendalian teknis perlu berjalan bersama penguatan kapasitas manusia dan budaya keamanan organisasi (Pollini et al., 2022; Triplett, 2022; Colabianchi et al., 2025).

Konteks tersebut penting bagi pegawai perbankan karena pekerjaan mereka bersinggungan dengan data nasabah, komunikasi layanan, informasi internal, dan proses transaksi. Pesan yang menggunakan nama pihak yang dikenal, permintaan perubahan data, lampiran pekerjaan, atau instruksi segera dapat terlihat wajar ketika diterima di tengah tekanan aktivitas. Kesadaran keamanan karena itu tidak cukup dibangun melalui hafalan jenis ancaman. Pegawai memerlukan pola keputusan yang dapat digunakan ketika konteks belum jelas: menahan respons, membaca indikator, memeriksa kewenangan, menggunakan saluran pembanding, melindungi kredensial, dan mengeskalasi indikasi insiden. Pelatihan yang adaptif, relevan dengan peran, dan menggunakan kasus lebih berpeluang menghubungkan pengetahuan dengan tindakan dibandingkan materi generik (Khando et al., 2021; Ben Salamah et al., 2023; Prümmer et al., 2024).

KCP PT Bank Mandiri (Persero), Tbk Perak Timur Surabaya menjadi mitra program KKN Tematik Kelompok Nusantara Universitas Bhayangkara Surabaya. Survei lapangan dan wawancara awal dengan pimpinan mitra pada Mei 2026 menunjukkan perlunya pembaruan materi mengenai phishing, rekayasa sosial, perlindungan kata sandi dan kredensial, data pribadi, serta prosedur respons terhadap pesan mencurigakan. Asesmen tidak diarahkan untuk menilai konfigurasi keamanan bank atau membahas insiden tertentu. Fokusnya adalah menentukan bentuk pembelajaran yang aman, relevan, dan dapat digunakan oleh pegawai dalam komunikasi digital sehari-hari.

Kajian keamanan berpusat pada manusia menempatkan pegawai bukan sekadar sebagai sumber kesalahan, tetapi sebagai pengamat aktif yang dapat mengenali anomali dan menghentikan tindakan impulsif. Lingkungan organisasi tetap perlu menyediakan prosedur, saluran pelaporan, dukungan manajemen, dan materi yang diperbarui. Program kesadaran yang berkelanjutan juga memerlukan kombinasi pembelajaran, penguatan budaya, dan evaluasi berkala (Alsharida et al., 2023; Taherdoost et al., 2024; Armas et al., 2025). Atas dasar tersebut, pengabdian dirancang sebagai rangkaian edukasi kolaboratif berbasis kasus yang menghubungkan kebutuhan mitra, pengetahuan teknis, prinsip pelindungan data pribadi, dan keputusan respons aman. Artikel ini menganalisis bagaimana intervensi bekerja, tema respons yang muncul dalam diskusi, serta kontribusi praktisnya bagi pelatihan keamanan siber berbasis peran.

2. TEORI

2.1 Kesadaran Keamanan Siber sebagai Kapasitas Mengambil Keputusan

Kesadaran keamanan siber mencakup pengetahuan tentang ancaman, perhatian terhadap risiko, dan kesiapan memilih perilaku perlindungan. Hubungan ketiganya tidak otomatis. Pegawai dapat mengenali istilah phishing, tetapi tetap mengikuti instruksi ketika pesan menggunakan identitas yang familier, menyentuh tugas rutin, atau menciptakan rasa mendesak. Karena itu, kesadaran perlu dipahami sebagai kapasitas kontekstual untuk membaca tanda, menunda respons, dan memilih langkah yang dapat mengurangi risiko (Li et al., 2022; Alsharida et al., 2023).

Dalam konteks pekerjaan, keputusan aman dapat diamati melalui cara seseorang memeriksa pengirim, tujuan tautan, jenis data yang diminta, kesesuaian kewenangan, dan jalur verifikasi. Kapasitas tersebut lebih mudah dikembangkan ketika peserta menghadapi skenario yang menyerupai situasi nyata dan diminta menjelaskan alasan pilihannya. Pembahasan alasan penting karena jawaban yang tampak benar dapat lahir dari tebakan, sedangkan pemahaman yang lebih fungsional terlihat ketika peserta mampu menggunakan prinsip yang sama pada variasi kasus.

2.2 Keamanan Berpusat pada Manusia dan Tanggung Jawab Organisasi

Pendekatan keamanan berpusat pada manusia memandang pegawai sebagai bagian dari sistem pertahanan organisasi. Kemampuan mereka perlu ditopang oleh antarmuka yang jelas, prosedur verifikasi, pembagian kewenangan, dan budaya pelaporan yang tidak menyalahkan orang yang menyampaikan indikasi secara bertanggung jawab. Perspektif ini menghindari dua ekstrem: membebankan seluruh kegagalan kepada individu atau menganggap teknologi akan selalu menghentikan ancaman. Faktor manusia, desain organisasi, dan teknologi perlu dibaca sebagai satu sistem (Mc Mahon & Brézillon, 2020; Pollini et al., 2022; Colabianchi et al., 2025).

2.3 Edukasi Kolaboratif Berbasis Kasus

Edukasi kolaboratif menempatkan mitra sebagai pemilik konteks kebutuhan, perguruan tinggi sebagai fasilitator pengetahuan, dan peserta sebagai pengambil keputusan dalam skenario. Asesmen kebutuhan mengarahkan pemilihan materi, sedangkan diskusi kasus membuka ruang untuk menguji alasan, memperjelas prosedur, dan menemukan bagian yang perlu diperkuat. Pola ini sejalan dengan perkembangan pelatihan keamanan siber yang bergerak menuju metode adaptif, simulatif, dan berbasis peran (Alnajim et al., 2023; Ben Salamah et al., 2023; Prümmer et al., 2024).

Dalam program ini, kasus tidak digunakan untuk menguji kerentanan internal bank. Seluruh skenario bersifat hipotetis dan disusun pada tingkat literasi umum. Prinsip pelindungan data pribadi diterjemahkan ke dalam pembatasan akses, kehati-hatian berbagi informasi, dan penggunaan data sesuai tujuan sebagaimana ditekankan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

3. METODE

Program menggunakan pendekatan edukasi kolaboratif berbasis kebutuhan mitra. Rangkaian kegiatan berlangsung pada 25 Mei-5 Juni 2026 di KCP PT Bank Mandiri (Persero), Tbk Perak Timur Surabaya. Webinar utama dilaksanakan pada 3-4 Juni 2026 melalui Zoom Meeting, dimulai pukul 10.00 WIB. Tim pelaksana terdiri atas 13 mahasiswa KKN Tematik Kelompok Nusantara dengan pendampingan dosen pembimbing lapangan, sedangkan penerima manfaat merupakan pegawai mitra yang mengikuti rangkaian edukasi.

Tahap pertama berupa survei dan wawancara semi-terstruktur dengan pimpinan mitra. Pertanyaan diarahkan pada kebutuhan pembaruan pengetahuan, bentuk komunikasi digital yang perlu diwaspadai, pengalaman umum menghadapi pesan mencurigakan, format pembelajaran yang memungkinkan, dan aspek hukum yang relevan. Catatan asesmen diringkas menjadi tema kebutuhan tanpa memuat nama pegawai, data nasabah, rincian insiden, kredensial, atau konfigurasi sistem.

Tahap kedua adalah perancangan materi dan skenario. Tim mengelompokkan kebutuhan menjadi pengenalan ancaman, rekayasa sosial, perlindungan kredensial dan data, verifikasi identitas, serta pelaporan indikasi insiden. Kasus hipotetis memuat pesan dengan tekanan waktu, permintaan kode autentikasi, tautan dokumen, dan instruksi perubahan informasi. Setiap kasus dibahas melalui tiga pertanyaan: tanda apa yang perlu dicermati, tindakan apa yang harus ditunda atau dilakukan, dan saluran apa yang digunakan untuk verifikasi atau pelaporan.

Tahap ketiga adalah webinar dan diskusi. Penjelasan singkat digunakan untuk memberi kerangka, kemudian peserta diajak menilai kasus serta mengemukakan alasan di balik keputusan. Fasilitator menanggapi jawaban dengan menelusuri risiko, kewenangan, dan prosedur yang relevan. Tahap keempat berupa refleksi kualitatif dan umpan balik untuk memetakan tema respons serta kebutuhan tindak lanjut.

Evaluasi difokuskan pada proses pembelajaran. Catatan fasilitator, pembahasan skenario, dan refleksi peserta dikelompokkan menurut pengenalan ancaman, verifikasi, perlindungan data, pelaporan, dan tanggung jawab organisasi. Dokumentasi ditampilkan setelah identitas peserta dianonimkan. Program tidak menggunakan pengukuran sebelum-sesudah atau pemantauan perilaku, sehingga pembahasan diarahkan pada dinamika intervensi dan tema pembelajaran yang muncul.

4. HASIL DAN PEMBAHASAN

4.1 Kebutuhan Mitra dan Perancangan Respons Edukasi

Asesmen mitra memperlihatkan bahwa kebutuhan edukasi tidak berhenti pada pengenalan istilah teknis. Tantangan yang lebih dekat dengan pekerjaan adalah menentukan respons ketika sebuah pesan terlihat meyakinkan, menggunakan identitas yang dikenal, meminta tindakan cepat, atau mengarahkan pegawai untuk membagikan informasi. Karena itu, materi disusun dengan menghubungkan setiap kebutuhan pada risiko dan keputusan aman sebagaimana diringkas dalam Tabel 1.

Tabel 1. Hubungan Kebutuhan Mitra, Risiko, dan Respons Edukasi

Kebutuhan Mitra	Risiko Utama	Fokus Kasus	Respons Aman
Mengenali phishing	Pencurian kredensial	Pengirim, tautan, bahasa, dan urgensi	Berhenti dan periksa indikator

DOI: 10.55499/semeru.v3i1.1706

E-ISSN: 3047-6518
Halaman: 371-377

Kebutuhan Mitra	Risiko Utama	Fokus Kasus	Respons Aman
Menghadapi rekayasa sosial	Manipulasi keputusan	Permintaan data atau instruksi mendesak	Verifikasi melalui saluran resmi
Melindungi data dan akses	Kebocoran informasi	Kode autentikasi, kata sandi, dan dokumen	Batasi akses dan lindungi kredensial
Merespons indikasi insiden	Keterlambatan mitigasi	Pesan, tautan, atau aktivitas yang mencurigakan	Simpan informasi relevan dan laporkan
Memahami tanggung jawab	Respons tidak terkoordinasi	Peran pegawai, unit terkait, dan manajemen	Ikuti prosedur dan eskalasi sesuai kewenangan

Sumber: Dokumen program KKN Tematik Kelompok Nusantara, diolah penulis (2026).

Matriks tersebut menunjukkan bahwa phishing dan rekayasa sosial diperlakukan sebagai masalah pengambilan keputusan, bukan sekadar daftar modus. Prinsip pemeriksaan dibuat lintas media agar dapat digunakan pada email, pesan instan, telepon, kode QR, atau dokumen digital. Materi perlindungan data juga tidak berhenti pada ancaman sanksi, tetapi menjelaskan mengapa kredensial, kode autentikasi, dan informasi sensitif memerlukan pembatasan akses. Orientasi ini selaras dengan penelitian yang menekankan pentingnya pengetahuan, persepsi risiko, kemampuan mengatasi ancaman, dan dukungan organisasi dalam perilaku proteksi (Li et al., 2022; Taherdoost et al., 2024).

4.2 Pelaksanaan Kasus dan Dinamika Respons Peserta

Webinar dimulai dengan pengenalan bentuk ancaman dan faktor psikologis yang sering digunakan penyerang, seperti otoritas semu, rasa mendesak, rasa takut, atau iming-iming keuntungan. Materi kemudian dipindahkan ke kasus. Pada skenario phishing, peserta diarahkan memeriksa alamat pengirim, tujuan tautan, permintaan kredensial, kesesuaian bahasa, dan konteks pekerjaan. Pada skenario rekayasa sosial, diskusi memusatkan perhatian pada cara memverifikasi identitas melalui nomor atau kanal yang diperoleh secara mandiri, bukan melalui kontak yang diberikan dalam pesan mencurigakan.

Catatan fasilitator menunjukkan bahwa pembahasan berkembang pada lima tema keputusan. Pertama, respons tidak perlu diberikan seketika hanya karena pesan menggunakan bahasa mendesak. Kedua, tampilan profesional dan identitas yang familiar bukan bukti bahwa pengirim dapat dipercaya. Ketiga, verifikasi perlu dilakukan melalui saluran resmi dan sesuai kewenangan. Keempat, data serta akses akun harus dilindungi sebelum kerugian meluas. Kelima, pelaporan merupakan bagian dari pencegahan karena informasi awal memungkinkan organisasi melakukan penanganan yang lebih cepat. Tema tersebut tidak dibaca sebagai skor peningkatan, tetapi memperlihatkan bagaimana kasus mengarahkan diskusi dari pengenalan ancaman menuju pilihan tindakan.

Gambar 1. Tampilan Pembukaan Webinar Keamanan Siber yang Telah Dianonimkan
Sumber: Dokumentasi Tim KKN Tematik Kelompok Nusantara (2026).

DOI: 10.55499/semeru.v3i1.1706

Penggunaan contoh yang disamarkan menjaga diskusi tetap relevan tanpa membuka informasi internal bank. Dimensi hukum disampaikan melalui prinsip pelindungan data pribadi, kehati-hatian berbagi informasi, dan tanggung jawab mengikuti prosedur organisasi. Peserta tidak diarahkan melakukan investigasi mandiri. Fokus program adalah menguatkan jeda pengambilan keputusan dan penggunaan saluran yang tepat ketika menemukan indikasi ancaman.

4.3 Dari Pengetahuan Ancaman menuju Tanggung Jawab Bersama

Salah satu makna penting diskusi adalah penempatan keamanan siber sebagai tanggung jawab bersama. Unit teknologi informasi dan keamanan memiliki peran khusus, tetapi pegawai pada berbagai fungsi berada pada titik awal ketika pesan, telepon, atau permintaan data diterima. Keputusan untuk menghentikan tindakan, memeriksa kejanggalan, dan melapor dapat memutus rangkaian serangan sebelum mencapai sistem atau data yang lebih luas. Perspektif ini sesuai dengan pendekatan keamanan berpusat pada manusia yang menuntut kombinasi kapasitas pengguna, dukungan prosedur, dan kepemimpinan organisasi (Triplett, 2022; Colabianchi et al., 2025).

Kolaborasi dengan mitra juga membuat program tidak berhenti pada materi universal. Wawancara awal menentukan prioritas, format webinar menyesuaikan ketersediaan pegawai, dan kasus dibatasi pada situasi yang dapat dibahas secara aman. Pola tersebut memperlihatkan fungsi asesmen sebagai jembatan antara literatur keamanan siber dan kebutuhan organisasi. Pelatihan yang dimulai dari konteks peran memiliki peluang lebih besar untuk digunakan kembali dan diperbarui ketika modus berubah (Ben Salamah et al., 2023; Armas et al., 2025).

4.4 Kerangka Respons Aman dan Kontribusi Program

Refleksi atas materi dan dinamika kasus menghasilkan kerangka awal Berhenti-Periksa-Verifikasi-Lindungi-Laporkan. Berhenti memberi jeda agar keputusan tidak didorong oleh tekanan. Periksa mengarahkan perhatian pada pengirim, tautan, konteks, dan jenis informasi yang diminta. Verifikasi menggunakan saluran resmi yang diperoleh secara mandiri. Lindungi berarti tidak membagikan kredensial, membatasi akses, dan mengamankan akun atau data yang berisiko. Laporkan menghubungkan indikasi insiden dengan unit atau prosedur yang berwenang.

Gambar 2. Kerangka Awal Respons Aman Pada Pesan Atau Permintaan Digital Mencurigakan
Sumber: Refleksi program KKN Tematik Kelompok Nusantara, diolah penulis (2026).

Kerangka tersebut menjadi kontribusi praktis karena menyederhanakan banyak jenis ancaman ke dalam urutan keputusan yang dapat dipakai lintas saluran. Nilainya bukan menggantikan kebijakan keamanan bank, melainkan menyediakan bahasa pembelajaran yang menghubungkan karakteristik ancaman dengan respons pegawai. Secara metodologis, program menunjukkan bahwa asesmen kebutuhan, kasus yang relevan, diskusi alasan, dan refleksi dapat disusun sebagai satu siklus edukasi berbasis peran. Program lanjutan dapat menggunakan modul singkat untuk fungsi kerja yang berbeda, pembaruan skenario, simulasi yang disetujui organisasi, serta evaluasi berkala sebagaimana direkomendasikan dalam kajian pelatihan keamanan siber (Alnajim et al., 2023; Prümmer et al., 2024).

4.5 Makna, Keterbatasan, dan Keberlanjutan

Kegiatan bermakna karena mempertemukan pengetahuan teknis, perlindungan data, dan keputusan operasional dalam situasi yang dekat dengan pekerjaan. Pegawai tidak hanya menerima daftar ancaman, tetapi

diajak menilai mengapa sebuah pesan berisiko dan tindakan apa yang paling aman sebelum mengikuti instruksi. Cara ini membantu organisasi membangun bahasa bersama tentang verifikasi, perlindungan, dan pelaporan.

Evaluasi program masih terbatas pada proses diskusi dan refleksi; dokumentasi sumber juga belum menyediakan data agregat peserta maupun pengukuran sebelum-sesudah. Karena itu, kegiatan berikutnya perlu menilai respons berbasis skenario pada awal dan akhir sesi, retensi beberapa minggu setelah pelatihan, serta penggunaan jalur pelaporan tanpa membuka data sensitif. Keberlanjutan akan lebih kuat apabila materi diperbarui secara berkala, disesuaikan dengan peran kerja, dan didukung oleh pimpinan serta unit yang berwenang.

5. SIMPULAN

Program edukasi keamanan siber berbasis kasus di KCP Bank Mandiri Perak Timur Surabaya disusun dari asesmen kebutuhan mitra dan dilaksanakan melalui rangkaian webinar, diskusi skenario, serta refleksi. Intervensi memusatkan pembelajaran pada phishing, rekayasa sosial, perlindungan kredensial dan data pribadi, verifikasi identitas, serta pelaporan indikasi insiden. Pembahasan kasus menghubungkan tanda teknis dan psikologis dengan lima keputusan aman: Berhenti, Periksa, Verifikasi, Lindungi, dan Laporkan.

Kontribusi program terletak pada penerjemahan informasi keamanan menjadi orientasi tindakan yang relevan dengan pekerjaan perbankan serta pada pembentukan kerangka awal pelatihan kolaboratif berbasis peran. Keamanan siber ditempatkan sebagai tanggung jawab bersama yang ditopang oleh keputusan pegawai, prosedur organisasi, dan dukungan manajemen. Pengembangan berikutnya perlu menambahkan pengukuran berbasis skenario dan pemantauan berkala agar retensi serta penerapan perilaku aman dapat dinilai secara lebih kuat.

REFERENSI

Alnajim, A. M., Habib, S., Islam, M., Albelaihi, R., & Alabdulatif, A. (2023). Exploring cybersecurity education and training techniques: A comprehensive review of traditional, virtual reality, and augmented reality approaches. *Symmetry*, 15(12), 2175. https://doi.org/10.3390/sym15122175

Alsharida, R. A., Hammood, M. M., & Al-Emran, M. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, 73, 102223. https://doi.org/10.1016/j.techsoc.2023.102223

Armas, R., Hurtado, J., & Figueroa, M. (2025). Building a cybersecurity culture in higher education: A cybersecurity awareness and training framework. *Information*, 16(5), 336. https://doi.org/10.3390/info16050336

Ben Salamah, F., Alzahrani, A., & Alghamdi, A. (2023). An adaptive cybersecurity training framework for the development of the human factor. *Applied Sciences*, 13(17), 9595. https://doi.org/10.3390/app13179595

Colabianchi, S., Costantino, F., & Gravio, G. D. (2025). The role of human factors in enhancing cybersecurity. *Journal of Innovation & Knowledge*, 10, 100695. https://doi.org/10.1016/j.jik.2025.100695

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, 106, 102267. https://doi.org/10.1016/j.cose.2021.102267

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports*, 5, 100165. https://doi.org/10.1016/j.chbr.2021.100165

Mc Mahon, C., & Brézillon, P. (2020). In defence of the human factor. *Frontiers in Psychology*, 11, 1390. https://doi.org/10.3389/fpsyg.2020.01390

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology & Work*, 24, 371-390. https://doi.org/10.1007/s10111-021-00683-y

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security*, 136, 103585. https://doi.org/10.1016/j.cose.2023.103585

Taherdoost, H., Madanchian, M., & Zaman, M. (2024). Towards an innovative model for cybersecurity awareness programs. *Information*, 15(9), 512. https://doi.org/10.3390/info15090512

Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy*, 2(3), 573-586. https://doi.org/10.3390/jcp2030029

Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.