Original Article

e-XXXX-XXXX

Original Article

Analisis Kesadaran Keamanan Siber Pengguna terhadap Ancaman Social Engineering Berbasis OSINT

Andi Athifah Nur Aprilia[1]✉, Sulfiyanti Putri Absar[2] , Debora Patricia Joy Lubis[3], Rakhmadi Rahman[4]
[1,2,3]Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Indonesia,
Korespondensi Author: andiathifahnurapriliariri@gmail.com, sulfiyantiputriabsar23@gmail.com, dboralubis@gmail.com, rakhmadi.rahman@ith.ac.id

Abstrak:

Penelitian ini menganalisis tingkat kesadaran pengguna tentang keamanan siber terkait ancaman Social Engineering, dengan fokus pada manusia sebagai titik kelemahan utama dalam sistem keamanan. Tingkat kesadaran ini dievaluasi menggunakan pendekatan Knowledge, Attitude, and Behavior (KAB) dan instrumen HAIS-Q. Metode yang digunakan adalah campuran metode penjelasan berurutan melalui survei online terhadap 450 responden dan simulasi pengumpulan informasi terbuka (OSINT) yang terbatas. Hasil penelitian menunjukkan bahwa kesadaran keamanan pengguna berada pada tingkat sedang, dengan perbedaan yang signifikan antara pengetahuan mereka dan perilaku aktual mereka. Kerentanan utama terlihat pada kebiasaan berbagi informasi berlebihan di media sosial serta pengelolaan kata sandi yang kurang aman. Untuk meningkatkan ketahanan pengguna terhadap ancaman Social Engineering penelitian ini menyarankan integrasi solusi teknologi dengan edukasi perilaku.

Keywords: Keamanan siber, Social engineering, Kesadaran pengguna, Knowledge Attitude Behavior (KAB), HAIS-Q

Pendahuluan

Transformasi digital yang terjadi secara global, termasuk di Indonesia, telah mengubah secara fundamental cara individu dan organisasi mengelola informasi. Penggunaan teknologi digital di berbagai sektor, seperti layanan publik, pendidikan, dan aktivitas ekonomi, menghadirkan kemudahan dan efisiensi. Namun, perkembangan ini juga meningkatkan risiko terhadap ancaman keamanan siber, sehingga menuntut tingkat kesadaran keamanan yang memadai dari seluruh pengguna teknologi.

Meskipun teknologi keamanan modern, seperti enkripsi, autentikasi biometrik, dan sistem deteksi intrusi berbasis kecerdasan buatan, telah memberikan perlindungan

Received: November 20, 2025 – Revised: November 29, 2025 - Accepted: Desember 20, 2025 - Published online: January 12, 2026

teknis yang semakin canggih, insiden keamanan siber tetap terjadi. Faktor manusia masih sering menjadi titik lemah dalam rantai keamanan informasi karena kelalaian, kurangnya kewaspadaan, dan rendahnya pemahaman terhadap risiko keamanan.

Social engineering merupakan metode serangan yang mengeksploitasi aspek psikologis manusia. Serangan ini tidak menargetkan sistem secara langsung, melainkan memanipulasi korban agar secara sukarela memberikan informasi sensitif atau melakukan tindakan yang merugikan. Efektivitas social engineering semakin meningkat dengan maraknya penggunaan media sosial, yang mendorong praktik berbagi informasi pribadi secara terbuka.

Melalui metode Open-Source Intelligence (OSINT), pelaku kejahatan siber dapat mengumpulkan dan mengevaluasi data publik pengguna untuk membangun profil sasaran yang komprehensif. Data ini kemudian digunakan untuk merancang skenario serangan yang lebih personal dan sulit dideteksi. Fenomena ini menunjukkan adanya kesenjangan antara kemampuan teknis pengguna dalam mengoperasikan perangkat digital dengan pemahaman mereka mengenai keamanan siber, yang dikenal sebagai cybersecurity awareness gap.

Berdasarkan kondisi tersebut, penelitian ini berfokus pada analisis kesadaran keamanan siber pengguna terhadap ancaman social engineering dengan menggunakan kerangka Knowledge, Attitude, dan Behavior (KAB). Kerangka ini digunakan untuk memahami hubungan antara pengetahuan, sikap, dan perilaku pengguna dalam menjaga keamanan informasi.

Tinjauan Pustaka

Social Engineering

Social engineering adalah teknik serangan dalam keamanan siber yang memanfaatkan kelemahan manusia dibandingkan kelemahan teknis sistem. Serangan ini bekerja melalui manipulasi psikologis, seperti rasa takut, kepercayaan, rasa ingin tahu, atau urgensi, untuk mendorong korban melakukan tindakan yang menguntungkan penyerang. Bentuk serangan social engineering bervariasi, antara lain phishing melalui email, vishing melalui telepon, smishing melalui SMS, pretexting, dan baiting yang dirancang dengan skenario tertentu.

Berbagai penelitian menunjukkan bahwa serangan social engineering cenderung lebih efektif dibandingkan serangan teknis murni. Hal ini disebabkan oleh rendahnya kewaspadaan pengguna terhadap risiko non-teknis serta minimnya pengetahuan mengenai praktik dasar keamanan informasi. Oleh karena itu, social engineering dianggap sebagai ancaman serius yang memerlukan penanganan melalui peningkatan kesadaran dan perilaku pengguna.

Open-Source Intelligence (OSINT)

Open-Source Intelligence (OSINT) adalah metode sistematis untuk mengumpulkan, memproses, dan menganalisis informasi dari sumber terbuka yang legal diakses publik. Sumber informasi OSINT meliputi media sosial, situs resmi, forum online, blog pribadi, basis data publik, dan mesin pencari. Meskipun data yang diperoleh OSINT bersifat sah, pengguna harus berhati-hati agar informasi tersebut tidak disalahgunakan.

Dalam konteks keamanan siber, OSINT memiliki fungsi ganda: sebagai alat pertahanan dan sebagai alat serangan. Secara defensif, OSINT membantu lembaga dan peneliti keamanan memantau kebocoran data, mengidentifikasi pola ancaman, dan

Received: November 20, 2025 – Revised: November 29, 2025 - Accepted: Desember 20, 2025 - Published online: January 12, 2026

mengembangkan kebijakan perlindungan informasi yang lebih efektif. Sebaliknya, pelaku kejahatan siber memanfaatkan OSINT untuk mengumpulkan informasi pribadi pengguna, membangun profil target, dan merancang serangan social engineering yang lebih personal dan sulit dikenali korban.

Penggunaan OSINT menekankan bahwa ancaman keamanan tidak hanya berasal dari sistem, tetapi juga dari bagaimana pengguna mengelola informasi pribadi di dunia digital. Oleh karena itu, pengetahuan tentang OSINT penting untuk meningkatkan kesadaran keamanan siber, terutama dalam membatasi data yang dipublikasikan dan mengurangi risiko penyalahgunaan.

Kesadaran Keamanan Siber (Cybersecurity Awareness)

Kesadaran keamanan siber mencakup sejauh mana individu memahami, peduli, dan siap mengidentifikasi serta menanggapi ancaman terhadap informasi saat menggunakan teknologi digital. Konsep ini tidak hanya mencakup pengetahuan teknis, tetapi juga sikap dan perilaku pengguna dalam melindungi kerahasiaan, integritas, dan ketersediaan informasi.

Kesadaran keamanan siber melibatkan kemampuan mengenali ancaman, seperti tautan palsu, permintaan informasi mencurigakan, dan penggunaan kata sandi yang tidak aman. Pengguna dengan kesadaran tinggi biasanya lebih berhati-hati dalam memberikan informasi pribadi, memverifikasi sumber informasi, dan mematuhi kebijakan keamanan. Rendahnya kesadaran sering menjadi faktor utama keberhasilan serangan social engineering.

Oleh karena itu, upaya meningkatkan kesadaran keamanan siber harus menekankan pembentukan budaya aman secara berkelanjutan, termasuk pembelajaran relevan, latihan menghadapi ancaman, serta perbaikan prosedur keamanan yang mudah dipahami oleh semua pengguna. Pendekatan ini diharapkan dapat mengurangi risiko serangan yang memanfaatkan aspek perilaku manusia.

Kerangka Knowledge, Attitude, and Behavior (KAB)

Kerangka Knowledge, Attitude, and Behavior (KAB) adalah model konseptual yang digunakan untuk menganalisis tingkat kesadaran individu terhadap suatu isu, termasuk keamanan siber. Model ini menekankan bahwa perilaku individu dipengaruhi oleh pengetahuan dan sikap terhadap risiko serta ancaman tertentu.

Dimensi pengetahuan (knowledge) mencakup pemahaman pengguna tentang konsep dasar keamanan informasi, jenis ancaman siber, dan konsekuensi pelanggaran keamanan. Dimensi sikap (attitude) mencerminkan persepsi, keyakinan, dan kepedulian pengguna terhadap pentingnya keamanan siber. Sementara dimensi perilaku (behavior) menggambarkan tindakan nyata dalam menjaga keamanan informasi, seperti membatasi informasi yang dibagikan, tidak sembarangan mengklik tautan, dan mematuhi kebijakan keamanan.

Kerangka KAB memungkinkan identifikasi kesenjangan antara pengetahuan dan perilaku akibat sikap atau kebiasaan yang terbentuk. Pendekatan ini relevan untuk menganalisis kesadaran keamanan siber secara komprehensif dan merancang intervensi yang tepat, baik melalui peningkatan pengetahuan, perubahan sikap, maupun pembentukan perilaku aman yang berkelanjutan.

Received: November 20, 2025 – Revised: November 29, 2025 - Accepted: Desember 20, 2025 - Published online: January 12, 2026

Human Aspect of Information Security Questionnaire (HAIS-Q)

Human Aspect of Information Security Questionnaire (HAIS-Q) adalah instrumen untuk mengevaluasi aspek manusia dalam keamanan informasi secara sistematis. HAIS-Q mengukur kesadaran keamanan siber pengguna melalui tiga dimensi utama: pengetahuan, sikap, dan perilaku, selaras dengan kerangka KAB.

Instrumen ini menilai domain kritis keamanan informasi, seperti pengelolaan kata sandi, penggunaan email, pemanfaatan media sosial, keamanan perangkat seluler, penggunaan internet, dan pelaporan insiden. HAIS-Q menyoroti perbedaan antara pengetahuan pengguna dan tindakan nyata dalam kehidupan sehari-hari, sehingga memudahkan identifikasi area perilaku yang paling rentan terhadap serangan social engineering.

Dalam penelitian ini, HAIS-Q dijadikan dasar konseptual untuk menyusun pengukuran kesadaran keamanan siber. Pemilihan HAIS-Q didasari relevansinya terhadap aspek manusia, fleksibilitas penerapan pada berbagai konteks digital, serta kemampuannya membantu analisis keterkaitan antara pengetahuan, sikap, dan perilaku pengguna terkait keamanan informasi.

Hasil dan Pembahasan

Penelitian ini bertujuan untuk memberikan kontribusi empiris dalam bidang keamanan siber, khususnya terkait kesadaran pengguna terhadap ancaman Social Engineering. Hasil penelitian disajikan melalui beberapa aspek utama, yang kemudian dibahas secara mendalam.

Penilaian Kesadaran Keamanan Siber Berdasarkan KAB

Dengan menggunakan kerangka Knowledge, Attitude, and Behavior (KAB), penelitian ini menilai kesadaran keamanan siber pengguna secara menyeluruh. Hasil menunjukkan:

1. Knowledge (Pengetahuan)

   Responden memiliki pemahaman dasar tentang ancaman keamanan siber, termasuk phishing, manajemen kata sandi, dan risiko berbagi informasi di media sosial.

2. Attitude (Sikap)

   Pengguna menunjukkan sikap yang cukup peduli terhadap keamanan siber, tetapi tidak selalu konsisten dalam perilaku sehari-hari.

3. Behavior (Perilaku)

   Perilaku nyata pengguna masih menunjukkan kelemahan, terutama pada pengelolaan kata sandi dan pola berbagi informasi di media sosial, yang dapat dimanfaatkan oleh pelaku Social Engineering.

4. Instrumen HAIS-Q

   Digunakan untuk menilai kesadaran ini, dan temuan menunjukkan adanya kesenjangan antara pengetahuan dan praktik nyata pengguna.

Analisis OSINT dan Risiko Informasi Publik

Simulasi Open-Source Intelligence (OSINT) menunjukkan bahwa informasi publik yang dibagikan secara berlebihan meningkatkan efektivitas serangan Social Engineering. Temuan penting meliputi:

1. Profiling target dapat dilakukan dari data yang dibagikan di media sosial, seperti identitas, lokasi, rutinitas harian, dan hubungan sosial.

Received: November 20, 2025 – Revised: November 29, 2025 - Accepted: Desember 20, 2025 - Published online: January 12, 2026

2. Informasi yang tersedia secara publik dapat digunakan untuk meningkatkan keberhasilan serangan spear phishing, pretexting, atau baiting.

Identifikasi Kesenjangan Pengetahuan dan Perilaku

Penelitian ini menyoroti adanya kesenjangan signifikan antara pengetahuan dan perilaku pengguna. Contohnya:

1. Meskipun mengetahui pentingnya kata sandi yang kuat, banyak pengguna tetap menggunakan kata sandi yang sama di berbagai layanan.
2. Pengaturan privasi media sosial belum dioptimalkan sehingga memudahkan pihak ketiga memprofil pengguna.

Strategi Mitigasi yang Direkomendasikan

Berdasarkan temuan penelitian, mitigasi terhadap Social Engineering dapat dilakukan melalui dua pendekatan:

1. Mitigasi Berbasis Teknologi: Multi-Factor Authentication (MFA), Sistem penyaringan email dan pesan otomatis dan Sandboxing lampiran dan proteksi endpoint
2. Mitigasi Berbasis Perilaku dan OSINT: Pengelolaan jejak digital (Digital Footprint Management), Optimalisasi pengaturan privasi (Privacy Setting Optimization) dan Pelatihan kesadaran keamanan (Security Awareness Training / SAT)

Pendekatan ini menggabungkan teknologi dan perilaku pengguna untuk meminimalkan risiko serangan.

Faktor Manusia sebagai Titik Lemah

Hasil penelitian menunjukkan bahwa faktor manusia tetap menjadi titik lemah utama dalam keamanan siber. Pengetahuan tidak selalu diterjemahkan ke dalam perilaku aman karena kebiasaan, tekanan sosial, atau persepsi risiko yang rendah.

Peran OSINT dalam Social Engineering

Analisis OSINT memperlihatkan bahwa informasi publik dapat digunakan untuk membangun profil target yang rinci, sehingga meningkatkan keberhasilan serangan Social Engineering. Hal ini menegaskan pentingnya pengelolaan jejak digital dan pengaturan privasi yang tepat.

Kesenjangan Knowledge-Attitude-Behavior

Kerangka KAB membantu mengidentifikasi kesenjangan antara pengetahuan, sikap, dan perilaku. Temuan ini menegaskan bahwa intervensi keamanan siber harus bersifat holistik:

1. Meningkatkan pengetahuan melalui edukasi dan pelatihan
2. Membentuk sikap yang positif terhadap praktik keamanan
3. Mendorong perilaku aman secara konsisten

Implementasi Mitigasi Berlapis

Pendekatan mitigasi berlapis (layered approach) yang memadukan teknologi dan perilaku dinilai paling efektif. Teknologi berfungsi sebagai lapisan pertahanan awal, sementara mitigasi perilaku mengurangi kemungkinan serangan berhasil dengan membangun kesadaran dan tanggung jawab pengguna.

Received: November 20, 2025 – Revised: November 29, 2025 - Accepted: Desember 20, 2025 - Published online: January 12, 2026

Implikasi Praktis

Hasil penelitian ini dapat digunakan untuk:

1. Mengembangkan program edukasi dan pelatihan keamanan siber di institusi pendidikan dan organisasi.
2. Membimbing pengguna untuk mengelola jejak digital dan privasi secara lebih aman.
3. Memberikan dasar bagi legislator untuk menyusun kebijakan yang mendorong praktik keamanan siber yang lebih baik.

Kontribusi terhadap Literatur dan Praktik

Penelitian ini menambah bukti empiris tentang pentingnya faktor manusia dalam keamanan siber. Dengan menggabungkan KAB dan OSINT, penelitian ini menegaskan bahwa mitigasi Social Engineering harus holistik, mencakup aspek teknis, perilaku, dan pengelolaan informasi publik.

Jadwal Penelitian

Penelitian ini dijadwalkan berjalan selama enam bulan, mulai dari Januari hingga Juni 2026, dengan tahapan sebagai berikut:

Tabel 1. Jadwal Kegiatan

No	Kegiatan	Jan	Feb	Mar	Apr	Mei	Jun
1	Studi literatur dan perumusan instrumen penelitian	✓					
2	Uji validitas dan reliabilitas kuesioner	✓					
3	Pengumpulan data kuantitatif (survei)		✓				
4	Analisis data kuantitatif (SEM-PLS)			✓			
5	Simulasi OSINT dan pengumpulan data kualitatif			✓			
6	Triangulasi data dan pembahasan hasil				✓		
7	Penyusunan model mitigasi dan rekomendasi					✓	
8	Finalisasi laporan dan publikasi ilmiah						✓

Received: November 20, 2025 – Revised: November 29, 2025 - Accepted: Desember 20, 2025 - Published online: January 12, 2026

Kesimpulan

Berdasarkan hasil penelitian, dapat disimpulkan bahwa tingkat pengetahuan pengguna terhadap keamanan siber, khususnya terkait ancaman Social Engineering, masih tergolong terbatas. Meskipun sebagian besar responden telah mengenal bentuk serangan dasar seperti phishing, terdapat kesenjangan yang signifikan antara pengetahuan tersebut dan perilaku nyata dalam aktivitas digital sehari-hari. Praktik berisiko seperti berbagi informasi berlebihan di media sosial, penggunaan pengaturan privasi yang lemah, serta penerapan kata sandi yang tidak aman masih sering ditemukan.

Hasil simulasi Open-Source Intelligence (OSINT) menunjukkan bahwa informasi pribadi pengguna relatif mudah diakses melalui akun publik, sehingga meningkatkan potensi serangan yang memanfaatkan manipulasi psikologis. Temuan ini menegaskan bahwa faktor manusia masih menjadi titik lemah utama dalam sistem keamanan siber. Oleh karena itu, upaya peningkatan ketahanan pengguna sebagai garis pertahanan pertama dalam keamanan siber perlu dilakukan melalui pendekatan yang terintegrasi, dengan mengombinasikan solusi teknologi dan peningkatan kesadaran serta perubahan perilaku pengguna secara berkelanjutan.

Saran

Berdasarkan hasil penelitian ini, disarankan agar upaya peningkatan keamanan siber tidak hanya berfokus pada penguatan aspek teknis, tetapi juga pada pembentukan perilaku pengguna secara berkelanjutan. Pengguna dan organisasi perlu menerapkan program Security Awareness Training (SAT) yang terstruktur dan berkesinambungan, dengan penekanan pada pengelolaan kata sandi yang aman, optimalisasi pengaturan privasi media sosial, serta pengendalian jejak digital. Selain itu, pemanfaatan teknologi pendukung seperti Multi-Factor Authentication (MFA), sistem penyaringan email, dan perlindungan endpoint perlu dioptimalkan sebagai lapisan pertahanan tambahan untuk meminimalkan dampak serangan Social Engineering.

Di sisi lain, institusi pendidikan dan pembuat kebijakan diharapkan dapat mengintegrasikan literasi keamanan siber ke dalam kurikulum dan regulasi yang relevan, sehingga kesadaran terhadap risiko digital dapat dibangun sejak dini. Untuk pengembangan keilmuan, penelitian selanjutnya disarankan mengkaji efektivitas penerapan strategi mitigasi yang diusulkan melalui pendekatan kuantitatif dan kualitatif yang lebih mendalam, termasuk studi longitudinal guna mengamati perubahan perilaku pengguna dalam jangka panjang setelah dilakukan intervensi keamanan siber.

Daftar Pustaka

Afrizal Zein. (2023). Analisa Penyerangan untuk Cyber Security Social Engineering. Jurnal Informatika Universitas Pamulang, 8(4), 642–648.

Nurhakim, R., Habibi, C., & Marwondo. (2024). Analisis Dan Mitigasi Ancaman Social Engineering Pada Pengguna Facebook Dengan Pendekatan OSINT. Prosiding Seminar Nasional CORISINDO.

Badan Siber dan Sandi Negara (BSSN). (2023). Laporan Tahunan Monitoring Keamanan Siber Indonesia.

Hadlington, L. (2017). Human Factors in Cybersecurity: Examining the Link Between Fear of Missing Out, Internet Addiction, and Risky Cybersecurity Behavior. Royal

Received: November 20, 2025 – Revised: November 29, 2025 - Accepted: Desember 20, 2025 - Published online: January 12, 2026

Society Open Science.
Putu, I., Pratama, A. E., dkk. (2019). Penerapan Proxy Server Berbasis Clearos 7 Untuk Manajemen Akses Pada Internet. Jurnal Mantik Penusa.
Razzaq, A., dkk. (2022). Serangan Hacking Tools sebagai Ancaman Siber dalam Sistem Pertahanan Negara. Global Political Studies Journal.
Slamet. (2022). Pertahanan Pencegahan Serangan Social Engineering Menggunakan Two Factor Authentication (2FA) Berbasis SMS. Darmaningrat, E. W. T., dkk. (2022). Sosialisasi Bahaya dan Upaya Pencegahan Social Engineering. Jurnal Pengabdian Masyarakat.

Received: November 20, 2025 – Revised: November 29, 2025 - Accepted: Desember 20, 2025 - Published online: January 12, 2026