JISTIC
Journal of Information Technology, Information System and Communications
Department of Information System, Faculty of Sains and Technology, PGRI Kanjuruhan University
E-ISSN: 3021-8322
Vol. 4, No. 1, 2026

EVALUASI SIMULASI *PHISHING* SEBAGAI UPAYA PENINGKATAN KESADARAN KEAMANAN INFORMASI

Naufalarizqa Ramadha Meisa Putra
Teknik Informatika, Universitas Satya Negara Indonesia
naufalarizqa@usni.ac.id

Abstract. Phishing attacks remain one of the most prevalent information security threats in organizations because they exploit human behavior through social engineering rather than technical vulnerabilities. In the financial services sector, extensive reliance on corporate email and digital applications further increases potential exposure and organizational impact. This study evaluates the effectiveness of phishing simulations as a method to assess user behavior and information security awareness within an organizational environment. The research employs a quantitative descriptive approach using a controlled phishing simulation distributed through official organizational email channels. Interaction data were collected from 17,062 successfully delivered simulation emails and analyzed using behavioral indicators, including email open rate, link click rate, data submission rate, and response time. These metrics provide insight into user susceptibility and behavioral risk patterns when exposed to simulated phishing scenarios. The results indicate that most users did not perform risky actions; however, a small proportion progressed to critical stages, such as clicking malicious links or submitting credentials. Although incidents involving users with privileged or critical access were limited, they represent a disproportionate security risk due to their potential organizational impact. Response time analysis reveals that many clicks occurred shortly after email receipt, suggesting rapid decision-making without sufficient verification, particularly when messages emphasized urgency. These findings highlight the importance of risk-based mitigation strategies and demonstrate that phishing simulations should be integrated into a continuous improvement process combining targeted awareness training, user segmentation, and scenario variation to enhance organizational resilience against phishing threats.

Keywords: phishing simulation, security awareness, user behavior, information security, risk-based mitigation

PENDAHULUAN

Transformasi digital pada organisasi sektor keuangan mendorong peningkatan penggunaan layanan berbasis aplikasi, pemanfaatan surat elektronik korporat, serta integrasi sistem internal yang semakin kompleks. Perkembangan ini meningkatkan efisiensi dan kualitas layanan, namun pada saat yang sama memperluas permukaan serangan dan meningkatkan risiko keamanan informasi. Salah satu risiko yang paling signifikan berasal dari serangan *phishing*, yaitu teknik rekayasa sosial yang memanfaatkan interaksi manusia untuk mengecoh pengguna agar melakukan tindakan berisiko, seperti mengklik tautan berbahaya atau mengungkapkan informasi sensitif. Berbagai studi menunjukkan bahwa phishing tetap menjadi salah satu vektor serangan paling efektif karena mampu mengeksploitasi keterbatasan persepsi dan pengambilan keputusan pengguna dalam konteks kerja sehari-hari (Alkhalil dkk. 2021).

Pengendalian *phishing* tidak dapat hanya mengandalkan mekanisme teknis, karena keberhasilan serangan sangat dipengaruhi oleh perilaku pengguna. Faktor-faktor seperti persepsi urgensi, legitimasi visual pesan, dan representasi otoritas pengirim terbukti berkorelasi dengan kecenderungan pengguna untuk berinteraksi dengan email mencurigakan. Penelitian empiris di lingkungan kerja menunjukkan bahwa isyarat sosial tersebut meningkatkan probabilitas klik, khususnya pada skenario spear phishing yang disesuaikan dengan konteks organisasi (Williams dkk. 2018). Dengan demikian, pengukuran risiko *phishing* perlu memperhatikan perilaku aktual pengguna ketika berhadapan dengan stimulus *email* yang menyerupai kondisi operasional nyata.

Dalam konteks pengambilan keputusan individu, bias kognitif seperti *authority bias* dan *urgency bias* dapat memengaruhi penilaian pengguna terhadap legitimasi suatu pesan. Pesan yang menampilkan simbol formal, bahasa teknis, atau ancaman gangguan operasional cenderung dipersepsikan lebih kredibel dan mendorong respons cepat tanpa verifikasi yang memadai (Sharma dkk. 2023). Namun demikian, penelitian juga menunjukkan bahwa kerentanan terhadap *phishing* tidak bersifat seragam dan tidak selalu dapat direpresentasikan melalui satu indikator tunggal. Variasi karakteristik pesan, jenis umpan (*scam type*), serta konteks organisasi berkontribusi terhadap perbedaan tingkat respons pengguna, sehingga evaluasi perlu dilakukan secara terukur dan berbasis data perilaku (Sommestad dan Karlzén 2024).

Dalam praktik organisasi, simulasi *phishing* (*phishing drill simulation*) digunakan secara luas sebagai pendekatan evaluatif untuk mengukur tingkat kerentanan pengguna dan efektivitas program *security awareness*. Melalui simulasi terkontrol, organisasi dapat mengumpulkan data kuantitatif berupa tingkat pembukaan email (*open rate*), tingkat klik tautan (*click rate*), serta interaksi lanjutan yang merepresentasikan perilaku berisiko. Studi berskala besar menunjukkan bahwa kampanye simulasi yang dilakukan secara berulang dapat memengaruhi perilaku pengguna, ditandai dengan penurunan kecenderungan klik pada kampanye berikutnya (Gordon dkk. 2019). Namun, kajian lain juga menegaskan bahwa pelatihan kesadaran keamanan yang bersifat umum dan tahunan sering kali memberikan dampak terbatas, sehingga diperlukan evaluasi berbasis bukti untuk merancang intervensi yang lebih kontekstual dan efektif (Liu dkk. 2025).

Untuk kebutuhan benchmarking, KnowBe4 menggunakan metrik Phish-prone Percentage atau PPP, yaitu persentase pengguna yang gagal pada uji phishing terkontrol melalui tindakan berisiko seperti mengklik tautan simulasi atau membuka lampiran berbahaya. KnowBe4 membagi evaluasi ke dalam tiga fase yaitu baseline sebelum pelatihan, hasil dalam 90 hari setelah pelatihan, dan hasil setelah satu tahun atau lebih pelatihan serta simulasi berkelanjutan. Dalam laporan KnowBe4 tahun 2024, sektor perbankan pada organisasi berukuran besar dengan lebih dari 1000 pegawai dilaporkan mencapai PPP sebesar 5,2% pada fase setelah satu tahun atau lebih pelatihan dan simulasi berkelanjutan, yang menunjukkan bahwa program awareness yang konsisten dapat menurunkan kerentanan namun tidak menghilangkan risiko sepenuhnya (KnowBe4 2024).

Selain indikator klik, aspek pelaporan email mencurigakan juga merupakan komponen penting dalam ketahanan organisasi terhadap *phishing*. Pelaporan yang cepat memungkinkan peningkatan deteksi dini dan respons insiden yang lebih efektif. Budaya keamanan informasi, kejelasan kebijakan, serta kemudahan mekanisme pelaporan berkontribusi terhadap terbentuknya perilaku pelaporan yang konsisten. Penelitian menunjukkan bahwa lingkungan organisasi yang mendukung keamanan informasi berkorelasi positif dengan tingkat partisipasi pengguna dalam pelaporan *phishing* (Petrič dan Just 2025). Oleh karena itu, evaluasi simulasi *phishing* idealnya tidak hanya berfokus pada identifikasi perilaku berisiko, tetapi juga menjadi dasar perbaikan sistemik pada program *awareness* dan mekanisme organisasi.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengevaluasi respons pengguna terhadap skenario phishing yang disimulasikan melalui pendekatan kuantitatif deskriptif. Evaluasi dilakukan dengan menganalisis data log interaksi pengguna terhadap *email* simulasi, meliputi pembukaan email, klik tautan, pengisian data pada halaman simulasi, serta waktu respons. Fokus penelitian diarahkan pada pemetaan tingkat kerentanan secara agregat, identifikasi pola perilaku berisiko, serta analisis kelompok pengguna dengan karakteristik akses kritikal. Hasil penelitian diharapkan dapat menjadi dasar perumusan rekomendasi peningkatan *security awareness* dan penguatan pengendalian phishing berbasis risiko yang dapat diterapkan secara berkelanjutan dalam lingkungan organisasi sektor jasa keuangan.

METODE PENELITIAN

Desain dan Jenis Penelitian

Penelitian ini menggunakan desain kuantitatif deskriptif dengan pendekatan evaluatif melalui simulasi phishing terkontrol (*phishing drill simulation*). Desain ini bertujuan mengukur perilaku aktual pengguna ketika berhadapan dengan pesan email yang dirancang menyerupai

skenario rekayasa sosial, serta mengevaluasi efektivitas program peningkatan kesadaran keamanan berdasarkan indikator perilaku yang dapat diamati. Unit analisis penelitian adalah interaksi pengguna terhadap email simulasi pada level kampanye dan kelompok agregat. Penelitian tidak menggunakan hasil untuk penilaian individu, melainkan untuk pemetaan risiko dan perumusan tindak lanjut peningkatan *awareness*.

Setting, Populasi, dan Subjek Penelitian

Penelitian dilakukan pada sebuah organisasi di sektor jasa keuangan (identitas organisasi dianonimkan), dengan kanal utama menggunakan email organisasi. Populasi penelitian adalah seluruh pengguna email organisasi yang masuk ke dalam daftar target kampanye simulasi. Pada kampanye ini, jumlah target penerima adalah 17.177 pengguna. Kriteria inklusi meliputi akun email aktif yang terdaftar sebagai target dan tercatat menerima email simulasi. Kriteria eksklusi meliputi email yang gagal terkirim (misalnya akun tidak aktif atau kendala teknis) dan data interaksi yang tidak dapat dipetakan secara valid ke log sistem.

Jadwal dan Durasi Pengumpulan Data

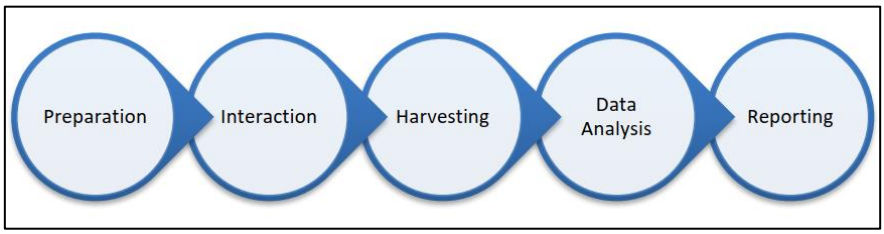
Penyusunan skenario dilakukan pada 05–12 Agustus 2025. Penyiapan sistem dilakukan pada 13–14 Agustus 2025. Pengiriman email simulasi dilakukan pada 26 Agustus 2025. Pengumpulan data interaksi dilakukan selama 26 Agustus–12 September 2025 agar semua kemungkinan respons tertangkap, termasuk respons yang tertunda. Penyusunan laporan hasil dilakukan pada 15–23 September 2025. Detail durasi ini penting untuk menjelaskan bahwa interaksi tidak hanya diukur "hari H", tetapi juga selama masa observasi pasca pengiriman.

Skenario Simulasi dan Stimulus Email

Skenario *phishing* dalam penelitian ini dirancang dengan meniru notifikasi layanan *email* yang mengangkat tema peringatan kapasitas *mailbox* yang hampir penuh. Pemilihan tema tersebut didasarkan pada tingkat relevansi yang tinggi terhadap aktivitas kerja harian pengguna, sehingga secara psikologis dapat memicu respons cepat akibat adanya persepsi ancaman terhadap kelancaran komunikasi kerja. Karakteristik stimulus *email* yang digunakan dalam simulasi meliputi beberapa elemen utama sebagai berikut:

a. Nama Pengirim
   Nama pengirim ditampilkan seolah-olah berasal dari layanan *email* yang umum dan familiar bagi pengguna, guna meningkatkan tingkat kepercayaan terhadap pesan yang diterima.
b. Alamat Pengirim
   Alamat *email* pengirim menggunakan domain yang menyerupai domain resmi dari layanan email populer, sehingga secara visual tampak kredibel dan meyakinkan.
c. Subjek *Email*
   Subjek *email* dirancang singkat dan mengandung unsur urgensi, seperti peringatan bahwa "mailbox hampir penuh", untuk mendorong pengguna segera membuka dan merespons email tersebut.
d. Isi *Email*
   Isi pesan memuat informasi mengenai tingginya persentase penggunaan kapasitas mailbox, disertai dengan konsekuensi operasional apabila tidak segera dilakukan tindakan. Pada bagian ini juga disisipkan tautan sebagai *call to action* bagi pengguna.
e. Tautan (*Link*)
   Tautan yang disediakan mengarahkan pengguna ke halaman simulasi (*landing page*) yang menyerupai tampilan *login* layanan *email*. Hal ini bertujuan untuk mengukur perilaku pengguna pada titik kritis, yaitu saat diminta memasukkan kredensial.

Prosedur Penelitian



Gambar 1. Tahapan Rekayasa Sosial

Prosedur penelitian disusun dengan mengacu pada kerangka tahapan rekayasa sosial yang dioperasionalkan ke dalam lima fase utama, yaitu *preparation, interaction, harvesting, data analysis*, dan *reporting*.

a. *Preparation*
   Tahap ini mencakup penetapan tujuan simulasi, penyusunan daftar target, serta perancangan konten *email* beserta taktik persuasi yang digunakan. Selain itu, dilakukan penyiapan *landing page* simulasi dan konfigurasi mekanisme pelacakan (*tracking*) serta pencatatan *log* untuk mendukung proses pengumpulan data.
b. *Interaction*
   Pada tahap ini dilakukan pengiriman *email* simulasi kepada target yang telah ditentukan. Selanjutnya, dilakukan pemantauan respons awal penerima melalui pencatatan *event log*, seperti pembukaan *email* dan interaksi klik pada tautan yang disediakan.
c. *Harvesting*
   Tahap ini berfokus pada pencatatan interaksi lanjutan pengguna pada *landing page* simulasi. Tujuannya adalah untuk mengukur apakah pengguna melanjutkan hingga tahap pengisian data pada formulir simulasi. Data yang dikumpulkan berupa status kejadian interaksi serta metadata teknis yang relevan untuk analisis perilaku, dan tidak digunakan untuk tujuan autentikasi.
d. *Data Analysis*
   Tahap analisis meliputi proses pembersihan data (*data cleaning*), konsolidasi log, perhitungan metrik utama, serta analisis pola respons pengguna. Analisis dilakukan baik pada tingkat kampanye secara keseluruhan maupun berdasarkan segmentasi tertentu yang telah ditetapkan.
e. *Reporting*
   Tahap akhir mencakup penyusunan temuan penelitian, interpretasi tingkat risiko, serta perumusan rekomendasi. Rekomendasi difokuskan pada perbaikan program *security awareness*, penguatan kontrol keamanan, serta strategi tindak lanjut bagi kelompok pengguna dengan tingkat risiko yang lebih tinggi.

Variabel Penelitian dan Definisi Operasional

Penelitian ini menggunakan variabel utama yang berfokus pada perilaku pengguna dalam merespons *email* simulasi *phishing*. Variabel tersebut dioperasionalkan ke dalam beberapa indikator yang dapat diukur berdasarkan data *log* sistem sebagai berikut:

a. *Open Rate*
   Persentase pengguna yang membuka *email* simulasi dibandingkan dengan total *email* yang berhasil terkirim.
b. *Click Rate*
   Persentase pengguna yang melakukan klik pada tautan yang terdapat dalam *email* simulasi.
c. *Data Submission Rate*
   Persentase pengguna yang melanjutkan interaksi hingga memasukkan data pada formulir di halaman simulasi (*landing page*).
d. *Response Time*
   Kecepatan respon dihitung dari waktu pembukaan *email* hingga interaksi seperti klik atau pengisian data dilakukan.

Seluruh variabel diukur pada tingkat agregat dan digunakan untuk mengidentifikasi pola kerentanan serta perilaku pengguna dalam konteks simulasi *phishing*.

HASIL DAN IMPLEMENTASI

Hasil

Simulasi *phishing* menargetkan 17.177 penerima. Dari jumlah tersebut, 17.062 *email* berhasil terkirim (99,33%) dan 115 *email* gagal terkirim (0,67%). Perhitungan metrik interaksi pada bagian hasil menggunakan basis *email* yang berhasil terkirim sebagai denominator utama agar hasil tidak bias oleh akun tidak aktif atau kendala teknis pengiriman.

Tabel 1. Ringkasan hasil simulasi phishing (basis: *email* terkirim sukses)

Indikator	Jumlah	Persentase
Open	5.213	30,35%
Click	188	1,09%
Submission	74	0,43%
No action	11.849	68,98%
Error (gagal terkirim)	115	0,67%

Distribusi tahapan perilaku menunjukkan bahwa sebagian besar penerima tidak berinteraksi atau hanya berhenti pada tahap membuka *email*. Secara rinci, terdapat *open only* sebanyak 5.025 (29,25%), *click* tanpa *submission* sebanyak 114 (0,66%), *submission* sebanyak 74 (0,43%), dan *no action* sebanyak 11.849 (68,98%). Temuan ini menegaskan bahwa meskipun proporsi perilaku berisiko relatif kecil, masih terdapat interaksi yang mencapai tahap kritis (*submission*) yang berpotensi merepresentasikan risiko kebocoran kredensial apabila skenario serupa terjadi pada serangan nyata. Analisis pada kelompok akun akses kritikal dilakukan untuk menilai risiko pada akun dengan akses yang berdampak tinggi. Total akun akses kritikal yang dianalisis adalah 818, terdiri dari kategori akses jarak jauh (459) dan kategori manajemen akses istimewa (359). Pada kelompok ini tercatat 35 kejadian klik dan 14 kejadian *submission*.

Tabel 2. Interaksi pada kelompok akun akses kritikal

Kategori akun akses kritikal	Total pengguna	Klik	*Submission*
Akses jarak jauh	459	15	7
Manajemen akses istimewa	359	20	7
Total	818	35	14

Tabel 3. Analisis waktu klik

Waktu klik	Jumlah	Persentase
< 1 jam	85	45%
> 1 jam	103	55%

Dari sisi kecepatan respons, analisis waktu klik menunjukkan 85 kejadian klik (45%) terjadi dalam kurang dari 1 jam, sedangkan 103 kejadian klik (55%) terjadi lebih dari 1 jam. Pola ini memberi indikasi adanya sebagian penerima yang merespons relatif cepat terhadap email simulasi, yang dalam konteks rekayasa sosial dapat berkorelasi dengan rendahnya verifikasi sebelum bertindak.

Tabel 4. Perilaku klik ulang pada pengguna dengan riwayat klik sebelumnya

Kategori	Jumlah	Persentase
Melakukan klik pada tautan	7	6%
Tidak melakukan klik pada tautan	105	94%

Sebagai evaluasi berkelanjutan, terdapat 112 penerima yang pada fase sebelumnya pernah melakukan klik dan kembali diikutsertakan pada fase berjalan. Hasilnya, 105 (94%) tidak mengulang klik, sedangkan 7 (6%) kembali melakukan klik. Temuan ini menunjukkan adanya

perbaikan perilaku pada mayoritas kelompok yang dipantau, namun tetap terdapat kelompok kecil dengan kerentanan berulang yang perlu ditangani secara lebih terarah.

Implementasi

Implementasi simulasi dilakukan melalui siklus terstruktur yang mencakup penyusunan skenario, penyiapan sistem, pengiriman email, pengumpulan data interaksi, serta penyusunan pelaporan. Skenario disusun pada 05–12 Agustus 2025, penyiapan sistem pada 13–14 Agustus 2025, pengiriman email dilakukan pada 26 Agustus 2025, dan pengumpulan data interaksi dilaksanakan selama 26 Agustus–12 September 2025 untuk menangkap respons yang tidak selalu terjadi pada hari pengiriman. Kompilasi pelaporan dilakukan pada 15–23 September 2025.

Tabel 5. Timeline implementasi simulasi

Tahap	Rentang waktu	Keluaran utama
Penyusunan skenario	05–12 Agustus 2025	Templat email umpan dan rancangan *landing page*
Penyiapan sistem	13–14 Agustus 2025	Konfigurasi pelacakan dan pencatatan log
Eksekusi kampanye	26 Agustus 2025	Pengiriman *email* dan aktivasi event tracking
Observasi interaksi	26 Agustus–12 September 2025	*Log open*, *click*, *submission*, dan waktu respons
Pelaporan	15–23 September 2025	Ringkasan hasil, segmentasi risiko, rekomendasi

Skenario *email* dirancang menyerupai notifikasi layanan *email* bertema kapasitas kotak masuk hampir penuh, dengan *call-to-action* berupa tautan yang mengarahkan penerima menuju *landing page* simulasi yang meniru halaman login layanan *email*. Tujuan implementasi skenario ini adalah mengukur perilaku penerima pada tiga titik kritis, yaitu pembukaan email, keputusan klik tautan, dan keputusan memasukkan data pada *landing page*. Setelah interaksi tertentu, pengguna diarahkan pada halaman pemberitahuan bahwa aktivitas merupakan simulasi, sebagai kontrol edukatif agar kegiatan tidak menimbulkan dampak operasional.

Tabel 6. Hasil pelaksanaan *awareness email phishing*

Keterangan	Jumlah	Persentase
Mengikuti *awareness*	73	99%
Tidak mengikuti *awareness*	1	1%

Sebagai tindak lanjut, sistem menjalankan mekanisme awareness otomatis bagi peserta yang mencapai tahap berisiko. Materi awareness terdiri dari empat video edukasi berdurasi sekitar lima menit dan kuis interaktif berisi lima pertanyaan berbasis skenario. Implementasi *awareness* dipantau melalui tingkat partisipasi penyelesaian materi, yang menunjukkan 73 peserta (99%) mengikuti *awareness* dan 1 peserta (1%) belum mengikuti pada periode pelaksanaan.

Implementasi evaluasi juga memasukkan segmentasi hasil agar temuan dapat ditindaklanjuti secara terarah, yaitu segmentasi berdasarkan unit kerja untuk mengidentifikasi konsentrasi klik dan *submission*, segmentasi kelompok akun akses kritikal untuk prioritas penguatan kontrol dan pembinaan, analisis waktu respons untuk membaca kecenderungan respons cepat, serta pemantauan kelompok dengan riwayat klik pada fase sebelumnya untuk menilai perubahan perilaku.

Pembahasan

Tabel 7. Hasil simulasi *phishing*

Kategori Interaksi	Jumlah	Persentase
Email Terkirim (*Sent*)	17.062	99,33%
Membuka *Email* (*Open Rate*)	5.213	30,35%
Klik Tautan (*Click Rate*)	188	1,09%
Input Kredensial (*Data Submission Rate*)	74	0,43%

Tidak Berinteraksi (*No Action*)	11.849	68,98%
Tidak Terkirim (*Error*)	115	0,67%

Hasil simulasi menunjukkan bahwa dari 17.062 *email* yang terkirim sukses, *open rate* mencapai 30,35% (5.213), sedangkan *click rate* 1,09% (188) dan *data submission rate* 0,43% (74). Pola ini mengindikasikan bahwa stimulus *email* cukup relevan untuk menarik perhatian penerima, tetapi sebagian besar penerima yang membuka *email* tidak melanjutkan ke tindakan berisiko. Namun, keberadaan submission tetap menjadi temuan penting karena merepresentasikan perilaku yang paling dekat dengan kompromi kredensial apabila skenario yang sama terjadi dalam serangan nyata.

Proporsi *no action* sebesar 68,98% (11.849) dapat dibaca sebagai sinyal positif, tetapi secara metodologis *no action* tidak selalu berarti penerima mengenali *email* sebagai *phishing*, namun bisa juga karena *email* diabaikan, tertutup oleh beban kerja, atau tidak sempat dibaca. Karena itu, interpretasi tingkat "kesadaran" sebaiknya tidak hanya didasarkan pada *no action*, melainkan dipahami bersama indikator yang lebih kuat seperti *click* dan *submission* serta, bila tersedia, indikator pelaporan *email* mencurigakan.

Jika dibandingkan dengan temuan dalam *KnowBe4 Phishing by Industry Benchmarking Report 2024*, hasil kampanye ini menunjukkan pola yang selaras dengan sektor perbankan pada organisasi berskala besar. Pada Phase 3 (setelah satu tahun atau lebih pelatihan dan simulasi berkelanjutan), KnowBe4 melaporkan bahwa sektor perbankan dengan jumlah pegawai lebih dari 1000 mencapai *Phish-Prone Percentage (PPP)* sebesar 5,2%. Meskipun metrik PPP tidak identik dengan click rate yang diukur dalam penelitian ini, click rate kampanye yang relatif rendah (1,09%) dapat dipandang sebagai indikasi awal perilaku pengguna yang relatif terkendali pada skenario simulasi yang diuji. Namun demikian, perbandingan terhadap benchmark perlu dilakukan secara hati-hati, karena hasil simulasi sangat dipengaruhi oleh karakteristik skenario, jenis umpan, konteks operasional organisasi, serta konfigurasi sistem keamanan email. Oleh karena itu, hasil dari satu skenario simulasi tidak dapat dianggap merepresentasikan secara menyeluruh tingkat ketahanan organisasi terhadap seluruh variasi ancaman phishing yang mungkin dihadapi.

Temuan yang paling strategis muncul pada kelompok akun akses kritikal. Dari total 818 akun akses kritikal, tercatat 35 klik dan 14 *submission*. Walaupun jumlahnya relatif kecil dibanding total populasi, risiko dari kelompok ini bersifat tidak proporsional karena kredensial akses kritikal berpotensi memperluas dampak bila terjadi pada serangan nyata. Dengan demikian, pendekatan mitigasi yang bersifat "*risk-based*" menjadi relevan, yaitu memberikan kontrol tambahan dan pembinaan yang lebih intensif pada pemegang akses kritikal, bukan hanya pelatihan umum yang seragam untuk seluruh pengguna.

Analisis waktu klik memperlihatkan 45% klik terjadi dalam kurang dari satu jam, sedangkan 55% klik terjadi setelah lebih dari satu jam. Klik dalam waktu singkat dapat mencerminkan kecenderungan bertindak cepat sebelum verifikasi, terutama ketika skenario memanfaatkan tema urgensi operasional. Implikasi praktisnya adalah materi *awareness* perlu menekankan kebiasaan "*pause and verify*" sebelum mengklik tautan dan memperkuat rutinitas verifikasi pengirim dan tautan pada situasi yang terlihat mendesak. Di sisi lain, klik yang terjadi setelah lebih dari satu jam menunjukkan bahwa risiko tidak hanya muncul dari respons impulsif; pengguna yang menunda tetap bisa melakukan klik ketika kembali membuka *email*, sehingga pencegahan perlu konsisten sepanjang siklus kerja, bukan hanya pada momen awal penerimaan *email*.

Evaluasi berkelanjutan pada kelompok dengan riwayat klik sebelumnya menunjukkan adanya perbaikan perilaku yang kuat. Dari 112 pengguna yang pernah klik pada fase sebelumnya, 105 tidak mengulang klik dan 7 kembali mengulang klik. Secara interpretatif, temuan ini mengarah pada dua kesimpulan. Pertama, terdapat indikasi bahwa paparan edukasi dan simulasi sebelumnya berdampak pada mayoritas pengguna yang dipantau. Kedua, adanya kelompok kecil yang mengulang klik mengindikasikan "kerentanan persisten" yang umumnya memerlukan

intervensi yang lebih personal, misalnya coaching berbasis studi kasus, penguatan kebiasaan verifikasi, atau pengaturan kontrol tambahan pada akun mereka.

Dari sisi implementasi tindak lanjut, mekanisme *awareness* pasca simulasi menunjukkan tingkat keterlibatan yang sangat tinggi, yakni 73 peserta mengikuti *awareness* dan 1 peserta belum mengikuti pada periode pelaksanaan. Tingginya partisipasi ini merupakan faktor pendukung penting bagi pendekatan perbaikan berkelanjutan karena kegiatan tidak berhenti pada pengukuran, tetapi langsung diikuti intervensi edukatif. Meski demikian, efektivitas *awareness* tidak hanya diukur dari partisipasi, melainkan perlu dikaitkan dengan perubahan perilaku pada kampanye berikutnya, terutama pada kelompok *submission* dan kelompok akses kritikal.

Secara keseluruhan, hasil kampanye memperlihatkan profil risiko yang relatif terkendali pada indikator *click*, namun tetap menyisakan risiko yang bermakna pada indikator *submission* dan pada akun akses kritikal. Karena itu, strategi peningkatan ke depan dapat diarahkan pada penguatan intervensi berbasis risiko, variasi skenario simulasi agar mencerminkan spektrum ancaman yang lebih luas, serta penguatan mekanisme tindak lanjut untuk kelompok yang menunjukkan pola risiko berulang.

KESIMPULAN

Penelitian ini menunjukkan bahwa simulasi *phishing* berbasis email dapat digunakan sebagai instrumen evaluatif yang efektif untuk memetakan perilaku pengguna dan tingkat kerentanan organisasi terhadap ancaman rekayasa sosial. Berdasarkan analisis data log interaksi, mayoritas pengguna tidak menunjukkan tindakan berisiko. Namun demikian, masih ditemukan sejumlah kecil interaksi yang mencapai tahap kritis, yaitu klik tautan dan pengisian data pada halaman simulasi. Temuan ini mengindikasikan bahwa meskipun profil risiko secara agregat relatif terkendali, potensi kompromi kredensial tetap ada apabila skenario serupa terjadi pada serangan nyata. Analisis waktu respons juga menunjukkan bahwa sebagian klik terjadi dalam waktu singkat setelah email diterima, yang mencerminkan kecenderungan pengambilan keputusan cepat tanpa verifikasi memadai, khususnya pada pesan dengan tema urgensi operasional.

Hasil penelitian juga menegaskan pentingnya pendekatan mitigasi *phishing* yang berbasis risiko. Interaksi berisiko yang terjadi pada kelompok akun dengan akses kritikal memiliki dampak yang tidak proporsional dibandingkan jumlahnya, sehingga memerlukan perhatian dan pengendalian yang lebih intensif. Implementasi mekanisme *security awareness* pascasimulasi menunjukkan tingkat partisipasi yang sangat tinggi dan berkorelasi dengan perbaikan perilaku pada sebagian besar pengguna yang sebelumnya pernah melakukan klik. Oleh karena itu, simulasi phishing sebaiknya tidak diposisikan semata sebagai alat pengukuran, tetapi sebagai bagian dari siklus perbaikan berkelanjutan yang mencakup variasi skenario, segmentasi risiko pengguna, serta intervensi edukatif yang lebih terarah. Ke depan, penelitian lanjutan disarankan dilakukan secara longitudinal melalui beberapa gelombang simulasi dengan variasi umpan dan teknik serangan, serta memasukkan metrik respons tambahan seperti pelaporan email mencurigakan dan pengukuran efektivitas intervensi (misalnya perbandingan antar metode edukasi), agar evaluasi ketahanan organisasi menjadi lebih komprehensif dan mampu menangkap dinamika risiko di lingkungan kerja sektor jasa keuangan.

DAFTAR PUSTAKA

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A survey of detection methods, vulnerabilities, and future challenges. *IEEE Communications Surveys & Tutorials, 23*(2), 1124–1155. https://doi.org/10.1109/COMST.2021.3055870

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies, 117*, 1–13. https://doi.org/10.1016/j.ijhcs.2018.04.002

Sharma, R., Chen, J., & Liu, Y. (2023). Cognitive bias and decision-making in phishing email responses. *Computers & Security, 124*, 102969. https://doi.org/10.1016/j.cose.2022.102969

Sommestad, T., & Karlzén, H. (2024). Measuring phishing susceptibility: The influence of scam types. *Journal of Cybersecurity, 10*(1), tyae004. https://doi.org/10.1093/cybsec/tyae004

Gordon, W. J., Fairhall, A., & Landman, A. (2019). Threats to information security—Public health implications. *New England Journal of Medicine, 380*(4), 301–303. https://doi.org/10.1056/NEJMp1814070

Liu, S., Wang, J., & Zhang, Y. (2025). Effectiveness of security awareness training against phishing attacks. *Information & Computer Security, 33*(1), 45–60. https://doi.org/10.1108/ICS-03-2024-0058

Petrič, G., & Just, N. (2025). Organizational culture and employee reporting behavior in information security incidents. *Computers & Security, 131*, 103304. https://doi.org/10.1016/j.cose.2023.103304

KnowBe4, Inc. (2024). Phishing by industry benchmarking report: 2024 edition. KnowBe4.