ANALISIS TINGKAT KESADARAN MAHASISWA TERHADAP KEAMANAN INFORMASI MELALUI SIMULASI SERANGAN *EMAIL PHISHING* MENGGUNAKAN *GOPHISH*

Putri Nuranisa, Nurmi Hidayasari, Pretti Ristra
Teknik Informatika, Politeknik Negeri Bengkalis
Jalan Bathin Alam Desa Sungai Alam, Kec. Bengkalis, Kab.Bengkalis, Indonesia
putrinuranisaaa044@gmail.com

ABSTRAK

Email phishing masih menjadi salah satu ancaman utama dalam keamanan informasi dan sering memanfaatkan rendahnya kewaspadaan pengguna, termasuk mahasiswa di lingkungan Perguruan Tinggi. Permasalahan yang muncul adalah masih terbatasnya penelitian yang mengukur tingkat kewaspadaan mahasiswa terhadap *phishing* berdasarkan perilaku nyata pengguna melalui simulasi serangan. Penelitian ini bertujuan untuk menganalisis tingkat kewaspadaan mahasiswa terhadap keamanan informasi melalui simulasi serangan *email phishing* menggunakan *GoPhish*. Metode penelitian yang digunakan adalah metode eksperimen dengan menerapkan simulasi serangan *email phishing* kepada mahasiswa sebagai responden. Simulasi dilakukan menggunakan *GoPhish* untuk mengirimkan *email phishing* dan mencatat respons responden. Hasil penelitian menunjukkan bahwa dari 96 *email phishing* yang dikirimkan, sebanyak 87 *email* dibuka (90,6%), 72 responden melakukan klik pada tautan *phishing* (75,0%), dan 68 responden melakukan pengiriman data melalui *landing page* (70,8%). Berdasarkan indikator *non-klik*, tingkat kewaspadaan mahasiswa terhadap serangan *phishing* sebesar 25%, sedangkan tingkat kerentanan mencapai 75%. Hasil ini menunjukkan bahwa tingkat kewaspadaan mahasiswa terhadap keamanan informasi masih tergolong rendah, sehingga diperlukan peningkatan edukasi dan sosialisasi terkait ancaman *phishing* di lingkungan akademik.

Kata kunci : *Phishing*, Keamanan Informasi, Simulasi *Phishing*, *Gophish*

1. PENDAHULUAN

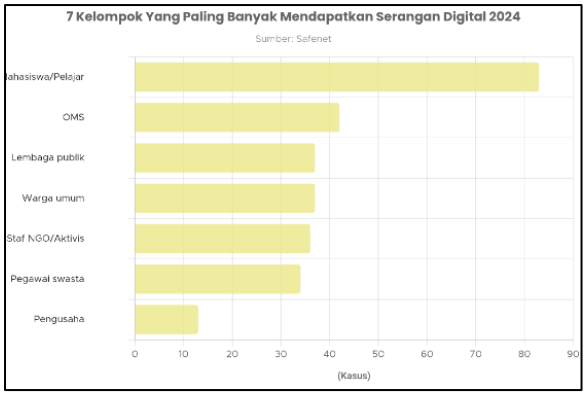
Pada masa transformasi teknologi yang cepat, internet telah menjadi alat yang sangat penting bagi kehidupan sehari-hari, menawarkan kemudahan dan efisiensi. Meskipun internet telah menyederhanakan berbagai tugas mulai dari komunikasi hingga pencarian informasi, internet juga menimbulkan tantangan yang signifikan dalam bidang keamanan siber. Pengguna tidak hanya berpotensi menjadi korban, tetapi juga dapat menjadi pelaku kejahatan siber yang tidak disadari. Hal ini menyoroti kebutuhan mendesak akan kesadaran keamanan siber di Perguruan Tinggi. Keamanan informasi sendiri merupakan praktik perlindungan informasi dari berbagai ancaman yang bertujuan untuk menjamin kelangsungan operasional, meminimalkan risiko dan melindungi aset informasi dari akses yang tidak sah, penggunaan, pengungkapan, gangguan, modifikasi atau perusakan yang tidak sah.

Namun, pada kenyataannya kesadaran mahasiswa terhadap keamanan informasi masih tergolong rendah. Salah satu ancaman paling umum dan berbahaya yang sering dimanfaatkan oleh pelaku kejahatan siber adalah *phishing*, khususnya dalam bentuk *email phishing*. *Email phishing* merupakan teknik penipuan berbasis rekayasa sosial (*social engineering*) dimana pelaku menyamar sebagai pihak yang tepercaya seperti institusi keuangan, Perguruan Tinggi atau layanan digital untuk mengelabui korban agar memberikan informasi sensitif seperti kata sandi, data pribadi atau informasi keuangan. Sejalan dengan hal tersebut, penelitian [1] menegaskan bahwa kesadaran mahasiswa di Indonesia terhadap ancaman siber masih rendah, di mana hanya sekitar 40% yang merasa yakin dapat mengenali serangan *phishing* maupun *malware*.

Teknik manipulasi psikologis yang digunakan dalam *email phishing* sering kali memanfaatkan emosi korban, seperti rasa takut, urgensi, rasa ingin tahu atau kepatuhan terhadap otoritas. Studi oleh [2], menunjukkan bahwa *email phishing* yang menggunakan tema kontekstual dan emosional, seperti informasi beasiswa, pengumuman akademik mendesak atau isu kesehatan seperti *COVID-19*, memiliki tingkat keberhasilan lebih tinggi dalam mengecoh mahasiswa. Mereka cenderung mengklik tautan atau menyerahkan informasi tanpa melakukan verifikasi karena mengira sumbernya tepercaya.

Namun, sebagian besar penelitian sebelumnya menggunakan pendekatan survei, sedangkan penelitian berbasis simulasi serangan nyata pada mahasiswa di lingkungan Perguruan Tinggi vokasi masih terbatas.

Berdasarkan laporan [3] menunjukkan 7 golongan yang mendapatkan serangan digital tahun 2024 yang tertinggi adalah mahasiswa atau pelajar. Sektor pendidikan menempati peringkat teratas sebagai kelompok yang paling sering menjadi target serangan digital. Hal ini menunjukkan bahwa institusi pendidikan, seperti sekolah, universitas dapat menjadi sasaran utama akibat lemahnya sistem keamanan informasi serta rendahnya kesadaran pengguna terhadap ancaman siber.



Gambar 1. 7 Kelompok paling banyak mendapatkan serangan *digital*

Dengan melihat tren ini, dapat disimpulkan bahwa *phishing* bukan lagi sekadar ancaman teknis, tetapi telah menjadi isu strategis dalam tata kelola keamanan informasi. Dalam organisasi, termasuk institusi pendidikan, dituntut untuk tidak hanya memperkuat sistem keamanan teknis, tetapi juga mengembangkan pendekatan edukatif dan preventif melalui peningkatan kesadaran pengguna.

Fenomena yang terjadi pada mahasiswa Politeknik Negeri Bengkalis adalah mahasiswa yang belum mengetahui pemahaman yang optimal dalam mengenali *email phishing*, sehingga masih terdapat potensi kerentanan terhadap ancaman *siber* seperti penipuan melalui *email*.

Untuk mengatasi hal tersebut, peneliti akan melakukan simulasi seangan *phishing* dengan menggunakan *GoPhish* untuk mengukur tingkat kesadaran keamanan siber mahasiswa. *GoPhish* merupakan perangkat lunak *open-source* yang dirancang khusus untuk membuat dan mengelola simulasi *phishing*. Platform ini memungkinkan peneliti untuk mengirim *email* palsu yang menyerupai *email* asli kepada target pengguna, yaitu mahasiswa aktif dari semester 1 - 8 di Politeknik Negeri Bengkalis, lalu menganalisis respons mereka.

Simulasi ini bertujuan memberikan pengalaman langsung kepada mahasiswa dalam mengenali modus *phishing* serta mengukur tingkat kewaspadaan mereka terhadap potensi serangan *siber*. Dengan menggunakan *GoPhish*, simulasi serangan ini dapat dilakukan secara sistematis dan temuan penelitian ini akan menjadi dasar untuk menciptakan program pelatihan keamanan informasi yang lebih baik untuk mahasiswa dan Perguruan Tinggi.

2. TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

Penelitian terkait menjadi acuan penulis untuk melakukan penelitian sehingga penulis dapat memperbanyak referensi yang relevan terkait dengan penelitian yang akan dilakukan. Selain itu, penelitian sebelumnya juga membantu penulis dalam mengidentifikasi celah penelitian (*research gap*) dan merumuskan metodologi yang tepat sesuai dengan konteks permasalahan yang diangkat.

Beberapa penelitian sebelumnya telah menunjukkan urgensi dan efektivitas pendekatan berbasis simulasi dalam meningkatkan kesadaran keamanan informasi. Penelitian [4] melakukan simulasi serangan *email phishing* terhadap mahasiswa dengan tujuan mengevaluasi kesadaran mereka terhadap ancaman siber. Hasil dari penelitian tersebut menunjukkan bahwa mayoritas mahasiswa masih rentan terhadap *email phishing*, khususnya yang dikemas menyerupai komunikasi resmi institusi. Meski belum menggunakan platform terotomatisasi seperti *Gophish*, pendekatam yang dilakukan cukup relevan sebagai pembanding karena mengukur respon aktual mahasiswa terhadap *email* tiruan.

Terkait dengan penggunaan *Gophish*, penelitian oleh [5] mengembangkan sistem otomatisasi kampanye *phishing* berbasis *Gophish* yang terintegrasi dengan *Microsoft azure active directory*. Pendekatan ini memungkinkan penilaian risiko pengguna secara *real-time* serta penyampaian pelatihan keamanan informasi yang disesuaikan dengan tingkat kerentanan masing-masing individu. Hasil penelitian menunjukkan bahwa integrasi simulasi teknis tersebut mampu mengingkatkan efektivitas pelatihan keamanan informasi di lingkungan organisasi.

2.2. Analisis Kesadaran

Kesadaran keamanan informasi (*security awareness)* adalah tingkat pengetahuan dan sikap individu dalam mengenali serta merespon ancaman keamanan informasi. Kesadaran ini dapat diukur dari bagaimana individu memperhatikan tanda-tanda mencurigakan, menghindari interaksi dengan potensi ancaman, serta melaporkan insiden yang terjadi.

Dalam penelitian ini, respon mahasiswa terhadap *email phishing* dicatat secara otomatis oleh *Gophish*, yang mencakup tindakan seperti: membuka *email*, mengklik tautan *phishing*, dan mengisi data pada halaman palsu. Data tersebut kemudian dianalisis untuk mengetahui tingkat kewaspadaan mahasiswa terhadap ancaman *phishing*. Untuk mendukung proses analisis dan memperoleh hasil yang terstruktur dan sistematis, data yang diperoleh dari *Gophish* akan diolah menggunakan *Statistical for the Social Sciences (SPSS)*. pengolahan data meliputi perhitungan frekuensi dan presentase respons.

Menurut penelitian [6], analisis kesadaran keamanan siber pada mahasiswa dilakukan dengan menggunakan *Statistical for the Social Sciences (SPSS)* untuk mengolah data survei. Analisis deskriptif seperti frekuensi, presentase, tabel dan grafik digunakan agar hasil penelitian lebih mudah dipahami dan memberikan gambaran tingkat kesadaran mahasiswa terhadap keamanan siber.

Rumus yang digunakan untuk menganalisa adalah perhitungan frekuensi dan presentase, berikut adalah rumusnya:

$$P = \frac{F}{N} \times 100 \quad (1)$$

Keterangan:
P= Presentase
F= Jumlah responden pada kategori
N= Jumlah responden keseluruhan

$$TK = \frac{N - Jumlah\ email\ diklik}{N} \times 100\% \qquad (2)$$

Keterangan:
TK= Tingkat kewaspadaan
N= Jumlah responden

Langkah ini dilakukan untuk menyajikan hasil simulasi dalam bentuk kuantitatif, sehingga interpretasi data menjadi lebih jelas, objektif serta mudah dipahami.

2.3. Keamanan informasi

Keamanan informasi merupakan praktik perlindungan informasi dari berbagai ancaman yang bertujuan untuk menjamin kelangsungan bisnis, meminimalkan risiko dan memaksimalkan peluang[7].

Berdasarkan penelitian [8], keamanan sistem informasi terdiri dari perlindungan terhadap aspek-aspek berikut:

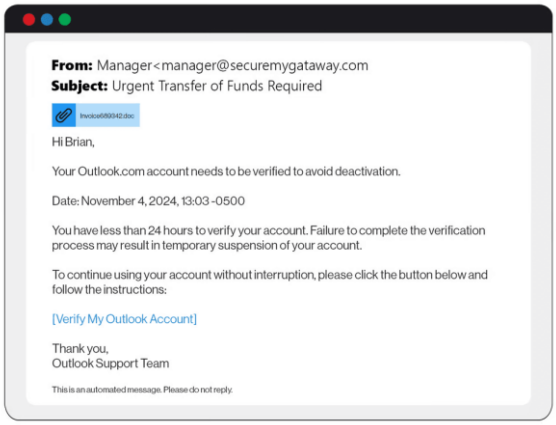
a. *Confidentiality* atau kerahasiaan adalah aspek yang menjamin adanya kerahasian data dari sumber informasi.
b. *Integrity* atau integritas adalah aspek yang menjamin bahwa informasi tidak dapat diubah tanpa seizin pihak berwenang, menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integritas.
c. *availability* atau ketersediaan adalah aspek yang menjamin bahwa informasi akan tersedia saat dibutuhkan oleh pihak berwenangatau yang memiliki hak akses dan memastikan pengguna yang berhak dapat mengakses informasi.

Dalam konteks Perguruan Tinggi, ketiga elemen ini sangat penting, terutama untuk melindungi data pribadi mahasiswa, nilai akademik dan informasi sensitif lainnya.

2.4. *Phishing* dan *Email Phishing*

Phishing adalah suatu bentuk serangan *social engineering* yang dilakukan dengan cara memberikan teknik manipulasi dan penipuan melalui media elektronik, terutama *email*, dengan maksud untuk memperoleh informasi sensitif dari korban. Penyerang menyamar sebagai entitas yang tepercaya maupun layanan resmi untuk membujuk korban agar secara sukarela memberikan data penting, seperti kredensial login, informasi keuangan, atau data pribadi lainnya[9].

Email Phishing merupakan metode penipuan dimana pelaku penyerangan dengan cara mengirimkan *email* seolah-olah seperti dari sumber terpercaya untuk mencuri informasi yang bersifat pribadi, misalnya kata sandi atau kartu kredit[10]. Pesan yang dikirim akan menggunakan logo dari suatu perusahaan kemudian menggunakan bahasa yang meyakinkan. Dalam *email* tersebut, terdapat tautan yang mengarah ke situs web palsu yang dirancang untuk meniru situs asli.



Gambar 2. Contoh *email phishing*

2.5. *Gophish*

Gophish adalah sebuah platform *open-source* yang digunakan untuk melakukan simulasi serangan *phishing* dan pelatihan kesadaran keamanan informasi. *Gophish* dirancang agar mudah digunakan oleh peneliti keamanan, administrator sistem dan pelatih keamanan siber dalam mengelola kampanye *phishing*, melacak siapa yang mengklik tautan, mengisi formulir palsu atau menyerahkan kredensial, sehingga dapat membantu mengukur tingkat kesadaran keamanan informasi dalam suatu organisasi[11].

Gophish berperan sebagai alat dalam pengujian *email phishing* dan program pelatihan kesadaran siber, karena memungkinkan simulasi serangan yang etis dan terkontrol untuk mengidentifikasi kelemahan dan meningkatkan kesadaran pengguna secara proaktif.

3. METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah metode eksperimen. Metode penelitian eksperimen merupakan metode penelitian yang digunakan untuk mencari pengaruh treatment (perlakuan) tertentu [12]. Metode ini diterapkan dengan melakukan simulasi serangan *email phishing* kepada mahasiswa yang berperan sebagai responden penelitian. Simulasi dirancang menyerupai skenario serangan *phishing* yang umum terjadi, baik dari segi konten *email*, tampilan maupun tautan yang di lampirkan.

Melalui penerapan metode eksperimen, peneliti dapat mengamati secara langsung perilaku responden dalam merespons *email phishing*, seperti tindakan membuka *email*, mengklik tautan, mengisi data atau melaporkan *email* sebagai *phishing*. Hasil dari simulasi kemudian dianalisis untuk mengukur tingkat kewaspadaan dan kesadaran mahasiswa terhadap ancaman keamanan informasi, khususnya serangan *email phishing*.

3.1. Populasi dan Sampel

Populasi dalam penelitian ini adalah mahasiswa aktif semester 1-8 Politeknik Negeri Bengkalis, yang menggunakan *email* sebagai sarana komunikasi akademik. Sampel penelitian dipilih dari populasi tersebut untuk dijadikan responden eksperimen dengan tujuan mempresentasikan perilaku mahasiswa dalam menghadapi serangan *email phishing* di lingkungan Perguruan Tinggi.

3.2. Perancangan Simulasi

Simulasi serangan *email phishing* dirangcang dengan menyesuaikan karakteristik serangan *phishing* yang umum terjadi di dunia nyata. Perancangan meliputi penyusunan subjek *email*, isi pesan, tautan dan *landing page* dengan memanfaatkan teknik rekayasa sosial (*social engineering*) sepeeti penggunaan bahasa persuasif, unsur urgensi dan pencantuman identitas institusi yang dikenal oleh responden.

3.3. Pelaksanaan Simulasi

Eksperimen dilaksanakan dengan mengirimkan *email phishing* simulasi kepada responden tanpa pemberitahuan sebelumnya. Pendekatan ini bertujuan untuk memperoleh respons yang alami dan menghindari bias perilaku sehingga tindakan responden dalam merespons *email* dapat mencerminkan kondisi sebenarnya saat menghadapi serangan *phishing.*

3.4. Pengumpulan dan Analisis Data

Data respons responden terhadap *email phishing* dicatat secara otomatis oleh *Gophish*, dimana mencakup tindakan seperti membuka *email*, mengklik tautan *phishing* dan mengisi data pada halaman palsu. Data yang terekam tersebut kemudian dianalisis secara deskriptif untuk mengetahui tingkat kewaspadaan nyata mahasiswa terhadap ancaman *phishing*. Analisis ini bertujuan untuk menggambarkan sejauh mana mahasiswa mampu mengenali dan menghindari serangan *email phishing* dalam praktik, bukan hanya secara teoritis.

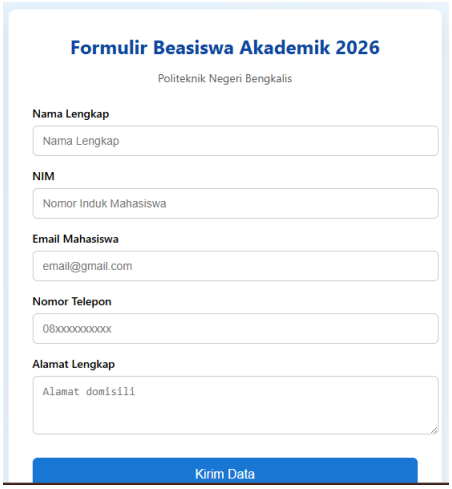
4. HASIL DAN PEMBAHASAN

4.1. Eksperimen

Eksperimen yang dilakukan pada penelitian ini adalah untuk mencapai tujuan penelitian, yaitu menganalisis tingkat kewaspadaan mahasiswa terhadadp keamanan informasi melalui simulasi serangan *email phishing* menggunakan *Gophish.* Eksperimen ini dirancang untuk memperoleh data empiris mengenai perilaku responden dalam merespons *email phishing*, khususnya terkait tindakan membuka *email*, mengklik tautan, mengirimkan data, serta melaporkan *email phishing.*

Pelaksanaan eksperimen diawali dengan konfigurasi *Gophish* sesuai dengn skenario yang telah ditentukan, yaitu pemberitahuan program beasiswa berprestasi untuk mahasiswa. Konfigurasi ini meliputi pembuatan *template email phishing*, pengaturan *landing page* untuk menangkap interaksi responden, serta penentuan daftar *email* responden. Setelah konfigurasi selesai, *email phishing* dikirimkan kepada responden dalam satu priode eksperimen, yaitu sekitar dua minggu.

Gambar 3. Isi pesan *email*



Gambar 4. Tampilan *landing page*

Gophish secara otomatis mencatat aktivitas responden terhadap *email phishing* yang dikirimkan. Parameter yang diukur dalam eksperimen ini meliputi jumlah *email* yang berhasil dikirimkan (*sent),* jumlah *email* yang dibuka (*opened),* jumlah tautan *phishing* yang diklik (*clicked),* jumlah data yang dikirimkan melalui *landing page (submitted),* serta jumlah responden yang melaporkan *email phishing* sebagai *email* mencurigakan (*report).*

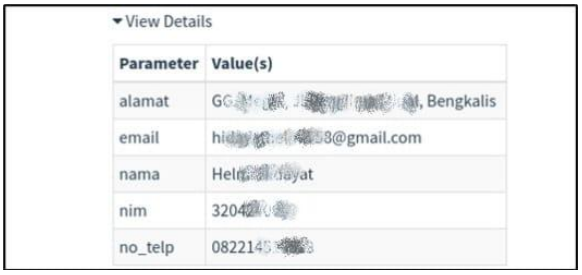
Gambar 5. *Dashboard gophish*

Hasil dari pengukuran parameter tersebut digunakan sebagai dasar untuk mengetahui tingkat kewaspadaan responden terhadap serangan *phishing.* Data hasil eksperimen selanjutnya disajikan dalam bentuk tabel untuk memberikan gambaran kuantitatif mengenai respons responden terhadap simulasi serangan *phishing.* Ringkasan hasil eksperimen ditunjukkan pada tabel 1.

Tabel 1. Hasil eksperimen simulasi serangan *email phishing*

No	Parameter	Jumlah
1	*Email* terkirim (*Sent)*	96
2	*Email* dibuka (*Opened)*	87
3	Tautan diklik (*Clicked)*	72
4	Data terkirim (*Submitted)*	68
5	*Email* dilaporkan *(Report)*	10

Berdasarkan Tabel 1, diketahui bahwa dari total 96 *email phishing* yang berhasil dikirimkan kepada responden, sebanyak 87 *email* dibuka. Selanjutnya 72 responden melakukan klik pada tautan *phishing* yang terdapat dalam *email,* dan 68 responden melakukan pengiriman data pada halaman *landing page.* Selain itu, terdapat 10 responden yang melaporkan *email phishing* sebagai *email* mencurigakan.



Gambar 6. Data tersimpan

4.2. Analisis

Analisis pada penelitian ini dilakukan untuk menginterpretasikan hasil eksperimen simulasi serangan *email phishing* menggunakan *Gophish* dalam rangka mengukur tingkat kewaspadaan mahasiswa terhadap keamanan informasi. Perhitungan ini didasarkan pada data empiris yang diperoleh dari respons responden terhadap *email phishing*, yang meliputi parameter *opened, clicked, submitted* dan *report.*

Untuk memperoleh gambaran kuantitatif mengenai respons responden terhadap *email phishing,* dilakukan perhitungan presentase pada setiap kategori respons. Berdasarkan rumus diatas, persentase masing-masing respons responden terhadap *email phishing* yang dikirimkan dalam penelitian ini dihitung kemudian dianalisis untuk mengetahui tingkat kewaspadaan mahasiswa terhadap serangan *phishing.*

4.3. Persentase *Email* Dibuka

Berdasarkan hasil eksperimen penyebaran *email,* dari total 96 pesan *email phishing* yang dikirimkan kepada responden, sebanyak 87 *email* dibuka. Dengan menggunakan rumus peresentase, diperoleh persentase *email* dibuka sebagai berikut:

$$P = \frac{87}{96} \times 100 = 90{,}6\% \qquad (3)$$

Persentase tersebut menunjukkan bahwa sebagian besar responden membuka *email* yang diterima tanpa terlebih dahulu melakukan proses identifikasi terhadap kemungkinan *email phishing.* Kondisi ini mengindikasi bahwa tingkat kewaspadaan awal responden terhadap ancaman *phishing* masih tergolong rendah. Dengan demikian, responden cenderung langsung berinteraksi dengan *email* yang diterima tanpa mempertimbangkan aspek keamanan informasi.

4.4. Persentase Klik *Email*

Hasil analisis terhadap perilaku responden menunjukkan adanya interaksi yang cukup signifikan terhadap tautan *phishing* yang disertakan dalam pesan *email.* Tercatat sebanyak 72 responden melakukan klik pada tautan tersebut, dimana ini mengindikasikan bahwa masih terdapat tingkat kewaspadaaan yang rendah dalam mengenali indikasi *email phishing.* Berdasarkan perhitungan persentase dari total responden yang terlibat, diperoleh nilai sebagai berikut:

$$P = \frac{72}{96} \times 100 = 75{,}0\% \qquad (4)$$

Hasil ini menunjukkan bahwa sebagian besar responden masih melakukan interaksi lanjutan terhadap *email* yang diterima. Kondisi ini mengindikasikan bahwa adanya tingkat kerentanan yang cukup tinggi terhadap serangan *phishing.*

4.5. Persentase Mengirimkan Data

Berdasarkan responden yang melakukan klik pada tautan, diketahui bahwa sebagian besar diantaranya melanjutkan interaksi hingga pengiriman data melalui halaman *landing page.* Tercatat sebanyak 68 responden yang melakukan pengisian dan pengiriman data tersebut, yang menunjukkan tingkat keberhasilan simulasi *phishing* dalam mengecoh responden. Berdasarkan hasil perhitungan persentase terhadap jumlah responden yang terlibat, diperoleh nilai sebagai berikut:

$$P = \frac{68}{96} \times 100 = 70{,}8\% \qquad (5)$$

Tingginya persentase pengiriman data menunjukkan bahwa responden tidak hanya terpapar pada tahap awal serangan *phishing,* tetapi juga melanjutkan interaksi hingga tahap lanjutan yang berpotensi menimbulkan risiko kebocoran data dan informasi. Kondisi ini mengindikasi bahwa sebagian responden belum memiliki kemampuan yang memadai dalam mengenali tanda-tanda *phishing* secara komprehensif.

4.6. Persentase *Email* Dilaporkan

Hasil eksperimen menunjukkan bahwa sebanyak 10 responden melaporkan *email phishing* sebagai pesan yang mencurigakan, yang mencerminkan adanya tingkat kewaspadaan terhadap ancaman keamanan informasi. Berdasarkan hasil perhitungan persentase dari total responden yang terlibat, diperoleh hasil sebagai berikut:

$$P = \frac{10}{96} \times 100 = 10{,}4\% \qquad (6)$$

Hasil ini menunjukkan bahwa sebagian kecil responden telah memiliki tingkat kesadaran terhadap ancaman *phishing* dan mampu mengenali indikasi *email* yang berpotensi membahayakan keamanan informasi. Kemampuan tersebut tercermin dari tindakan responden dalam mengidentifikasi serta melaporkan *email* yang mencurigakan. Temuan ini mengindikasikan bahwa meskipun tingkat kewaspadaan masih terbatas, upaya peningkatan literasi dan kesadaran keamanan informasi telah mulai terbentuk pada sebagian responden.

4.7. Persentase Tingkat Kewaspadaan

Dalam menghitung tingkat kewaspadaan mahasiswa terhadap serangan phishing, menggunakan indikator *non-klik*, yaitu persentase responden yang tidak melakukan klik pada tautan *phishing* dalam pesan *email*. Indikator tersebut merepresentasikan kemampuan responden dalam mengidentifikasi dan menghindari *email phishing* pada tahap awal. Tingkat kewaspadaan dihitung menggunakan perhitungan sebagai berikut:

$$TK = \frac{96-72}{96} \times 100\% = 25\% \quad (7)$$

Hasil tersebut menunjukkan bahwa tingkat kewaspadaan mahasiswa terhadap serangan *phishing* berada pada angka 25%, sementara tingkat kerentanan terhadap *phishing* mencapai 75%. Berdasarkan penelitian [13] yang mengacu pada klasifikasi tingkat kewaspadaan, membagi kategori seperti pada tabel dibawah:

Tabel 2. Klasifikasi tingkat kewaspadaan.

Kategori	Nilai
Baik	100 – 80 %
Sedang	79 – 60 %
Rendah	≤ 59%

Berdasarkan tabel tersebut, maka tingkat kewaspadaan mahasiswa dalam penelitian ini termasuk dalam kategori rendah. Selain itu, tingkat kewaspadaan *email phishing* juga dievaluasi melalui simulasi *phishing*, di mana persentase klik yang tinggi menunjukkan rendahnya kewaspadaan pengguna.

Proporsi tersebut mengindikasikan bahwa mayoritas responden masih berada pada kondisi rentan terhadap serangan *phishing*. Temuan ini menunjukkan bahwa sebagian besar responden belum sepenuhnya mampu mengenali serta menghindari *email phishing* secara efektif baik pada tahap awal interaksi maupun pada tahap lanjutan.

Berdasarkan keseluruhan hasil analisis, simulasi serangan *phishing* menggunakan *GoPhish* mampu memberikan gambaran empiris mengenai tingkat kewaspadaan mahasiswa terhadap keamanan informasi. Temuan penelitian ini menegaskan adanya kebutuhan untuk meningkatkan edukasi dan sosialisasi terkait keamanan informasi, khususnya mengenai ancaman *phishing* di lingkungan akademik.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian simulasi serangan *email phishing* menggunakan *Gophish* berhasil diimplementasikan sebagai pendekatan utuk mengukur tingkat kewaspadaan mahasiswa terhadap keamanan informasi. Hasil eksperimen menunjukkan bahwa tingkat kewaspadaan mahasiswa yang diukur berdasarkan indikator *non-klik* menunjukkan nilai sebesar 25%, sedangkan tingkat kerentanan mencapai 75%. Mengacu pada klasifikasi tingkat kewaspadaan, hasil tersebut menunjukkan bahwa tingkat kewaspadaan mahasiswa terhadap serangan *phishing* masih berada pada kategori rendah. Oleh karena itu, diperlukan peningkatan edukasi dan sosialisasi keamanan informasi di lingkungan Perguruan Tinggi, khususnya terkait ancaman *phishing.*

Selain itu, untuk penelitian selanjutnya disarankan untuk mengembangkan simulasi *phishing* dengan skenario yang lebihberagam dan melibatkan jumlah responden yang lebih besar untuk memperoleh hasil yang lebih komprehensif.

DAFTAR PUSTAKA

[1] Humaira, S. Azzahra, and A. Atqiya, “Membangun Kesadaran Mahasiswa Dalam Menghadapi Tantangan Cyber Security di Era Digital,” 2024. [Online]. Available: http://jurnal.bundamediagrup.co.id/index.php/iuris

[2] D. E. D. Vivas, W. Y. G. Pena, S. P. C. Botero, and A. E. Rojas, “A Controlled Phishing Attack in a University Community: A Case Study,” *Journal of Internet Services and Information Security*, vol. 14, no. 2, pp. 98–110, May 2024, doi: 10.58346/JISIS.2024.I2.007.

[3] B. R. Alfathi, “Mahasiswa Jadi Target Utama Serangan Digital 2024,” Data GoodStats.

[4] N. Vadila and A. R. Pratama, “Analisis Kesadaran Keamanan Terhadap Ancaman Phishing,” 2024.

[5] S. Guduru, “PHISHING SIMULATION AUTOMATION: GOPHISH CAMPAIGNS WITH AZURE AD CONDITIONAL ACCESS AND USERRISK-BASED TRAINING,” *INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING AND TECHNOLOGY*, vol. 13, no. 1, pp. 87–97, Feb. 2022, doi: 10.34218/IJCET_13_01_008.

[6] L. Alzahrani, “Statistical Analysis of Cybersecurity Awareness Issues in Higher Education Institutes.” [Online]. Available: www.ijacsa.thesai.org

[7] M. E. Whitman and H. Mattord, “Principles of Information Security,” 2005. [Online]. Available: https://www.researchgate.net/publication/200446660

[8] A. N. Puriwigati, “Sistem Informasi Manajemen-Keamanan Informasi.” [Online]. Available:

https://www.researchgate.net/publication/341293613

[9] L. A. Febrika Ardy, I. Istiqomah, A. E. Ezer, and S. N. Neyman, "Phishing di Era Media Sosial: Identifikasi dan Pencegahan Ancaman di Platform Sosial," *Journal of Internet and Software Engineering*, vol. 1, no. 4, p. 11, Jun. 2024, doi: 10.47134/pjise.v1i4.2753.

[10] K. Subandi, M. Ahmad, V. I. Sugara, A. S. Aryani, and & Hermawan, "Awareness Cybercrime Phishing Email Menggunakan Secure Socket Layer Sebagai Interpretasi Information Security," vol. 9, p. 2024, 2024.

[11] J.Wright, "What is Gophish?," https://docs.getgophish.com/user-guide/what-is-gophish .

[12] Prof. Dr. Sugiyono, *METODE PENELITIAN KUANTITATIF, KUALITATIF, DAN RD*. J1. Gegerkalong Hilir No. 84 Bandung: ALFABETA, CV., 2013.

[13] R. B. Permadi and K. Ramli, "Analysis of Measuring Information Security Awareness for Employees at Institution XYZ," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 4, no. 4, pp. 1330–1338, Jul. 2024, doi: 10.57152/malcom.v4i4.1453