BAB I
PENDAHULUAN

1.1 Latar Belakang

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[1]. Tiga elemen utama dalam keamanan informasi meliputi kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan *(availability*). Dalam konteks Perguruan Tinggi, elemen-elemen ini sangat penting untuk melindungi data pribadi mahasiswa, nilai akademik, serta sistem informasi akademik secara keseluruhan. Secara ideal, semua sivitas akademika termasuk mahasiswa harus memiliki tingkat kesadaran yang memadai terhadap keamanan informasi untuk melindungi mereka dari ancaman keamanan.

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[2]. Umumnya, *email phishing* dirancang menyerupai pesan resmi, yang menggunakan bahasa formal dan tautan yang mengarah ke situs palsu yang tampak autentik. Hal ini membuat pengguna yang kurang waspada terhadap pesan *email* akan mudah tertipu dan akhirnya membocorkan data dan informasi penting.

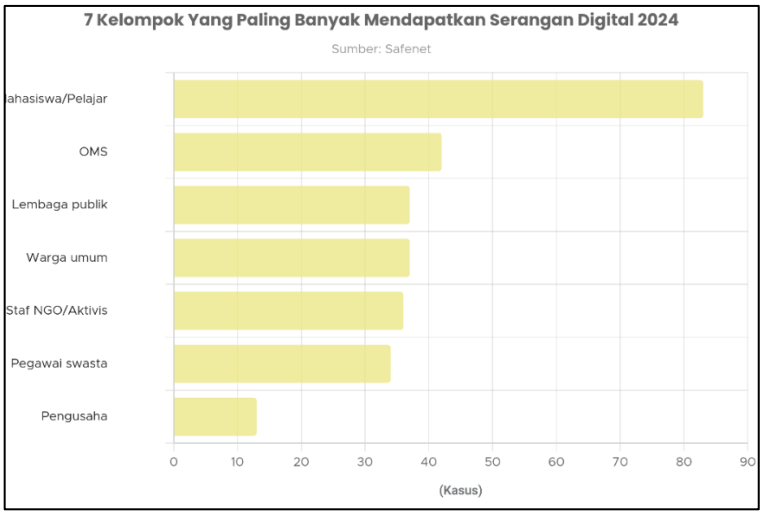
Teknik manipulasi psikologis yang digunakan dalam *email phishing* sering kali memanfaatkan emosi korban, seperti rasa takut, urgensi, rasa ingin tahu atau kepatuhan terhadap otoritas. Misalnya, pelaku dapat mengirim *email* palsu yang tampak seolah-olah berasal dari pihak administrasi kampus, berisi pesan seperti: *"Segera verifikasi akun mahasiswa anda dalam 24 jam untuk menghindari penangguhan akses."* Kalimat seperti ini dirancang untuk menciptakan tekanan waktu dan rasa panik, sehingga korban bertindak tanpa berpikir kritis. Studi oleh Vivas (2024)[3] 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. Oleh karena itu, pemahaman terhadap pola manipulasi dalam serangan *phishing* menjadi sangat penting dalam upaya peningkatan kesadaran keamanan informasi di lingkungan Perguruan Tinggi.

Berdasarkan laporan BSSN (2023) mencatat 86% dari 1.417 aduan siber di Indonesia berkategori *cybercrime*, dengan *phishing* sebagai vektor utama. Data ini mengindikasikan bahwa serangan *phishing* tidak hanya merupakan tren global, tetapi juga menjadi tantangan signifikan di tingkat nasional, termasuk di sektor pendidikan, pemerintahan dan layanan publik.

Berdasarkan *Verizon Data Breach Investigations Report* (2024), unsur manusia terkandung dalam 68% pelanggaran. Dari jumlah tersebut, *Comcast Business Cybersecurity Threat Report* menyebutkan 80-95% diawali oleh serangan *phishing*, dan total volume serangan *phishing* telah meroket sebesar

4.151% sejak munculnya *ChatGPT* pada tahun 2022. Pada tahun 2023, *Verizon* juga menyebutkan bahwa 36% insiden pelanggaran data diawali oleh serangan *phishing*, dengan sektor pendidikan sebagai salah satu yang paling terdampak. Fakta ini mengindikasikan adanya kesenjangan yang cukup besar antara kesadaran ideal dan kondisi aktual di lapangan, sehingga diperlukan intervensi yang tepat melalui pendekatan berbasis simulasi.

Dari segi sasaran, *phishing* cenderung lebih banyak menyasar entitas kolektif. Sebesar 65% serangan *phishing* ditujukan kepada organisasi, termasuk institusi pemerintahan, perusahaan swasta dan sektor pendidikan. Sementara itu, 35% sisanya menargetkan individu, baik secara acak maupun berdasarkan data pribadi yang telah diperoleh melalui pelanggaran keamanan sebelumnya.



Gambar 1.1 7 Kelompok Paling Banyak Mendapatkan Serangan Digital 2024

Berdasarkan laporan GoodStats (2025)[4], menunjukkan grafik 7 golongan yang mendapatkan serangan digital tahun 2024 yang tertinggi adalah mahasiswa/pelajar. Sektor pendidikan menempati peringkat teratas sebagai kelompok yang paling sering menjadi target serangan digital. Hal ini menunjukkan bahwa institusi pendidikan, seperti sekolah dan universitas dapat menjadi sasaran utama akibat lemahnya sistem keamanan informasi serta rendahnya kesadaran pengguna terhadap ancaman siber.

Kebutuhan akan penelitian ini semakin mendesak seiring meningkatnya aktivitas digital pascapandemi *COVID-19*, di mana proses pembelajaran, komunikasi, dan pengelolaan data akademik lebih banyak dilakukan secara daring. Selain itu, rendahnya literasi digital dan minimnya edukasi formal mengenai keamanan siber di kalangan mahasiswa juga menjadi masalah utama. Banyak mahasiswa yang aktif menggunakan teknologi informasi, namun belum memiliki kemampuan dasar untuk mengenali dan menghindari ancaman seperti *email phishing*. Kurangnya pelatihan praktis dalam mengenali serangan siber menyebabkan mereka cenderung abai terhadap keamanan data pribadi maupun institusional.

Penelitian oleh Guduru (2022), mengembangkan sistem otomatis berbasis *GoPhish* yang terintegrasi dengan *Microsoft Azure Active Directory* untuk menilai risiko pengguna dan memberikan pelatihan keamanan secara adaptif. Temuan ini menunjukkan bahwa simulasi berbasis *GoPhish* tidak hanya mampu meningkatkan kesadaran tetapi juga dapat diintegrasikan dalam sistem keamanan institusional[5]. Selain itu, penelitian oleh Wibowo (2024) juga menunjukkan efektivitas penggunaan *GoPhish* dalam lingkungan organisasi nyata. Melalui simulasi *email phishing* terhadap karyawan, mereka menemukan bahwa meskipun sebagian besar karyawan menunjukkan kesadaran terhadap ancaman *phishing*, masih terdapat celah signifikan dalam kemampuan mendeteksi serangan[6]. Penggunaan *GoPhish* terbukti efektif dalam merancang, mengelola dan memantau kampanye *phishing* serta memberikan wawasan mendalam untuk perbaikan strategi pelatihan keamanan siber secara berkelanjutan.

Fenomena yang terjadi pada pengguna internet khususnya 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 serangan *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* dengan *email*. 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.

1.2 Perumusan Masalah

Berdasarkan tingginya risiko kebocoran data akibat serangan *phishing* melalui *email* serta rendahnya kemampuan mahasiswa dalam mengenali ciri-ciri *email phishing,* menunjukkan bahwa tingkat kesadaran keamanan informasi mahasiswa belum optimal. Kurangnya edukasi dan pelatihan keamanan siber di lingkungan Perguruan Tinggi menjadi salah satu faktor penyebab kondisi tersebut. Oleh karena itu, diperlukan kajian untuk menganalisis tingkat kesadaran mahasiswa terhadap anacaman *phishing* serta penerapan simulasi serangan *phishing* menggunakan *gophish* sebagai upaya peningkatan kesadaran keamanan informasi.

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini mencakup beberapa aspek penting untuk memperjelas ruang lingkup penelitian. Penelitian ini difokuskan pada analisis tingkat kesadaran mahasiswa terhadap keamanan informasi dalam konteks serangan *email phishing*, dimana simulasi serangan dilakukan menggunakan platform *Gophish* dan difokuskan pada mahasiswa di Politeknik Negeri Bengkalis. Ruang lingkup penelitian berfokus pada perilaku pengguna

dan tingkat kesadaran terhadap ancaman *email phishing* tanpa membahas aspek teknis keamanan sistem maupun bentuk serangan siber lainnya.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian dengan judul "Analisis Tingkat Kesadaran Mahasiswa terhadap Keamanan Informasi Melalui Simulasi Serangan *email phishing* Menggunakan *GoPhish"*, adalah sebagai berikut:

a. Merancang simulasi serangan *phishing* menggunakan platform *GoPhish* sebagai sarana pengujian kesadaran keamanan informasi.
b. Menganalisis tingkat kesadaran mahasiswa terhadap keamanan informasi, terutama dalam konteks serangan *phishing.*

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah:

a. Memberikan kontribusi dalam pengembangan literatur terkait kesadaran keamanan informasi dikalangan mahasiswa.
b. Memberikan rekomendasi bagi Perguruan Tinggi dalam merancang strategi peningkatan kesadaran keamanan informasi secara efektif.
c. Memberikan gambaran awal mengenai tingkat kesadaran mahasiswa yang dapat digunakan sebagai bahan pertimbangan dalam penyusunan program pelatihan di masa mendatang
d. Memberikan gambaran nyata tentang kesadaran mahasiswa Politeknik Negeri Bengkalis terhadap *phishing* khususnya serangan *email phishing,* melalui simulasi yang menyerupai kondisi nyata.
e. Mengurangi risiko serangan *phishing* dengan meningkatkan kewaspadaan mahasiswa melalui simulasi menggunakan *Gophish.*