BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi telah mempercepat pertukaran data dan kolaborasi antar divisi dalam perusahaan. Namun, kemajuan ini juga meningkatkan risiko serangan siber, khususnya melalui teknik *phishing* yang menargetkan individu dalam perusahaan maupun organisasi untuk mengakses informasi sensitif. Di Indonesia, serangan *phishing* dan insiden kebocoran data menunjukkan tren peningkatan yang mengkhawatirkan. Badan Siber dan Sandi Negara (BSSN) dalam Laporan Lanskap Keamanan Siber tahun 2024 mencatat sebanyak 26.771.610 aktivitas *phishing* terjadi di Indonesia (Badan Siber dan Sandi Negara, 2024). Selain itu, Asosiasi Anti *Phishing* Dunia atau *Anti-Phishing Work Group* (APWG) juga mengamati bahwa pada kuartal ketiga tahun 2024 sebanyak 932.923 serangan *phishing* terjadi, jumlah itu dikatakan naik dari 877.536 yang terjadi pada kuartal kedua (APWG, 2024). Fenomena ini menyoroti kerentanan perusahaan terhadap serangan *phishing* dan pentingnya upaya pengukuran tingkat kesadaran keamanan siber di perusahaan (Wibowo & Hidayat, 2024).

Di lingkungan perusahaan, risiko serangan *phishing* semakin nyata karena karyawan menjadi pengguna utama pada sistem informasi yang beroperasi dalam perusahaan, sering kali karyawan menjadi target utama dalam serangan *phishing*. Laporan *Data Breach Investigations Report* (DBIR) 2024 oleh Verizon mengungkapkan bahwa sebanyak 68% insiden keamanan siber disebabkan oleh faktor manusia, dengan *phishing* sebagai metode paling dominan digunakan oleh pelaku kejahatan siber (Verizon Business, 2024). Hal ini menegaskan bahwa rendahnya kesadaran keamanan siber karyawan dapat meningkatkan keberhasilan serangan *phishing*.

Seiring meningkatnya ancaman *phishing*, berbagai penelitian telah berusaha mengukur tingkat kesadaran keamanan siber sebagai upaya mitigasi. Studi yang dipublikasikan dalam Jurnal Teknologi dan Informasi (JATI) oleh Tan dkk. (2024) menemukan bahwa tingkat kesadaran keamanan siber mahasiswa universitas di Kota Batam tergolong rendah (Tan dkk., 2024). Temuan serupa juga disampaikan oleh Kusumaningrum, Wijayanto, dan Raharja (2022) yang mengukur kesadaran keamanan siber mahasiswa selama masa pandemi menggunakan metode *Multiple Criteria Decision Analysis* (MCDA). Hasilnya menunjukkan tingkat kesadaran berada pada level "sedang" dengan skor tertinggi pada dimensi pengetahuan dan skor terendah pada perilaku (Kusumaningrum dkk., 2022).

Menurut Wibowo dan Hidayat (2024) dalam evaluasi strategi peningkatan kesadaran keamanan siber karyawan di PT XYZ menggunakan Gophish untuk sebagai salah satu instrumen dalam pembuatan simulasi *phishing* pada tahapan studinya, menunjukkan adanya celah signifikan dalam kemampuan karyawan dalam mendeteksi serangan *phishing*, meskipun kesadaran secara umum berdasarkan hasil evaluasi dari metode yang digunakan sudah cukup baik. Namun, penelitian tersebut tidak menjelaskan secara rinci metode analisis yang digunakan untuk mengevaluasi hasil *pra-test*, simulasi, dan *post-test*, sehingga diperlukan pendekatan yang lebih terstruktur (Wibowo & Hidayat, 2024).

Sementara itu, penelitian oleh Kostelić (2025) mengembangkan kerangka kerja berbasis *Technique for Order Preference by Similarity to Ideal Solution* (TOPSIS) dan pembobotan *Analytical Hierarchy Process* (AHP) untuk menilai risiko keamanan siber karyawan. Studi ini menunjukkan bahwa kombinasi metode tersebut efektif dalam membedakan karyawan dengan risiko tinggi dan rendah berdasarkan data hasil simulasi dan kuesioner (Kostelić, 2025).

Temuan-temuan ini menunjukkan perlunya metode yang lebih sistematis untuk mengukur kesadaran siber di lingkungan perusahaan. Berbagai penelitian telah dilakukan untuk mengukur tingkat kesadaran siber dan penggunaan metode *Multi-Criteria Decision Analysis* (MCDA) telah banyak digunakan dalam

berbagai konteks. Namun, masih terdapat kesenjangan dalam integrasi metode MCDA dengan simulasi *phishing* berbasis data perilaku nyata. Penggunaan simulasi *phishing* dengan analisis berbasis banyak kriteria, seperti TOPSIS masih memiliki ruang pengembangan lebih lanjut untuk memberikan evaluasi yang lebih terhadap kesadaran keamanan siber di lingkungan kerja.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis tingkat kesadaran keamanan siber karyawan terhadap serangan *phishing* dengan menggunakan Gophish dan *Technique for Order Preference by Similarity to Ideal Solution* (TOPSIS). Gophish dipilih karena memiliki keunggulan dibandingkan alat *phishing* lainnya. Sebagai perangkat lunak *open-source*, Gophish memungkinkan simulasi *phishing* dilakukan dengan biaya rendah dan mudah diakses. Selain itu, alat ini memiliki antarmuka grafis yang intuitif, *API REST* untuk integrasi dengan sistem lain, serta kemampuan menjalankan berbagai serangan *phishing* secara bersamaan. Dibandingkan dengan alat lain seperti King Phisher dan SET Toolkit, Gophish lebih unggul dalam kemudahan implementasi dan pelaporan hasil secara *real-time* (Sudhakar & Chellapandy, 2022).

Penelitian ini mengusulkan kebaruan melalui integrasi Gophish v0.12.1 dengan metode analisis data TOPSIS yang mempengaruhi kesadaran siber. Selain itu, fokus penelitian ini berada di lingkungan PT XYZ yang bergerak di bidang elektronika untuk industri pertahanan nasional, energi terbarukan, ICD & navigasi, serta transportasi perkeretaapian sehingga pengukuran ini lebih menekankan kepada karyawan sebagai subjek utama karena dianggap sering kali menjadi titik terlemah dalam sistem keamanan siber yang fokus pada perkembangan *people, process, and technology* (Collier, 2022). Penelitian ini menggunakan data perilaku nyata, yang tidak hanya memberikan hasil yang akurat tetapi juga dapat digunakan sebagai dasar untuk pengambilan keputusan strategis tentang bagaimana mengelola risiko siber di perusahaan. Oleh karena itu, untuk mengukur tingkat kesadaran keamanan siber karyawan, perlu dilakukan simulasi serangan *phishing*.

1.2 Perumusan Masalah

Berdasarkan latar belakang, rumusan masalah dalam penelitian ini adalah tindak serangan *phishing* menjadi ancaman nyata bagi PT XYZ karena dapat menyebabkan pencurian identitas, menghambat bisnis perusahaan, kerugian finansial, bahkan melemahkan sistem dan infrastruktur IT yang sedang berlangsung. Jenis serangan *phishing* yang umum terjadi di lingkungan perusahaan adalah *email phishing* dan *spear phishing* yang menargetkan individu maupun *stakeholder* perusahaan. Oleh karena itu, perlu dilakukan pengukuran tingkat kesadaran keamanan siber karyawan melalui simulasi serangan *phishing* menggunakan Gophish guna memberikan gambaran tingkat kesadaran karyawan PT XYZ terhadap berbagai insiden keamanan siber serta sejauh mana pengukuran kesadaran ini memberikan kontribusi nyata dalam perancangan strategi keamanan siber di lingkungan PT XYZ.

1.3 Batasan Penelitian

Batasan ini disusun untuk mencapai tujuan penelitian yang diinginkan dan membuat penelitian lebih fokus dan terarah. Berikut ini adalah batasan penelitian yang dimaksud:

1. Jenis *phishing* yang digunakan dalam simulasi serangan *phishing* menggunakan Gophish pada penelitian ini hanya *email phishing* dan *spear phishing*.
2. Segala bentuk saran dari mentor yang memuat teknis di lapangan dalam memperhatikan aspek keamanan informasi menjadi pedoman bagi peneliti.
3. Sampel dalam pengukuran tingkat kesadaran ini terbatas, hanya pada jumlah yang ditentukan oleh mentor dan manajer divisi IT & IO dengan memperhatikan risiko keamanan, waktu penelitian, dan batasan minimal sampel sebanyak 30.

1.4 Pertanyaan Penelitian

1. Bagaimana implementasi serangan *phishing* menggunakan Gophish dengan TOPSIS dalam mengukur tingkat kesadaran keamanan siber di lingkungan PT XYZ?
2. Bagaimana hasil analisis tingkat kesadaran keamanan siber karyawan terhadap serangan *phishing* menggunakan Gophish dan TOPSIS?

1.5 Tujuan Penelitian

Adapun tujuan pada penelitian ini adalah untuk mengukur tingkat kesadaran keamanan siber karyawan PT XYZ dengan mengimplementasikan simulasi serangan *phishing* menggunakan Gophish dan menganalisis data hasil simulasi serangan *phishing* menggunakan *Technique for Order Preference by Similarity to Ideal Solution* (TOPSIS).

1.6 Manfaat Hasil Penelitian

Penelitian ini diharapkan dapat memberikan manfaat antara lain:

1. Membantu PT XYZ mengidentifikasi kelemahan dalam kesadaran keamanan siber karyawan dan memberikan dasar untuk menyusun kebijakan keamanan yang lebih efektif.
2. Menjadikan penggunaan Gophish sebagai referensi *tools* utama pengukuran kesadaran dan pengetahuan karyawan dalam lingkup keamanan siber.
3. Membantu dalam perencanaan strategi pengelolaan risiko berdasarkan hasil pengukuran tingkat kesadaran keamanan siber karyawan.