BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Penggunaan teknologi informasi semakin meningkat dalam banyak hal. Peningkatan penggunaan ini akan membawa kebiasaan baru pengguna dalam mengumpulkan informasi. Keinginan untuk mendapatkan informasi dengan cepat mengarah pada fakta bahwa pengguna terkadang tidak menyadari kebenaran dan keakuratan informasi yang tersedia (Wijayanto, Muhammad and Hariyadi, 2020). Hal ini membuat pengguna rentan terhadap serangan di dunia digital, termasuk *phishing* (Gunawan, 2019). *Phishing* adalah upaya untuk mendapatkan informasi sensitif dari pengguna atau organisasi menggunakan SMS, email, atau pesan yang dikirim melalui situs web palsu, yang mengakibatkan kerugian finansial atau pencurian data sensitif (Destya, 2018). Berdasarkan laporan perusahaan *cybersecurity*, Kaspersky tentang serangan phishing di Asia Tenggara, khususnya Indonesia, yang menempati urutan ketiga setelah Vietnam dan Malaysia. Pada 2019, jumlah korban *phishing* adalah 14,316%. Angka ini meningkat dari sekitar 10,719% pada tahun sebelumnya (Irawan, 2020). Penelitian menunjukkan bahwa penipuan dan pencurian data adalah motif di balik kejahatan *phishing* ini. Rangkuman laporan konten negatif di laman *patrolsiber.id* menunjukkan bahwa penipuan terjadi melalui perangkat digital di Indonesia dengan 4601 laporan, tingkat kejahatan tertinggi dibandingkan kejahatan lainnya (*Laporan Kasus Kejahatan Siber*, 2021).

Survei yang mengukur tingkat kesadaran mahasiswa program sarjana Teknik Komputer (Tekkom) di Universitas Amikom Yogyakarta menemukan bahwa mahasiswa Tekkom cenderung memiliki kesadaran keamanan informasi yang lebih tinggi. Ini karena kita sudah tahu apa artinya menggunakan teknologi informasi, terutama potensi serangan siber (Destya, 2020). Berdasarkan observasi ditunjukkan bahwa masih banyak kasus pelanggaran merugi di kalangan mahasiswa di Kampus l Universitas Jenderal Ahmad Yani Yogyakarta. Lima

kasus serupa didaftarkan dari 2018 hingga 2022. Para korban adalah empat mahasiswa Fakultas Teknik dan Teknologi Informasi (FTTI) dan satu mahasiswa Fakultas Ekonomi dan Ilmu Sosial (FES). Pelaku menargetkan siswa dengan tujuan membajak akun media sosial dan menghasilkan kerugian dalam bentuk uang tunai dan pinjaman. Kerentanan terhadap serangan rekayasa sosial, termasuk penipuan dalam bentuk *phishing* (Vadila and Pratama, 2021), salah satu cara untuk mengatasinya adalah dengan meningkatkan kesadaran akan ancaman siber kepada pengguna akhir atau pengguna *(human firewall)* (Huwaidi and Destya, 2022). Inilah sebabnya mengapa diperlukan pengukuran tingkat kesadaran pengguna untuk mempertimbangkan langkah selanjutnya dalam membentuk *human firewall*. Kesadaran pengguna juga diukur oleh Mukhlis Amin menggunakan metode pengumpulan data dengan menyebarkan kuesioner dan analisis data menggunakan metode *Multiple Criteria Decision Analysis* (MCDA) (Amin, 2014). Penelitian serupa menggunakan metode ANOVA (analisis varians) dilakukan oleh Nunu Vadila dan Ahmad R. Pratama dan menunjukkan bahwa faktor demografi seperti *gender* mempengaruhi kesadaran keamanan informasi. Hasil penelitian ini menunjukkan bahwa perempuan lebih rentan terhadap ancaman *phishing* (Vadila and Pratama, 2021).

Kun Saidi juga melakukan pengukuran kesadaran siber dalam sebuah penelitian untuk menentukan metrik kunci untuk keamanan informasi menggunakan model *Technology Threat Aversion Theory* (TTAT) (Saidi and Prayudi, 2021). Penelitian ini hanya menggunakan instrumen kuesioner yang disebarkan. Di sisi lain, dalam penelitian ini, kami melakukan analisis komparatif untuk mengukur tingkat kesadaran pengguna terhadap serangan *phishing* berdasarkan tingkat pendidikan, kami menggunakan model *phishing*. Hasil penelitian ini diharapkan dapat menjadi bahan pertimbangan dalam pengembangan metode pelatihan kesadaran keamanan alternatif untuk meningkatkan kesadaran akan kejahatan penipuan, khususnya *phishing*, di dunia digital.

1.2 PERUMUSAN MASALAH

Penelitian ini terkait tingkat kesadaran keamanan informasi pengguna terhadap ancaman *phishing*. Menggunakan objek penelitian mahasiswa Universitas Jenderal Achmad Yani Yogyakarta, Fakultas Teknik dan Teknologi Informasi (FTTI). Skor Kesadaran Pengguna didasarkan pada prototipe pengukuran kesadaran keamanan informasi menggunakan metode *Technology Threat Aversion Theory* (TTAT) dan analisis data *phishing test* menggunakan metode MANOVA.

1.3 PERTANYAAN PENELITIAN

Adapun pertanyaan yang mendasari penelitian ini adalah sebagai berikut:

1. Bagaimana cara menjalankan uji *phishing test* terhadap target penelitian peneliti?
2. Bagaimana cara mengumpulkan data dari objek sampel yang ada?
3. Bagaimana cara menganalisis faktor pengaruh terhadap kejahatan digital khususnya serangan *phishing*?

1.4 TUJUAN PENELITIAN

Adapun tujuan dari penelitian ini adalah untuk mengetahui tingkat kesadaran keamanan siber mahasiswa Fakultas Teknik dan Teknologi Informasi, Universitas Jenderal Ahmad Yani Yogyakarta. Mengetahui apakah terdapat faktor yang sangat mempengaruhi tingkat kesadaran keamanan siber setiap objek dari analisis MANOVA yang dilakukan.

1.5 MANFAAT HASIL PENELITIAN

Manfaat dari penelitian ini adalah untuk memberikan kampanye terhadap potensi penipuan berupa *phishing*, dengan menggunakan instrumen untuk mengukur kesadaran kejahatan di dunia digital *(Cyber Security Awareness).* Kuesioner berdasarkan model *Technology Threat Aversion Theory* (TTAT) dengan objek mahasiswa Fakultas Teknik dan Teknologi Informasi. Penelitian ini diharapkan dapat memberikan wawasan tentang ancaman yang ditimbulkan oleh perkembangan teknologi dan cara menghindarinya.