BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Pada tahun 2021, penggunaan atau pemanfaatan internet di masyarakat Indonesia terus mengalami peningkatan dari tahun-tahun sebelumnya. Berdasarkan data hasil survei dari Asosiasi Penyelenggara Jasa Internet Indonesia atau disebut dengan APJII, pengguna internet di Indonesia mengalami peningkatan mencapai 210.026.769 jiwa pada periode 2021-2022 (Finaka et al., 2023). Internet juga mempermudah aktivitas sehari-hari seperti komunikasi, media sosial, transaksi, dan belanja. Sebanyak 89,03% pengguna lebih sering mengakses internet melalui smartphone atau tablet, menjadikannya target utama serangan siber. Riset McKinsey & Company menunjukkan bahwa Indonesia memiliki adopsi digital tercepat di Asia, terutama dalam perbankan digital, dengan penduduk perkotaan menggunakan 2 sampai 3 layanan perbankan digital. Oleh karena itu, peningkatan penggunaan *smartphone*, pertumbuhan *e-commerce*, dan digitalisasi bank menjadi pendorong transisi ke layanan perbankan digital (Ramadhan & Purwandari, 2023), Survei Populix Tahun 2022 menunjukkan bahwa 64% responden menggunakan aplikasi finansial atau perbankan melalui *smartphone* (GoodStat, 2022).

Data ini mengindikasikan tingginya penggunaan *mobile banking* di Indonesia, yang diperkirakan terus meningkat setiap tahun. Aktivitas masyarakat, seperti bersosial media, bertransaksi, dan menyimpan data di internet, turut meningkatkan utilitas layanan perbankan digital. Namun, hal ini juga memperbesar risiko terhadap ancaman keamanan digital yang mengancam data dan privasi pengguna (Ramadhan & Purwandari, 2023). Seiring dengan meningkatnya literasi keamanan siber, penelitian sebelumnya masih mengidentifikasi adanya kesenjangan dalam tingkat kesadaran terhadap ancaman seperti *phishing* dan rekayasa sosial. Laporan dari (Badan Siber dan Sandi Negara, 2020), mencatat bahwa dalam satu tahun terakhir, insiden serangan siber mengalami peningkatan hingga lima kali lipat, dengan sektor publik menjadi salah satu sasaran utama. Adapun insiden serangan siber yang ter data adalah serangan *trojan*, dan *email phishing*. Oleh karena itu,

diperlukan pendekatan yang terstruktur dan komprehensif dalam mengukur tingkat kesadarakeamanan informasi. Salah satu metode yang telah teruji efektivitasnya adalah *Human Aspects Of Information Security Questionnaire* (HAIS-Q), yang dirancang untuk mengevaluasi tiga dimensi utama yaitu, Pengetahuan, Sikap, dan Perilaku pengguna dalam menjaga keamanan informasi.

Untuk penelitian kedua dilakukan survei terhadap 58 mahasiswa tentang pemahaman bahaya *phishing*, dimana menunjukkan tingkat literasi yang beragam yaitu: sebanyak 8 orang mahasiswa sangat tidak paham, 10 orang mahasiswa tidak paham, 14 orang mahasiswa cukup paham, 16 orang mahasiswa mulai paham, dan 10 orang mahasiswa sangat paham. Hasil ini menunjukkan bahwa pemahaman masyarakat khususnya pada mahasiswa tentang dampak dan mitigasi serangan *phishing* masih terbatas (Ryansyah et al., 2023). Dari hasil data survei tersebut, dapat diuraikan bahwa masyarakat khususnya mahasiswa belum semua memahami literasi mengenai dampak serta mitigasi dalam menangani serangan *phishing* atau juga *Social Engineer*.

Dalam penelitian ini peneliti lebih fokus terhadap bagaimana menilai kesadaran pengguna khususnya pegawai Dinas Perdagangan, Perindustrian Dan Koperasi Usaha Kecil Dan Menengah Kabupaten Buleleng terhadap ancaman serangan *phishing* pada penggunaan layanan M-Banking. Penelitian ini dilakukan berdasarkan temuan awal mengenai potensi ancaman keamanan informasi yang dihadapi oleh pegawai Dinas Perdagangan, Perindustrian, dan Koperasi Usaha Kecil dan Menengah Kabupaten Buleleng. Berdasarkan observasi dan wawancara terhadap I Gusti Agung Adi Dharma selaku pegawai dinas pada bidang kepegawaian, terdapat indikasi bahwa beberapa pegawai menghadapi situasi yang melibatkan ancaman *phishing*. Dimana lima pegawai melaporkan pengalaman mereka menerima pesan dan telepon dari pihak yang tidak dikenal. Adapun penjelasan masalah yang dialami dapat diuraikan sebagai berikut:

1. Dua pegawai menerima SMS yang berisi tautan dengan klaim "Hadiah Kejutan dari Aplikasi Dana". Pesan tersebut meminta penerima untuk mengeklik tautan guna mengklaim hadiah, yang berpotensi merupakan upaya *phishing* untuk mencuri data pribadi atau informasi akun. Meskipun kedua pegawai tersebut mengakses tautan yang diberikan, dua pegawai tersebut

tidak mengisi data pribadi mereka. Walaupun tidak langsung memberikan informasi sensitif, tindakan ini menunjukkan rendahnya pengetahuan dan sikap terhadap bahaya *phishing*. Perlu juga untuk diketahui, mengeklik tautan yang mencurigakan dapat membuka risiko lain, seperti pencurian data atau penyebaran *malware* yang tidak disadari.

2. Dua pegawai menerima panggilan telepon yang mengaku dari bank BPD Bali dan Bank BNI, dimana menawarkan hadiah uang dengan syarat memberikan informasi kartu ATM seperti nomor kartu, tanggal kadaluwarsa, dan kode CVV untuk syarat penerimaannya. Meskipun pegawai tersebut waspada dan tidak memberikan informasi pribadi, pegawai ini tidak mengaktifkan fitur *auto-blocker* sebagai proteksi panggilan berbahaya yang bisa mencegah panggilan seperti ini. Tindakan ini juga mengindikasikan bahwa pegawai tersebut belum sepenuhnya memahami pentingnya langkah-langkah pencegahan lain, seperti mengaktifkan proteksi panggilan dan spam, untuk melindungi diri dari potensi ancaman di masa depan.
3. Satu pegawai melaporkan menerima pesan mencurigakan melalui WhatsApp yang berisi tautan palsu yang mengarah ke halaman login yang menyerupai situs web Bank Mandiri. Meskipun pegawai tersebut waspada terhadap pesan tersebut, ia tidak mengaktifkan fitur peramban yang aman yang seharusnya dapat mencegah akses ke tautan berbahaya. Akibatnya, ia tetap mengeklik tautan itu meskipun tidak mengisi data pribadi. Kejadian ini menunjukkan bahwa pegawai tersebut belum sepenuhnya memahami pentingnya langkah pencegahan, seperti mengaktifkan fitur peramban yang aman, untuk melindungi diri dari ancaman online, khususnya serangan *phishing*.

Dari permasalahan tersebut, kesadaran keamanan informasi menjadi aspek krusial dalam menghadapi ancaman digital, terutama dalam penggunaan layanan M-Banking pada lingkungan pemerintahan. Namun, Meskipun berbagai penelitian mengenai kesadaran keamanan informasi telah banyak dilakukan, terdapat sebuah fenomena yang secara konsisten muncul namun belum sepenuhnya menjelaskan apa yang menjadi celah dari penelitian terdahulu. Adapun penelitian yang dilakukan oleh Ramadhan & Purwandari (2023) menemukan bahwa meskipun

skor pengetahuan (84,45%) dan sikap (84,68%) pengguna perbankan digital tergolong baik, skor perilaku justru jauh lebih rendah (78,06%). Lalu hal serupa juga ditemukan oleh Ramadhani & Sari (2024) dan Nurjanah & Destya (2022), yang sama-sama menyimpulkan bahwa meskipun pemahaman sudah memadai, implementasi dalam tindakan nyata masih menjadi tantangan utama. Namun, penelitian tersebut cenderung hanya melaporkan adanya kesenjangan tanpa secara sistematis mengidentifikasi indikator perilaku spesifik mana yang paling rentan dan menjadi kontributor utama dari sebuah kesenjangan. Penelitian tersebut hanya berhenti pada kesimpulan umum bahwa bagian perilaku memiliki skor rendah tanpa memetakan secara rinci area mana yang paling rendah dan kritis. Oleh karena itu, penelitian ini bertujuan untuk mengisi gap tersebut dengan tidak sekadar mengukur tingkat kesadaran pada setiap dimensi, melainkan secara spesifik akan mengidentifikasi dan menyusun peringkat indikator perilaku yang paling lemah, sehingga dapat memberikan rekomendasi mitigasi yang jauh lebih terfokus dan berbasis bukti dan bukan sekadar saran umum untuk meningkatkan kesadaran pada bagian dimensi.

Selain itu, konteks organisasi pemerintahan daerah yang memiliki regulasi internal, tingkat literasi digital, serta budaya kerja birokratis yang berbeda, membutuhkan pendekatan yang berlainan dari sektor industri swasta atau pendidikan, namun konteks ini masih jarang dieksplorasi dalam literatur keamanan informasi. Di samping itu, hingga kini juga belum tersedia data empiris yang secara spesifik mengukur tingkat pengetahuan, sikap, dan perilaku pegawai Dinas Perdagangan Perindustrian Dan Koperasi Usaha Kecil Dan Menengah Kabupaten Buleleng terhadap praktik keamanan informasi dalam menghadapi serangan *phishing* pada penggunaan layanan M-Banking. Selain kurangnya data tersebut, pendekatan yang secara sistematis dengan menyusun pemeringkatan dimensi kerentanan juga belum banyak digunakan, padahal identifikasi terhadap dimensi yang paling lemah sangat penting untuk merumuskan langkah mitigasi yang lebih tepat sasaran. Oleh karena itu, penelitian ini bertujuan untuk mengisi kekosongan tersebut dengan menerapkan metode *Human Aspects of Information Security Questionnaire* (HAIS-Q) dan pendekatan pemeringkatan kerentanan berdasarkan Dimensi Pengetahuan, Sikap, Dan Perilaku, sehingga dapat

memberikan rekomendasi yang kontekstual dan tepat guna dalam penguatan keamanan informasi di sektor pemerintahan daerah.

Pemilihan metode *Human Aspects of Information Security Questionnaire* (HAIS-Q) dalam penelitian ini didasarkan pada kemampuan dalam mengukur kesadaran keamanan informasi melalui tiga dimensi utama yaitu, dimensi pengetahuan, sikap, dan dimensi perilaku. Penggunaan metode HAIS-Q ini juga memberikan pendekatan yang lebih menyeluruh dengan menilai tidak hanya sejauh mana individu mengetahui ancaman keamanan informasi (Pengetahuan), tetapi juga bagaimana sikap dalam menanggapi ancaman tersebut (Sikap), serta apakah individu benar-benar menerapkan praktik keamanan yang sesuai dalam kesehariannya atau tidak (Perilaku). Kelebihan lain dari metode HAIS-Q adalah bahwa metode ini telah diuji validitas dan reliabilitasnya dalam berbagai penelitian keamanan informasi, sehingga hasil yang diperoleh lebih dapat diandalkan dan aplikatif dalam konteks organisasi (Kruger & Kearney, 2006). Jadi penggunaan metode HAIS-Q lebih cocok dalam menangkap aspek psikologis dan perilaku pengguna dalam konteks keamanan informasi. Kontribusi yang diberikan dari penelitian ini adalah untuk mengukur dan meningkatkan pemahaman pegawai Dinas Perdagangan Perindustrian Dan Koperasi Usaha Kecil Dan Menengah Kabupaten Buleleng tentang ancaman serangan *phishing*. Tujuannya adalah untuk memahami tingkat pengetahuan pegawai Dinas Perdagangan Perindustrian Dan Koperasi Usaha Kecil Dan Menengah Kabupaten Buleleng terhadap ancaman serangan *phishing* pada penggunaan layanan M-Banking.

Berdasarkan uraian, maka penelitian ini akan melakukan analisis menggunakan metode analisis data deskriptif kuantitatif yang berfokus kepada pengumpulan data, survei, penyusunan dan penentuan keputusan, serta tingkat keamanan informasi pegawai dengan judul "Analisis Kesadaran Keamanan Informasi Penggunaan Layanan M-Banking Oleh Pegawai Dinas Perdagangan, Perindustrian, Dan Koperasi Usaha Kecil Dan Menengah Kabupaten Buleleng Menggunakan Metode Human Aspects Of Information Security Questionnaire (HAIS-Q)". Hasil penelitian ini diharapkan dapat menjadi panduan bagi para pemangku kebijakan, instansi pemerintahan, organisasi keamanan siber, dan

masyarakat umum dalam upaya melindungi diri dari serangan *phishing* yang semakin kompleks khususnya dalam perbankan digital.

1.2 Batasan Masalah

Agar pembahasan pada penelitian ini lebih spesifik pada tujuan yang telah diuraikan di atas, maka penelitian ini menerapkan ruang lingkup sebagai berikut:

1. Penelitian ini secara spesifik mengukur kesadaran keamanan informasi pegawai Dinas Perdagangan, Perindustrian, dan Koperasi Usaha Kecil dan Menengah Kabupaten Buleleng dalam konteks ancaman *phishing* pada penggunaan layanan M-Banking. Pengumpulan data dilakukan dengan menggunakan Metode Human Aspects of Information Security Questionnaire (HAIS-Q) yang akan mencakup dimensi pengetahuan, sikap, dan perilaku pegawai terhadap keamanan informasi.
2. Penelitian ini akan berfokus pada pembuatan instrumen survei menggunakan kertas lembar pernyataan pengisian kuesioner sebagai alat untuk menyebarkan pertanyaan kepada pegawai, dengan tujuan untuk memahami tanggapan dan pemahaman mereka terhadap keamanan informasi pada penggunaan layanan M-Banking.
3. Penelitian ini akan menganalisis dimensi mana yang memiliki dampak terbesar terhadap keamanan informasi pada penggunaan layanan M-Banking, dimana akan digunakan untuk menyusun rekomendasi mitigasi yang lebih efektif dalam mengurangi risiko serangan *phishing* di lingkungan dinas.

1.3 Rumusan Masalah

Berdasarkan uraian latar belakang permasalahan diatas, maka rumusan masalah yang didapat yaitu:

1. Bagaimana tingkat kesadaran keamanan informasi pegawai Dinas Perdagangan, Perindustrian, dan Koperasi UKM Kabupaten Buleleng berdasarkan pengukuran menggunakan metode Human Aspects of Information Security Questionnaire (HAIS-Q)?

2. Dimensi dan indikator mana yang memiliki tingkat kesadaran paling rendah dan dapat dijadikan dasar utama dalam menentukan prioritas rekomendasi mitigasi terhadap kerentanan keamanan informasi?

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah diatas, maka tujuan dari penelitian ini adalah:

1. Untuk mengetahui tingkat kesadaran keamanan informasi pegawai Dinas Perdagangan, Perindustrian, dan Koperasi UKM Kabupaten Buleleng berdasarkan pengukuran menggunakan metode Human Aspects of Information Security Questionnaire (HAIS-Q).
2. Untuk mengidentifikasi dimensi dan indikator dalam metode HAIS-Q yang memiliki tingkat kesadaran paling rendah dan dapat dijadikan dasar utama dalam menentukan prioritas rekomendasi mitigasi terhadap kerentanan keamanan informasi.

1.5 Manfaat Penelitian

Berdasarkan tujuan dari penelitian yang telah diuraikan di atas, diharapkan manfaat yang didapatkan sebagai berikut:

1. Menjadi pedoman referensi untuk penelitian sejenis yang akan dibuat oleh peneliti selanjutnya.
2. Memberikan manfaat dalam meningkatkan kesadaran pegawai terhadap keamanan informasi khususnya yang melibatkan sektor finansial dan perbankan M-Banking
3. Memberikan analisis tingkat kesadaran terhadap ancaman keamanan informasi pada pegawai Dinas Perdagangan Perindustrian Dan Koperasi Usaha Kecil Dan Menengah Kabupaten Buleleng serta berdasarkan faktor demografis yang berbeda pada setiap pegawai.