# BAB I

# PENDAHULUAN

## 1.1 LATAR BELAKANG MASALAH

Kemajuan teknologi di era digital saat ini mendorong perubahan mendalam di berbagai aspek kehidupan manusia, termasuk sektor perbankan (Arner, Barberis & Buckley, 2016). Penggunaan *mobile banking* kian marak di masyarakat luas, terutama pada kelompok Generasi Z yang memanfaatkan kepraktisannya untuk memproses berbagai keperluan perbankan secara fleksibel tanpa harus datang langsung ke bank, seperti transfer uang, pembayaran berbagai tagihan, maupun transaksi produk finansial lainnya (Alalwan, 2020). Bagi mahasiswa Generasi Z yang dikategorikan sebagai *digital natives*, keakraban mereka dengan teknologi digital menjadikan aplikasi perbankan sebagai pilihan utama yang jauh lebih diandalkan dibandingkan metode perbankan konvensional dalam memenuhi kebutuhan finansial sehari-hari (Prensky, 2001; Ozkan & Solmaz, 2015). Akan tetapi, kemudahan ini menyembunyikan tantangan yang cukup besar terkait kesadaran akan keamanan *(security awareness)* dalam penggunaan *mobile banking*.

Mahasiswa sebagai bagian dari Generasi Z sering kali mengutamakan kepraktisan dalam menggunakan teknologi, tetapi tidak selalu memiliki kesadaran yang tinggi terhadap keamanan informasi (Jones & Mitchell, 2016). Mahasiswa merupakan salah satu kelompok yang paling terpengaruh oleh perkembangan teknologi. Mereka sangat bergantung pada teknologi, baik untuk kebutuhan akademik, sosial, maupun pribadi. Namun, banyaknya data pribadi yang disimpan secara digital, mahasiswa dihadapkan dengan risiko tinggi terhadap ancaman siber seperti *phishing, malware, social engineering,* pencurian identitas, hingga peretasan dan kebocoran data yang menjadi tantangan utama dalam keamanan *mobile banking* (Dinarti et al., 2024).

Sering kali, mahasiswa merasa nyaman menggunakan berbagai platform digital tanpa sepenuhnya menyadari risiko yang ada seperti mengabaikan pentingnya memverifikasi sumber email atau tautan yang di terima, yang dapat menyebabkan mereka secara tidak sadar memberikan informasi sensitif kepada peretas yang berpotensi membuka celah bagi serangan siber, seperti *man-in-the-middle attacks*

(Mitnick & Simon, 2011). Guna meminimalisasi risiko tersebut, peningkatan kesadaran mengenai esensi penjagaan privasi dan data pribadi menjadi hal yang krusial. Mahasiswa dituntut untuk memahami sekaligus mempraktikkan mitigasi dasar, seperti mengaplikasikan sandi yang kuat, mendeteksi skema phishing, serta mengelola pengaturan kerahasiaan data di platform media sosial dengan cermat (Putra dkk., 2024).

Sebagai institusi akademik, universitas dan perguruan tinggi memegang peranan penting dalam menumbuhkan literasi digital serta kesadaran akan keamanan informasi di kalangan mahasiswanya. Hal ini dikaji sebagai bagian dari penelitian mengenai sejauh mana mahasiswa memahami pentingnya keamanan informasi saat menggunakan layanan perbankan seluler *(mobile banking)*. Dengan demikian, studi ini menjadi penting untuk menganalisis tingkat kesadaran keamanan di kalangan mahasiswa Undiksha, sekaligus menentukan sejauh mana mereka memahami, mematuhi, dan menerapkan praktik-praktik keamanan saat menggunakan layanan perbankan seluler.

Kesadaran terhadap aspek keamanan merupakan hal yang esensial dalam kehidupan modern saat ini, terutama untuk membentengi diri dari berbagai risiko pihak eksternal yang berupaya mengeksploitasi atau mencuri data pribadi demi kepentingan merugikan. Pengetahuan mengenai kesadaran keamanan sebaiknya ditanamkan sejak masa sekolah dan diterapkan dalam praktik (Kusumaningrum dkk., 2022). Menurut Tiatama (2016), kesadaran keamanan informasi merefleksikan kondisi saat pengguna dalam organisasi mengerti sekaligus berkomitmen pada misi-misi pengamanan. Konsep ini turut merepresentasikan dimensi kognitif, di mana cara pandang seseorang terhadap keamanan informasi di sebuah organisasi dikondisikan oleh seperangkat kebijakan keamanan informasi yang ada (Bauer & Bernroider, 2017).

Kesadaran keamanan *(security awareness)* merujuk pada pemahaman dan kesadaran seseorang mengenai berbagai ancaman, risiko, serta langkah-langkah yang dapat melindungi sistem dan informasi dari serangan atau akses yang tidak sah. Kesadaran ini mencakup pengetahuan tentang cara mengidentifikasi ancaman, menggunakan kata sandi yang aman, mengelola akses, dan merespons insiden keamanan siber (Kruger & Kearney, 2006). Kesadaran keamanan berperan penting

dalam mengurangi risiko kejahatan siber. Ketika individu dan organisasi memiliki pengetahuan yang cukup tentang ancaman siber dan cara mengatasinya, mereka dapat menentukan langkah-langkah proaktif untuk mengamankan mereka. Misalnya, kesadaran tentang phishing dapat membantu pengguna mengenali dan menghindari pesan yang mencurigakan, sehingga mengurangi kemungkinan menjadi korban pencurian identitas atau informasi (Parsons et al., 2017).

Kerangka kerja model Kruger-Kearney diaplikasikan untuk mengolah data survei serta mengkuantifikasi tingkat kesadaran keamanan informasi, dengan menitikberatkan pada tiga pilar utama yakni *knowledge* (pengetahuan), *attitude* (sikap), dan *behavior* (perilaku). Hasil analisis ini diharapkan dapat memberikan implikasi positif bagi penelitian mendatang serta penguatan program keterlibatan publik yang berfokus pada kesadaran mahasiswa akan keamanan informasi. Kemudahan dalam penggunaan *mobile banking* oleh mahasiswa Generasi Z di Universitas Pendidikan Ganesha (Undiksha) membawa konsekuensi tersembunyi. Sebagai pengguna aktif teknologi, mereka sangat mungkin memprioritaskan kepraktisan di atas keamanan, namun belum ada data kuantitatif yang spesifik dan terukur mengenai sejauh mana tingkat kesadaran keamanan informasi (*security awareness*) mereka yang sebenarnya.

Masalah utamanya terletak pada kesenjangan antara tingginya tingkat penerimaan layanan perbankan seluler di kalangan mahasiswa Undiksha dengan kurangnya kesadaran mereka mengenai risiko yang mungkin mereka hadapi. Anggapan umum bahwa mereka rentan terhadap serangan siber seperti *phishing*, perangkat lunak berbahaya *(malware)*, dan rekayasa sosial *(social engineering)* (Dinarti dkk., 2024) tidaklah cukup untuk dijadikan dasar dalam pengambilan keputusan kebijakan. Tanpa penilaian yang jelas mengenai tingkat pengetahuan, sikap, dan perilaku saat ini terkait keamanan, baik pihak universitas maupun para mahasiswa tidak memiliki landasan yang kuat untuk melakukan inisiatif perbaikan. Ketiadaan data diagnostik semacam itu menimbulkan risiko bahwa upaya peningkatan kesadaran keamanan siber mungkin tidak tepat sasaran dan menjadi tidak efektif. Oleh karena itu, studi ini sangat diperlukan untuk menjembatani kesenjangan data tersebut.

## 1.2 IDENTIFIKASI MASALAH DAN RUMUSAN MASALAH

Kemudahan dalam penggunaan teknologi tidak selalu diimbangi dengan pemahaman dan kesadaran akan pentingnya menjaga keamanan informasi pribadi. Ketergantungan mahasiswa pada aspek kemudahan sering kali mengesampingkan risiko keamanan siber yang ada. Tanpa implementasi standar keamanan informasi yang cermat, mereka rentan terhadap ancaman serius seperti kejahatan phishing, ancaman malware, penyalahgunaan identitas, serta peretasan data pribadi (Dinarti et al, 2024). Kurangnya kesadaran ini menciptakan celah keamanan yang dapat dimanfaatkan oleh penjahat siber untuk mencuri data pribadi atau informasi sensitif. Diperlukan penilaian yang jelas mengenai tingkat kesadaran keamanan di kalangan mahasiswa khususnya di Universitas Pendidikan Ganesha mengingat mereka termasuk dalam Generasi Z. Demi mendapatkan gambaran mendalam terkait evaluasi kesadaran keamanan informasi di kalangan mahasiswa, yang dikenal luas sebagai pengguna aktif perangkat digital namun masih sering abai terhadap prinsip-prinsip pengamanan. Berdasarkan permasalahan tersebut, dirumuskanlah pertanyaan-pertanyaan penelitian berikut.

1. Bagaimana tingkat kesadaran keamanan informasi pada kalangan mahasiswa Universitas Pendidikan Ganesha?
2. Bagaimana perbedaan dari tingkat kesadaran keamanan informasi berdasarkan dari faktor demografis umur?

## 1.3 TUJUAN PENELITIAN

1. Untuk mengukur tingkat kesadaran keamanan mahasiswa Undiksha Generasi Z.
2. Untuk merepresentasikan tingkat kesadaran keamanan informasi berdasarkan faktor demografis.

## 1.4 BATASAN MASALAH

1. Penelitian ini berfokus untuk mahasiswa Generasi Z di Universitas Pendidikan Ganesha dengan rentang usia antara 18 hingga 22 tahun sebagai subjek penelitian.
2. Sebagai alat ukur penelitian, *Human Aspects of Information Security Assessment* (HAIS-Q) diterapkan guna mengkuantifikasi tingkat kesadaran pengamanan informasi. Pengukuran tersebut menitikberatkan

pada tiga aspek dasar *KAB* (pengetahuan/*knowledge*, sikap/*attitude*, dan perilaku/*behavior*) dalam konteks interaksi pengguna dengan internet serta teknologi informasi.

3. Penelitian ini menerapkan pendekatan kuantitatif serta data deskriptif.
4. Data yang digunakan diperoleh dari responden yaitu generasi Z di Universitas Pendidikan Ganesha dengan cara menyebar kuesioner menggunakan *google form*.
5. Penelitian ini hanya sampai memberikan hasil dari analisis yang sudah diidentifikasi yaitu simpulan.
6. Penelitian hanya mencakup aspek keamanan informasi dalam konteks *mobile banking* dan tidak mencakup aspek teknis dari sistem keamanan perbankan.

## 1.5 MANFAAT HASIL PENELITIAN

1. Manfaat Teoritis

Diharapkan penelitian ini akan memberikan informasi dan literatur tentang kesadaran keamanan digital pengguna layanan mobile banking, khususnya tentang tingkat kesadaran mereka tentang keamanan informasi. Ini juga akan membantu mengembangkan teori tentang keamanan informasi, terutama yang berkaitan dengan Generasi Z, yang sering menggunakan teknologi. Penelitian ini juga akan menjadi acuan bagi penelitian selanjutnya yang ingin mengeksplorasi masalah atau memperdayakan masalah serupa.

2. Manfaat Praktis

Dengan melakukan penelitian ini, diharapkan dapat memberikan informasi yang digunakan oleh mahasiswa untuk mengidentifikasi dan meningkatkan kesadaran mereka tentang pentingnya keamanan digital dan pengelolaan kata sandi yang baik serta dapat mengurangi potensi risiko keamanan pada layanan *mobile banking* di kalangan mahasiswa melalui perilaku yang lebih aman dalam pengelolaan *mobile banking*.

3. Manfaat bagi Peneliti

Meningkatkan pengetahuan dan pengalaman dalam melakukan riset ilmiah di bidang keamanan informasi serta perilaku pengguna digital. Peneliti dapat

mengembangkan keterampilan analisis data kuantitatif, penyusunan instrumen penelitian, dan pengolahan hasil melalui pendekatan ilmiah. Selain itu, peneliti juga memperoleh wawasan aktual mengenai fenomena keamanan informasi yang terjadi di kalangan generasi Z, yang sangat relevan dengan tantangan dunia digital saat ini.