BAB I
PENDAHULUAN

1.1 Gambaran Umum Objek Penelitian

1.1.2 Profil Universitas Telkom

Gambar 1. 1 Logo Universitas Telkom

Sumber: *Website* Resmi Universitas Telkom (2024)

Telkom University, yang terletak di Bandung, Jawa Barat, didirikan pada tahun 2013 dengan menggabungkan empat institusi pendidikan tinggi di bawah naungan Yayasan Pendidikan Telkom. Dilansir dari *website* resmi Universitas Telkom (2024), Universitas ini memiliki visi untuk menjadi universitas riset dan kewirausahaan (*research and entrepreneurial university*) yang tidak hanya menyediakan pendidikan berkualitas tinggi tetapi juga berfokus pada pengembangan riset dan inovasi yang memberikan dampak positif bagi masyarakat serta perekonomian nasional.

Telkom University memiliki beragam program studi yang tersebar di tujuh fakultas, yaitu:

1. Fakultas Teknik Elektro (FTE
2. Fakultas Teknik Informatika (FTI)
3. Fakultas Rekayasa Industri (FRI)
4. Fakultas Ekonomi dan Bisnis (FEB)

5. Fakultas Komunikasi dan Bisnis (FKB)
6. Fakultas Industri Kreatif (FIK)
7. Fakultas Ilmu Terapan (FIT)

Dengan jumlah mahasiswa aktif yang berjumlah 48.127, Telkom University mengedepankan pendekatan pendidikan inovatif dan berkomitmen memberikan layanan pendidikan berkualitas yang diakui dengan akreditasi "A" dari BAN-PT. Beberapa program studinya juga telah memperoleh pengakuan internasional. Dalam mendukung visi riset dan inovasi, Telkom University memiliki fasilitas unggulan seperti Bandung Techno Park, yang berfungsi sebagai pusat inovasi dan kolaborasi antara universitas dan industri. Selain itu, kampus ini mendorong partisipasi mahasiswa dalam program Merdeka Belajar Kampus Merdeka, yang memberikan pengalaman belajar di luar kampus untuk mengembangkan kompetensi dan wawasan mahasiswa secara lebih luas.

1.2 Latar Belakang

Mihalčová *et al,* (2023) serta Susanto & Maulana (2024) mengungkapkan di era kemajuan pesat dalam sistem informasi dan internet, keamanan sistem informasi menjadi hal yang sangat krusial bagi organisasi maupun perusahaan. Dengan berkembangnya teknologi, ancaman terhadap keamanan informasi pun semakin bertambah. Kebebasan berkomunikasi melalui jejaring sosial dapat memicu berbagai ancaman, seperti penyebaran informasi palsu (*hoax*) hingga kehilangan data. Sejalan dengan hal tersebut, Hwang *et al,* (2021) menegaskan bahwa beragam upaya dapat dilakukan untuk melindungi data dan informasi dari ancaman, termasuk pencurian data, peretasan, dan penyalahgunaan informasi oleh pihak yang tidak memiliki wewenang. Oleh karena itu, menekankan pemahaman individu terhadap keamanan informasi perlu ditanamkan dengan baik.

Menjaga privasi data pribadi, baik milik diri sendiri maupun orang lain, adalah tanggung jawab dan hak yang perlu dilindungi oleh setiap individu. Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) (2023) melaporkan bahwa pada periode 2022–2023, jumlah pengguna internet di Indonesia mencapai 215,63 juta jiwa dari total populasi sebesar 275,78 juta jiwa, hal ini menunjukkan tingginya penetrasi internet di masyarakat. Tingginya jumlah pengguna ini diiringi dengan

maraknya insiden kebocoran data. CNN Indonesia (2021) melaporkan bahwa pada tanggal 22 Mei 2020, akun Twitter @underthebreach mengklaim telah membobol dan menyebarluaskan 2,3 juta data warga dan pemilih Indonesia dari Komisi Pemilihan Umum (KPU) dalam sebuah forum hacker. Kasus yang lebih besar kemudian terjadi di BPJS Kesehatan. Kompas.com (2021) melaporkan bahwa sebanyak 279 juta data peserta BPJS diduga diperjualbelikan di forum hacker Raid Forums, yang berisi data pribadi seperti NIK, nama, alamat, nomor telepon, email, hingga besaran gaji. Ancaman siber pun semakin nyata, terbukti dari laporan Media Indonesia (2021) yang menyebutkan bahwa pada periode Januari–Mei 2021, Badan Siber dan Sandi Negara (BSSN) mencatat sebanyak 448.491.256 serangan siber (anomali trafik) yang terjadi di Indonesia. Fenomena ini menunjukkan bahwa meskipun kemajuan teknologi dapat dinikmati oleh semua individu di dunia, hal ini juga menambah risiko penyalahgunaan data pribadi sebagaiamana yang disampaikan oleh Ariadi *et al*, (2024).

Lebih lanjut, Akraman *et al*, (2018) mengungkapkan bahwa rendahnya kesadaran pengguna terhadap keamanan informasi masih menjadi persoalan serius, terutama dalam hal pelaporan insiden keamanan yang kerap diabaikan. Pengguna cenderung menyelesaikan permasalahan sendiri tanpa melibatkan otoritas terkait, yang justru memperbesar potensi risiko lanjutan.

Menurut Ramadhani & Pratama, (2020) kesadaran akan keamanan siber atau "*cybersecurity awareness*" adalah pengetahuan yang sangat penting bagi setiap pengguna internet. Pengetahuan ini sangat diperlukan untuk melindungi diri dalam berbagai aktivitas digital, terutama saat menggunakan media sosial. Dengan memiliki kesadaran terhadap keamanan siber saat bermedia sosial, pengguna internet dapat mengambil langkah pencegahan terhadap potensi serangan siber yang mungkin dilakukan oleh peretas. DataReportal (2023) mencatat bahwa pada Februari 2023, terdapat 212,9 juta pengguna internet aktif di Indonesia, yang setara dengan sekitar 77% dari populasi Indonesia, dengan usia rata-rata penduduk Indonesia sebesar 29,8 tahun. Dari jumlah tersebut, 49,5% berusia antara 13 hingga 44 tahun, menunjukkan tingginya tingkat penggunaan internet di kalangan kaum muda untuk berbagai aktivitas, termasuk studi. Tan *et al*, (2024) menambahkan

bahwa usia rata-rata mahasiswa di Indonesia yang berkisar antara 17 hingga 22 tahun termasuk dalam rentang usia pengguna internet aktif di Indonesia . Hal ini menunjukkan bahwa mayoritas pemuda, terutama mahasiswa, sangat rentan terhadap risiko serangan siber akibat kurangnya kesadaran tentang pentingnya menjaga data pribadi dan privasi digital. Nopriadi (2024) mengungkapkan bahwa kesadaran akan risiko di kalangan anak muda, termasuk mahasiswa, masih tergolong rendah. Sebuah penelitian menunjukkan bahwa meskipun 80% responden peduli terhadap privasi mereka, hanya 25% yang secara aktif mengubah pengaturan privasi di akun media sosial mereka. Temuan ini diperkuat oleh penelitian Puspita Kencana Sari & Candiwan (2020) yang menyatakan bahwa meskipun pengguna memiliki tingkat pengetahuan yang tinggi mengenai keamanan informasi, perilaku nyata mereka dalam menerapkan praktik tersebut masih belum optimal.

Dikutip dari GMA News Online (2020), salah satu contoh kasus peretasan yang terjadi di kalangan mahasiswa adalah insiden yang terjadi di Filipina pada tahun 2020, di mana seorang mahasiswa jurusan Teknologi Informasi ditangkap karena diduga meretas dan merusak sistem manajemen portal universitasnya. Peretasan ini melibatkan akses terhadap data pribadi mahasiswa lain serta kredensial login, yang menyebabkan kerentanannya terhadap informasi yang tercatat dalam sistem universitas tersebut. Pihak berwenang menemukan perangkat seperti kartu Paymaya dan alat skimming saat penangkapan, yang menunjukkan bahwa motif kejahatan siber di kalangan mahasiswa dapat beragam, mulai dari vandalisme hingga pencurian data untuk keuntungan finansial. Kompas.com (2021) melaporkan di Indonesia kasus kebocoran data yang melibatkan institusi pendidikan terjadi pada Universitas Diponegoro (Undip) pada tahun 2021, di mana ribuan data pribadi mahasiswa dilaporkan bocor dan dijual di forum daring illegal. Data yang bocor meliputi nama lengkap, nomor induk mahasiswa (NIM), alamat email, nomor telepon, serta beberapa informasi akademik lainnya, yang berpotensi disalahgunakan untuk tindakan kriminal seperti phishing, pencurian identitas, atau penipuan berbasis rekayasa sosial (social engineering). Asia Times (2022) mencatat Indonesia mengalami 423,4 juta serangan siber pada tahun 2020, dan tingginya

tingkat ancaman ini menunjukkan perlunya peningkatan kesadaran keamanan siber di kalangan mahasiswa.

Azizi *et al,* (2024) mengungkapkan mahasiswa yang sering menggunakan teknologi, penting untuk mengetahui cara mengamankan data yang dimiliki serta memahami risiko dan langkah-langkah pencegahan terkait keamanan siber. Dengan meningkatkan kesadaran terhadap keamanan siber, kita dapat melindungi diri dan berpartisipasi dengan aman dalam dunia digital. Menurut Alqahtani (2022), Kesadaran keamanan siber di kalangan mahasiswa dipengaruhi oleh berbagai faktor utama yang saling berinteraksi. Pertama, pengetahuan teknis memiliki peran penting dalam menentukan sejauh mana seseorang sadar dan mampu melindungi data pribadi. Semakin baik pemahaman teknis seseorang mengenai keamanan online, misalnya terkait pengaturan kata sandi dan pengaturan browser, semakin tinggi tingkat kesadaran sibernya Kovacevic *et al,* (2020) serta Sangwan (2024) mengungkapkan bahwa pengalaman pribadi dalam menghadapi ancaman siber, seperti menjadi korban serangan siber, juga berpengaruh signifikan. Mahasiswa yang pernah mengalami atau menyaksikan kejadian semacam itu cenderung lebih berhati-hati dan lebih Memahami terkait risiko dalam dunia digital. Di lingkungan kampus, sosialisasi melalui pelatihan dan seminar mengenai keamanan siber dapat meningkatkan pemahaman dan kesiapsiagaan mahasiswa terhadap ancaman ini. Faktor lainnya adalah pengaruh teman sebaya dan lingkungan. Mahasiswa sering memperoleh informasi tentang praktik keamanan siber dari teman-temannya atau media sosial. Paparan terhadap informasi dari lingkungan sekitar ini memperkuat pemahaman mereka tentang pentingnya langkah pencegahan terhadap serangan siber. Teman sebaya yang memiliki pengetahuan tentang keamanan siber dapat berperan sebagai sumber yang berharga dalam membentuk sikap dan perilaku yang lebih proaktif terkait pengelolaan data di kalangan mahasiswa. Oleh karena itu, lingkungan kampus yang memiliki ekosistem digital yang intensif berpotensi memperkuat interaksi dan pertukaran informasi terkait keamanan siber.

Beberapa perguruan tinggi di Indonesia telah menerapkan konsep *kampus digital* sebagai bentuk adaptasi terhadap perkembangan teknologi informasi. Berdasarkan Informasi dari *website* resmi Universitas Indonesia (2022),

Universitas Indonesia (UI) mengembangkan *Integrated Academic Information System* (SIAK-NG) untuk mendukung layanan akademik secara daring, Hal serupa juga diterapkan oleh Universitas Bina Nusantara (Binus) , dikutip dari *website* resmi Universitas Binus (2021), Universitas Bina Nusantara (Binus) menggunakan platform *Binusmaya* sebagai sistem pembelajaran dan administrasi berbasis teknologi , Sementara itu, Universitas Telkom turut mengadopsi konsep *smart campus* dengan mengintegrasikan teknologi digital ke dalam berbagai aspek kegiatan akademik dan administrasi. Berdasarkan Informasi dari *website* Telkom University (2023), Penerapan konsep ini mencakup pemanfaatan sistem informasi dan layanan berbasis teknologi yang mendukung proses pembelajaran, administrasi, dan interaksi seluruh civitas akademika, sehingga menciptakan lingkungan kampus yang terhubung secara digital. Universitas Telkom telah mengintegrasikan teknologi digital ke dalam seluruh aspek layanan akademik, administrasi, dan kehidupan kampus. Penerapan konsep *smart campus* yang terhubung dengan berbagai layanan berbasis *cloud*, seperti *Learning Management System* (LMS), sistem presensi digital, dan Microsoft 365 untuk seluruh civitas akademika, hal ini menjadikan Universitas Telkom sebagai ekosistem digital yang sangat intensif. Tingginya ketergantungan terhadap teknologi ini membuat mahasiswa Universitas Telkom memiliki tingkat paparan risiko siber yang signifikan, sehingga menjadi objek yang relevan dan strategis untuk mengukur perbedaan tingkat kesadaran keamanan siber berdasarkan karakteristik demografis.

Mahasiswa Universitas Telkom, yang berada dalam lingkungan berbasis teknologi informasi dan komunikasi serta telah menerapkan konsep kampus *digital*, menghadapi risiko signifikan terhadap ancaman keamanan siber. Sebagai pengguna aktif internet dan teknologi, mahasiswa sering kali terpapar berbagai ancaman siber, seperti *phishing*, *malware*, dan pencurian data. Urgensi perlindungan terhadap data dan sistem digital semakin meningkat setelah insiden keamanan yang terjadi pada sistem Learning Management System (LMS) Universitas Telkom pada tahun 2021. Berdasarkan wawancara dengan Bapak Yusza Reditya Murti, S.T., M.Kom., selaku *Assistant Manager IP & Technology Transfer Bandung Techno Park*, terungkap bahwa *server cloud* LMS yang digunakan oleh institusi mengalami serangan siber

berupa infiltrasi malware yang dimanfaatkan untuk aktivitas penambangan Bitcoin secara ilegal. Serangan ini tidak langsung menargetkan aplikasi pengguna, melainkan menyerang infrastruktur server yang digunakan, sehingga menyebabkan lonjakan biaya operasional *server* yang mencapai ratusan juta rupiah. Kejadian ini memperlihatkan bahwa ancaman keamanan tidak hanya bersifat teoritis, tetapi telah menimbulkan kerugian finansial nyata bagi institusi. Pasca kejadian tersebut, dilakukan berbagai tindakan mitigasi seperti penggunaan sistem keamanan tambahan, pemindaian keamanan berkala, penerapan 2FA, dan penguatan otentikasi login melalui Microsoft 365.

Kejadian tersebut menjadi cerminan bahwa kesadaran keamanan siber tidak hanya diperlukan pada level teknis pengelola sistem, tetapi juga pada tingkat pengguna akhir, khususnya mahasiswa. Penelitian ini memiliki tingkat urgensi yang tinggi karena kesadaran terhadap keamanan siber tidak hanya memengaruhi kemampuan mahasiswa dalam melindungi data pribadi, tetapi juga berkontribusi pada upaya menjaga integritas akademik serta privasi data institusi. Sebagai calon profesional di bidang teknologi, mahasiswa Universitas Telkom memiliki peran penting dalam menjamin keamanan informasi, baik pada tingkat individu maupun institusional.

Dalam konteks ini, penting untuk meninjau apakah kesadaran keamanan siber di kalangan mahasiswa menunjukkan perbedaan jika dilihat dari karakteristik demografis tertentu. Faktor-faktor seperti jenis kelamin, usia, pengalaman menggunakan internet, dan pendapatan keluarga dipilih karena masing-masing memiliki potensi memengaruhi perilaku dan kewaspadaan terhadap ancaman siber. Jenis kelamin dapat berkaitan dengan perbedaan preferensi dan kebiasaan dalam penggunaan teknologi, usia memengaruhi kemampuan adaptasi terhadap perkembangan teknologi, pengalaman penggunaan internet menentukan tingkat familiaritas terhadap risiko daring, sedangkan pendapatan keluarga dapat memengaruhi akses terhadap perangkat dan literasi digital. Penelitian sebelumnya menunjukkan hasil yang beragam, seperti Alsobeh *et al,* (2023) serta Kovacevic *et al,* (2020), menunjukkan bahwa adanya perbedaan tingkat kesadaran keamanan siber di antara kategori demografis tersebut. Di sisi lain, penelitian seperti

Ramadhani & Pratama (2020) serta Mahendra *et al*, (2024), melaporkan bahwa tidak semua faktor, seperti jenis kelamin, menunjukkan perbedaan yang berarti. Namun sebaliknya, Sari & Sihotang (2016) menegaskan bahwa terdapat variasi kesadaran keamanan informasi berdasarkan usia, latar belakang pendidikan, dan pendapatan.

Variasi temuan dari penelitian-penelitian sebelumnya menunjukkan perlunya kajian yang lebih mendalam dan kontekstual untuk memahami sejauh mana perbedaan tingkat kesadaran keamanan siber dapat terjadi antar kelompok demografis. Meskipun topik ini telah banyak dibahas, sebagian besar penelitian berfokus pada hubungan atau pengaruh faktor demografi, sementara studi yang secara spesifik menyoroti perbedaan tingkat kesadaran keamanan siber di lingkungan akademik yang memiliki karakteristik digitalisasi tinggi masih terbatas. Universitas Telkom, sebagai perguruan tinggi berbasis teknologi dengan ekosistem *smart campus*, menjadi objek yang tepat untuk melihat bagaimana faktor demografis membentuk variasi kesadaran keamanan siber. Oleh karena itu, penelitian ini memiliki urgensi untuk mengisi kekosongan kajian tersebut dan memberikan kontribusi strategis bagi peningkatan kesadaran keamanan siber di kalangan mahasiswa.

1.3 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Apakah terdapat perbedaan tingkat kesadaran keamanan siber berdasarkan jenis kelamin pada mahasiswa Universitas Telkom?
2. Apakah terdapat perbedaan tingkat kesadaran keamanan siber berdasarkan kelompok usia pada mahasiswa Universitas Telkom?
3. Apakah terdapat perbedaan tingkat kesadaran keamanan siber berdasarkan pengalaman penggunaan internet pada mahasiswa Universitas Telkom?
4. Apakah terdapat perbedaan tingkat kesadaran keamanan siber berdasarkan tingkat pendapatan keluarga pada mahasiswa Universitas Telkom?

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah, tujuan dari penelitian ini adalah:

1 Untuk mengetahui adanya perbedaan tingkat kesadaran keamanan siber berdasarkan jenis kelamin pada mahasiswa Universitas Telkom.

2 Untuk mengetahui adanya perbedaan tingkat kesadaran keamanan siber berdasarkan kelompok usia pada mahasiswa Universitas Telkom.

3 Untuk mengetahui adanya perbedaan tingkat kesadaran keamanan siber berdasarkan pengalaman penggunaan internet pada mahasiswa Universitas Telkom.

4 Untuk mengetahui adanya perbedaan tingkat kesadaran keamanan siber berdasarkan tingkat pendapatan keluarga pada mahasiswa Universitas Telkom.

1.5 Manfaat Penelitian

1.5.1 Aspek Teoritis

Penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan literatur di bidang manajemen, teknologi informasi, dan keamanan siber, khususnya yang berkaitan dengan analisis perbedaan tingkat kesadaran keamanan siber berdasarkan faktor demografi. Hasil penelitian ini dapat menjadi referensi bagi akademisi dalam memahami bagaimana variabel demografi seperti jenis kelamin, usia, pengalaman penggunaan internet, dan pendapatan keluarga berperan dalam membentuk kesadaran keamanan siber. Selain itu, temuan ini dapat memperkaya kajian teori tentang hubungan antara karakteristik individu dan perilaku keamanan siber dalam konteks lingkungan akademik digital.

1.5.2. Aspek Praktis

Secara praktis, hasil penelitian ini dapat menjadi masukan bagi pihak Universitas Telkom dan institusi pendidikan tinggi lainnya dalam merancang program sosialisasi, pelatihan, dan kebijakan keamanan siber yang lebih efektif dan tepat sasaran berdasarkan karakteristik demografis mahasiswa. Temuan ini juga dapat membantu pengelola teknologi informasi di kampus untuk mengidentifikasi kelompok mahasiswa yang memerlukan perhatian atau intervensi khusus dalam meningkatkan kesadaran keamanan siber. Selain itu, penelitian ini dapat

memberikan wawasan bagi mahasiswa untuk meningkatkan sikap proaktif dalam menjaga keamanan data pribadi dan privasi digital.

1.7 Ruang Lingkup Penelitian

1.7.1 Lokasi dan Objek Penelitian

a. Penelitian ini berlokasi di Indonesia.
b. Objek penelitian adalah Mahasiswa Universitas Telkom Bandung.

1.7.2 Sistematika Penulisan Tugas Akhir

a. BAB I PENDAHULUAN

Bagian ini memberikan gambaran umum mengenai objek penelitian, yang mencakup latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian dari sisi teori dan praktik, ruang lingkup penelitian, serta susunan sistematika penulisan tugas akhir.

b. BAB II TINJAUAN PUSTAKA

Pada bab ini, dijelaskan berbagai teori yang relevan dan mendukung penelitian yang dilakukan. Selain itu, juga dibahas penelitian-penelitian sebelumnya yang berkaitan dengan topik atau permasalahan yang diteliti.

c. BAB III METODE PENELITIAN

Bab ini menguraikan metode yang digunakan untuk mengumpulkan serta menganalisis data yang diperlukan guna menjawab atau menjelaskan permasalahan penelitian.

d. BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini memaparkan hasil penelitian yang diperoleh, kemudian membahasnya secara kronologis dan sistematis sesuai dengan rumusan masalah serta tujuan penelitian.

e. BAB V KESIMPULAN DAN SARAN

Bagian ini berisi kesimpulan yang didasarkan pada hasil penelitian untuk menjawab rumusan masalah yang telah ditentukan sebelumnya. Selain itu, disertakan juga saran dari penulis, baik untuk pengembangan teori maupun penerapan praktis.