BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi informasi dan internet telah membawa perubahan signifikan dalam cara kita menjalani kehidupan sehari-hari. Di era yang semakin digital ini, teknologi telah menjadi bagian yang tidak terpisahkan dari aktivitas sehari-hari, mengubah cara kita berkomunikasi, bekerja, dan berinteraksi. Ketergantungan terhadap teknologi telah merambah ke berbagai aspek kehidupan, penggunaan internet sudah menjadi hal yang lumrah, bahkan mendominasi proses Bisnis, Kesehatan, Administrasi dan Pendidikan. Berdasarkan dari *We Are Social and Hotsuite* pada kuartal pertama tahun 2021 total pertumbuhan penduduk Indonesia sebesar 274,9 juta jiwa. Sedangkan populasi penggunaan *Smartphone* sebesar 125,6% dari total penduduk. Untuk pengguna Internet sebesar 73,7%. Dari sisi pengunaan sosial media, urutan pertama ditempati oleh *Whatsapp*, kemudian *Facebook* dan *Instagram*. Selain media sosial, penggunaan aplikasi selama pandemi juga sangat tinggi. Penggunaan aplikasi belanja sebesar 78,2%, finansial dan perbankan 39,2%, dan kesehatan 23,4% (Abthal et al., 2022).

Pemanfaatan teknologi informasi dan internet sudah menjadi bagian yang tidak terpisahkan dari kehidupan di era digital ini termasuk oleh mahasiswa. Mahasiswa mengandalkan perangkat digital dan jaringan internet untuk berbagai aktivitas, mulai dari pembelajaran, komunikasi, hingga penyimpanan data. Namun dalam konteks ketergantungan ini, muncul risiko serius terkait privasi data pribadi. Data pribadi, seperti identitas pribadi, informasi akademis, dan informasi keuangan, menjadi semakin rentan terhadap potensi pelanggaran dan penyalahgunaan.

Salah satu ancaman serius yang harus diwaspadai adalah "*Phishing*". *Phishing* adalah teknik penipuan *online* yang digunakan oleh penjahat dunia maya untuk mendapatkan informasi pribadi, seperti kata sandi, nomor kartu kredit, dan data keuangan lainnya, dengan menyamar sebagai entitas tepercaya. Biasanya, penjahat dunia maya akan mengirimkan pesan palsu yang tampaknya berasal dari lembaga keuangan, perusahaan, atau situs web resmi lainnya kepada korbannya. *Phishing* berasal dari kata *fishing* yaitu memancing. Kegiatan *Phishing* memang bertujuan memancing orang untuk memberikan informasi pribadi secara sukarela tanpa disadari. Padahal informasi yang dibagikan tersebut akan digunakan untuk tujuan kejahatan (W. Hidayat et al., 2023).

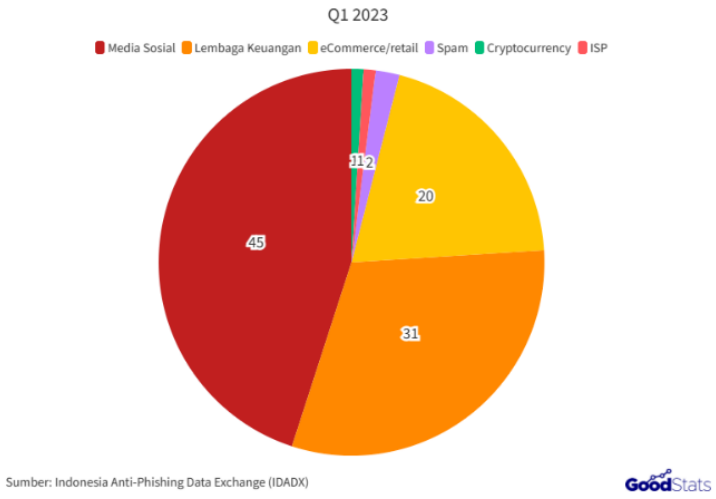
Berdasarkan laporan *National Cyber Security Index* (NCSI), pada tahun 2022 Indonesia memperoleh nilai indeks keamanan siber sebesar 38,96 poin dari total 100 poin. Hasil ini menempatkan Indonesia pada peringkat ketiga terendah di antara negara-negara anggota G20. Secara global, Indonesia berada di peringkat 83 dari total 160 negara yang terdokumentasi dalam laporan tersebut. Penilaian yang dilakukan NCSI didasarkan pada sejumlah faktor, antara lain peraturan hukum terkait keamanan siber di Tanah Air, keberadaan lembaga pemerintah yang fokus pada keamanan siber, tingkat kerja sama pemerintah dalam mengenai keamanan siber, serta bukti publik seperti situs resmi pemerintah atau program terkait (National Cyber Security Index, 2022).

Sumber : Goodstats.id

Gambar 1. 1 Kasus Phishing di Indonesia Kuartal I 2023

Menurut data Indonesia *Anti-Phishing Data Exchange* (IDADX), jumlah pengaduan serangan *Phishing* di Indonesia tahun 2023 meningkat secara signifikan. IDADX mencatat sebanyak 26.675 laporan serangan pada periode kuartal I 2023. Sedangkan pada periode kuartal 4 2022 hanya terdapat sekitar 6.106 laporan *Phishing*. Hal tersebut mengalami kenaikan sebanyak 20.569 laporan *Phishing*. Jika diperinci untuk kuartal pertama tahun 2023, terjadi peningkatan kasus serangan *Phishing* terbanyak pada bulan Februari, dengan jumlah pengaduan mencapai 15.050 kasus. Sementara itu, jumlah kasus pada bulan Januari sekitar 7.665 kasus, dan pada bulan Maret tercatat sebanyak 3.960 kasus. Peningkatan kasus kebocoran data internet di Indonesia secara global menyebabkan Indonesia menduduki peringkat pertama sebagai negara dengan tingkat kebocoran data terbesar di kawasan Asia Tenggara. Kebocoran

data di Indonesia pada kuartal kedua tahun 2022 bahkan mengalami kenaikan sebesar 143 persen dibandingkan dengan kuartal pertama tahun 2022.



Sumber : Goodstats.id

Gambar 1. 2 Persentase Industri Rentan Phishing di Indonesia

Menurut laporan IDADX, sektor industri yang paling umum menjadi target serangan *Phishing* dari Januari hingga Maret 2023 adalah media sosial, dengan proporsi sebesar 45%. Lalu, diikuti oleh sektor lembaga keuangan dengan proporsi 31%, ritel/*eCommerce* sebesar 20%, spam 2%, serta ISP dan mata uang kripto (*cryptocurrency*) masing-masing sebesar 1%.

Dengan maraknya terjadi *cybercrime* di Indonesia, hingga saat ini hukum yang mengatur perlindungan data pribadi tersebar dalam beberapa peraturan perundang-undangan yang berlaku, termasuk di antaranya Pasal 79 ayat (1) Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (UU Administrasi Kependudukan), Pasal 58 Peraturan Pemerintah Nomor 37 Tahun 2007 mengenai Pelaksanaan Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (PP Administrasi Kependudukan), dan Pasal 26 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (dikenal sebagai UU ITE).

Meskipun sudah ada perlindungan hukum terhadap *cybercrime,* Mahasiswa sebagai pengguna aktif teknologi dan internet rentan terhadap serangan *Phishing*. Riset dari *National Cybersecurity Alliance* menemukan bahwa generasi Z (18-25 tahun) dan generasi Y atau millenial (26-42 tahun) paling rentan terhadap penipuan online. Generasi Z paling sering menjadi korban

phishing, dengan 34 persen dari mereka terdampak. Sementara generasi Y atau milenial cenderung lebih sering menjadi korban *romance scam*, alias tertipu dalam hubungan asmara sebesar 18 persen dan mengalami pencurian data pribadi sebesar 20 persen (National Cybersecurity Alliance, 2023). Data dari Badan Pusat Statistik (BPS) pada Maret 2023 menunjukkan bahwa 94,16% anak muda Indonesia yang termasuk dalam generasi Z dan millenial (16-30 tahun) mengakses internet pada quartal pertama 2023 untuk mengakses media sosial (84,37%), yang mana merupakan salah satu media utama penyebaran phishing (Muhamad, 2023).

Kesadaran mereka dalam menjaga privasi data pribadi sangat penting untuk mengurangi risiko pencurian data dan kerugian yang mungkin timbul akibat serangan tersebut. Kurangnya pemahaman dan kesadaran ini menimbulkan perlunya penelitian mendalam mengenai tingkat kesadaran mahasiswa dalam menjaga privasi data pribadinya. Penelitian ini akan membantu mengidentifikasi tingkat kesadaran mahasiswa dan pemahaman mereka tentang risiko privasi data. Penelitian ini akan menggunakan model analisis *Information Security Awareness* (ISA) oleh Kruger dan Kearney. Metode ini digunakan untuk mengembangkan alat ukur yang didasarkan pada teknik yang diambil dari bidang psikologi sosial yang mengusulkan bahwa kecenderungan yang dipelajari untuk merespons dengan cara yang menguntungkan atau tidak menguntungkan untuk objek tertentu, memiliki tiga komponen yaitu *Knowledge*, *Attitude*, dan *Behavior* (Kuslaila et al., 2023).

Berdasarkan hasil beberapa penelitian sebelumnya ditemukan berbagai temuan yang relevan. Pertama, penelitian (Alif & Pratama, 2021a) dengan model *Information Security Awareness* (ISA) dan menggunakan metode analisis *Multiple Criteria Decision Analysis* (MCDA) menunjukkan bahwa kesadaran keamanan pengguna E-Wallet di Indonesia secara keseluruhan sudah memadai. Namun, masih terdapat potensi untuk meningkatkan pengetahuan, sikap, dan sikap pengguna, terutama dalam aspek seperti penggunaan *Password*/OTP, pemahaman tentang perangkat lunak, dan penggunaan internet yang masih memiliki tingkat kesadaran yang lebih rendah dibandingkan dengan aspek perangkat keras. Kedua, penelitian oleh (Vadila & Pratama, 2021) dengan metode ANOVA mengindikasikan bahwa masyarakat Indonesia secara garis besar masih belum mampu mengenali ancaman *Phishing*. Hasil riset menemukan kasus penipuan *online* dengan cara memanipulasi untuk menipu korban dan kesadaran pengguna terhadap informasi tentang kerahasiaan password.

Information Security Awareness (ISA) dipilih sebagai model penelitian yang akan digunakan dalam penelitian ini adalah karena model ini dapat membantu

dalam memahami tahapan kesadaran individu, termasuk memahami ancaman dalam mengambil tindakan pencegahan dengan mudah. Model ISA hanya menggunakan 3 variabel yang sudah mampu untuk mengukur tingkat kesadaran mahasiswa dari bahaya *Phishing*. Model ini juga membantu mengidentifikasi hambatan yang mungkin menghambat langkah-langkah perlindungan privasi, dengan tujuan mengembangkan rekomendasi untuk meningkatkan kesadaran mahasiswa dan langkah-langkah pencegahan terhadap *Phishing*.

Penelitian ini dilakukan di Universitas Jambi dikarenakan dari studi awal, terlihat ada masalah yang sesuai dengan fokus penelitian peneliti. Ternyata, belum ada penelitian serupa di lingkungan mahasiswa Universitas Jambi. Peneliti memilih lokasi ini juga karena ingin mendapatkan pandangan yang seimbang dari berbagai jurusan mengenai kesadaran privasi data.

Berdasarkan survey pra-penelitian yang telah dilakukan, diperoleh jawaban dari total 39 responden. Hasil dari survey pra-penelitian adalah saat survey penelitian dilakukan diperoleh 34 (89,5%) responden sudah mengetahui apa itu *phishing*, meskipun demikian 24 (61,5%) responden pernah menjadi korban *phishing* melalui website, Instagram, WhatsApp, Facebook, Telegram dan Email. Penyebabnya adalah 5 (12,9%) responden mengatakan iklan/pesan terlihat menarik dan meyakinkan, 8 (20.5%) responden pada saat itu belum mengetahui apa itu *phising* dan 13 (33,3%) responden tidak sengaja mengakses.

Gambar 1. 3 Survey Pra-Penelitian

Selain itu, kurangnya pelajaran khusus tentang privasi data dan ancaman *Phishing* menjadi salah satu faktor dari terjadinya hal ini. Mahasiswa hanya mendapatkan informasi umum dari mata kuliah tertentu, dan minimnya informasi dari media mengenai privasi data.

Berdasarkan permasalahan yang telah diuraikan, maka perlu dilakukan penelitian tentang tingkat kesadaran mahasiswa dalam menjaga privasi data

pribadi dengan judul **"EVALUASI KESADARAN MAHASISWA UNIVERSITAS JAMBI TERHADAP PRIVASI DATA PRIBADI DARI BAHAYA *PHISHING*"**. Penelitian ini diharapkan dapat memberikan kontribusi penting dalam meningkatkan pemahaman dan kesadaran mahasiswa tentang pentingnya privasi data pribadi mereka di era digital.

1.2 Rumusan Masalah

Berikut ini adalah rumusan masalah yang akan digunakan pada penelitian ini :

1. Bagaimana tingkat kesadaran mahasiswa Universitas Jambi terhadap keamanan data pribadi dari bahaya *phishing*?
2. Apakah terdapat pengaruh yang signifikan dari jenis kelamin, angkatan, dan fakultas terhadap kesadaran mahasiswa Universitas Jambi dalam menjaga privasi data pribadi dari bahaya *phishing* melalui metode analisis regresi linear berganda?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah diatas, maka tujuan pada penelitian ini adalah sebagai berikut :

1. Untuk mengetahui tingkat kesadaran mahasiswa Universitas Jambi mengenai keamanan data pribadi dari bahaya *phishing*
2. Untuk mengetahui pengaruh dari jenis kelamin, angkatan, dan fakultas terhadap kesadaran mahasiswa Universitas Jambi dalam menjaga privasi data pribadi dari bahaya *phishing* metode analisis regresi linear berganda

1.4 Batasan Masalah

Berdasarkan pemasalahan yang telah diuraikan diatas, maka dalam penulisan tugas akhir ini membatasi permasalahan tersebut dalam beberapa hal, yaitu :

a. Penelitian ini akan membatasi responden pada Mahasiswa Universitas Jambi yang akan dipilih secara acak dan sesuai proporsi di setiap fakultas.
b. Data yang digunakan dalam penelitian ini akan didasarkan hanya pada tanggapan dan jawaban mahasiswa Strata-1 angkatan 2020-2023 terhadap kuesioner yang diberikan.

1.5 Manfaat Penelitian

Dengan dilakukan penelitian ini, diharapkan hasil dari penelitian ini dapat menjadi bahan acuan dalam pengembangan kesadaran pentingnya menjaga privasi data pribadi dari bahaya *Phishing.*