Analisis Tingkat Kesadaran Keamanan Informasi Pribadi Mahasiswa Politeknik Negeri Batam Dalam Menghadapi Tindakan Doksing Pada Media Sosial Menggunakan Instrumen Human Aspects Of Information Security Questionnaire (HAIS-Q)

TUGAS AKHIR

Disusun Oleh:

Ikhsanul Fiqri

4332011005

Disusun untuk memenuhi salah satu syarat memperoleh gelar Sarjana Terapan Rekayasa Keamanan Siber

PROGRAM STUDI REKAYASA KEAMANAN SIBER

JURUSAN TEKNIK INFORMATIKA

POLITEKNIK NEGERI BATAM

BATAM

2026

HALAMAN PENGESAHAN TUGAS AKHIR

Analisis Tingkat Kesadaran Keamanan Informasi Pribadi Mahasiswa Politeknik Negeri Batam Dalam Menghadapi Tindakan Doksing Pada Media Sosial Menggunakan Instrumen Human Aspects Of Information Security Questionnaire (HAIS-Q)

Oleh:

Ikhsanul Fiqri

4332011005

Telah diuji dan dipertahankan di depan Tim Penguji

dalam Sidang Tugas Akhir

Pada tanggal 17 Juli 2026

Dan dinyatakan **LULUS**

Batam, 24 Juli 2026

Disetujui oleh,

Pembimbing ,

TTE oleh:

Antoni Haikal, S.S.T., M.T
24th July 2026

Perihal oleh:

Persetujuan untuk halaman pengesahan , tertanggal 24 July 2026

Untuk:

Ikhsanul Fiqri
4332011005

Pindai QRCode untuk Verifikasi.

Pastikan URL di if.polibatam.ac.id/tugas-akhir

Antoni Haikal, S.S.T., M.T

NIK : 122276

DAFTAR ISI

DAFTAR TABEL & GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi telah mendorong banyak transformasi digital di berbagai aspek dalam kehidupan, termasuk pendidikan, ekonomi, pemerintahan, dan interaksi sosial. Pemanfaatan internet serta media digital yang cenderung masif memberikan berbagai kemudahan dalam memperoleh dan membagikan informasi. Namun, di balik kemudahan tersebut muncul berbagai ancaman keamanan siber yang dapat mengganggu keamanan informasi pribadi pengguna. Keamanan informasi merupakan upaya untuk melindungi informasi agar tetap terjaga kerahasiaannya (confidentiality), integritasnya (integrity), dan ketersediaannya (availability) dari penggunaan, pengungkapan, gangguan, modifikasi,atau perusakan yang tidak sah. Masyarakat yang semakin terhubung secara digital, diperlukan pemahaman yang baik mengenai pentingnya perlindungan informasi, baik di tingkat individu maupun organisasi [1].

Dalam menjalankan dunia digital, tentu tidak selalu berjalan dengan baik seperti yang kita perkirakan. Tentu saja ada banyak hal yang menjadi suatu penghalang, salah satunya ialah tindakan doksing. Doksing merupakan kejahatan yang dilakukan dengan cara menargetkan dan menggabungkan informasi pribadi yang bukan miliknya yang dilakukan tanpa persetujuan dan kemudian selanjutnya disebarluaskan. Tindakan doksing dengan niat jahat yang berbahaya sering kali dilakukan dengan maksud untuk mengancam, mengintimidasi serta dapat membahayakan fisik maupun psikis. Meskipun hanya pengumpulan dan penyebaran data pribadi itu sudah merupakan pelanggaran terhadap privasi seseorang dan dapat di kategorikan sebagai kejahatan siber [1]. Tindakan doksing umumnya memanfaatkan informasi pribadi yang tersedia secara terbuka di internet maupun media sosial. Informasi tersebut dapat diperoleh dari berbagai sumber, seperti unggahan media sosial, profil publik, komentar, lokasi, nomor telepon, alamat surat elektronik, maupun informasi lain yang dibagikan oleh pengguna secara sadar ataupun tidak sadar. Semakin banyak informasi pribadi yang tersedia di ruang digital, semakin mudah pelaku melakukan pengumpulan, analisis, dan penyebaran data pribadi korban. Data dari Southeast Asia Freedom of Expression Network (SAFEnet) dalam laporan situasi hak digital indonesia 2026 menunjukkan bahwa kasus serangan digital berupa doksing menempati posisi kedua (28 kasus) [2]. Selain itu data dari komdigi pada tahun 2026 juga menunjukan ada-nya 325 situs kategori pelanggaran keamanan informasi dimana salah satunya ada memuat situs terkait doksing [11]. Kasus doksing yang terjadi di indonesia juga di dominasi di lingkungan mahasiswa, sebut saja ketika terjadi aksi demonstrasi pada tahun 2025 lalu, 5 kasus dilaporkan dengan kategori doksing, karena

adanya usaha untuk pembungkaman kritik terhadap pemerintah. Dan adapun jenis kasus doksing yang kita temui di dunia digital seperti, penagihan pinjaman online ilegal, pengungkapan identitas terhadap pelaku kejahatan dan lain sebagainya.

Mahasiswa merupakan kelompok yang aktif memanfaatkan media sosial untuk kegiatan akademik maupun interaksi sosial. Tingginya intensitas penggunaan media sosial menyebabkan mahasiswa lebih sering membagikan informasi pribadi, seperti identitas, lokasi, aktivitas sehari-hari, hingga jaringan pertemanan. Apabila informasi tersebut tidak dikelola dengan baik, maka dapat dimanfaatkan oleh pelaku doksing untuk mengidentifikasi maupun menyebarluaskan data pribadi korban. Salah satu langkah yang dapat dilakukan adalah dengan mengukur tingkat kesadaran mahasiswa terhadap perlindungan data pribadi dan risiko terkait dengan doksing. Pengukuran ini penting agar mahasiswa menyadari potensi kejahatan doksing agar mahasiswa tidak menjadi korban maupun pelaku di dunia digital. Oleh karena itu, penting untuk mengukur kesadaran mahasiswa mengenai keamanan informasi pribadi agar dapat merancang strategi yang tepat untuk meningkatkan pemahaman mahasiswa.

Keberhasilan pelaku doksing dalam memperoleh informasi pribadi tidak selalu disebabkan oleh kelemahan teknologi, tetapi juga dipengaruhi oleh perilaku pengguna dalam mengelola informasi pribadi. Penggunaan kata sandi yang lemah, pengaturan privasi media sosial yang tidak tepat, kebiasaan membagikan lokasi secara real-time, maupun kurangnya kehati-hatian saat menggunakan internet dapat meningkatkan peluang terjadinya doksing. Oleh karena itu, tingkat kesadaran keamanan informasi menjadi faktor penting yang perlu diukur sebagai upaya mengetahui kesiapan individu dalam melindungi data pribadinya. Salah satu metode yang dapat digunakan untuk mengukur tingkat kesadaran keamanan informasi ini adalah Human Aspects ofInformation Security Questionnaire (HAIS-Q). Metode ini bertujuan untuk mengukur pengetahuan, sikap, dan perilaku individu terkait keamanan informasi pribadi. Hasil pengukuran ini akan memberikan sebuah gambaran mengenai sejauh mana mahasiswa memahami ancaman serta menerapkan langkah-langkah yang tepat dalam menjaga data pribadi. Dengan menggunakan HAIS-Q, hasil yang diperoleh akan memberikan wawasan penting untuk merancang intervensi yang efektif guna meningkatkan kesadaran keamanan informasi pribadi. Metode ini bertujuan untuk mengukur pengetahuan, sikap, dan perilaku individu terkait keamanan informasi. Hasil pengukuran ini akan memberikan gambaran mengenai sejauh mana mahasiswa memahami ancaman serta menerapkan langkah-langkah yang tepat dalam menjaga data pribadi. Dengan menggunakan HAIS-Q, hasil yang diperoleh akan memberikan wawasan penting untuk merancang intervensi yang efektif guna meningkatkan kesadaran keamanan informasi [1].

Sebagai perguruan tinggi berbasis vokasi yang memiliki program studi di bidang teknologi informasi, mahasiswa Politeknik Negeri Batam memiliki tingkat interaksi yang tinggi dengan teknologi digital. Kondisi tersebut menjadikan mahasiswa sebagai kelompok yang relevan untuk diteliti dalam mengukur tingkat kesadaran keamanan informasi pribadi terhadap ancaman doksing. Penelitian sebelumnya lebih banyak mengkaji tingkat kesadaran keamanan informasi secara umum menggunakan instrumen HAIS-Q pada lingkungan organisasi, pegawai, maupun mahasiswa. Namun, penelitian yang secara khusus mengadaptasi HAIS-Q untuk mengukur kesadaran keamanan informasi pribadi dalam menghadapi tindakan doksing pada mahasiswa di Indonesia, khususnya di Politeknik Negeri Batam, masih sangat terbatas.

Oleh sebab itu penelitian ini bertujuan menganalisa tingkat kesadaran keamanan informasi pribadi mahasiswa Politeknik Negeri Batam dalam menghadapi tindakan doksing di dunia digital menggunakan instrumen yang dimuat dalam Human Aspects of Information Security Questionnaire (HAIS-Q). Menurut pengembangan dan validasi instrumen HAIS-Q didasarkan pada model *Knowledge, Attitude, dan Behavior* (KAB), yang menunjukkan bahwa peningkatan pengetahuan tentang kebijakan keamanan informasi dapat mempengaruhi sikap dan perilaku risiko-averse dalam penggunaan teknologi. Hasil penelitian diharapkan menjadi dasar dalam penyusunan strategi peningkatan literasi keamanan informasi dan perlindungan data pribadi di lingkungan perguruan tingg

1.2 Rumusan Masalah

A. Bagaimana tingkat kesadaran keamanan informasi pribadi mahasiswa Politeknik Negeri Batam dalam menghadapi tindakan doksing di dunia digital berdasarkan aspek pengetahuan (knowledge), sikap (attitude), dan perilaku (behavior) menggunakan metode domain Human Aspects of Information Security Questionnaire (HAIS-Q)?
B. Bagaimana tingkat kesadaran keamanan informasi pribadi mahasiswa politeknik negeri batam pada setiap domain HAIS-Q yang digunakan, yaitu pengelolaan kata sandi yaitu pengelolaan kata sandi (password management), penggunaan internet (internet use), pengelolaan informasi (information handling), dan penggunaan media sosial (social media use) dalam menghadapi tindakan doksing di dunia digital?

1.3 Batasan Masalah

Agar membatasi ruang lingkup masalah yang terlalu luas agar penelitian dapat fokus untuk dilakukan, penulis menetapkan batasan masalah sebagai berikut:

A. Penelitian ini hanya melakukan analisa terhadap tingkat kesadaran, pengetahuan, serta tindakan mahasiswa terhadap keamanan informasi pribadi agar tidak terkena doksing di media sosial. Perihal kesuksesan implementasi berada diluar ranah penelitian.

B. Cakupan penelitian hanya di kampus Politeknik Negeri Batam, tidak mencakup semua kampus yang berada di Kota Batam.

C. Penelitian ini menggunakan *Human Aspects of Information Security Questionnaire* (HAIS-Q) mencakup tiga dimensi utama yaitu pengetahuan, sikap, dan perilaku, serta mencakup empat fokus area keamanan informasi. Data diperoleh melalui penyebaran kuisioner secara daring kepada mahasiswa/i aktif. Analisis dilakukan dengan menghitung persentase rata - rata pada masing masing dimensi dan domain.

1.4 Tujuan Penelitian

A. Bertujuan untuk mengukur tingkat kesadaran mahasiswa politeknik negeri batam terhadap keamanan informasi pribadi agar tidak terkena doksing dari pihak yang tidak bertanggung jawab.

B. Memberikan data ke pihak kampus Politeknik Negeri Batam agar bisa mengevaluasi jika tingkat kesadaran dari mahasiswa dikategorikan rendah.

1.5 Manfaat Penelitian

A. Mendukung mahasiswa Politeknik Negeri Batam agar meningkatkan kesadaran, pengetahuan, dan prilaku terhadap keamanan informasi pribadi supaya terhindar dari tindak kejahatan doksing.

BAB II
LANDASAN TEORI

2.1 Tinjauan Pustaka

Penelitian ini menggunakan beberapa referensi yang berkaitan dengan penelitian lainnya yang di jadikan referensi untuk mengidentifikasi penelitian ini agar dapat dibedakan dengan penelitian lainnya atau sebagai bentuk perbandingan. Beberapa penelitian terdahulu yang digunakan untuk referensi terkait doksing. Yang disajikan pada tabel *2.1* di bawah ini.

Tabel 2.1 Tinjauan Pustaka

No	Judul Penelitian	Penulis, Tahun	Metode Penelitian	Kesimpulan/Hasil Penelitian
1	Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan *HAIS - Q*: Mengungkapkan Kesenjangan Antara Sikap Dan Pengetahuan Mahasiswa	Shebila Fisabil Arum, Ariyan Zubaidi, Raphael Bianco Huwae. 2025	Kuantitaif, HAIS-Q	Temuan ini menunjukkan bahwa meskipun mahasiswa memiliki sikap positif, penerapannya dalam keseharian masih belum optimal.
2	Pelindungan Data Pribadi dalam Tindakan doksing Berdasarkan Undang-Undang Nomor 27 Tahun 2022	Jeane Neltje Saly, Lubna Tabriz Sulthanah, 2023	Yuridis-normatif	Berdasarkan pada pembahasan sebelumnya, dapat disimpulkan bahwa tindakan doksing merupakan salah satu cybercrime yang kegiatannya berupa mengumpulkan dan menyebarluaskan data seseorang dan/atau sekelompok orang yang

				sudah ditargetkan tanpa melalui izin dari yang memiliki data dengan tujuan tertentu seperti mengancam dan mengintimidasi
3	Kesadaran akan Ancaman Serangan Berbasis Backdoor di Kalangan Pengguna Smartphone Android	Muhammad Raffi Akhyari, Ahmad R. Pratama, 2026	Kuantitatif	Berdasarkan penelitian yang telah dilakukan ini, telah didapat hasil tingkatan kesadaran keamanan atau security awareness pengguna smartphone android di Indonesia yaitu berada pada tingkatan rata-rata. Hasil ini berdasarkan nilai kesadaran total yang ada pada Gambar 1 sebelumnya yaitu 80 dari nilai maksimal keseluruhan 100. Dengan begitu hasilnya berada pada tingkatan kategori rata-rata, maka masih dapat ditingkatkan kembali di beberapa bagian, terutama pada area fokus Backdoor, Hardware dan Android OS yang cukup

				tertinggal jika dibandingkan dengan area fokus Permission, Apps
4	Penerapan HAIS-Q dalam Pengukuran Tingkat Kesadaran Keamanan Informasi Pegawai Disdukcapil Kota Malang	Bima Yusuf Dharmahita, Mukhlis Prasetyo Aji2 , Ermadi Satriya Wijaya3 , Agung Purwo Wicaksono. 2025	Kuantitatif, HAISQ	Penelitian ini berhasil mengidentifikasi kondisi kesadaran keamanan informasi di lingkungan Disdukcapil Kota Malang berdasarkan analisis terhadap pegawai pada tiga posisi strategis, yakni Administrator Basis Data, Layanan Pelanggan, dan Operator. Hasil analisis menunjukkan bahwa secara umum tingkat kesadaran pegawai berada pada kategori baik, namun masih terdapat area fokus yang memerlukan perhatian lebih, khususnya pada manajemen kata sandi, penggunaan perangkat selular, dan surat elektronik (Ringkasan hasil utama). Temuan ini menegaskan bahwa aspek perilaku masih menjadi tantangan

				utama, meskipun aspek pengetahuan dan sikap tergolong cukup baik.
5	Pengukuran Tingkat Kesadaran Keamanan Informasi Mahasiswa pada Pembelajaran Online	Devi Nurjanaha , Senie Destyaa. 2022	Kuantitatif	Berdasarkan penelitian yang sudah dilakukan, secara umum level kesadaran keamanan informasi mahasiswa yang melakukan pembelajaran online sudah berada pada level “sedang” dengan total perhitungan nilai keseluruhan mencapai 66 %. Dengan demikian perlu dipertahankan yang baik dan perlu peningkatan pada mahasiswa yang berada pada level rendah. Perlu tindakan monitoring berkelanjutan setelah adanya feedback dari kuisioner untuk memastikan peningkatan yang terjadi setelah itu. Diperlukan juga adanya Kerjasama antara semua pihak

				yang terkait untuk peningkatan kesadaran keamanan informasi.
6	a Prototype For Assessing Information Security Awareness	H.A. Krugera, ,W.D. Kearney. (2006)		There are numerous reasons why organisations have to spend effort and resources on the evaluation or measurement of information security awareness successes. Posthumus and Von Solms (2004) motivated the need to integrate information security into corporate governance and proposed a framework to aid organisations in their integration efforts.
7	How To Choose a Sampling Technique And Determine Sample Size For Research: a Simplified Guide For Researchers	Sirwan Khalid Ahmed, (2024)		The precision of methodology in research depends on the selection of proper sampling techniques and calculation of an adequately powered sample size. Probability sampling, for example, stratified and cluster

				sampling, is thus fundamental in those studies that tend to make statistically significant inferences about the wider population.

2.2 Keamanan Siber

Keamanan siber adalah praktik melindungi komputer, jaringan, aplikasi perangkat lunak, sistem kritis dan data dari potensial ancaman digital. Organisasi memiliki tanggung jawab untuk mengamankan data guna menjaga kepercayaan pelanggan dan memenuhi kepatuhan terhadap peraturan. Organisasi menggunakan langkah-langkah dan alat keamanan siber untuk melindungi data sensitif dari akses yang tidak sah, serta mencegah gangguan dalam operasi bisnis karena aktivitas jaringan yang tidak diinginkan. Organisasi mengimplementasikan keamanan siber dengan menyederhanakan pertahanan digital di antara orang, proses, dan teknologi [4].

2.3 Kesadaran Keamanan Siber

Kesadaran keamanan informasi merupakan suatu proses yang bersifat dinamis terkait dengan tantangan dan risiko yang terus berubah, sehingga kesadaran terhadap keamanan informasi harus diukur dan dikelola sesuai dengan bentuk perubahan dan perkembangan risiko. Kesadaran keamanan informasi harus dilakukan secara terus menerus, dan berkesinambungan menjadi bagian dari budaya organisasi atau perusahaan. *Adapau schlienger* dan Teufel menyatakan bahwa tujuan yang diharapkan dari kesadaran keamanan informasi pengguna, Krueger dan Kearney membangun suatu model yang dapat digunakan sebagai media pengukuran untuk kesadaran keamanan. Pengukuran tersebut dilakukan pada tiga aspek yang meliputi, di antaranya: pengetahuan (*knowledge),* Sikap (*Attitude),* Perilaku *(Behaviour).* Berdasarkan tiga aspek tersebut, dibagi kembali menjadi lima area fokus. Setiap fokus yang ada, akan dibagi menjadi beberapa faktor dan kemudian dibagi kembali dengan subbagian. Model ini dikenal dengan nama KAB (*Knowledge-Attitude-Behaviour*) [5].

2.4 Doksing

Doksing berasal dari kata “Dox” yang merupakan singkatan dari kata “Dokumen”. Secara etimologi berasal dari ungkapan “dropping dox” atau “dropping documents”. Menurut terjemahan Oxford British and World English Dictionary, “doksing berarti mencari dan menyebarluaskan atau mengunggah informasi pribadi tentang orang tertentu di internet”, seringkali dengan maksud atau tujuan kejahatan. David M. Douglas melalui tulisannya mengenai Analisis Konseptual doksing (2016) menyampaikan pendapatnya terkait doksing bahwa doksing tidak semuanya diniati dengan niat yang jahat.

a) Deanonymizing.

Tindakan doksing yang mempublikasi-kan informasi berupa identitas pribadi milik seseorang dan/atau sekelompok orang yang identitasnya tidak diketahui (anonim) oleh publik atau dikenal dengan memiliki nama samaran.

b) Targeting.

Tindakan doksing ini mempublikasikan informasi mengenai keberadaan fisik seseorang, dalam artian tindakan ini dapat melacak sampai ditemukan lokasi tempat keberadaaan-nya dalam waktu yang nyata.

c) Delegitimizing.

Tindakan ini mempublikasikan informasi pribadi seseorang dan/atau sekelompok orang dengan tujuan untuk merusak atau menjatuhkan kredibilitas, reputasi ataupun karakter.

Julia M.MacAllister melalui tulisan dalam jurnalnya (2017) mengklasifikasikan beberapa tujuan dilakukannya yaitu

a) Doksing untuk tujuan jahat.

Jenis doksing ini adalah dimana individu melakukan doksing pada orang lain hanya untuk menimbulkan kerugian, kesusahan atau rasa malu yang dapat dimotivasi oleh balas dendam, kemarahan, atau sebatas hanya keinginan untuk melecehkan seseorang. Melalui internet, memungkinkan doksing yang dilakukan akan menimbulkan kerugian yang besar dibandingkan dengan pelecehan secara langsung.

b) Doksing untuk tujuan politik.

Doksing dengan tujuan politik untuk meningkatkan transparansi, mengungkap apa yang mereka anggap tidak adil atau menungkap informasi yang layak diberitakan untuk kepentingan publik

c) Doksing untuk tujuan pengaturan mandiri.

Pengungkap yang memanfaatkan kategori doxing ini untuk mengungkap identitas orang lain yang kehilangan dukungan rekan-rekannya karena berbagai alasan.

Jika dikaitkan dengan UU PDP, ketentuan mengenai doxing dalam UU PDP tidak memperlihatkan perbedaan bentuk dan tujuan doxing. Dalam UU PDP seolah-olah menggeneralisasi bahwa bisa mengkriminalisasi doxing dengan hukuman yang sama [2].

2.5 Keamanan Informasi

Keamanan informasi didefinisikan sebagai sebuah perlindungan dan sumber daya terhadap upaya perubahan dan perusakan oleh seseorang yang tidak diizinkan. Keamanan informasi diperoleh dengan mengimplementasi seperangkat alat kontrol yang layak, yang dapat berupa kebijakan-kebijakan, praktek-praktek, prosedur prosedur, struktur-struktur organisasi dan perangkat lunak. Keamanan informasi meliputi beberapa aspek diantaranya adalah:

a) Confidentiality (kerahasiaan)

Aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.

b) Integrity (integritas)

Aspek yang menjamin bahwa data tidak dirubah tanpa ada izin pihak yang berwenang (authorized), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk manajemen aspek integrity ini.

c) Availability (ketersediaan)

Aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan) [6].

2.6 Human Aspects of Information Security Questionnaire (HAIS-Q)

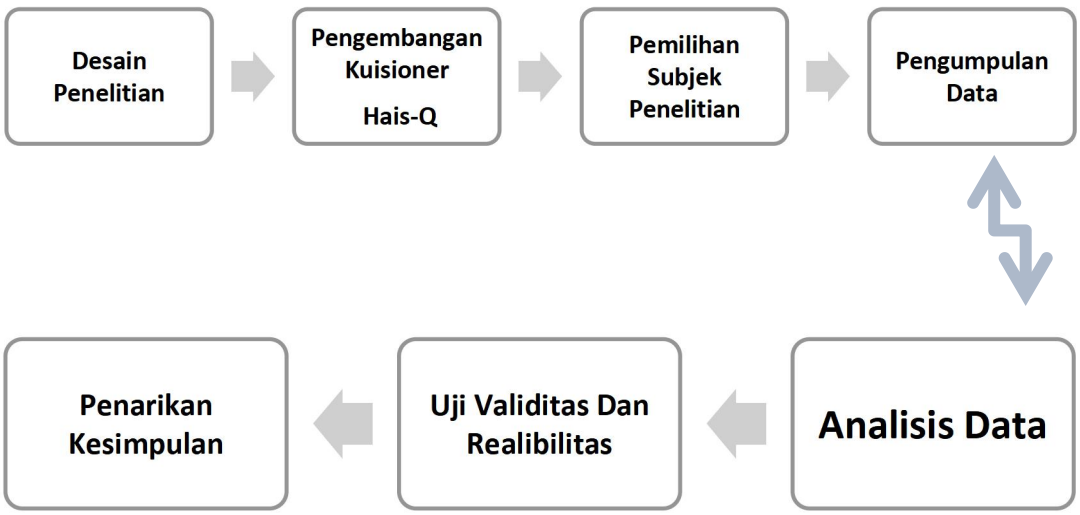
Salah satu instrumen yang telah banyak digunakan untuk mengukur kesadaran keamanan informasi adalah Human Aspects of Information Security Questionnaire (HAIS-Q). Instrumen ini dikembangkan oleh Kathryn Parsons dan timnya yang dijelaskan dalam jurnal "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies", instrumen ini terdiri dari 7 area fokus dan 21 sub-area serta dirancang berdasarkan dimensi KAB yang mencakup tiga aspek utama, yaitu Knowledge (pengetahuan), Attitude (sikap), dan Behavior (perilaku) [7].

BAB III
METODELOGI PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif deskriptif dengan *HAIS-Q* sebagai instrumen utama untuk mengukur kesadaran keamanan informasi pada mahasiswa Politeknik Negeri Batam. HAIS-Q merupakan metode dengan fokus pada tiga aspek utama yaitu pengetahuan *(Knowledge*), sikap (*Attitude*), dan perilaku (*Behavior*) mahasiswa terkait dengan keamanan informasi. Instrumen ini menggunakan skala Likert 1 – 5 untuk mengukur jawaban responden pada setiap item pertanyaan.

Penelitian ini dilakukan di lingkungan Politeknik Negeri Batam dengan subjek penelitian yaitu mahasiswa dari berbagai fakultas. Data diperoleh melalui penyebaran kuesioner kepada responden secara daring. Jumlah total pertanyaan dalam kuesioner adalah 9 item yang mencakup 4 domain dimana setiap domain memuat 3 pertanyaan terkait dengan *Knowledge, Attitude, Behaviour* terkait keamanan informasi. Data yang terkumpul selanjutnya dianalisis untuk menggambarkan tingkat kesadaran keamanan informasi mahasiswa. Langkah-langkah yang di lakukan pada penelitian ini dapat dilihat pada tabel 3.1 di bawah ini.

Tabel 3.1 Kerangka Penelitian



3.1 Desain Penelitian

Desain penelitian ditentukan guna untuk merencanakan metode dan strategi yang akan digunakan, seperti penyusunan kuesioner secara tertutup yang mencakup aspek-aspek penting dari kesadaran keamanan informasi pribadi, pemilihan responden, penyebaran kuesioner secara online kepada responden serta pengolahan data untuk menggambarkan hasil yang diperoleh dengan tujuan untuk memperoleh data yang valid dan dapat dipertanggung jawabkan kebenaran-nya [1].

3.2 Pengembangan Kuisioner HAIS-Q

Pada tahap pengembangan kuesioner HAIS-Q, instrumen disusun berdasarkan pendekatan KAB yang bertujuan untuk mengukur tingkat pengetahuan, sikap, dan perilaku individu terkait keamanan informasi serta mengacu pada 4 domain yang telah ditetapkan pada HAIS-Q [1].

Password Management melindungi akun supaya tidak diambil alih oleh pihak pihak luar yang tidak bertanggung jawab sehingga memungkinkan untuk mendapatkan informasi pribadi.

Internet Use mengukur kewaspadaan saat menelusuri internet seperti, mengakses tautan dan menginput data pribadi.

Information Handling domain yang berkaitan erat dengan doksing dimana hadir untuk mengukur bagaimana responden mengelola, menyimpan serta membagikan informasi pribadi didunia digital.

Social Media use mengukur perilaku responden dalam menggungah informasi, mengatur privasi akun serta membatasi akses terhadap data pribadi. Domain ini juga relevan dengan doksing.

Tabel 3.2 Tabel Pertanyaan Kuesioner

Domain	KAB	Kuesioner
Password Management	*Knowledge*	● P1 Saya mengetahui bahwa penggunaan kata sandi yang kuat dapat melindungi akun dari akses pihak yang tidak bertanggung jawab. ● P2 Saya mengetahui

		bahwa penggunaan kata sandi yang sama pada beberapa akun media sosial dapat meningkatkan risiko kebocoran data pribadi. ● P3 Saya mengetahui bahwa autentikasi dua faktor (2FA) dapat membantu mencegah penyalahgunaan akun media sosial.
	Attitude	● P4 Saya menganggap pentingnya menggunakan kata sandi yang berbeda di setiap akun media sosial. ● P5 Saya merasa perlu menjaga kerahasiaan kata sandi dari orang lain. ● P6 Saya percaya bahwa keamanan akun pribadi media sosial berperan penting dalam mencegah tindakan doksing.
	Behaviour	● P7 Saya menggunakan password media sosial

		saya dengan kombinasi antara huruf, angka dan karakter. ● P8 Saya tidak membagikan kata sandi akun media sosial saya kepada orang lain. ● P9 Saya mengaktifkan autentikasi dua faktor disetiap media sosial yang mendukung fitur tersebut.
Internet Use	*Knowledge*	● I1 Saya mengetahui bahwa tautan mencurigakan dapat digunakan untuk mencuri data pribadi. ● I2 Saya mengetahui bahwa situs web palsu dapat menyerupai situs resmi untuk menipu pengguna media sosial. ● I3 Saya mengetahui bahwa penggunaan Wi-Fi publik memiliki risiko terhadap kebobolan keamanan data pribadi.

	Attitude	● I4 Saya merasa perlu berhati-hati saat membuka tautan dari sumber yang tidak dikenal. ● I5 Saya menganggap penting untuk memeriksa keamanan situs web sebelum menginput data pribadi. ● I6 Saya percaya bahwa kewaspadaan saat menggunakan internet dapat mengurangi risiko pencurian informasi pribadi.
	Behaviour	● I7 Saya selalu memeriksa alamat situs web sebelum memasukkan informasi pribadi ● I8 Saya menghindari mengunduh file dari sumber yang tidak terpercaya. ● I9 Saya berhati-hati saat menggunakan Wi-Fi publik untuk mengakses akun pribadi.
Information Handling	*Knowledge*	● H1 Saya mengetahui

		bahwa alamat rumah termasuk informasi pribadi yang harus dilindungi. ● H2 Saya mengetahui bahwa nomor telepon dapat disalahgunakan oleh pihak yang tidak bertanggung jawab ● H3 Saya mengetahui bahwa informasi pribadi yang tersebar di internet dapat dimanfaatkan untuk tindakan doksing.
	Attitude	● H4 Saya menganggap penting untuk menjaga kerahasiaan informasi pribadi di dunia digital. ● H5 Saya merasa perlu membatasi penyebaran informasi pribadi di internet. ● H6 Saya percaya bahwa perlindungan informasi pribadi merupakan tanggung jawab setiap pengguna internet.
	Behaviour	● H7 Saya membatasi informasi pribadi yang

		saya bagikan secara online. ● H8 Saya mempertimbangkan risiko sebelum membagikan informasi pribadi di internet. ● H9 Saya menghapus informasi pribadi yang tidak perlu ditampilkan kepada publik.
Social Media Use	*Knowledge*	● S1 Saya mengetahui bahwa unggahan di media sosial dapat digunakan untuk mengidentifikasi seseorang ● S2 Saya mengetahui bahwa pengaturan privasi media sosial dapat membatasi akses orang lain terhadap informasi pribadi. ● S3 Saya mengetahui bahwa pelaku doksing dapat mengumpulkan informasi korban dari berbagai platform digital.
	Attitude	● S4 Saya menganggap penting

		untuk mengatur privasi akun media sosial. ● S5 Saya merasa perlu membatasi informasi pribadi yang dapat dilihat oleh publik. ● S6 Saya percaya bahwa penggunaan media sosial secara bijak dapat mengurangi risiko tindakan doksing.
	Behaviour	● S7 Saya secara rutin memeriksa pengaturan privasi akun media sosial saya. ● S8 Saya membatasi siapa saja yang dapat melihat unggahan saya di media sosial. ● S9 Saya menghindari membagikan lokasi atau aktivitas secara real-time di media sosial.

3.3 Pemilihan Subjek Penelitian

Pemilihan subjek pada penelitian ini dilakukan dengan memilih mahasiswa aktif dalam berbagai fakultas dan program studi di kampus Politeknik Negeri Batam. Pemilihan subjek juga dilakukan dengan mempertimbangkan keragaman

seperti jenjang semester, rentang usia, dan jenis kelamin. Adapun dalam pengambilan sampel dari mahasiswa tersebut untuk menentukan jumlah sampel dari populasi yang diketahui, digunakan rumus *Yamane* dengan *margin of error tertentu*, sebagaimana ditunjukkan pada Persamaan (x) di bawah ini [8].

$$n = \frac{N}{1 + Ne^2} \qquad \text{(x)}$$

Dalam rumus tersebut, *n* diartikan sebagai jumlah sampel yang harus digunakan dalam penelitian, sedangkan N menunjukkan jumlah populasi secara keseluruhan dan *e* merupakan *margin of error* atau tingkat kesalahan yang di-toleransi dalam pengambilan sampel, yang dalam penelitian ini ditetapkan sebesar 5% (0,05). Penggunaan *margin of error* ini bertujuan agar hasil penelitian tetap memiliki tingkat ketelitian yang dapat dipertanggung jawab-kan meski pun tidak menggunakan seluruh populasi. Dalam penelitian ini, total populasi (N) pada mahasiswa aktif di Politeknik Negeri Batam sekitar 11.745, dengan tingkat kesalahan (*e*) yang ditetapkan sebesar 5% (0.05). Adapun untuk perhitungannya sebagai berikut [7] :

$$n = \frac{11.745}{1 + 11.745\ (0.05)^2} = 386.8$$

Dengan demikian, jumlah sampel pada penelitian ini untuk mengukur tingkat kesadaran keamanan informasi pada mahasiswa di Politeknik Negeri Batam minimal sebanyak 387 sampel mahasiswa.

3.4 Pengumpulan Data dan Waktu Pengumpulan Data

Teknik pengumpulan data dilakukan dengan menyebarkan kuesioner yang berbasis beberapa domain dari *HAIS-Q* secara online kepada mahasiswa Politeknik Negeri Batam yang menjadi responden menggunakan google form. Kuesioner terdiri dari beberapa pernyataan yang terdiri dari 4 domain yaitu pengelolaan password, penggunaan internet, pengelolaan informasi, penggunaan media sosial. Setiap domain memiliki 3 pertanyaan yang mencakup 3 aspek yaitu aspek pengetahuan, sikap dan perilaku. Responden akan diminta untuk menjawab menggunakan skala likert 5 poin yang mengukur ketiga aspek tersebut

dalam konteks keamanan informasi, dengan rentang jawaban 1 untuk sangat tidak setuju hingga 5 untuk sangat setuju.

Tabel 3.3 Tahapan waktu penelitian

Keterangan	Waktu
Penyebaran kuesioner secara tertutup guna untuk menguji instrumen penelitian (*Uji Validitas & Uji Realibilitas*).	*26 Juni 2026 s/d 29 Juni 2026*
Penyebaran kuesioner penelitian secara terbuka guna untuk melakukan analisis data penelitian .	*1 Juli 2026 s/d 7 Juli 2026*
Tahap Analisis data	*8 Juli 2026 s/d 10 Juli 2026*

3.6 Uji Validitas dan Reliabilitas

Penelitian ini menggunakan metode deskriptif kuantitatif, dimana sumber pengumpulan data terbesar nya ialah dari pengumpulan kuesioner pernyataan. Untuk itu uji validitas dan reliabilitas dilakukan sebelum penyebaran kuesioner utama dengan tujuan untuk memastikan kuesioner yang digunakan memiliki keakuratan dan konsistensi yang tinggi selain itu juga memastikan apakah instrumen pada penelitian ini dapat berfungsi dengan baik dan pertanyaan yang diajukan dapat dipahami.Uji validitas dilakukan menggunakan korelasi *Pearson Product Moment*, dimana item dinyatakan valid jika nilai r hitung > r tabel. Sedangkan untuk uji reliabilitas diukur dengan *Cronbach's Alpha*, dimana instrumen dianggap reliabel apabila nilai alpha > 0.7 [1].

Sebelum mengumpulkan data utama, peneliti melakukan pengujian secara tertutup terhadap validitas dan reliabilitas terhadap instrumen penelitian dengan cara melakukan uji coba (*pilot testing*) yang melibatkan sekitar 69 mahasiswa dari Politeknik Negeri Batam. Dalam pengujian ini dilakukan terhadap 36 item pertanyaan dalam kuesioner dengan membandingkan nilai *r hitung* setiap item dengan nilai *r tabel* nya. Instrumen dapat dianggap valid jika nilai dari *r hitung* > *r tabel*, yang dimana pada penelitian ini nilai *r tabel* dengan derajat kebebasan (df) sebesar 69 adalah 0,237. Nilai tersebut didapatkan dari tabel *Critical Values for Pearson's Correlation Coefficien*t [9]. Untuk menentukan jumlah derajat kebebasan menggunakan Persamaan (y) berikut.

$$df = n - 2$$
$$df = 69 - 2 \qquad \text{(y)}$$
$$df = 67$$

Derajat kebebasan (df) dihitung berdasarkan jumlah responden (n) yang digunakan dalam suatu penelitian , dimana nilainya ditentukan dengan mengurangi jumlah responden tersebut sebanyak dua. Derajat kebebasan berfungsi untuk menentukan batas dalam pengujian statistik, khususnya saat melakukan uji validitas, sehingga hasil perhitungan dapat dibandingkan dengan nilai pada tabel distribusi *r*. Berdasarkan hasil uji validitas, terlihat bahwa semua item pada kuesioner memiliki *nilai r hitung* yang melebihi *r tabel*. Oleh karena itu, seluruh item dalam kuesioner ini dinyatakan valid dan layak digunakan untuk pengumpulan data. Hal ini diharapkan dapat memberikan hasil pengujian yang lebih akurat karena seluruh instrumen dapat digunakan untuk menilai kesadaran mahasiswa terhadap kemanan informasi pribadi di Politeknik Negeri batam. Berikut merupakan hasil dari data yang telah diuji, sebagaimana yang telah disajikan pada tabel 3.4

Tabel 3.4 Hasil Uji Validitas

Item	r ~ Hitung (Total)	r ~ Tabel	Ket	Item	r ~ Hitung (Total)	r ~ Tabel	Ket
P1	0,677	0,237	Valid	H1	0,734	0,237	Valid
P2	0,727	0,237	Valid	H2	0,740	0,237	Valid
P3	0,689	0,237	Valid	H3	0,803	0,237	Valid
P4	0,618	0,237	Valid	H4	0,724	0,237	Valid
P5	0,710	0,237	Valid	H5	0,768	0,237	Valid
P6	0,774	0,237	Valid	H6	0,684	0,237	Valid
P7	0,711	0,237	Valid	H7	0,644	0,237	Valid
P8	0,699	0,237	Valid	H8	0,781	0,237	Valid
P9	0,802	0,237	Valid	H9	0,809	0,237	Valid
I1	0,591	0,237	Valid	S1	0,799	0,237	Valid
I2	0,741	0,237	Valid	S2	0,625	0,237	Valid

I3	0,773	0,237	Valid	S3	0,566	0,237	Valid
I4	0,797	0,237	Valid	S4	0,766	0,237	Valid
I5	0,650	0,237	Valid	S5	0,771	0,237	Valid
I6	0,668	0,237	Valid	S6	0,708	0,237	Valid
I7	0,759	0,237	Valid	S7	0,673	0,237	Valid
I8	0,760	0,237	Valid	S8	0,769	0,237	Valid
I9	0,780	0,237	Valid	S9	0,794	0,237	Valid

Tabel 3.4 menunjukan bahwa seluruh item dalam kuesioner terbukti valid karena nilai *r-hitung* lebih besar dari *r-tabel*. Dalam hal ini menunjukkan setiap item pada kuesioner memiliki hubungan yang kuat dengan hasil jawaban responden secara keseluruhan sehingga mampu mengukur aspek yang ingin diteliti. Validitas yang baik ialah yang memastikan bahwa tiap pertanyaan dalam kuesioner benar-benar mewakili kesadaran terhadap keamanan informasi. Setelah kuesioner dinyatakan valid, langkah selanjutnya melakukan uji reliabilitas untuk mengukur konsistensi instrumen secara keseluruhan ketika dilakukan pengukuran berulang. Uji ini dilakukan menggunakan metode *Cronbach's Alpha* yang dimana instrumen dinyatakan reliabel jika nilai alpha diatas 0.70. Dalam penelitian ini, nilai Cronbach's Alpha yang diperoleh sebesar 0.976 yang memperlihatkan bahwa seluruh item pada kuesioner tersebut reliabel atau memiliki tingkat ke-andalan yang baik, dengan konsistensi tinggi dan hasil yang stabil.

Tabel 3.5 Hasil tabel Cronbach's Alpha

Reliability Statistics

Cronbach's Alpha	N of Items
0,976	36

3.8 Analisis Data

Setelah data terkumpul, dilakukan analisis data dengan menghitung skor rata-rata pada setiap aspek untuk melihat tingkat kesadaran keamanan informasi pada mahasiswa. Setiap aspek akan diberi bobot yang berbeda sesuai dengan pentingnya kontribusi terhadap kesadaran keamanan informasi, yaitu 30% untuk

Knowledge, 20% untuk *Attitude* dan 50% untuk *Behaviour*. Menurut Kruger dan Kearney, aspek behaviour (perilaku) memiliki pengaruh yang besar karena mencerminkan langsung tindakan nyata pengguna sehingga diberi bobot tertinggi [1].

Tabel 3.6 Pembagian Bobot Dimensi

Dimensi	Bobot
Knowledge	30 %
Attitude	20 %
Behaviour	50 %

Tabel 3.7 Tingkat Kesadaran Keamanan Informasi

Kesadaran	Persentase
Baik	**80 - 100%**
Menengah	**60 - 79 %**
Buruk	**59 % - < Dibawah nya**

Pembagian bobot dimensi serta tingkat kesadaran keamanan informasi mengacu pada prototype penelitian tingkat kesadaran keamanan informasi *H.A.Kruger,W.D.Kearney* [9].

3.9 Penarikan Kesimpulan

Pada tahap terakhir, hasil dari analisis data digunakan untuk mengklasifikasi tingkat kesadaran keamanan informasi mahasiswa berdasarkan indikator pengetahuan, sikap, dan perilaku terhadap keamanan informasi pribadi. Kesimpulan dari analisis ini menjadi dasar untuk memberikan rekomendasi yang tepat dalam meningkatkan pemahaman dan penerapan perilaku yang aman dalam penggunaan teknologi informasi.

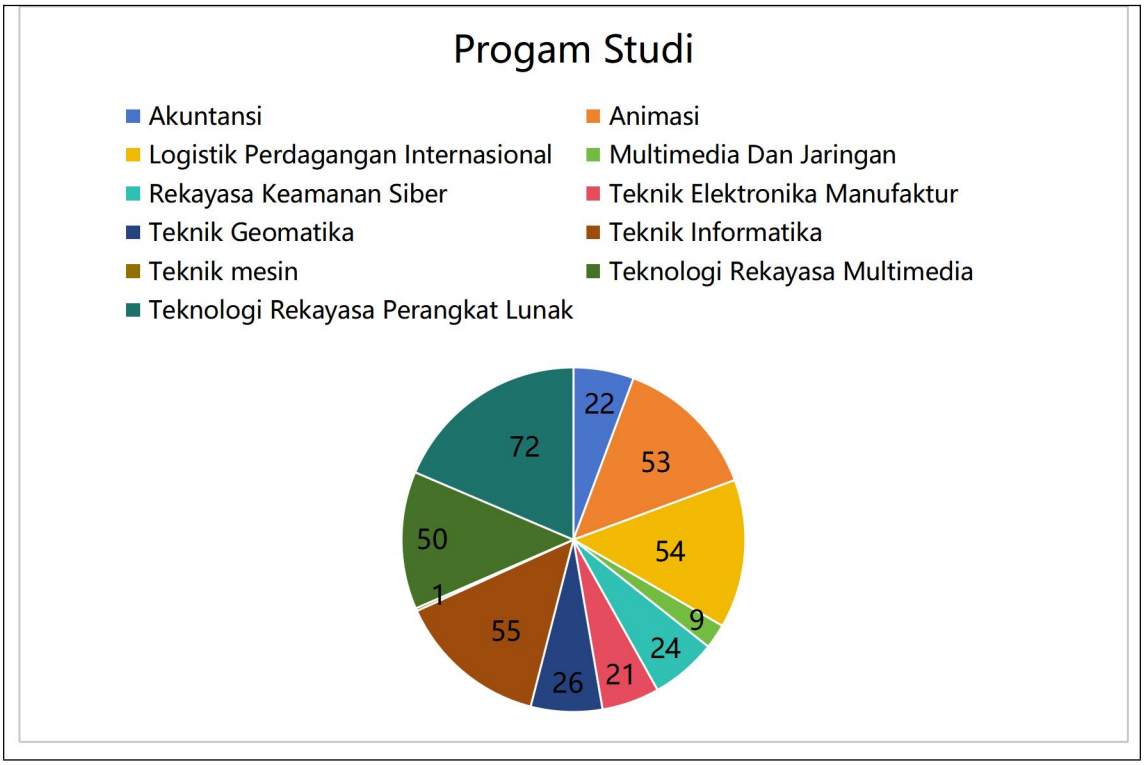
BAB IV
HASIL DAN PEMBAHASAN

Berdasarkan hasil penyebaran kuesioner secara daring dan luring kepada mahasiswa di Politeknik Negeri Batam, Jumlah responden yang berhasil mengisi kuesioner tersebut sebanyak 398 orang. Jumlah tersebut telah melebihi batas maksimum sampel yang dibutuhkan dan dite, yaitu sekitar 387 responden [3.3]. Adapun data karakteristik responden dalam penelitian ini ditunjukan pada tabel 4.1 berikut

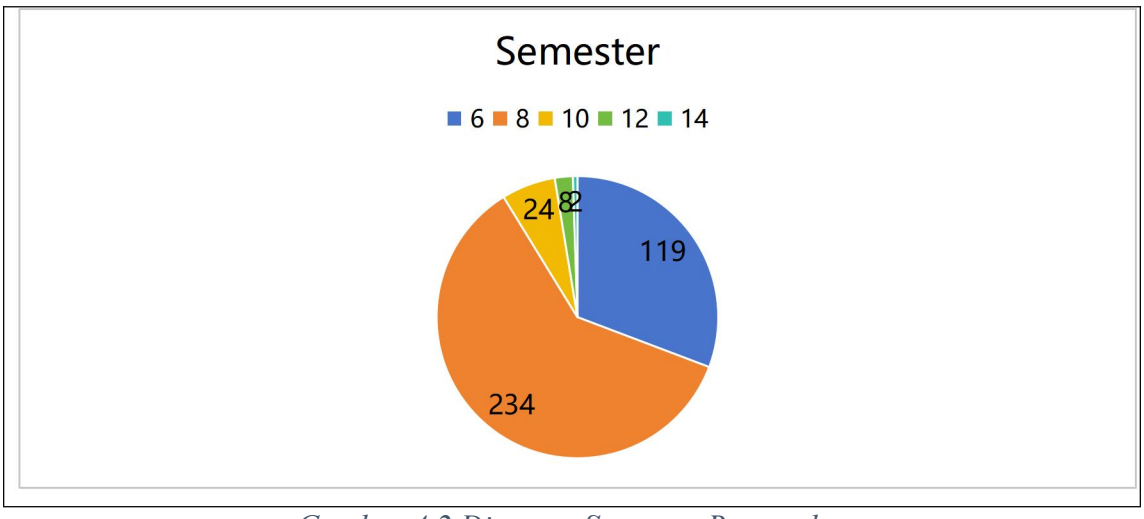
Tabel 4.1 Karakteristik Responden

Kriteria	Kategori	Frekuensi	Persen
Program Studi	Akuntansi	22	5,68%
	Animasi	53	13,70%
	Logistik Perdagangan Internasional	54	13,95%
	Multimedia Dan Jaringan	9	2,33%
	Rekayasa Keamanan Siber	24	6,20%
	Teknik Elektronika Manufaktur	21	5,43%
	Teknik Geomatika	26	6,72%
	Teknik Informatika	55	14,21%
	Teknik mesin	1	0,26%
	Teknologi Rekayasa Multimedia	50	12,92%
	Teknologi Rekayasa Perangkat Lunak	72	18,60%
Jenis Kelamin	Laki - Laki	225	58%
	Perempuan	162	42%
Usia	20	20	5,17%
	21	46	11,89%
	22	115	29,72%
	23	85	21,96%
	24	80	20,67%
	25	41	10,59%

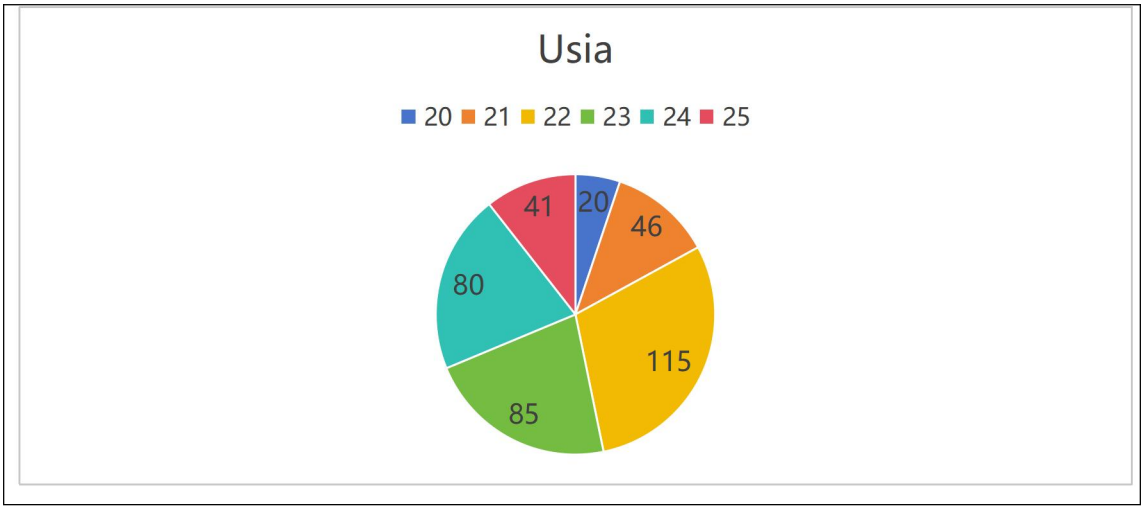
Semester	6	119	30,75%
	8	234	60,47%
	10	24	6,20%
	12	8	2,07%
	14	2	0,52%
Apakah aktif menggunakan media sosial?	Ya	373	96,38%
	Tidak	14	3,62%



Gambar 4.1 Diagram Program Studi Responden



Gambar 4.2 Diagram Semester Responden



Gambar 4.3 Diagram Usia Responden

Gambar 4.4 Diagram aktif media sosial respondem

Tabel 4.1 diatas menggambarkan karakteristik dari responden berdasarkan data mengenai program studi, jenis kelamin, usia, semester dan aktif dalam menggunakan media sosial. Dari tabel berikut, dapat kita ketahui bahwa jumlah responden terbanyak dari program studi rekayasa perangkat lunak dan mayoritas pengisi kuesioner ialah laki-laki, sebagian besar responden berusia 20 - 25 tahun dan rerata responden berasal dari semester 8, yang menunjukan bahwa kuesioner tersebut lebih banyak diisi oleh mahasiswa yang sedang sidang TA *(Tugas Akhir)*.

Setelah dilakukan pengolahan data, diperoleh hasil tingkat kesadaran keamanan infomasi pada mahasiswa berdasarkan 4 domain *Password Management, Internet Use, Information Handling, dan Social Media Use* [3.2]. Pengukuran dilaksanakan pada 3 aspek *Knowledge (30%), Attitude (20%), and Behaviour (50%).* Setiap domain dianalisis

berdasarkan skor rata rata dari masing masing KAB, kemudian menghitung total awareness berdasarkan pembobotan yang dilakukan oleh Kruger dan Kearney [3.8]. Rumus perhitungan data sebagai (z) dan (z1). dan hasil perhitungan tingkat kesadaran keamanan informasi dilampirkan pada tabel 4.2

$$Skor\ Maksimum\ =\ Ttal\ Responden\ x\ Jml\ Pertanyaan\ Per\ Domain\ x\ Ttal\ Liker$$

$$SkorMaksimum = 387x\ 3x\ 5$$

$$Skor\ Maksimum\ =\ 5.805 \quad (z)$$

$$Rumus\ perhitungan\ =\ \frac{\text{Total skor aktual}}{\text{Skor maksimum}}\ \text{x}\ 100\% \quad (z1)$$

A. Perhitungan Domain *Password Management*

a) Aspek *Knowledge*

$$\frac{4735}{5805}\ *\ 100\%$$

$$Total\ nilai\ Aspek\ Knowledge\ =\ 81.57\%$$

b) Aspek *Attitude*

$$\frac{4885}{5805}\ *\ 100\%$$

$$Total\ nilai\ Aspek\ Attitude\ =\ 84.15\%$$

c) Aspek *Behaviour*

$$\frac{3992}{5805}\ *\ 100\%$$

$$Total\ nilai\ Aspek\ Attitude\ =\ 68.77\%$$

d) Total *Awareness* = (N. A *K* * 30%) + (N.A *A* * 20 %) + (N.A **B** * 50 %) * 100 % =
= (81.57 * 30%) + (84.15 * 20%) + (68.77 * 50%) *100 % =
= (24.47) + (16.83) + (34.38) *100 %
= 75.68 %

B. Perhitungan Domain *Internet Use*

a) Aspek *Knowledge*

$$\frac{4717}{5805}\ *\ 100\%$$

$$Total\ nilai\ Aspek\ Knowledge\ =\ 81.26\%$$

b) Aspek *Attitude*

$$\frac{4624}{5805}\ *\ 100\%$$

$$Total\ nilai\ Aspek\ Attitude\ =\ 79.66\%$$

c) Aspek *Behaviour*

$$\frac{3854}{5805}\ *\ 100\%$$

$$Total\ nilai\ Aspek\ Attitude\ =\ 66.39\%$$

d) Total *Awareness* = (N. A ***K*** * 30%) + (N.A ***A*** * 20 %) + (N.A **B** * 50 %) * 100 % =
= (81.26 * 30%) + (79.66 * 20%) + (66.39 * 50%) *100 % =

= (24.38) + (15.93) + (33.20) *100 %

= 73.50 %

C. Perhitungan Domain *Information Handling*

$$\frac{4764}{5805} * 100\%$$

a) Aspek *Knowledge*

$$Total\ nilai\ Aspek\ Knowledge = 82.07\%$$

$$\frac{4871}{5805} * 100\%$$

b) Aspek *Attitude*

$$Total\ nilai\ Aspek\ Attitude = 83.91\%$$

$$\frac{3847}{5805} * 100\%$$

c) Aspek *Behaviour*

$$Total\ nilai\ Aspek\ Attitude = 66.27\%$$

d) Total *Awareness* = (N. A ***K*** * 30%) + (N.A ***A*** * 20 %) + (N.A **B** * 50 %) * 100 % =

= (82.07 * 30%) + (83.91 * 20%) + (66.27 * 50%) *100 % =

= (24.38) + (15.93) + (33.20) *100 %

= 74.54 %

D. Perhitungan Domain *Social Media Use*

$$\frac{4727}{5805} * 100\%$$

a) Aspek *Knowledge*

$$Total\ nilai\ Aspek\ Knowledge = 81.43\%$$

$$\frac{4929}{5805} * 100\%$$

b) Aspek *Attitude*

$$Total\ nilai\ Aspek\ Attitude = 84.91\%$$

$$\frac{3673}{5805} * 100\%$$

c) Aspek *Behaviour*

$$Total\ nilai\ Aspek\ Attitude = 63.27\%$$

d) Total *Awareness* = (N. A ***K*** * 30%) + (N.A ***A*** * 20 %) + (N.A **B** * 50 %) * 100 % =

= (81.43 * 30%) + (84.91 * 20%) + (63.27 * 50%) *100 % =

= (24.43) + (16.98) + (31.64) *100 %

= 73.05 %

E.* Perhitungan Rata Rata *Awareness

Skor Rata rata = $\frac{\sum Rata\ rata\ Domain}{Total\ Domain} * 100\%$

Skor Rata Rata = $\frac{=75.68+73.50 + 74.54 + 73.05}{4} * 100\%$

Skor Rata Rata = $\frac{296.77}{4} * 100\%$

Skor Rata rata = 74.19 %

Berdasarkan Tabel [3.7] Tingkat rata rata kesadaran responden digolongkan ke "**Menengah**"

Tabel 4.2 Tingkat Kesadaran Keamanan Informasi

Domain	Knowledge	Attitude	Behaviour	Total Awareness	Rata Rata	Status
Password Management	81,57%	84,15%	68,77%	75,68%	74,19%	**Menengah**
Internet Use	81,26%	79,66%	66,39%	73,50%		
Information Handling	82,07%	83,91%	66,27%	74,54%		
Social Media Use	81,43%	84,91%	63,27%	73,05%		

Tingkat penilaian terhadap kesadaran keamanan informasi dalam penelitian ini dibagi menjadi tiga kategori yaitu "Baik" apabila memperoleh skor > 80 %, "Menengah" apabila berada rentang skor 60 hingga 79%, dan "Buruk" apabila memperoleh skor kurang dari 60 [3.8]. Kategori ini digunakan untuk mempermudah interpretasi hasil dan melihat sejauh mana mahasiswa memahami penerapan keamanan informasi pribadi.

Berdasarkan perhitungan tersebut, diperoleh total nilai rata rata sebesar 74.19 % yang memperlihatkan kesadaran mahasiswa terhadap keamanan informasi di Politeknik Negeri Batam berada pada level "Menengah". Ada terdapat celah antara pemahaman tersebut dengan dan penerapan nyata dalam kehidupan sehari hari. Secara umum aspek *Behaviour* cenderung rendah dibandingkan dengan aspek *Knowledge* dan *Attitude,* yang menunjukan bahwa meskipun mahasiswa memiliki pengetahuan dan sikap yang cukup baik terhadap keamanan informasi, penerapannya dalam perilaku sehari hari masih sangat perlu ditingkatkan. Variasi skor ini jugaa terlihat diberbagai fokus area, yang mendefinisikan adanya perbedaan tingkatan pemahaman dan penerapan keamanan informasi pada mahasiswa.

Jika dilihat dari masing masing domain, hasil tertinggi terdapat pada fokus area *Password Management* (*74.19%*), dengan aspek *Knowledge (81.57%), Attitude (84.15%) dan Behaviour (68.77%).* Hal ini menunjukan bahwa mahasiswa cukup menyadari penting nya pengelolaan password yang baik dimana kerahasiaan kata sandi yang kuat serta menggunakan kata sandi yang berbeda di setiap akun media sosial. Meskipun ada perbedaan yang cukup signifikan dengan domain *(Behaviour),* dimana penggunaan autentifikasi 2 faktor pada akun media sosial masih sangat jarang diterapkan.

Fokus area *Internet Use* Juga menunjukan hasil yang cukup baik dengan skor total 73.50% dan dikategorikan "Menengah". Pada domain ini aspek *Behaviour (66.39%)* masih berada di aspek yang paling rendah dibandingkan dengan 2 aspek yang lain *Knowledge (81.26%)* dan *Attitude (79.66%).* Fokus ini menampilkan *Knowledge* dan *Behaviour* bertolak belakang, dimana pengetahuan yang baik terhadap penggunaan internet tidak serta merta dengan tindakan. Pengetahuan yang baik terhadap situs web yang mencurigakan tidak mencerminkan dengan tindakan yang baik ketika mengunjungi situs web yang akan ditelusuri.

Fokus area *Information Handling* juga menunjukan hasil "Menengah" dengan skor (*74.54%)* dimana aspek *Knowledge (82.07%), Attitude (83.91%). Behaviour (66.27%)*. Pada domain ini aspek *Attitude* menunjukan angka tertinggi yaitu *(83.91%).* Sikap untuk membatasi penyebaran informasi pribadi di internet ialah sikap yang baik dalam rangka mencegah tindakan doksing dimedia sosial. Selanjutnya disusul dengan aspek *Knowledge* (*82.07%*) yang menampilkan pengetahuan bahwasannya alamat pribadi yang tersebar dimedia sosial dapat memicu tindakan doksing di-kemudian hari. Setelah itu aspek *Behaviour* masih aspek terendah (66.27%). Sikap dan pengetahuan yang tinggi tanpa diiringi dengan tindakan dapat memunculkan celah terhadap keamanan informasi pribadi di kemudian hari.

Fokus area terakhir yaitu *Social Media Use,* merupakan domain yang memiliki rerata terendah pada penelitian ini dengan skor rata rata (*73.05%*). Pada fokus area ini aspek *Attitude* memiliki skor rata rata tertinggi dibandingkan dengan domain lainnya (*84.91%)*, hal ini menunjukan sikap kewaspadaan yang baik ketika menggunakan media sosial, dimana sudah menganggap penting-nya mengatur privasi dalam berbagi konten di media sosial. Namun pada penerapannya masih dibawah kategori "Baik", terlihat dari skor aspek *Behavior* dengan rata rata (63.27%). Peningkatan terhadap implementasi pada domain ini sangat perlu ditingkatkan dimana faktor utama ketika seseorang terkena doksing itu dimulai dari penggunaan media sosial nya

Jika dibandingkan dengan penelitian sebelumnya, temuan ini sejalan dengan penelitian [1] yang mengkategorikan skor tingkat kesadaran keamanan informasi mahasiswa dalam level sedang yaitu 79.61%, namun skor pada penelitian ini jauh lebih rendah yaitu 74.19%. Hal ini bisa disebabkan adanya beberapa perbedaan domain dalam pengujian nya, penggunaan domain pada penelitian ini lebih sedikit dibandingkan dengan penelitian sebelum nya, karena fokus domain pada penlitian ini hanya yang berkaitan dengan tindakan keamanan informasi dari tindakan doksing dimedia sosial saja. Responden yang digunakan pada penelitian ini juga lebih sedikit dibandingkan dengan penelitian sebelumnya, adanya perbedaan jumlah mahasiswa antar universitas nya juga turut menjadi faktor perbedaan responden. Pada penelitian [12] juga mengukur kesadaran keamanan informasi dalam penggunaan E-wallet dengan subjek penelitian gen z. Pada penelitian ini fokus penelitian hanya sebatas aspek KAB dari Kruger and Kearney tidak terfokus dengan adanya domain standar seperti HAIS-Q. Pada penelitian tersebut analisa hubungan keamanan informasi dengan aspek KAB dikategorikan positif dimana aspek KAB dari Kruger and Kearney sangat sesuai dengan penelitian keamanan informasi. Pada penelitian ini pengukuran tingkat kesadaran keamanan informasi mahasiswa memiliki satu fokus terhadap tindakan kejahatan doksing dimedia sosial. Berbeda dengan penelitian [1] dimana pengukuran tingkat kesadaran keamanan informasi dilakukan terhadap serangan siber yang melingkupi universal. Pada penelitian ini domain *Social Media Use* menjadi domain yang memiliki skor terendah,

sementara dalam pembahasannya media sosial adalah pintu utama yang menjadi penghubung ke kehidupan nyata. Namun tidak menutup kemungkinan adanya peningkatan kesadaran keamanan informasi kedepannya, mengingat nilai aspek *Attitude* & *Knowledge* yang memiliki rata rata yang "Bagus", dimana aspek tersebut dapat dijadikan pondasi yang baik dalam meningkatkan nilai aspek *Behaviour.*

Hasil penelitian ini menunjukan bahwa aspek behaviour menjadi aspek dengan nilai rata rata paling rendah dibandingkan dengan aspek lainnya. Temuan ini mencerminkan bahwa mahasiswa masih inkonsisten menerapkan perilaku yang mendukung keamanan informasi, khususnya dalam melindungi data pribadi dan mencegah risiko terjadinya tindakan doksing di media sosial.

BAB V
KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa tingkat kesadaran keamanan informasi pribadi mahasiswa Politeknik Negeri Batam dalam menghadapi ancaman doksing pada media sosial berada pada kategori menengah, dengan nilai rata-rata keseluruhan sebesar 74,19%. Hasil tersebut menunjukkan bahwa mahasiswa telah memiliki tingkat kesadaran yang cukup baik terhadap pentingnya menjaga keamanan informasi pribadi, namun belum mencapai kategori yang optimal. Jika dilihat dari masing masing dimensi, sikap mahasiswa terhadap keamanan informasi menempati posisi tertinggi, disusul oleh pengetahuan dan yang terendah ialah perilaku. Ini menunjukan bahwa meskipun mahasiswa telah memiliki pemahaman yang baik serta sikap yang bagus terhadap penting nya keamanan informasi, pemahaman dan sikap tersebut belum sepenuhnya diwujudkan dalam perilaku di kehidupan nyata ketika aktif menggunakan media sosial.Oleh karena itu, upaya peningkatan kesadaran perlu diarahkan tidak hanya pada pemberian informasi, tetapi juga pada penguatan sikap dan pembiasaan perilaku aman dalam aktivitas digital sehari-hari. Kontribusi penelitian ini terletak pada pemetaan kesadaran keamanan informasi mahasiswa secara lebih rinci berdasarkan dimensi pengetahuan, sikap, dan perilaku, sehingga dapat menjadi referensi bagi pengembangan program edukasi keamanan informasi yang lebih efektif di lingkungan Politeknik Negeri Batam. Hasil penelitian ini memiliki perbedaan dengan studi sebelumnya yang menunjukkan bahwa kesadaran keamanan informasi dipengaruhi oleh sikap dan perilaku, sedangkan pada penelitian ini kesadaran keamanan informasi dipengaruhi dengan sikap dan pengetahun, domain pada HAIS-Q juga berbeda fokus dalam pelaksanaannya. Meski demikian, keterbatasan penelitian ini terletak pada fokusnya yang hanya pada mahasiswa di Politeknik Negeri Batam saja sehingga temuan keamanan hanya mencerminkan kondisi di kampus tersebut.

B. Saran

Bagi Mahasiswa Politeknik Negeri Batam, diharapkan untuk dapat meningkatkan penerapan praktik keamanan informasi dalam kehidupan sehari-hari, khususnya saat menggunakan media sosial. Mahasiswa harus lebih berhati hati ketika membagikan informasi pribadi mereka dimedia sosial, lalu untuk selalu menggunakan kata sandi yang kuat dan berbeda disetiap akun media soalnya, dan selalu mengaktifkan 2AF (*Two-factor-authentication*) di setiap media sosial yang mendukung fitur tersebut, serta memahami pengaturan privasi pada setiap platform

media sosial guna untuk meminimalkan risiko menjadi korban doksing, dan selalu menjaga etika dalam bermedia sosial.

Bagi Politeknik Negeri Batam, disarankan untuk melaksanakan program peningkatan pengetahuan (*edukasi)* tentang keamanan informasi pribadi di media sosial melalui seminar, pelatihan, workshop, maupun kampanye literasi digital secara berkala bisa melalui instagram, facebook, youtube maupun media lainnya. Kegiatan tersebut diharapkan mampu meningkatkan tidak hanya pengetahuan dan sikap mahasiswa, tetapi juga bisa mendorong perubahan perilaku sehingga praktik keamanan informasi dapat diterapkan secara konsisten.

Bagi Program Studi Rekayasa Keamanan Siber, hasil penelitian ini dapat dijadikan sebagai bahan evaluasi dalam penyusunan program pembelajaran maupun kegiatan akademik yang berfokus pada peningkatan kesadaran keamanan informasi. Selain itu, studi kasus mengenai ancaman doksing dan perlindungan data pribadi dapat diintegrasikan ke dalam proses bahan pembelajaran agar mahasiswa lebih memahami penerapan keamanan informasi dalam kehidupan nyata.

Bagi Peneliti Selanjutnya, disarankan untuk memperluas cakupan penelitian dengan melibatkan responden dari perguruan tinggi lain atau kelompok masyarakat yang berbeda sehingga hasil penelitian dapat dibandingkan secara lebih luas. Penelitian selanjutnya juga dapat membahas apa saja faktor-faktor yang memengaruhi perilaku keamanan informasi, seperti pengalaman menjadi korban kejahatan siber, intensitas penggunaan media sosial, maupun pengaruh dari lingkungan, selain itu disarankan untuk melibatkan dosen dan staff dengan tambahan sebagai responden.

DAFTAR PUSTAKA

[1] S. F. Arum, A. Zubaidi, and R. B. Huwae, "Pengukuran tingkat kesadaran keamanan informasi menggunakan HAIS-Q: Mengungkap kesenjangan antara sikap dan pengetahuan mahasiswa," Jurnal Bumigora Information Technology, vol. 7, no. 2, 2025, https://doi.org/10.30812/bite.v7i2.5430

[2] J. N. Saly and L. T. Sulthanah, "Pelindungan data pribadi dalam tindakan doxing berdasarkan Undang-Undang Nomor 27 Tahun 2022," Jurnal Kewarganegaraan, vol. 7, no. 2, 2023, https://doi.org/10.31316/jk.v7i2.5413

[3] T. Tanuwijaya, "Di balik akun bodong ada ancaman doksing yang melemahkan demokrasi," The Conversation Indonesia, Jun. 15, 2026. [Online]. Available: https://theconversation.com/di-balik-akun-bodong-ada-ancaman-doksing-yang-melemahkan-demokrasi-283691

[4] Amazon Web Services (AWS), "Apa itu keamanan siber?," 2026. [Online]. Available: *https://aws.amazon.com/id/what-is/cybersecurity/*

[5] M. R. Akhyari and A. R. Pratama, "Kesadaran akan ancaman serangan berbasis backdoor di kalangan pengguna smartphone Android," Automata, vol. 2, no. 2, 2021. [Online]. Available: https://journal.uii.ac.id/AUTOMATA/article/view/17317

[6] IBM, "Apa itu keamanan informasi?," IBM Think, 2026. [Online]. Available: https://www.ibm.com/id-id/think/topics/information-security

[7] B. Y. Dharmahita, M. P. Aji, E. S. Wijaya, and A. P. Wicaksono, "Penerapan HAIS-Q dalam pengukuran tingkat kesadaran keamanan informasi pegawai Disdukcapil Kota Malang," Jurnal Pendidikan dan Teknologi Indonesia (JPTI), vol. 5, no. 2, 2025, https://doi.org/10.52436/1.jpti.1228

[8] D. Nurjanah and S. Destya, "Pengukuran tingkat kesadaran keamanan informasi mahasiswa pada pembelajaran online," JUSTIN (Jurnal Sistem dan Teknologi Informasi), vol. 10, no. 1, 2022, d
https://doi.org/10.26418/justin.v10i1.44362

[9] H. A. Kruger and W. D. Kearney, “A prototype for assessing information security awareness,” Computers & Security, vol. 25, no. 4, pp. 289–296, 2006, . https://doi.org/10.1016/j.cose.2006.02.008

[10] S. K. Ahmed, “How to choose a sampling technique and determine sample size for research: A simplified guide for researchers,” Oral Oncology Reports, vol. 12, 2024, https://doi.org/10.1016/j.oor.2024.100662

[11] Nur, M. A. R. (2024). *Analisis kesadaran keamanan dengan model Kruger & Kearney dalam penggunaan e-wallet pada Generasi Z (Gen-Z) di Indonesia.*

https://repository.polibatam.ac.id/items/9a86729f-c309-47bd-bbd2-da3dd87505c5