Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 4 No. 4 (2026) pp: 8091-8101
P-ISSN: 2963-9298, e-ISSN: 2963-914X

Analisis Tingkat Kesadaran Mahasiswa terhadap Keamanan Data Pribadi di Era Digital: Studi Komparatif antara Mahasiswa Teknik Informatika dan Non-Teknik Informatika

Jadiaman Parhusip, Fatiya Ummu Hanifah Zahra, Agatha Monalisa, Muhammad Rony Kurniawan, Ni Putu Lowryanty
Program Studi Teknik Informatika, Fakultas Teknik, Universitas Palangkaraya
parhusip.jadiaman@it.upr.ac.id, fatyauhz01@gmail.com, agathamona12@gmail.com, ronykrbaek08@gmail.com, niputulowryantylowry@gmail.com

Abstrak

Pesatnya perkembangan teknologi digital dan tingginya penggunaan layanan daring meningkatkan risiko kebocoran serta penyalahgunaan data pribadi, khususnya di kalangan mahasiswa sebagai pengguna aktif teknologi. Kondisi ini menegaskan pentingnya kesadaran keamanan digital yang mencakup pengetahuan, sikap, dan perilaku dalam penggunaan layanan digital. Penelitian ini bertujuan menganalisis tingkat kesadaran keamanan data pribadi mahasiswa serta membandingkan pengetahuan, sikap, dan perilaku keamanan digital antara mahasiswa Teknik Informatika (TI) dan Non-Teknik Informatika (Non-TI). Penelitian menggunakan pendekatan kuantitatif melalui survei terhadap 100 responden, terdiri dari 50 mahasiswa TI dan 50 mahasiswa Non-TI. Instrumen penelitian mengukur tiga dimensi utama kesadaran keamanan digital, yaitu pengetahuan, sikap, dan perilaku, menggunakan skala Likert lima poin. Data dianalisis menggunakan statistik deskriptif, korelasi Spearman, uji t independen, dan regresi linier. Hasil penelitian menunjukkan bahwa mahasiswa TI memiliki skor rata-rata yang lebih tinggi pada ketiga dimensi dibandingkan mahasiswa Non-TI, namun perbedaan signifikan secara statistik hanya ditemukan pada aspek pengetahuan ($p = 0{,}007$). Analisis korelasi menunjukkan hubungan positif sedang antara pengetahuan dan perilaku ($r = 0{,}383$) serta antara sikap dan perilaku ($r = 0{,}409$), sementara hubungan antara pengetahuan dan sikap tergolong sangat lemah ($r = -0{,}062$). Analisis regresi menunjukkan bahwa sikap memiliki pengaruh yang relatif lebih kuat terhadap perilaku keamanan digital dibandingkan pengetahuan. Temuan ini menunjukkan bahwa peningkatan pengetahuan teknis saja belum cukup untuk membentuk perilaku keamanan digital yang optimal, sehingga diperlukan pendekatan edukatif yang menekankan pembentukan sikap dan pengalaman praktis di lingkungan pendidikan tinggi.

Kata kunci: Keamanan Data Pribadi, Kesadaran Digital, Keamanan Siber, Perilaku Digital.

1. Latar Belakang

Perkembangan teknologi digital dalam satu dekade terakhir telah meningkatkan ketergantungan masyarakat terhadap layanan berbasis internet, termasuk media sosial, sistem informasi akademik, layanan kesehatan, dan aplikasi keuangan. Di Indonesia, penggunaan teknologi informasi telah merambah ke berbagai sektor seperti perbankan, e-commerce, pendidikan, dan administrasi publik, yang memang memungkinkan layanan lebih cepat dan efisien, namun sekaligus membuka celah baru terhadap potensi kebocoran dan penyalahgunaan data pribadi [1]. Dalam konteks hukum nasional, perlindungan data pribadi juga telah diatur dalam regulasi seperti Undang-Undang ITE dan PP No. 71 Tahun 2019 yang menegaskan pentingnya menjaga kerahasiaan, integritas, dan keamanan informasi digital [2].

Kesadaran keamanan digital (cyber awareness) menjadi faktor penting dalam meminimalkan risiko serangan siber yang semakin kompleks. Kesadaran ini tidak hanya terkait dengan pengetahuan mengenai ancaman, tetapi juga mencakup bagaimana individu mengembangkan sikap yang hati-hati dan perilaku yang tepat dalam penggunaan perangkat digital serta pengelolaan akun daring. Namun, berbagai penelitian menunjukkan bahwa mahasiswa sebagai pengguna aktif teknologi masih memiliki kelemahan dalam praktik keamanan sehari-hari. Hal ini terlihat pada penelitian tentang mahasiswa di Kota Batam, di mana 75,3% mahasiswa menggunakan kata sandi yang digunakan sebelumnya, 74% menggunakan satu kata sandi yang kuat untuk akun yang berbeda, dan 78,5%

mengatakan bahwa memiliki kata sandi yang panjang dan kuat terasa menjengkelkan [3]. Temuan tersebut menunjukkan bahwa meskipun mahasiswa memahami pentingnya keamanan digital, perilaku yang ditunjukkan belum sepenuhnya mencerminkan kesadaran yang baik, sehingga menimbulkan kesenjangan antara pengetahuan dan tindakan yang dapat meningkatkan kerentanan terhadap ancaman siber.

Perbedaan latar belakang pendidikan juga berpotensi memengaruhi tingkat kesadaran keamanan digital mahasiswa. Mahasiswa Teknik Informatika (TI) biasanya mendapat paparan lebih mendalam mengenai keamanan jaringan, rekayasa perangkat lunak, serta praktik keamanan digital dalam kurikulum mereka, sehingga secara teori memiliki pemahaman teknis yang lebih kuat. Sebaliknya, mahasiswa non-TI cenderung memiliki kemampuan teknis yang lebih terbatas sehingga lebih rentan terhadap ancaman seperti phishing, penggunaan kata sandi yang lemah, atau rekayasa sosial. Penelitian oleh Al Affan dkk. menegaskan bahwa masih terdapat kesenjangan pengetahuan spesifik yang dimiliki mahasiswa tentang cybersecurity, yang menunjukkan bahwa meskipun mahasiswa aktif menggunakan internet, pemahaman mereka tidak selalu merata [4]. Temuan tersebut memperkuat perlunya membandingkan mahasiswa TI dan non-TI untuk melihat apakah pengetahuan teknis benar-benar berpengaruh terhadap sikap dan perilaku keamanan digital.

Berdasarkan fenomena tersebut, penelitian ini perlu dilakukan untuk mengukur secara sistematis tingkat pengetahuan, sikap, dan perilaku keamanan digital mahasiswa. Perbandingan antara mahasiswa Teknik Informatika (TI) dan non-TI menjadi penting untuk melihat apakah perbedaan latar belakang pendidikan berpengaruh pada tingkat kesadaran keamanan digital yang mereka miliki. Penelitian sebelumnya juga menegaskan bahwa masih terdapat kesenjangan pemahaman keamanan siber di kalangan mahasiswa, sehingga evaluasi yang lebih terarah diperlukan untuk memetakan faktor-faktor yang berkontribusi terhadap kesenjangan tersebut [4]. Selain itu, analisis hubungan antarvariabel—seperti pengetahuan, sikap, dan perilaku—diperlukan untuk mengetahui apakah pemahaman teoritis benar-benar diterjemahkan menjadi perilaku keamanan digital yang lebih baik. Hasil penelitian ini diharapkan dapat memberikan gambaran empiris mengenai kondisi kesadaran keamanan digital mahasiswa serta menjadi dasar bagi penyusunan program edukasi atau pelatihan keamanan digital yang lebih efektif di lingkungan perguruan tinggi.

2. Tinjauan Pustaka

2.1 Konsep Keamanan Data Pribadi

Privasi data adalah proses melindungi informasi pribadi dari akses, penggunaan, modifikasi, atau penyalahgunaan yang tidak sah. Keamanan data sangat penting karena data memiliki nilai strategis yang dapat dimanfaatkan untuk berbagai tujuan, termasuk potensi penggunaannya dalam keamanan siber [5]. Privasi data merujuk pada informasi apa pun yang dapat digunakan untuk mengidentifikasi individu, baik secara langsung maupun tidak langsung. Oleh karena itu, penting untuk mempertimbangkan privasi (kerahasiaan), integritas (konsistensi), keaslian (keaslian), ketersediaan (ketersediaan), dan pengendalian akses (pengendalian akses). Dalam konteks hukum nasional, konsep ini tercantum dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, yang menjamin hak untuk membela diri, rasa aman, dan kebebasan dari ancaman yang melanggar hak asasi manusia.

Dasar-dasar perlindungan data pribadi di Indonesia diatur dalam berbagai peraturan sektoral, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang telah diimplementasikan melalui Undang-Undang Nomor 19 Tahun 2016, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Pelaksanaan Sistem dan Transaksi Elektronik, serta Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2020. Menurut PP No. 71 Tahun 2019, pengembangan sistem elektronik harus mematuhi prinsip-prinsip transparansi, pembatasan tujuan, pertanggungjawaban, keamanan penyimpanan, dan kemampuan individu untuk mengantisipasi dan menilai data mereka sendiri. Prinsip-prinsip tersebut bertujuan untuk memastikan bahwa pengumpulan dan analisis data dilakukan secara adil, tepat, dan konsisten yang menghormati hak-hak pemilik data.

Ancaman terkait keamanan data pribadi umumnya berupa kerusakan data, serangan siber, penggunaan internal oleh karyawan, atau kelemahan sistem keamanan teknologi informasi. Terdapat 29 kasus pelanggaran perlindungan data pribadi di Indonesia antara tahun 2019 dan 2021, dengan 93% dari kasus tersebut disebabkan oleh insiden siber [5]. Data set besar, seperti 91 juta pengguna Tokopedia pada tahun 2020 dan 279 juta pengguna BPJS Kesehatan pada tahun 2021, menunjukkan bahwa ada dampak sosial dan ekonomi yang signifikan terhadap

DOI: https://doi.org/10.31004/riggs.v4i4.4516

data pribadi. Oleh karena itu, privasi data bukan hanya persyaratan teknis bagi organisasi yang mengelola sistem elektronik, tetapi juga persyaratan norma nasional untuk melindungi privasi digital masyarakat.

2.2 Kesadaran Keamanan Digital (Cyber Awareness)

Kesadaran keamanan digital (cyber awareness) merujuk pada pemahaman individu tentang pentingnya melindungi informasi pribadi mereka serta kemampuan mereka untuk mendeteksi dan mengidentifikasi ancaman di dunia maya. Menurut penelitian yang diterbitkan dalam jurnal, studi ini berfokus pada tiga aspek utama: pemahaman, sikap, dan perilaku. Aspek pengetahuan mencakup bagaimana orang memahami berbagai jenis ancaman siber, seperti phishing, malware, kebocoran data, dan rekayasa sosial, serta cara melindungi diri melalui langkah-langkah keamanan dasar, seperti menggunakan kata sandi yang kuat dan otentikasi dua faktor. Aspek sikap berfokus pada komitmen individu terhadap pentingnya keamanan digital, termasuk kemampuan untuk teliti dalam mengumpulkan informasi pribadi, memeriksa keaslian sumber, dan memperkuat kebijakan privasi.

Literasi digital, pembelajaran, dan lingkungan pendidikan memiliki dampak yang signifikan terhadap tingkat keamanan digital individu. Penelitian dalam jurnal yang disebutkan di atas menunjukkan bahwa mahasiswa dapat mengalami peningkatan yang signifikan dalam ketiga aspek tersebut melalui kegiatan pendidikan, sosialisasi, dan pelatihan keamanan digital berbasis pembelajaran layanan. Peningkatan kesadaran akan menghasilkan pandangan positif terhadap keamanan data, yang kemudian akan didukung dalam lingkungan digital. Namun, hambatan seperti kurangnya literasi digital, akses informasi yang terbatas, dan kurangnya kesadaran terhadap ancaman siber terus menjadi kendala dalam pengembangan perilaku aman yang konsisten. Oleh karena itu, diperlukan peningkatan tingkat keamanan digital melalui kolaborasi antara lembaga pendidikan, pemerintah, dan masyarakat umum agar mahasiswa, baik yang berada di bidang teknologi informasi maupun tidak, dapat melindungi data pribadi mereka dan berpartisipasi dalam era digital yang terus berkembang.

2.3 Studi terdahulu mengenai kesadaran mahasiswa terhadap privasi digital

Kesadaran mahasiswa terhadap privasi digital merupakan komponen penting dari literasi digital yang memfasilitasi pemahaman, perilaku, dan sikap individu dalam melindungi data pribadi di dunia nyata [7]. Privasi digital merujuk pada kemampuan seseorang untuk mengontrol informasi pribadi mereka sehingga tidak diakses atau digunakan tanpa izin di lingkungan digital. Di era yang ditandai dengan meningkatnya aktivitas berani dan penggunaan media sosial, mahasiswa merupakan kelompok yang paling rentan terhadap risiko privasi karena cenderung membagikan informasi pribadi secara terbuka tanpa mempertimbangkan risiko keamanan yang mungkin timbul. Data pribadi, seperti identitas, lokasi, dan aktivitas internet, sering digunakan oleh pihak ketiga untuk tujuan komersial atau bahkan keamanan siber. Oleh sebab itu, kesadaran terhadap privasi digital menuntut mahasiswa untuk memahami risiko yang melekat pada penggunaan teknologi, sekaligus menerapkan langkah-langkah pencegahan seperti pengaturan privasi akun, penggunaan kata sandi yang kuat, serta kehati-hatian dalam berbagi informasi secara publik.

Penelitian yang dilakukan oleh [7] menunjukkan bahwa kesadaran mahasiswa terhadap privasi digital masih cukup rendah. Meskipun banyak mahasiswa memahami pentingnya menjaga data pribadi, perilaku yang dilakukan tidak sepenuhnya mencerminkan kesadaran tersebut. Misalnya, banyak mahasiswa yang masih menggunakan foto pribadi secara sembarangan, yang berpotensi menyebabkan pelanggaran privasi di media sosial. Di antara faktor-faktor yang mempengaruhi rendahnya kesadaran ini adalah pemahaman teknis, kepercayaan terhadap platform digital, dan pengaruh sosial dalam berbagi informasi. Selain itu, terdapat perbedaan berdasarkan tingkat pendidikan dan jenis pendidikan, dengan mahasiswa tingkat akhir dan perempuan menunjukkan tingkat privasi yang lebih tinggi dibandingkan mahasiswa baru dan laki-laki. Kondisi ini menunjukkan perlunya peningkatan literasi digital di kalangan mahasiswa melalui pendidikan formal, pelatihan keamanan siber, dan kampanye publik agar mereka mampu membangun perilaku digital yang lebih aman, bertanggung jawab, dan sadar privasi di era digital.

2.4 Studi terdahulu mengenai perbandingan pengguna TI dan non-TI

Membandingkan mahasiswa dengan latar belakang Teknologi Informasi (TI) dan non-Teknologi Informasi (non-TI) sangat penting untuk memahami tingkat pengetahuan, keterampilan, dan perilaku mereka dalam hal keamanan digital. Dibandingkan dengan mahasiswa non-TI, mahasiswa TI cenderung memiliki keahlian teknis yang lebih tinggi dan kesadaran yang lebih besar dalam menerapkan prinsip-prinsip keamanan [8]. Hal ini disebabkan oleh

DOI: https://doi.org/10.31004/riggs.v4i4.4516

perbedaan kurikulum dan materi pembelajaran terkait teknologi informasi yang signifikan. Mahasiswa TI umumnya mempelajari konsep-konsep penting seperti manajemen risiko, keamanan jaringan, enkripsi, dan prinsip Kerahasiaan, Integritas, dan Ketersediaan (CIA), yang menjadi dasar perlindungan data digital. Di sisi lain, mahasiswa non-TI umumnya tidak mendapatkan pengajaran tentang keamanan siber, sehingga mereka lebih rentan terhadap risiko seperti phishing, penggunaan kata sandi lemah, peretasan sistem, dan rekayasa sosial.

Studi ini juga menunjukkan bahwa ketidakmampuan mahasiswa non-TI dalam menerapkan praktik keamanan digital disebabkan oleh kurangnya literasi dan pemahaman teknis mereka terhadap dunia digital. Karena hal ini tidak langsung terkait dengan kegiatan akademik mereka, banyak mahasiswa non-TI menggunakan internet dan sistem digital secara aktif dalam kegiatan akademik maupun pribadi. Hasil survei menunjukkan bahwa meskipun banyak mahasiswa non-TI memiliki sikap positif terhadap keamanan mereka, pengetahuan dan perilaku mereka masih berada dalam kategori sedang. Selain itu, mahasiswa TI menunjukkan tingkat kewaspadaan yang lebih tinggi, terutama dalam penggunaan kata sandi, pemilihan jaringan aman, dan penggunaan autentikasi dua faktor. Oleh karena itu, studi perbandingan ini menegaskan perlunya penguatan literasi keamanan digital bagi mahasiswa non-TI melalui pelatihan, kampanye kesadaran, dan integrasi topik keamanan siber dalam kurikulum lintas disiplin agar tercipta keseimbangan kemampuan keamanan digital di antara kedua kelompok mahasiswa tersebut.

2.5 Penelitian terkait edukasi keamanan siber

Di era digital, keamanan siber merupakan isu krusial yang meningkatkan kesadaran publik terhadap berbagai ancaman digital, seperti kebocoran data, phishing, pharming, dan sniffing. Inisiatif riset dan pendidikan keamanan menyoroti pentingnya literasi digital sebagai langkah pencegahan untuk melindungi individu dari kebocoran data pribadi. Tujuan edukasi ini adalah memberikan pengetahuan tentang perlindungan identitas digital, perangkat keamanan, dan jejak digital secara sederhana dan mudah dipahami. Pendidikan interaktif dan berbasis aplikasi, seperti penggunaan otentikasi dua faktor dan perangkat pelacakan, dapat meningkatkan kesadaran dan partisipasi masyarakat dalam aktivitas digital sehari-hari [9]. Temuan studi juga menunjukkan bahwa instruksi berbasis pembelajaran bahasa lebih efektif dalam menumbuhkan kesadaran akan pentingnya keamanan informasi.

Selain itu, sejumlah penelitian lain mempunyai pendapat lain untuk memperkuat pentingnya edukasi keamanan siber sebagai sarana dalam membangun infrastruktur digital. Literasi digital yang didasarkan pada keterampilan bahasa praktis dapat mengurangi risiko pengguna dalam melindungi data pribadi [11, 12]. Literasi digital sangat penting sebagai bentuk perlindungan terhadap privasi individu [10], dan literasi digital tidak hanya berguna untuk meningkatkan pengetahuan tetapi juga untuk mengembangkan keterampilan sosial [13]. Berdasarkan beberapa studi yang telah disebutkan di atas, dapat disimpulkan bahwa pendidikan tentang keamanan siber sangat penting untuk mengembangkan kesadaran dan perilaku aman di dunia digital, terutama bagi mahasiswa yang menyewakan data mereka di era modern ini.

3. Metode Penelitian

3.1. Jenis Penelitian

Penelitian ini menggunakan pendekatan kuantitatif deskriptif-analitis, yaitu pendekatan yang digunakan untuk menggambarkan fenomena secara numerik berupa pengumpulan data dasar yang bersifat memberikan penjelasan atau deskripsi [14] sekaligus melakukan analisis lanjutan terhadap hubungan atau perbedaan antar variabel penelitian.

3.2. Tahapan Penelitian

Tahapan penelitian disusun untuk memastikan bahwa prosesnya terstruktur dan menghasilkan data yang valid. Tahapan yang dilaksanakan meliputi identifikasi masalah, penyusunan instrument penelitian, pengumpulan data, cleaning data atau pembersihan data, analisis data, dan hasil akhir.

DOI: https://doi.org/10.31004/riggs.v4i4.4516

Gambar 1. Tahap Penelitian

Penelitian ini dimulai dengan proses identifikasi masalah untuk memahami kesadaran mahasiswa terhadap keamanan data pribadi. Tujuan penelitian dirumuskan dan fokus analisis ditetapkan dengan membandingkan tingkat kesadaran mahasiswa Teknik Informatika dan Non-Teknik Informatika. Untuk mencapai tujuan tersebut, peneliti membuat instrumen penelitian berupa kuesioner berbasis skala *Likert* 5 poin yang mencakup metrik pengetahuan, sikap, dan perilaku keamanan digital. Untuk memudahkan akses responden, kuesioner kemudian disebarkan secara online melalui Google Form.

Data yang dikumpulkan kemudian diunduh dan diproses untuk memastikan validitas dan kelayakan. Proses ini mencakup penghapusan duplikat, koreksi *entri*, dan penanganan data kosong. Data yang telah bersih kemudian dianalisis menggunakan teknik statistik deskriptif dan inferensial untuk menggambarkan pola kesadaran digital mahasiswa serta menguji perbedaan dan hubungan antar variabel penelitian. Hasil analisis diinterpretasikan secara ringkas untuk memberikan gambaran tentang tingkat kesadaran mahasiswa mengenai keamanan data pribadi dan faktor-faktor yang memengaruhinya.

3.3. Variabel dan Indikator Penelitian

Variabel utama dalam penelitian ini adalah tingkat kesadaran mengenai keamanan data pribadi. Tiga indikator utama yang digunakan untuk mengukur tingkat kesadaran ini diantaranya:

1) Pengetahuan Keamanan Data Pribadi
Pengetahuan keamanan data pribadi adalah tingkat pemahaman responden tentang konsep, ancaman, serta prosedur dasar dalam menjaga keamanan digital. Aspek ini mencakup pemahaman responden tentang berbagai modus penipuan seperti phishing dan fungsi autentikasi dua faktor (2FA). Selain itu, indikator pengetahuan juga mencakup pemahaman responden tentang risiko penggunaan kata sandi yang sama pada berbagai akun digital, pentingnya praktik keamanan dasar seperti enkripsi, pengaturan privasi akun, dan kewaspadaan terhadap aplikasi yang meminta akses berlebihan.

2) Sikap terhadap Keamanan Data
Sikap terhadap keamanan data menggambarkan pandangan dan kesadaran responden mengenai pentingnya menjaga privasi serta melindungi informasi pribadi di lingkungan digital. Hal ini termasuk pemahaman terhadap

DOI: https://doi.org/10.31004/riggs.v4i4.4516

potensi risiko kebocoran data serta kesungguhan responden dalam menanggapi ancaman keamanan digital. Selain itu, sikap juga terlihat dari kesediaan responden untuk menerapkan langkah-langkah keamanan yang dianjurkan.

3) Perilaku Keamanan Digital

Perilaku keamanan digital menggambarkan tindakan nyata yang dilakukan responden dalam menjaga keamanan data pribadi mereka. Perilaku ini tercermin dari kebiasaan mengganti kata sandi secara berkala, penggunaan autentikasi dua faktor (2FA) pada berbagai layanan digital, serta kehati-hatian dalam memeriksa keaslian tautan sebelum mengaksesnya untuk menghindari ancaman phishing atau malware. Selain itu, perilaku keamanan juga meliputi praktik penyimpanan kata sandi yang aman seperti penggunaan password manager.

3.4. Pengumpulan Data

Pengumpulan data dilakukan melalui metode survei online berupa Google Form. Metode ini dipilih karena memungkinkan pengumpulan data yang cepat dan efektif serta menjangkau responden dalam jumlah besar dari berbagai lokasi. Survei ini disebarkan kepada mahasiswa yang terdiri dari mahasiswa Teknik Informatika dan mahasiswa Non-Teknik Informatika. Berdasarkan responden yang diperoleh, diambil sampel berupa 100 data mahasiswa yang terdiri dari 50 data mahasiswa Teknik Informatika dan 50 data mahasiswa Non-Teknik Informatika. Metode ini didasarkan pada pertimbangan bahwa semua responden harus merupakan mahasiswa yang aktif yang menggunakan internet dan aplikasi digital pada kegiatan sehari-hari. Kuesioner terdiri dari dua bagian utama:

1) Data demografis (usia, jenis kelamin, program studi, semester, lama penggunaan internet).

2) Pernyataan indikator penelitian menggunakan skala Likert 5 poin untuk mengukur tingkat pengetahuan, sikap, dan perilaku keamanan digital.

3.5. Tools

Beberapa alat pengolahan dan visualisasi data yang digunakan dalam penelitian ini diantaranya:

1) Google Colab (Python)

Digunakan untuk melakukan pembersihan data (*cleaning data*), penghitungan statistik deskriptif, penghitungan rata-rata skor pengetahuan, sikap dan perilaku, uji korelasi, uji t dan regresi linier, serta pembuatan visualisasi grafik seperti *bar chart*, *scatter plot*, dan *histogram*. Google Colab dipilih karena menyediakan lingkungan komputasi berbasis *cloud* yang mudah digunakan dan tidak memerlukan instalasi perangkat lunak tambahan.

2) Google Form dan Microsoft Excel

Google Form digunakan untuk pengumpulan data berupa kuesioner, sementara Microsoft Excel dipakai untuk menyimpan dan mengelola data sebelum dipindahkan ke Google Colab untuk analisis lanjut.

3.5 Teknik Analisis Data

1) Analisis Deskriptif Responden

Analisis ini digunakan untuk menggambarkan karakteristik umum responden serta pola jawaban pada setiap indikator. Variabel umum distribusi responden berupa jenis kelamin, usia, prodi, dan waktu online. Hasil analisis disajikan dalam tabel atau *pie chart.*

2) Analisis Korelasi Pearson

Digunakan untuk mengetahui hubungan antara variabel pengetahuan, sikap, dan perilaku keamanan digital. Uji korelasi menunjukkan seberapa kuat hubungan suatu variabel dengan variabel lain tanpa mempersoalkan apakah suatu variabel tertentu bergantung pada variabel lain [15].

3) Uji Perbedaan (Independent Sample T-Test)

Uji t digunakan untuk mengetahui apakah terdapat perbedaan signifikan antara mahasiswa Teknik Informatika dan Non-TI dalam hal tingkat pengetahuan, sikap, maupun perilaku. Uji ini sesuai digunakan untuk mengetahui apakah terdapat perbedaan dalam nilai antara dua sampel yang tidak memiliki hubungan satu sama lain [16].

DOI: https://doi.org/10.31004/riggs.v4i4.4516

4) Regresi Linier Sederhana

Analisis regresi digunakan untuk menentukan tingkat korelasi antara variabel yang akan diuji [17], variabel mana yang berpengaruh terhadap perilaku keamanan digital, misalnya apakah pengetahuan atau sikap memberikan pengaruh yang lebih besar.

4. Hasil dan Diskusi

4.1. Pembersihan (*Cleaning*)

Pada tahap pembersihan (*cleaning*), data mentah disiapkan agar layak digunakan untuk analisis dengan cara memperbaiki, menghapus, atau menyesuaikan nilai-nilai yang tidak konsisten. Proses ini mencakup mengatasi data hilang, mendeteksi kesalahan input, menormalkan format kolom, serta memastikan setiap data berada dalam bentuk yang seragam. Tujuannya adalah menghasilkan dataset yang rapi, akurat, dan siap dianalisis tanpa mengganggu hasil atau menyebabkan bias.

simpan_password_di_browser	mengenali_phishing	update_sistem_secara_rutin	gunakan_jaringan_publik	kesadaran_privasi_media_sosial	skor_pengetahuan	skor_sikap	skor_perilaku
Iseng	4	4	Kadang	3	5	5	5
Kadang	3	4	Jarang	5	5	3	5
Iseng	4	3	Kadang	4	3	3	3
Kadang	3	4	Tidak Pernah	3	4	3	4
Kadang	3	4	Iseng	5	4	4	4

Gambar 2. Output pembersihan data Non-IT

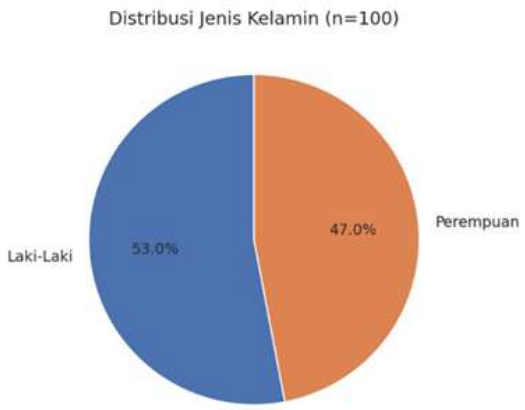
Output menghasilkan file dataset bersih dan menampilkan hasil output lanjutan dari tabel data Non-IT, berisi jawaban responden yang memuat informasi terkait perilaku keamanan digital, seperti frekuensi menyimpan sandi di browser, kemampuan mengenali phishing, kebiasaan memperbarui sistem, penggunaan jaringan publik, serta tingkat kesadaran privasi di media sosial. Data ini juga mencakup skor pengetahuan, sikap, dan perilaku keamanan siber setiap responden sebagai bahan analisis lebih mendalam.

4.2. Deskriptif Responden

Penelitian ini melibatkan 100 responden, yang terdiri dari 50 mahasiswa Program Studi Teknik Informatika (TI) dan 50 mahasiswa Non-Teknik Informatika (Non-TI). Penyajian deskriptif responden mencakup variabel jenis kelamin, program studi, usia, serta durasi penggunaan internet per hari.

1) Distribusi Jenis Kelamin

Berdasarkan hasil analisis, responden terdiri dari 53% laki-laki dan 47% perempuan. Komposisi ini menunjukkan bahwa proporsi responden laki-laki sedikit lebih besar dibandingkan perempuan.



Gambar 3. Distribusi Jenis Kelamin Responden

DOI: https://doi.org/10.31004/riggs.v4i4.4516

2) Distribusi Program Studi

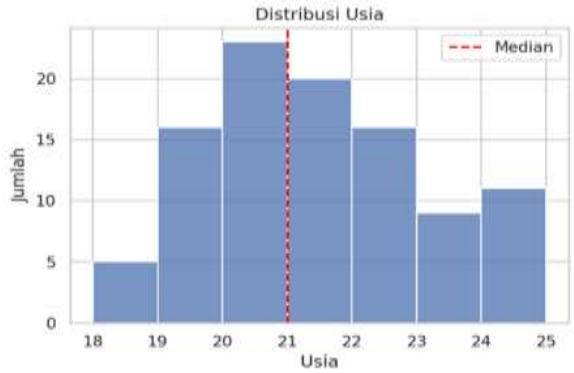
Sebanyak 50% responden merupakan mahasiswa Teknik Informatika, dan 50% lainnya berasal dari berbagai program studi Non-TI. Pembagian yang seimbang ini memastikan hasil analisis komparatif antara TI dan Non-TI dapat dilakukan secara proporsional.

Tabel 1. Distribusi Program Studi Responden

Program	Jumlah	Percent
Teknik Informatika	50	50
Non-Teknik Informatika	50	50

3) Distribusi Usia Responden

Rentang usia responden berada pada interval 18 hingga 24 tahun, dengan usia rata-rata 20,97 tahun. Nilai median adalah 21 tahun, sedangkan kuartil menunjukkan bahwa sebagian besar responden berada pada kelompok usia 20–22 tahun. Penyebaran usia tergolong merata dan mencerminkan karakteristik umum mahasiswa aktif.



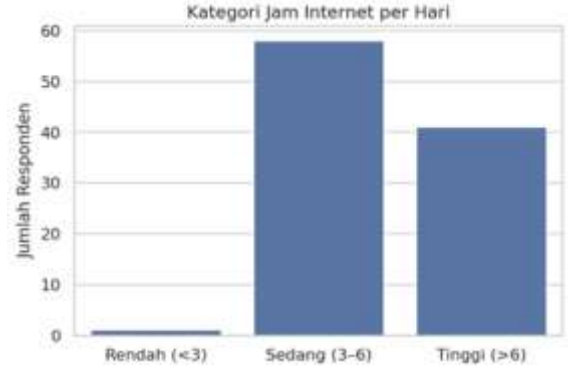
Gambar 4. Distribusi Usia Responden

4) Durasi Penggunaan Internet per Hari

Responden memiliki aktivitas penggunaan internet yang cukup tinggi, dengan rata-rata 6,21 jam per hari. Nilai minimum penggunaan adalah 2 jam, sedangkan maksimum mencapai 10 jam per hari. Berdasarkan kategorisasi durasi penggunaan internet, diperoleh hasil sebagai berikut:

- Rendah (< 3 jam) : 1 responden (1%)
- Sedang (3–6 jam) : 58 responden (58%)
- Tinggi (> 6 jam) : 41 responden (41%)

Mayoritas mahasiswa berada pada kategori sedang dan tinggi, menunjukkan intensitas penggunaan internet yang cukup besar di kalangan responden.



Gambar 5. Kategori Durasi Penggunaan Internet per Hari

DOI: https://doi.org/10.31004/riggs.v4i4.4516

Secara keseluruhan, karakteristik responden menunjukkan populasi yang seimbang antara mahasiswa TI dan Non-TI serta distribusi jenis kelamin yang relatif proporsional. Usia responden berada dalam rentang usia mahasiswa aktif pada umumnya, dan penggunaan internet harian menunjukkan tingkat intensitas yang tinggi. Temuan deskriptif ini memberikan konteks awal yang penting sebelum dilakukan analisis lanjutan terkait hubungan antarvariabel dan perbedaan antara kelompok TI dan Non-TI.

4.3 Analisis rata-rata kesadaran

Sebelum menganalisis skor rata-rata kesadaran, setiap dataset diberi label kategori "TI" dan "Non-TI" untuk memudahkan identifikasi kelompok dalam analisis berikutnya. Setelah itu, dataset digabungkan menjadi satu kesatuan dalam sebuah dataframe baru. Setelah data dari kedua kelompok mahasiswa berhasil digabungkan, langkah selanjutnya adalah menghitung rata-rata skor kesadaran melalui variabel mean_scores berdasarkan tiga indikator utama, yaitu skor_pengetahuan, skor_sikap, dan skor_perilaku. Hasil perhitungan kemudian ditampilkan dalam bentuk tabel.

```
mean_scores = df.groupby("Kelompok")[["skor_pengetahuan", "skor_sikap", "skor_perilaku"]].mean()

print("Rata-rata Skor Kesadaran per Kelompok:")
mean_scores

Rata-rata Skor Kesadaran per Kelompok:
```

Kelompok	skor_pengetahuan	skor_sikap	skor_perilaku
Non-TI	3.68	3.82	3.88
TI	4.10	4.04	4.04

Gambar 6. Output rata-rata skor kesadaran

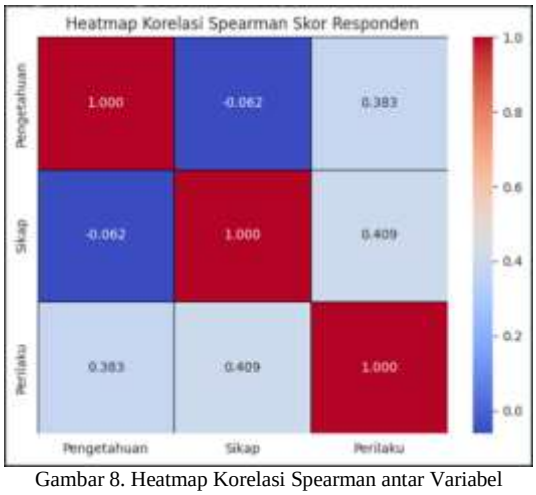
Setelah mendapatkan nilai rata-rata, langkah selanjutnya adalah memvisualisasikan hasil dalam bentuk diagram batang. Hasil visualisasi menunjukkan bahwa mahasiswa TI memiliki skor yang lebih tinggi pada tiga indikator dibandingkan mahasiswa Non-TI. Pada indikator pengetahuan, mahasiswa TI memperoleh skor rata-rata 4,10, lebih tinggi dibandingkan kelompok Non-TI, yaitu 3.68. Pada indikator sikap, mahasiswa TI juga sedikit lebih unggul, dengan skor rata-rata 4.04 dibandingkan 3.82 pada mahasiswa Non-TI. Hal serupa terlihat pada indikator perilaku, di mana mahasiswa TI meraih skor rata-rata 4.04, sedikit lebih tinggi dibandingkan mahasiswa Non-TI yang mencapai 3.88. Analisis skor rata-rata dan hasil pada grafik menunjukkan bahwa background studi memengaruhi kesadaran keamanan data, dengan mahasiswa TI lebih menyadari ketiga aspek.

Gambar 7. Hasil grafik skor rata-rata

4.4 Analisis Korelasi

Hasil korelasi Spearman ditunjukkan pada Gambar 1. Korelasi antara pengetahuan dan sikap sangat lemah dan tidak signifikan ($r = -0.062$). Sebaliknya, pengetahuan dan perilaku memiliki korelasi positif sedang ($r = 0.383$), begitu pula sikap dan perilaku ($r = 0.409$), keduanya signifikan ($p < 0.05$).

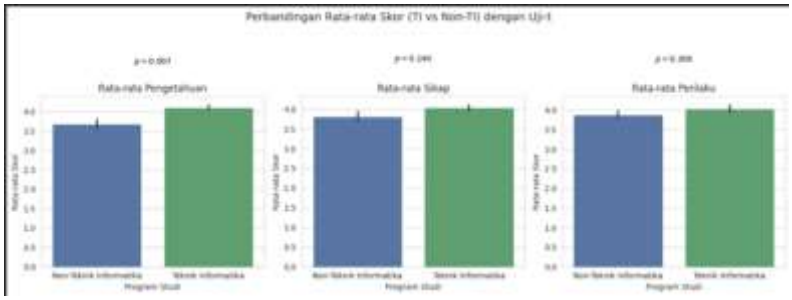
DOI: https://doi.org/10.31004/riggs.v4i4.4516



Gambar 8. Heatmap Korelasi Spearman antar Variabel

4.5 Analisis Komparatif (Uji-t)

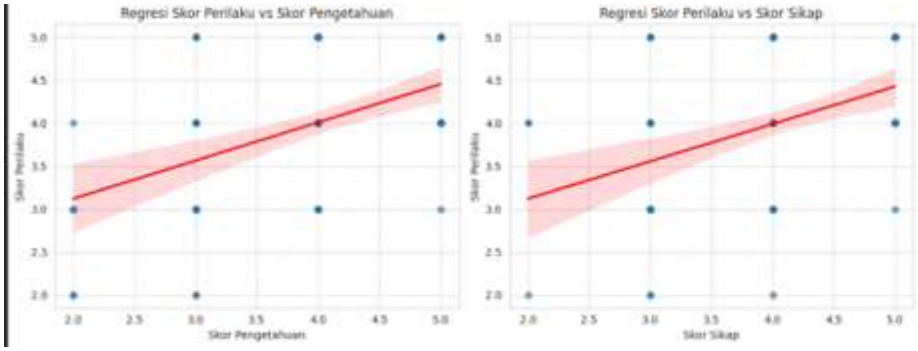
Perbandingan antara kelompok TI dan Non-TI ditunjukkan pada Gambar 9. Hanya skor pengetahuan yang menunjukkan perbedaan signifikan (p = 0.007). Tidak terdapat perbedaan signifikan pada skor sikap (p = 0.140) dan perilaku (p = 0.306).



Gambar 9. Perbandingan Rata-rata Skor TI vs Non-TI dengan Uji-t

4.6 Analisis Regresi

Hubungan antara variabel prediktor dan perilaku ditunjukkan pada Gambar 10. Baik pengetahuan maupun sikap memiliki hubungan positif dengan perilaku. Garis regresi menunjukkan bahwa sikap sedikit lebih kuat pengaruhnya dibanding pengetahuan.



Gambar 10. Plot Regresi Perilaku terhadap Pengetahuan dan Sikap

Perilaku mahasiswa dipengaruhi oleh pengetahuan dan sikap, namun hubungan keduanya tidak kuat, sehingga perilaku kemungkinan ditentukan juga oleh faktor lain seperti pengalaman, norma sosial, atau motivasi. Lemahnya hubungan pengetahuan–sikap menunjukkan bahwa peningkatan informasi saja tidak cukup untuk membentuk sikap yang positif. Meskipun mahasiswa TI memiliki pengetahuan lebih tinggi, hal tersebut tidak menghasilkan

DOI: https://doi.org/10.31004/riggs.v4i4.4516

perbedaan sikap maupun perilaku dibanding Non-TI. Regresi menunjukkan bahwa sikap sedikit lebih berpengaruh terhadap perilaku daripada pengetahuan, menegaskan pentingnya aspek afektif. Secara keseluruhan, perubahan perilaku memerlukan pendekatan yang tidak hanya berfokus pada pengetahuan, tetapi juga pembentukan sikap dan pengalaman nyata.

5. Kesimpulan

Penelitian ini menunjukkan bahwa tingkat kesadaran keamanan data pribadi mahasiswa berada pada kategori baik, dengan mahasiswa Teknik Informatika (TI) memiliki skor pengetahuan, sikap, dan perilaku yang lebih tinggi dibandingkan mahasiswa Non-TI, meskipun perbedaan signifikan hanya terlihat pada aspek pengetahuan. Korelasi menegaskan bahwa baik pengetahuan maupun sikap memiliki hubungan positif sedang terhadap perilaku keamanan digital, sementara hubungan pengetahuan dengan sikap sangat lemah sehingga peningkatan informasi semata tidak cukup untuk membentuk perilaku yang aman. Regresi juga memperlihatkan bahwa sikap sedikit lebih dominan dalam memengaruhi perilaku dibanding pengetahuan, menandakan bahwa perubahan perilaku lebih dipengaruhi oleh kesadaran personal dan keterlibatan emosional daripada pemahaman teknis saja. Berdasarkan temuan ini, disarankan agar upaya peningkatan keamanan digital di perguruan tinggi tidak hanya berfokus pada penyampaian materi teoretis, tetapi juga menekankan pembentukan sikap melalui pelatihan praktis, simulasi ancaman, kampanye kesadaran, serta integrasi literasi keamanan digital pada program studi non-TI untuk mengurangi kesenjangan pemahaman dan mendorong terbentuknya perilaku digital yang lebih aman dan konsisten.

Referensi

1. T. K. Utami, K. A. Putri, S. O. Suryanto, and F. Asriani, “Personal Data Breach Cases In Indonesia : Perspective Of Personal Data Protection Law,” *Customary Law Journal*, vol. 2, no. 2, pp. 21–21, Feb. 2025. doi: https://doi.org/10.47134/jcl.v2i2.3742.
2. Peraturan Pemerintah Republik Indonesia, “Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik”, Okt. 04, 2019.
3. T. Tan, H. Sama, T. Wibowo, G. Wijaya, and O. E. Aboagye, “Kesadaran Keamanan Siber pada Kalangan Mahasiswa Universitas di Kota Batam,” *Jurnal Teknologi dan Informasi*, vol. 14, no. 2, pp. 163–173, Sep. 2024. doi: https://doi.org/10.34010/jati.v14i2.12518.
4. M. A. A. Affan, M. Fronita, E. Saputra, M. L. Hamzah, and Zarnelly, “Measuring The Level of Cybersecurity Awareness of Social Media Users Among Students,” *INOVTEK Polbeng - Seri Informatika*, vol. 10, no. 1, pp. 134–145, Dec. 2024. doi: https://doi.org/10.35314/vycq9t65.
5. M. Mirna, Judhariksawan, and Maskum, “ANALISIS PENGATURAN KEAMANAN DATA PRIBADI DI INDONESIA,” *JURNAL ILMIAH LIVING LAW*, vol. 15, no. 1, pp. 16–30, Jan. 2023. doi: https://doi.org/10.30997/jill.v15i1.4726.
6. Novia et al. “Sosialisasi Kesadaran Keamanan Digital di Era Revolusi Industri 4.0,” *Jumat Informatika: Jurnal Pengabdian Masyarakat*, vol. 5, no. 1, pp. 49–55, Apr. 2024. doi: https://doi.org/10.32764/abdimasif.v5i1.4525.
7. Nopriadi, “Menjaga Privasi Digital: Studi Tentang Kesadaran Mahasiswa dalam Perlindungan Data Pribadi di Media Sosial,” *Polygon : Jurnal Ilmu Komputer dan Ilmu Pengetahuan Alam*, vol. 2, no. 6, pp. 87–97, Nov. 2024. doi: https://doi.org/10.62383/polygon.v2i6.297.
8. D. S. Y. Putra, M. L. Amanda, M. F. Al-Amien, “Risiko Keamanan TI Akibat Kelalaian Mahasiswa Non-IT dalam Keamanan Siber: Tinjauan Etis dan Solusi Preventif,” Jun. 10, 2025.
9. F. P. S. Surbakti, “Edukasi Keamanan Siber Berdigital dengan Aman,” *Prima Abdika Jurnal Pengabdian Masyarakat*, vol. 4, no. 4, pp. 868–878, Dec. 2024. doi: https://doi.org/10.37478/abdika.v4i4.4967.
10. M. D. Algamar and A. I. I. Ampri, “Hak Untuk Dilupakan: Penghapusan Jejak Digital Sebagai Perlindungan Selebriti Anak dari Bahaya Deepfake,” *JURNAL YUSTIKA: MEDIA HUKUM DAN KEADILAN*, vol. 25, no. 01, pp. 25–39, Aug. 2022. doi: https://doi.org/10.24123/yustika.v25i01.5091.
11. Y. Daeng, “Analisis Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia,” *Innovative: Journal of Social Science Research*, vol. 3, no. 6, pp. 1135–1145, Nov. 2023.
12. E. S. B. Herawati, Z. Mustofa, M. N. Sari, R. N. P. Mirsa, A. P. Widiyan, and Y. Astuti, “Edukasi Digital Safety Dalam Meningkatkan Kecakapan Bermedia Digital Siswa,” *LAMAHU Jurnal Pengabdian Masyarakat Terintegrasi*, vol. 3, no. 1, pp. 47–54, Feb. 2024. doi: https://doi.org/10.37905/ljpmt.v3i1.24090.
13. P. Sidiq, “Literasi Digital Pada Masyarakat: Etis Bermedia Sosial, Aman dan Nyaman,” *Jurnal Pengabdian Literasi Digital Indonesia*, vol. 3, no. 2, pp. 89–96, Oct. 2024. doi: https://doi.org/10.57119/abdimas.v3i2.125.
14. A. Riyanto and D. P. Arini, “ANALISIS DESKRIPTIF QUARTER-LIFE CRISIS PADA LULUSAN PERGURUAN TINGGI UNIVERSITAS KATOLIK MUSI CHARITAS,” *Jurnal Psikologi Malahayati*, vol. 3, no. 1, Mar. 2021. doi: https://doi.org/10.33024/jpm.v3i1.3316.
15. F. Jabnabillah and N. Margina, “ANALISIS KORELASI PEARSON DALAM MENENTUKAN HUBUNGAN ANTARA MOTIVASI BELAJAR DENGAN KEMANDIRIAN BELAJAR PADA PEMBELAJARAN DARING,” *JURNAL SINTAK*, vol. 1, no. 1, pp. 14–18, Sep. 2022.
16. D. Juliansyah, Hannie, and A. A. Hendriadi, “Penerapan Uji-T Independen untuk Sistem Chatbot Gaotek,” *Jurnal Syntax Admiration*, vol. 5, no. 6, pp. 2137–2146, Jun. 2024. doi: https://doi.org/10.46799/jsa.v5i6.1224.
17. L. Nurlia, “PENGARUH LOKASI TERHADAP KEPUTUSAN PEMBELIAN PENGUNJUNG DI MINIMARKET MENGGUNAKAN METODE REGRESI LINIER,” *Jurnal Riset Sistem Informasi dan Teknologi Informasi (JURSISTEKNI)*, vol. 3, no. 1, pp. 1–12, Jan. 2021. doi: https://doi.org/10.52005/jursistekni.v3i1.75.

DOI: https://doi.org/10.31004/riggs.v4i4.4516