Pengukuran Tingkat Kesadaran Keamanan Informasi Pada Mahasiswa Fakultas Informatika Menggunakan *Human Aspect of Information Security Questionnaire (HAIS-Q)* di Universitas Telkom Bandung

Tugas Akhir

diajukan untuk memenuhi salah satu syarat memperoleh gelar sarjana pada

Program Studi S1 Teknologi Informasi

Fakultas Informatika

Universitas Telkom

1303202099

Gregorio Bonggal Noveno Alvito

Program Studi Sarjana Teknologi Informasi
Fakultas Informatika
Universitas Telkom
Bandung
2024

LEMBAR PERNYATAAN

Dengan ini saya, Gregorio Bonggal Noveno Alvito menyatakan sesungguhnya bahwa Tugas Akhir saya dengan judul **Pengukuran Tingkat Kesadaran Keamanan Informasi Pada Mahasiswa Fakultas Informatika Menggunakan Human Aspect of Information Security Questionnaire (HAIS-Q) di Universitas Telkom Bandung** beserta dengan seluruh isinya adalah merupakan hasil karya sendiri, dan saya tidak melakukan penjiplakan yang tidak sesuai dengan etika keilmuan yang belaku dalam masyarakat keilmuan. Saya siap menanggung resiko/sanksi yang diberikan jika di kemudian hari ditemukan pelanggaran terhadap etika keilmuan dalam Laporan TA atau jika ada klaim dari pihak lain terhadap keaslian karya,

Bandung, 26 Juli 2024
Yang Menyatakan,

Gregorio Bonggal Noveno Alvito

LEMBAR PENGESAHAN

Pengukuran Tingkat Kesadaran Keamanan Informasi Pada Mahasiswa Fakultas Informatika Menggunakan *Human Aspect of Information Security Questionnaire (HAIS-Q)* di Universitas Telkom Bandung

Measurement the Level of Information Security Awareness Among Informatics College Students Using the Human Aspect of Information Security Questionnaire (HAIS-Q) at Telkom University Bandung

NIM: 1303202099

Gregorio Bonggal Noveno Alvito

Tugas akhir ini telah diterima dan disahkan untuk memenuhi sebagian syarat memperoleh gelar pada Program Studi Sarjana Teknologi Informasi

Fakultas Informatika

Universitas Telkom

Bandung, 26 Juli 2024

Menyetujui

Pembimbing I,	Pembimbing II,
Dr. FARISYA SETIADI, S.T., M.T.I.	MUHAMAD IRSAN, S.T., M.Kom.
21830002	23800001

Ketua Program Studi
Sarjana Teknologi Informasi

RIO GUNTUR UTOMO, S.T., M.T., Ph.D.
22900021

Pengukuran Tingkat Kesadaran Keamanan Informasi Pada Mahasiswa Fakultas Informatika Menggunakan Human Aspect of Information Security Questionnaire (HAIS-Q) di Universitas Telkom Bandung

Gregorio B N Alvito 1[1], Farisya Setiadi 2[1], Muhamad Irsan 3[2]
[1] Teknologi Informasi, Fakultas Informasika, Universitas Telkom , Indonesia,
ryonoveno@student.telkomuniversity.ac.id
[2] Teknologi Informasi, Fakultas Informasika, Universitas Telkom , Indonesia, farisyasetiadi@telkomuniversity.ac.id
[3] Teknologi Informasi, Fakultas Informasika, Universitas Telkom , Indonesia, irsanfaiz@telkomuniversity.ac.id

Abstract
On this study aims to evaluate the level of information security awareness of Telkom Informatics undergraduate students by adopting a mixed method approach. Quantitative data collection will be conducted through the HAIS-Q questionnaire which measures aspects such as password management, internet usage, and information handling. Qualitative data will complement this research to provide a more comprehensive understanding. The final results show that the overall level of information security awareness is good with an average of 85.24%, but there are shortcomings in the behavioral dimension, especially in internet usage and incident reporting, with an average score below 80%. Qualitative research through interviews revealed that although students understand security risks, they tend to ignore security practices when accessing information or using public Wi-Fi. Low points were also shown in the section on reporting incidents in the campus environment, where fear of prejudice and concerns of damaging social relationships may hinder their actions. This research shows that students need to improve their behavior to be more aware of information security especially in campus areas.
Keywords: college student, information security awareness, HAIS-Q, mixed method, Telkom University.

Abstrak
Penelitian ini bertujuan untuk mengevaluasi tingkat kesadaran keamanan informasi mahasiswa S1 Informatika Telkom dengan mengadopsi pendekatan mixed method. Pengumpulan data kuantitatif akan dilakukan melalui kuesioner HAIS-Q yang mengukur aspek-aspek seperti manajemen kata sandi, penggunaan internet, dan penanganan informasi. Data kualitatif akan melengkapi penelitian ini untuk memberikan pemahaman yang lebih komprehensif. Hasil akhir menunjukkan tingkat kesadaran keamanan informasi secara keseluruhan tergolong baik dengan rata-rata 85,24%, namun terdapat kekurangan pada dimensi perilaku, terutama dalam penggunaan internet dan pelaporan insiden, dengan nilai rata-rata di bawah 80%. Penelitian kualitatif melalui wawancara mengungkap bahwa meskipun mahasiswa memahami risiko keamanan, mereka cenderung mengabaikan praktik keamanan saat mengakses informasi atau menggunakan Wi-Fi publik. Poin yang rendah juga ditunjukkan pada bagian pelaporan insiden di lingkungan kampus, di mana ketakutan terhadap prasangka buruk dan kekhawatiran merusak hubungan sosial dapat menghambat tindakan mereka. Penelitian ini menunjukkan bahwa mahasiswa perlu meningkatkan perilaku mereka untuk lebih sadar akan keamanan informasi terutama di area kampus.

Kata kunci: HAIS-Q, mixed method, kesadaran keamanan informasi, mahasiswa, Universitas Telkom

---

I. PENDAHULUAN

Pada era digital ini pertukaran informasi merupakan proses utama dalam penggunaan teknologi setiap harinya [1]. Hal ini sejalan dengan peningkatan produksi informasi yang mengharuskan adanya komunikasi aman dan perlindungan data, seiring dengan perkembangan itu tingkat ancaman digital juga semakin canggih dan berisiko kerentanan pada data. Jika keamanan sistem informasi tidak terjaga dengan baik, beberapa risiko akan muncul dan

menjadi penghalang pada organisasi dalam mencapai tujuannya, hal itu juga dapat menyebabkan beberapa masalah muncul seperti kerugian materil, pelanggaran hukum, dan rusaknya integritas yang sudah terbangun dengan baik [2]. Oleh karena itu, perlindungan keamanan informasi merupakan suatu hal mutlak yang harus dihadapi serius oleh seluruh anggota pada organisasi tersebut. Dengan adanya keselamatan dan keamanan pada lingkungan di mana informasi tersebut berada, integritas, ketersediaan, dan kerahasiaan informasi di perusahaan pasti akan terjamin [3].

Kasus seputar dampak negatif karena kurangnya kesadaran keamanan dan privasi sudah marak terjadi, termasuk di Indonesia, hal ini diakibatkan oleh faktor kurangnya pehamanan akan keamanan informasi dan privasi saat mendapatkan pesan dari orang yang tidak dikenal dan menerima tautan palsu yang mengarah ke situs web yang dibuat dengan tujuan membuat device korban terkena serangan malware, hal itu mengakibatkan pengambilan data secara ilegal hingga kerusakan internal pada device yang digunakan [4]. Serangan siber tidak hanya terjadi pada masyarakat awam. Pada 20 Juni 2024, masyarakat Indonesia digegerkan mengenai insiden Pusat Data Nasional (PDN) mengalami serangan siber yang mengakibatkan kebocoran data, dan 282 layanan yang dijalankan instansi pemerintahan, baik untuk urusan internal ataupun layanan masyarakat tidak dapat digunakan [5]. Faktor yang memengaruhi terjadinya insiden ini adalah infeksi ransomware yang terjadi di pusat data nasional, ketika perangkat telah terinfeksi ransomware hacker sebagai pelaku utama pada kasus ini "menyandera" data-data penting negara dengan tebusan sebesar 8 juta dollar Amerika atau sekitar 131 milliar rupiah untuk memberikan akses kembali kepada data-data yang telah diambil. Pada kasus ini perangkat dapat terinfeksi ransomware tentu diakibatkan karena kelalaian oknum, kelalaian tersebut dapat terjadi diantaranya dengan cara membuka link yang mencurigakan, membuka website yang tidak terpercaya, jarang melakukan backup data-data.

Direktorat PUTI Universitas Telkom memiliki permasalahan mengenai tingkat kesadaran para mahasiswa terhadap manajemen keamanan informasi, menurut PUTI tingkat kesadaran mahasiswa terhadap manajemen keamanan informasi masih rendah. PUTI memiliki sistem yang dapat mendeteksi perangkat mahasiswa yang sedang menggunakan akun SSO Universitas Telkom, pada sistem tersebut terdeteksi bahwa sebagian besar perangkat pernah, dan sedang terjangkit malware. Hal tersebut diduga karena mahasiwa mengakses dan mengunduh file atau aplikasi yang berbahaya dari sumber asing dan tidak tepercaya. Selain itu PUTI selama ini sering berfokus dalam kesadaran keamanan informasi pada karyawannya, hal itu dilakukan untuk memastikan bahwa staff yang menjaga keamanan informasi mahasiswa dan civitas akademik di Telkom memiliki pemahaman yang tinggi dan mendetail mengenai pekerjaannya. Selama ini PUTI belum melaksanakan pengukuran tingkat kesadaran keamanan informasi pada Mahasiswa di Universitas Telkom, hal ini juga yang mendasari penulis untuk melaksanakan penelitian tentang pengukuran tingkat kesadaran keamanan informasi mahasiswa di Universitas Telkom. Harapannya penelitian ini akan membantu PUTI dalam mengetahui seberapa besar atau rendahnya tingkat kesadaran keamanan informasi pada mahasiswa di Universitas Telkom. Mahasiswa di Universitas Telkom, memiliki peran penting dalam menjaga keamanan informasi di lingkungan kampus. Kesadaran keamanan informasi di kalangan mahasiswa menjadi hal yang sangat penting, karena dengan adanya tingkat kesadaran yang tinggi dapat membantu mencegah ancaman keamanan informasi, seperti kebocoran data dan serangan siber.

Oleh karena itu, untuk menghadapi permasalahan tersebut, pada penelitian ini akan dilakukan pengukuran tingkat kesadaran keamanan informasi pada mahasiswa Universitas Telkom menggunakan instrumen Human Aspect of Information Security Questionnaire (HAIS-Q). Tujuannya untuk mengevaluasi sejauh mana pemahaman dan kesadaran mahasiswa terhadap risiko keamanan informasi, dengan harapan dapat mengidentifikasi area yang perlu mendapat perbaikan. Dengan demikian, hasil dari penelitian ini diharapkan dapat memberikan wawasan yang lebih mendalam tentang aspek-aspek kritis yang mempengaruhi kesadaran keamanan informasi, sehingga langkah-langkah strategis dan efektif dapat diambil untuk meningkatkan keamanan informasi di Universitas Telkom.

II. TINJAUAN LITERATUR

Kesadaran Keamanan Informasi

Kesadaran keamanan informasi didefinisikan sebagai pengetahuan dan pemahaman anggota organisasi terkait potensi isu-isu yang berkaitan dengan keamanan informasi dan konsekuensinya [13]. Keamanan informasi dan perlindungan data telah menjadi kekhawatiran dan tantangan yang harus dihadapi oleh organisasi. Meskipun upaya dan dana yang dihabiskan oleh organisasi untuk mengamankan aset mereka, banyak insiden pelanggaran data dan kehilangan informasi yang terus terjadi setiap tahun [14]. Merupakan hal yang penting dan krusial bagi organisasi untuk memiliki program kesadaran keamanan untuk memastikan seluruh anggotanya sadar akan pentingnya melindungi informasi sensitif, apa yang harus mereka lakukan untuk menjamin informasi dengan aman, dan risiko kesalahan penanganan informasi. Pemahaman mengenai konsekuensi organisasi dan pribadi dari kesalahan penanganan informasi sensitif sangat penting bagi keberhasilan organisasi [1].

Keamanan Informasi

Keamanan informasi adalah tindakan untuk menjaga data-data penting agar tidak disalahgunakan atau hilang. Tujuan utamanya adalah untuk memastikan bisnis berjalan lancar tanpa hambatan yang berarti. Dengan menjaga keamanan data, kita bisa mencegah kerugian finansial dan reputasi yang mungkin terjadi akibat kebocoran data. Selain itu, keamanan informasi juga membantu kita untuk memanfaatkan peluang bisnis secara maksimal [16]. Informasi merupakan aset yang berharga pada suatu organisasi, karena informasi adalah sumber daya yang penting dan strategis dalam meningkatkan value bisnis pada organisasi tersebut. Oleh karena itu, perlindungan keamanan informasi merupakan suatu hal mutlak yang harus mendapat perhatian serius oleh seluruh jajaran tertinggi pimpinan hingga pegawai terkait [3]. Sistem informasi yang mengalami perubahan pada tujuan, proses, produk, atau hubungan lingkungan dengan maksud membantu organisasi mencapai keunggulan daya saing atau mengurangi kelemahan mereka sebagai sistem informasi strategi [3].

Human Aspect Information Security Questionnaire (HAIS-Q)

HAIS-Q adalah alat yang digunakan untuk mengukur tingkat kesadaran manusia terhadap keamanan informasi, yang dikumpulkan melalui metode kuisioner [15]. Instrumen ini berfokus pada tujuh area keamanan informasi, yang disebut sebagai area fokus. Area fokus ini telah dipilih dan disempurnakan selama pengembangan instrumen. Area fokus dari HAIS-Q meliputi Manajemen Password, Penggunaan Email, Penggunaan Internet, Penggunaan Media Sosial, Perangkat Bergerak, Penanganan Informasi, dan Pelaporan Kejadian. Setiap area fokus dibagi lebih lanjut menjadi tiga sub-area tertentu. Sebagai contoh, area fokus Manajemen Password berpusat pada sub-area berikut, "Menggunakan password yang sama", "Berbagi password", dan "Menggunakan password yang kuat". Setiap sub-area ini diukur melalui item pengetahuan, sikap, dan perilaku yang terpisah [15]. Alat ini dapat digunakan untuk mengukur pengetahuan, sikap, dan perilaku karyawan guna memberikan manajemen suatu patokan, yang kemudian dapat digunakan untuk mengevaluasi efektivitas berbagai strategi kontrol teknologi informasi (TI) [17].

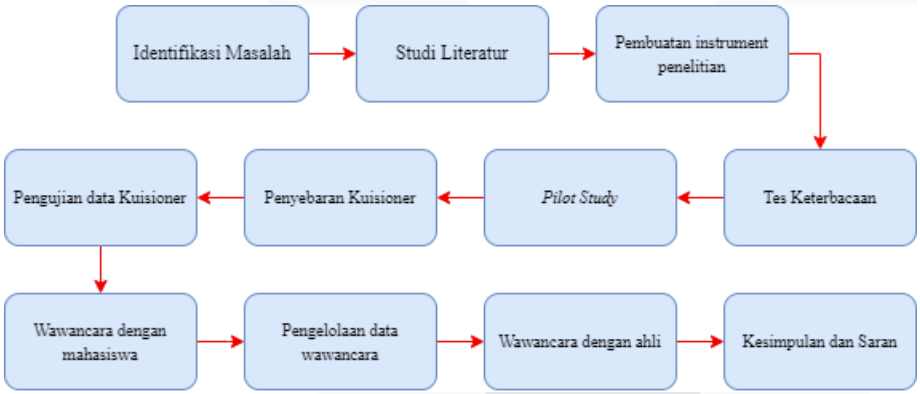
Mixed Method Research

Penelitian mixed method merupakan bidang studi yang sedang berkembang dan mungkin kurang dikenal daripada tradisi penelitian yang lebih konvensional. Mixed method didefinisikan sebagai suatu prosedur untuk mengumpulkan, menganalisis, dan menggabungkan data kuantitatif dan kualitatif pada tahap tertentu dari proses penelitian dalam satu studi guna memahami suatu masalah penelitian secara lebih lengkap [14][18]. Pada mixed method ini memiliki beberapa proses untuk mengevaluasi studi penelitian campuran, termasuk (a) menentukan apakah studi tersebut merupakan studi penelitian campuran; (b) memutuskan apakah metode campuran yang ketat digunakan; (c) mengidentifikasi pernyataan tujuan penelitian campuran, pertanyaan penelitian, jenis desain metode campuran, dan analisis data; dan (d) menentukan apakah penulis studi menyajikan informasi mengenai tantangan yang mungkin muncul selama studi (misalnya, ukuran sampel yang tidak seimbang, bagaimana peserta dipilih, langkah-langkah yang diambil sepanjang studi). Keempat poin ini penting untuk dipertimbangkan saat mengevaluasi

studi penelitian campuran; namun, masing-masing dari poin-poin ini tampak sangat luas. Seorang peneliti pemula mungkin melewatkan aspek-aspek studi dengan area yang begitu luas untuk diselidiki [19]. penelitian dimulai dari dari mengidentifikasi masalah, kemudian studi literatur, selanjutnya perancangan dan persiapan untuk pengumpulan data, setelah itu tahap pengumpulan data dari responden menggunakan cara penyebaran kuisioner dan wawancara, selanjutnya pengolahan data dan terakhi wawancara dengan ahli untuk mendapatkan saran guna mengembangkan kesadaran keamanann informasi kepada mahasiswa di Universitas Telkom.Dalam identifikasi masalah ini peneliti bertanya kepada Direktorat Pusat Teknologi informasi mengenai masala apa yang tengah dihadapi. Setelah itu mereka memberikan jawaban bahwa tingkat kesadaran para mahasiswa di Universitas Telkom masih rendah, dan usaha yang dilakukan oleh PUTI yaitu mengirimkan email kepada para mahasiswa mengenai pentingnya kesadaran dalam manajemen keamanan informasi. Setelah mengidentifikasi masalah yang dihadapi selanjutnya penulis melaksanakan studi literatur terhadap penelitian terdahulu. Pertama penulis mencari jurnal mengenai penelitian terdahulu yang berkaitan dan memiliki relevansi dengan masalah yang Tengah dihadapi oleh PUTI, setelah jurnal terkumpul selanjutnya melakukan analisis seperti apa masalah yang dihadapi pada penelitian terdahulu, tujuan dari penelitiannya, metode apa yang digunakan dalam penelitian tersebut, kekurangan dan kelebihan pada penelitian tersebut, hasil akhir yang diperoleh,pada penelitian terdahulu, dan saran dan kritik yang disampaikan. Studi literatur ini berguna untuk mempermudah dan memberikan wawasan dan teori yang dibutuhkan pada penelitian ini.

III. METODOLOGI PENELITIAN

Penelitian kuantitatif ini bertujuan untuk mengukur tingkat kesadaran keamanan informasi mahasiswa. Pengumpulan data melalui kuesioner, analisis data dengan statistik deskriptif dan inferensial, dan penarikan kesimpulan untuk memberikan saran untuk meningkatkan kesadaran keamanan data.



Gambar 1. Alur penelitian

A. Identifikasi Masalah

Dalam identifikasi masalah ini peneliti mewawancara salah satu staff Direktorat Pusat Teknologi informasi mengenai masalah apa yang tengah dihadapi. Setelah itu mereka memberikan jawaban bahwa tingkat kesadaran para mahasiswa di Universitas Telkom masih rendah, dan usaha yang dilakukan oleh PUTI yaitu mengirimkan email kepada para mahasiswa mengenai pentingnya kesadaran dalam manajemen keamanan informasi.

B. Studi Literatur

Setelah mengidentifikasi masalah yang dihadapi selanjutnya penulis melaksanakan studi literatur terhadap penelitian terdahulu. Pertama penulis mencari jurnal mengenai penelitian terdahulu yang berkaitan dan memiliki relevansi dengan masalah yang Tengah dihadapi oleh PUTI, setelah jurnal terkumpul selanjutnya melakukan analisis seperti apa masalah yang dihadapi pada penelitian terdahulu, tujuan dari penelitiannya,

metode apa yang digunakan dalam penelitian tersebut, kekurangan dan kelebihan pada penelitian tersebut, hasil akhir yang diperoleh,pada penelitian terdahulu, dan saran dan kritik yang disampaikan.

C. Pembuatan Instrumen Penelitian

Penelitian ini menggunakan HAIS-Q sebagai metode dalam pengukuran tingkat kesadaran keamanan informasi pada mahasiswa di Universitas Telkom. HAIS-Q memiliki tujuh fokus area [15]. Pertanyaan HAIS-Q dibagi menjadi tiga kategori yaitu: Knowledge(K), Attitude(A), dan Behaviour(B). Kuisioner ini terdiri dari 63 pertanyaan yang dikelompokan pada tujuh area fokus dan sub-area. Responden dapat memilih jawaban menggunakan skala likert yaitu memilih dalam skala 1-5.

D. Pengujian data kuisioner

Setelah data kuisioner terkumpul sesuai jumlah minimal yang ditentukan maka akan dilakukan uji validitas dan reliabilitas dari data tersebut. Setelah uji tersebut menghasilkan angka yang positif, maka data akan di analisis untuk mengetahui seberapa baik dan berapa persen tingkat kesadaran keamanan informasi pada mahasiswa S1 Fakultas Informatika di Universitas Telkom Bandung.

E. Tes keterbacaan

Tes Keterbacaan ini merupakan proses dimana peneliti akan melakukan uji keterbacaan. Pada uji keterbacaan ini akan dilakukan oleh responden yang tidak termasuk dalam sampel penelitian. Guna dari uji keterbacaan ini untuk memastikan setiap pertanyaan dari kuisioner yang akan dibagikan dapat dipahami dengan mudah oleh para responden penelitian.(tambah jumlah responden 5 orang).

F. Pilot Study

Setelah tes keterbacaan memiliki hasil dan telah merevisi instrumen pada kuisioner, maka dilakukan pilot study. Hal ini mencakup pengumpulan data pada sampel yang telah ditentukan, setelah data telah terkumpul lalu dilakukan pengujian pada kuisioner mengenai tingkat reliabilitas dan validitasnya. Pilot Study dilaksanakan untuk menghindari terjadinya tidak valid atau tidak reliabelnya data penelitian, dan untuk mematangkan kuisioner sebelum disebarkan pada sampel sesungguhnya.

G. Penyebaran kuisioner

Setelah melewati tes keterbacaan, kemudian melalui pilot study dan dari hasil uji validitas dan reliabilitas menunjukan angka yang positif dan memenuhi syarat maka kuisioner akan disebarkan kepada para sampel responden sesuai dengan jumlah yang di tetapkan berdasarkan teknik sampling yang menggunakan rumus slovin.

H. Pengujian data kuisioner

Setelah data kuisioner terkumpul sesuai jumlah minimal yang ditentukan maka akan dilakukan uji validitas dan reliabilitas dari data tersebut. Setelah uji tersebut menghasilkan angka yang positif, maka data akan di analisis untuk mengetahui seberapa baik dan berapa persen tingkat kesadaran keamanan informasi pada mahasiswa S1 Fakultas Informatika di Universitas Telkom Bandung. Data akan di catat dalam bentuk excel. Setelah itu data akan dikelompokan lagi sesuai dengan dimensi KAB (Knowledge, Attitude, Behaviour).

I. Wawancara dengan mahasiswa

Ketika data kuantitatif telah selesai dikumpulkan dan diuji, kemudian peneliti akan melakasanakan wawancara dengan mahasiwa untuk mendapatkan alasan mengapa responden mengisi kuisioner sebelumnya, hal ini dilakukan untuk mengetahui lebih mendalam tentang kesadaran mahasiswa mengenai keamanan informasinya. Terdapat lima mahasiswa dari seluruh program studi yang ada pada S1 Fakultas Informatika Universitas Telkom Bandung. Narasumber wawancara dipilih secara acak berdasarkan nilai kuisioner terendah dari seluruh fokus area yang diteliti.

J. Pengolahan data wawancara

Data wawancara dengan mahasiswa akan dicatat dan dirangkum untuk selanjutnya dianalisis. Dari data analisis tersebut harapannya akan ditemukan alasan mendalam apa yang menjadi penyebab atau faktor dari tinggi atau rendahnya tingkat kesadaran keamanan informasi mahasiswa. Hasil dari analisis itu dirangkum dan dicatat untuk diberitahukan kepada ahli sebagai bahan diskusi untuk perbaikan kedepannya.

K. Wawancara dengan ahli

Setelah dilaksanakan wawancara dengan mahasiswa dan hasil wawancara tersebut dianalisis, maka akan dilaksanakan juga wawancara dengan ahli dibidangnya. Narasumber ahli yang dipilih merupakan ahli yang memiliki pemahaman yang luas dan mendalam mengenai keamanan informasi. Kriteria yang dipilih untuk wawancara yaitu, ahli yang berpengalaman dan telah menempuh pendidikan minimal S2 dan mengajar mata kuliah mengenai information security atau cybersecurity dengan topik hasil wawancara yang telah dilaksanakan pada beberapa responden , Hal ini dilaksanakan untuk mendapatkan saran untuk perbaikan terhadap kesadaran keamanan informasi pada mahasiswa di Universitas Telkom kedepannya.

L. Kesimpulan dan saran

Tahapan terakhir dari penelitian ini yaitu menghasilkan kesimpulan dari seluruh proses yang telah dilaksanakan, mulai dari data kuantitatif atau pengisian kuisioner oleh mahasiswa dan kualitatif untuk mendapatkan jawaban mendalam mengenai alasan mahasiswa dalam menjawab pertanyaan kuisioner. Setelah seluruh rangkaian penelitian mendapatkan hasil, kemudian dirumuskanlah saran untuk perbaikan kedepannya tentunya menggunakan pendapat, saran dari ahli dibidangnya.

IV. HASIL DAN PEMBAHASAN

A. Hasil data *Pilot Testing*

Sebelum mengumpulkan data yang sesungguhnya, penulis melakukan *pilot testing* terlebih dahulu pada mahasiswa Fakultas Informatika, Telkom University. Pilot test dilakukan untuk menguji validitas dan reliabilitas pada penelitian ini sebelum kuesioner disebarkan pada responden. Melakukan uji coba dengan sekelompok kecil partisipan yang berjumlah 35 orang, harapannya instrumen penelitian ini dapat berguna untuk memastikan kuisioner penelitian berfungsi dengan baik dan pertanyaan yang diajukan dapat dipahami.

Tabel 1. Demografi responden *pilot testing*

Kriteria	Kategori	Frekuensi	Persentase
Jurusan	S1 Informatika	8	22.8%
	S1 Teknologi Informasi	17	48.5
	S1 Rekayasa Perangkat Lunak	5	14.2%
	S1 Sains Data	5	14.2%
Usia	Laki-laki	23	65.7%
	Perempuan	12	34.2%
Angkatan	2019	3	8.5%
	2020	20	57.1%
	2021	11	31.4%
	2022	2	5.7%

1. Uji Validitas *Pilot Testing*

Uji validitas dari *pilot testing* memberikan hasil yang positif, seluruh instrumen memberi hasil yang valid, jadi tidak ada instrumen atau pertanyaan dari kuisioner yang perlu dihilangkan. Instrumen dapat disimpulkan valid jika nilai r hitung lebih besar dari r tabel, nilai r tabel adalah 0.3338 untuk derajat kebebasan (*Degree of Freedom*) 33. Nilai 0.3338 untuk 33 sampel didapatkan dari tabel *Critical Values for Pearson's Correlation Coefficient*. Untuk menentukan jumlah kebebasan menggunakan rumus:

$$df = n - 2 \quad (1)$$

Keterangan:
df = derajat kebebasan (Degree of freedom)
n = jumlah responden

Dengan ini diharapkan akan memberikan hasil pengujian yang lebih akurat karena seluruh instrumen dapat digunakan untuk mengukur tingkat kesadaran keamanan informasi pada mahasiswa. Adapun data yang diuji merupakan hasil dari tiga sub-unit yaitu *Knowledge, Attitude, dan Behaviour.*

Tabel 2. Hasil pilot testing *knowledge*

Knowledge								
Item	r hitung	r tabel	keterangan		item	r hitung	r tabel	keterangan
QK1	0,782831	0,3338	Valid		QK11	0,902079	0,3338	Valid
QK2	0,829372	0,3338	Valid		QK12	0,855001	0,3338	Valid
QK3	0,867769	0,3338	Valid		QK13	0,760915	0,3338	Valid
QK4	0,684624	0,3338	Valid		QK14	0,916932	0,3338	Valid
QK5	0,869048	0,3338	Valid		QK15	0,873178	0,3338	Valid
QK6	0,94149	0,3338	Valid		QK16	0,856467	0,3338	Valid
QK7	0,7384	0,3338	Valid		QK17	0,914119	0,3338	Valid
QK8	0,870297	0,3338	Valid		QK18	0,879291	0,3338	Valid
QK9	0,858164	0,3338	Valid		QK19	0,829403	0,3338	Valid
QK10	0,876456	0,3338	Valid		QK20	0,80742	0,3338	Valid
					QK21	0,856916	0,3338	Valid

Tabel diatas merupakan hasil dari uji validitas mengenai dimensi *knowledge* atau pengetahuan mahasiswa mengenai kesadaran keamanan informasi. Dari data diatas dapat dilihat seluruh pertanyaan pada kuisioner mendapatkan hasil yang valid, dimana seluruh r hitung lebih besar nilainya daripada r tabel.

Tabel 3. Hasil pilot testing *attitude*

Attitude								
Item	r hitung	r tabel	keterangan		item	r hitung	r tabel	keterangan
QA1	0,588606	0,3338	Valid		QA11	0,720659	0,3338	Valid
QA2	0,925318	0,3338	Valid		QA12	0,852707	0,3338	Valid
QA3	0,859243	0,3338	Valid		QA13	0,76522	0,3338	Valid
QA4	0,840872	0,3338	Valid		QA14	0,795209	0,3338	Valid
QA5	0,851064	0,3338	Valid		QA15	0,903991	0,3338	Valid
QA6	0,928362	0,3338	Valid		QA16	0,951523	0,3338	Valid
QA7	0,724521	0,3338	Valid		QA17	0,841921	0,3338	Valid
QA8	0,851577	0,3338	Valid		QA18	0,975285	0,3338	Valid
QA9	0,835441	0,3338	Valid		QA19	0,909412	0,3338	Valid
QA10	0,826711	0,3338	Valid		QA20	0,789049	0,3338	Valid
					QA21	0,859817	0,3338	Valid

Tabel diatas merupakan hasil dari uji validitas mengenai dimensi *attitude* atau sikap mahasiswa mengenai kesadaran keamanan informasi. Dari data diatas dapat dilihat seluruh pertanyaan pada kuisioner mendapatkan hasil yang valid, dimana seluruh r hitung lebih besar nilainya daripada r tabel.

Tabel 4. Hasil pilot testing *behaviour*

Behaviour								
Item	r hitung	r tabel	keterangan		item	r hitung	r tabel	keterangan
QB1	0,731444	0,3338	Valid		QB11	0,545791	0,3338	Valid
QB2	0,890704	0,3338	Valid		QB12	0,74348	0,3338	Valid
QB3	0,813327	0,3338	Valid		QB13	0,801369	0,3338	Valid
QB4	0,873299	0,3338	Valid		QB14	0,924984	0,3338	Valid
QB5	0,906533	0,3338	Valid		QB15	0,882944	0,3338	Valid
QB6	0,956279	0,3338	Valid		QB16	0,862256	0,3338	Valid
QB7	0,843835	0,3338	Valid		QB17	0,859712	0,3338	Valid
QB8	0,853718	0,3338	Valid		QB18	0,923613	0,3338	Valid
QB9	0,717881	0,3338	Valid		QB19	0,921768	0,3338	Valid
QB10	0,91067	0,3338	Valid		QB20	0,895994	0,3338	Valid
					QB21	0,930591	0,3338	Valid

Tabel diatas merupakan hasil dari uji validitas mengenai dimensi *behaviour* atau kebiasaann mahasiswa mengenai kesadaran keamanan informasi. Dari data diatas dapat dilihat seluruh pertanyaan pada kuisioner mendapatkan hasil yang valid, dimana seluruh r hitung lebih besar nilainya daripada r tabel.

2. Uji Reliabilitas *Pilot Testing*

Pada uji reliabilitas ini peneliti mengukur tiga dimensi pada penelitian ini yaitu *Knowledge, Attitude, Behaviour*, dan dari seluruh pengujian mengasilkan nilai *Cronbach's Alpha* yang baik yaitu diatas 0,8 dari total 21 pertanyaan untuk masing-masing dimensinya. Pada dimensi *Knowledge* memberikan hasil 0.829 nilai nilai ini menunjukkan seluruh item pada dimensi tersebut reliabel. Pada dimensi *Attitude* memberikan hasil 0.855 nilai ini menunjukkan seluruh item pada dimensi tersebut reliabel. Pada dimensi *Behaviour* memberikan hasil 0.848 nilai ini menunjukkan seluruh item pada dimensi tersebut reliabel.

Tabel 5. Hasil uji reliabilitas pilot testing

Uji Reliabilitas *Pilot Testing*		
Dimensi	Nilai *Alpha Cronbach*	Total Item
Knowledge	0.829	21
Attitude	0.855	21
Behaviour	0.848	21

B. Hasil Uji dan Analisis Data Penuh

1. Demografi Responden Data Penuh

Populasi pada penelitian ini merupakan mahasiswa aktif dari setiap jurusan yang berada di Fakultas Informatika Telkom University di Kota Bandung, yang diantaranya yaitu jurusan S1 Informatika, S1 Teknologi Informasi, S1 Rekayasa Perangkat Lunak, S1 Sains Data. Responden data penuh pada penelitian ini berjumlah 101 mahasiswa. Berasal dari mulai angkatan 2019 hingga 2023.

Tabel 6. Demografi responden data penuh

Kriteria	Kategori	Frekuensi	Persentase
Jurusan	S1 Informatika	25	24.8%
	S1 Teknologi Informasi	29	28.7%
	S1 Rekayasa Perangkat Lunak	21	20.8%
	S1 Sains Data	26	25.7%
Jenis Kelamin	Laki-laki	73	72.3%
	Perempuan	28	27.7%
Angkatan	2019	4	4%
	2020	47	46.5%
	2021	32	31.7%
	2022	16	15.8%
	2023	2	2%

2. Perhitungan Nilai Tingkat Kesadaran Keamanan Informasi

Setelah dilakukan perhitungan pada tingkat kesadaran keamanan informasi, setiap hasil juga telah diberi warna untuk menandai tingkat kesadaran keamanan informasi pada tingkatannya sesuai dengan warna. Terdapat tiga warna yaitu diantaranya, merah yang melambangkan tingkat kesadaran keamanan informasi berada pada angka < 59 atau berada pada level yang buruk, warna kuning yang melambangkan tingkat kesadaran keamanan informasi berada pada angka 60-79 atau berada pada level yang sedang, dan warna hijau yang melambangkan tingkat kesadaran keamanan informasi berada pada angka 80-100 atau berada pada level yang baik [29]. Berdasarkan tabel tersebut dapat dilihat bahwa rata-rata tingkat kesadaran keamanan informasi tergolong baik

karena berada diangka 85.24%, namun masih ada beberapa poin yang masih menandakan tingkat kesadaran keamanan informasi mahasiswa masih ditaraf yang sedang, hal itu dapat dilihat pada dimensi *behaviour* dimana fokus area *internet use dan incident report* masih menunjukkan nilai dibawah 80%.

Tabel 7. Hasil perhitungan tingkat kesadaran keamanan informasi

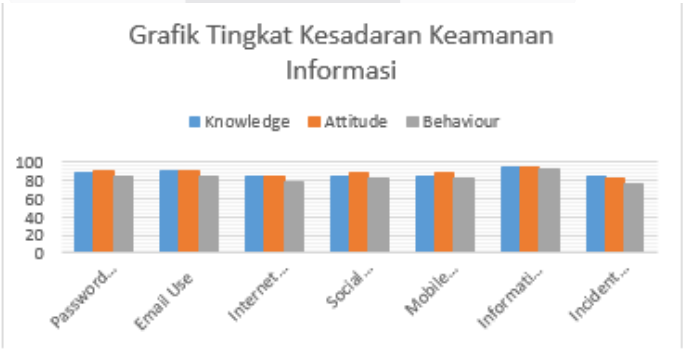
Fokus Area	Dimensi			Total *Awareness* (*Krueger & Kearney*)	Rata-Rata
	Knowledge (30%)	*Attitude* (20%)	*Behaviour* (50%)		
Password Management	89,17	90,56	84,68	87,20	85,24%
Email Use	90,62	90,75	84,95	87,81	
Internet Use	84,1	83,7	78,21	81,10	
Social Media Use	84,42	89,17	81,91	84,11	
Mobile Device	84,42	87,26	82,70	84,12	
Information Handling	93,33	93,66	91,41	92,43	
Incident Report	84,81	82,77	75,90	79,94	

Keterangan:
= Buruk (< 59)
= Sedang (60 - 79)
= Baik (≥ 80)

3. Analisis Tingkat Kesadaran Keamanan Informasi

Setelah dilakukannya perhitungan poin-poin yang berkaitan dengan tingkat kesadaran keamanan informasi pada mahasiswa berdasarkan kuisioner yang telah diisi oleh para responden, maka selanjutnya akan dilakukan analisis berdasarkan data dari kuisioner. Berdasarkan hasil perhitungan dan analisis pada data kuisioner ditemukan bahwa nilai area *information handling* meraih persentase paling tinggi dari seluruh fokus area, yaitu diangka 92,43Hal ini menunjukkan bahwa siswa cukup menyadari keamanan data. terutama pada area *information handling*, mahasiswa dapat memahami pentingnya menjaga informasi pribadi mereka dan mampu menerapkannya pada saat berkuliah.

Namun, terdapat beberapa area yang perlu mendapat perhatian lebih lanjut, yaitu *Incident Report*. Persentase yang paling rendah pada area ini menunjukkan bahwa masih banyak mahasiswa yang belum paham pentingnya melaporkan insiden keamanan informasi. Hal ini dapat berakibat pada kurangnya tindakan pencegahan terhadap pelanggaran atau pengabaian peraturan keamanan di lingkungan kampus.



Gambar 2. Grafik Tingkat kesadaran keamanan informasi mahasiswa .

- ***Password Management***

Pada fokus area *password management* mendapatkan total persentase tingkat kesadaran keamanan informasi sebesar 87,20%, angka ini masuk dalam kategori yang baik karena berada diatas 80%. Nilai ini menunjukkan bahwa pada penelitian ini para responden telah memahami pentingnya untuk menjaga dan memiliki password yang kuat untuk digunakan pada akun perkuliahannya, namun masih ada beberapa responden yang kurang menyadari dan memahami pentingnya memiliki password yang kuat pada akun perkuliahannya. Beberapa responden masih menggunakan password yang lemah seperti kurangnya variasi pada penggunaan huruf besar dan huruf kecil, karakter yang digunakan, dan angka yang masih berhubungan dengan data pribadi seperti tanggal lahir. Tetapi karena adanya kebijakan dari Universitas Telkom dalam pemilihan kata sandi, sehingga rata-rata mahasiswa memiliki kata sandi yang cukup kuat tetapi belum sampai tahap sangat kuat.

- ***Email Use***

Pada fokus area *email use* mendapatkan total persentase tingkat kesadaran keamanan informasi sebesar 87,81%, angka ini masuk dalam kategori yang baik karena berada diatas 80%. Nilai ini menunjukkan bahwa pada penelitian ini sebagian besar responden memiliki pengetahuan dan kesadaran yang baik ketika menggunakan email pada akun perkuliahannya. Namun, pada beberapa poin, mahasiswa masih menunjukkan kekurangan dalam praktik keamanan, seperti kurang waspada terhadap membuka link dari email yang sumbernya tidak dikenal, membuka lampiran dari sumber yang tidak dikenal, serta kurang berhati-hati membuka link meskipun sumbernya dari teman, atau orang terdekat yang dia kenal. Walaupun pada fokus area ini mendapatkan nilai yang baik, tetapi perlu adanya peningkatan kesadaran keamanan pada penggunaan email ini, karena resiko yang besar dapat mengancam jika mahasiswa tidak memiliki pengetahuan yang baik ketika menggunakan emailnya.

- ***Internet Use***

Pada fokus area *internet use* mendapatkan total persentase tingkat kesadaran keamanan informasi sebesar 81,10%, angka ini masuk dalam kategori yang baik karena berada diatas 80%. Nilai ini menunjukkan bahwa pada penelitian ini sebagian besar responden memiliki pengetahuan dan kesadaran yang baik ketika menggunakan internet. Namun pada dimensi *behaviour* atau kebiasaan mahasiswa mendapatkan persentase sebesar 78,21%, poin ini berada pada tingkatan sedang karena berada dibawah 80%. Pada poin ini dapat dilihat bahwa mahasiswa memiliki pengetahuan dan sikap yang baik ketika menggunakan internet, namun masih kurang pada prakteknya.

Rata-rata mahasiswa masih memiliki kebiasaan yang kurang baik ketika menggunakan internet di kampus maupun di tempat umum. Berdasarkan data pada kuisioner rata-rata mahasiswa selain mendapat materi dari LMS, untuk membantu perkuliahannya mereka mengunduh materi pembelajaran dari *website* yang menyediakan file itu. Kemudian mahasiswa juga ketika menggunakan *wifi* atau internet kampus, mereka tidak hanya membuka *website* untuk perkuliahan seperti LMS, IGracias, dll, tetapi mereka membuka situs lain diluar perkuliahan menggunakan *wifi* kampus atau publik. Selain itu sebagian mahasiswa juga kurang berhati-hati ketika memasukkan informasi pada sebuah *website* tanpa memperhatikan atau menilai terlebih dahulu keamanan keamanan situ yang mereka buka.

- ***Social Media Use***

Pada fokus area *social media use* mendapatkan total persentase tingkat kesadaran keamanan informasi sebesar 84,11%, angka ini masuk dalam kategori yang baik karena berada diatas 80%. Nilai ini menunjukkan bahwa pada penelitian ini sebagian besar responden memiliki pengetahuan dan kesadaran yang baik ketika menggunakan media sosial pribadi sehari-harinya. Rata-rata mahasiswa telah memiliki pengetahuan, sikap, dan kebiasaan yang baik ketika menggunakan media sosialnya. Penggunaan media sosial oleh mahasiswa dikategorikan baik karena pada kuisioner dari ketika dimensi yaitu, *knowledge*, *attitude*, *behaviour*, seluruhnya mendapatkan nilai rata-rata 84,11% dengan masing-masing dimensinya mendapatkan nilai diatas 80%.

Selain memiliki pengetahuan yang baik mengenai pengaturan privasi dan kesadaran akan konsekuensi dari aktivitas mereka lakukan di media sosial, mahasiswa juga menunjukkan sikap yang positif ketika menggunakan platform tersebut. Para mahasiswa cenderung berhati-hati dalam mengunggah informasi yang berkaitan dengan perkuliahan, menunjukkan kesadaran akan pentingnya menjaga privasi dan keamanan data pribadi mereka. Perilaku yang tercermin dari hasil penelitian ini menunjukkan bahwa mahasiswa tidak hanya memiliki baik dalam teori, tetapi juga mampu menerapkannya dalam kehidupan sehari-hari.

- ***Mobile Device***

Pada fokus area *mobile device* mendapatkan total persentase tingkat kesadaran keamanan informasi sebesar 84,12%, angka ini masuk dalam kategori yang baik karena berada diatas 80%. Nilai ini menunjukkan bahwa pada fokus area ini sebagian besar responden memiliki pengetahuan dan kesadaran yang baik ketika menggunakan perangkat mobile untuk sehari-hari dan ketika sedang melaksanakan perkuliahan. Seluruh fokus area berada pada nilai yang baik seperti, pada area *knowledge* mendapatkan nilai rata-rata 84,42%, fokus area *attitude* mendapatkan nilai rata-rata 87,26%, serta fokus area *behaviour* mendapatkan nilai rata-rata 82,70%. Dari seluruh nilai yang diperoleh menggambarkan mahasiswa memiliki pengetahuan, sikap, dan prakter yang baik untuk menggunakan perangkat mobilenya.

Mahasiswa memiliki pengetahuan yang baik mengenai pentingnya tidak meninggalkan perangkat mobile pribadi ketika sedang berada di tempat umum. Selain itu mahasiswa juga paham pentingnya mencegah mengirimkan informasi penting terutama terkait perkuliahan melalui jaringan *wifi* publik. Terakhir mahasiswa juga memiliki pemahaman, sikap, dan praktek yang baik untuk berhati-hati ketika sedang mengerjakan dokumen penting untuk tidak terlihat oleh orang lain, mereka paham resiko yang dapat terjadi jika dokumen pentingnnya dapat dengan mudah terlihat oleh orang lain.

- ***Information Handling***

Pada fokus area *information handling* mendapatkan total persentase tingkat kesadaran keamanan informasi sebesar 92,43%, angka ini masuk dalam kategori yang baik karena berada diatas 80%. Nilai ini menunjukkan bahwa pada penelitian ini sebagian besar responden memiliki pengetahuan dan kesadaran yang baik ketika menangani informasi penting dan sensitif terkait perkuliahannya. Dari seluruh fokus area, *information handling* mendapatkan nilai paling tinggi. Seluruh dimensi pada fokus area ini mendapatkan nilai diatas 90%. Pada dimensi *knowledge* total persentase rata-rata berada pada angka 93,33%, dimensi *attitude* mendapatkan persentase rata-rata 93,66%, dan pada dimensi *behaviour* total persentase rata-rata berada pada nilai 91,41%.

Nilai ini menggambarkan bahwa mahasiswa fakultas informatika sangat memahami pentingnya membuang atau memusnahkan hasil cetakan dokumen fisik yang penting ketika sudah tidak digunakan lagi. Mahasiswa juga memiliki kewaspadaan ketika hendak memasukkan perangkat keras (*hardware*) yang dapat dipindah-pindahkan seperti, flashdisk, hardisk, dll. Pengetahuan, sikap, dan kebiasaan mahasiswa juga dinilai baik ketika mereka sedang di tempat umum, mahasiswa memiliki kesadaran yang baik untuk tidak meninggalkan dokumen penting dan sensitive ketika berada di tempat umum. Seluruh sub-area pada fokus area ini dapat mahasiswa mengerti dan praktekkan dengan baik.

- ***Incident Report***

Pada fokus area *incident report* mendapatkan total persentase tingkat kesadaran keamanan informasi sebesar 79,94%, angka ini masuk dalam kategori yang sedang karena berada dibawah 80%. Nilai ini menunjukkan beberapa mahasiswa memiliki tingkat kesadaran yang kurang baik mengenai pelaporan kejadian atau pelaporan hal yang mencurigakan. Pada fokus area ini dimensi *behaviour* atau kebiasaan dan praktek mahasiswa belum cukup baik, karena persentase rata-rata berada di angka 75,90%. Fokus area *knowledge* mendapatkan hasil persentase rata-rata 84,81%, dan fokus area *attitude* memiliki persentase rata-rata 82,77%. Hal ini menunjukkan mahasiswa memiliki pengetahuan dan sikap yang baik mengenai pelaporan insiden keamanan, namun pengetahuan dan sikap tersebut belum dilaksanakan dengan baik.

Pada fokus area ini menjelaskan bahwa, mahasiswa memiliki pengetahuan dan sikap yang baik ketika melihat seorang individu memiliki perilaku yang mencurigakan di area kampus. Mahasiswa juga memiliki pengetahuan dan sikap yang baik untuk mengingatkan temannya yang memiliki perilaku keamanan informasi yang buruk. Wawasan mahasiswa juga baik terhadap pelaporan insiden keamanan yang terjadi. Tetapi pengetahuan dan sikap dari seluruh sub-area tersebut tidak dijalankan dengan praktek yang baik. Hal ini menjadi perhatian penting yang perlu ditingkatkan, karena jika memiliki pengetahuan atau sikap saja tidak akan berpengaruh bila tidak dilaksanakan dengan baik.

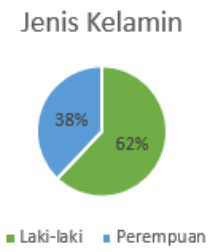
4. Klasifikasi Jawaban Responden

Setelah mendapatkan hasil dari pengukuran tingkat kesadaran keamanan informasi, selanjutnya peneliti mengklasifikasikan hasil temuan yang tergolong paling rendah dari keseluruhan data. Pada klasifikasi ini data responden dikelompokan menjadi dua kategori, diantaranya dikelompokkan berdasarkan jenis kelamin dan umur. Klasifikasi ini bertujuan untuk mengetahui kelompok responden mana yang memiliki tingkat kesadaran keamanan informasi paling rendah dari keseluruhan. Klasifikasi ini mengelompokan data responden yang paling rendah berdasarkan fokus area *internet use* dan *incident report*, poin ini diteliti lebih dalam karena dari seluruh data kedua fokus area inilah yang memiliki persentase paling rendah dari yang lain yaitu berada dikategori sedang.

Pada klasifikasi ini terdapat dua diagram untuk menggambarkan persentase tingkat kesadaran keamanan informasi yang rendah. Diagram yang digunakan untuk menggambarkan persentasenya, yaitu diagram pie (*pie chart*) untuk klasifikasi berdasarkan jenis kelamin, dan diagram batang untuk klasifikasi berdasarkan umur. Tahapan atau proses dari klasifikasi ini yaitu, penulis menganalisis data keseluruhan dari kuisioner, setelah itu ditemukan poin-poin yang rendah dari jawaban kuisioner yang telah dihitung. Poin yang rendah itu terdapat pada fokus area *internet use* dan *incident report*, setelah itu penulis melihat responden mana yang jawabannya berdampak membuat nilai kesadaran keamanan informasi pada fokus area tersebut menjadi rendah, kemudian setelah ditemukan beberapa responden yang memiliki hasil akhir yang rendah pada fokus area *internet use* dan *incident report* kemudian penulis mengelompokan responden-responden tersebut berdasarkan jenis kelamin dan umurnya.

A. Klasifikasi Berdasakan Jenis Kelamin

Pada klasifikasi ini responden yang memiliki tingkat kesadaran keamanan informasi yang kurang baik atau bisa disebut rendah dikelompokan berdasarkan jenis kelamin. Tahap awal klasifikasi yaitu, penulis menganalisis data keseluruhan dari kuisioner, setelah itu ditemukan poin-poin yang rendah dari jawaban kuisioner yang telah dihitung. Poin yang rendah itu terdapat pada fokus area *internet use* dan *incident report*, setelah itu penulis melihat responden mana yang jawabannya berdampak membuat nilai kesadaran keamanan informasi pada fokus area tersebut menjadi rendah, kemudian setelah ditemukan beberapa responden yang memiliki hasil akhir yang rendah pada fokus area *internet use* dan *incident report* kemudian penulis mengelompokan responden-responden tersebut berdasarkan jenis kelaminnya. Hasil dari pengelompokan itu disajikan dalam tabel pie seperti dibawah ini:



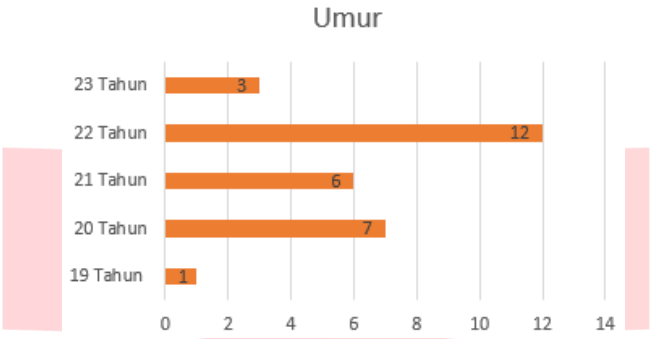
Gambar 3. Pie chart klasifikasi berdasarkan jenis kelamin

Pie chart yang ditampilkan di atas memberikan gambaran yang jelas tentang tingkat kesadaran keamanan yang paling rendah dari seluruh data kuisioner pada mahasiswa dalam konteks penggunaan internet dan pelaporan insiden. Dari total 29 mahasiswa, terlihat persentase 62% merupakan laki-laki, sedangkan 38% sisanya adalah perempuan. Persentase jumlah laki-laki tersebut menunjukkan bahwa mereka sebagian besar terwakili dalam kelompok yang kurang memperhatikan aspek-aspek penting terkait keamanan informasi, seperti kesadarannya ketika menggunakan internet dan respon terhadap insiden yang terjadi di area kampus. Hal ini menunjukkan bahwa ada kebutuhan khusus tentang bagaimana mahasiswa laki-laki ini menggunakan teknologi serta kesadaran mereka akan risiko yang mungkin terjadi.

Lebih dalam lagi, hubungan dari *pie chart* ini menjelaskan adanya perbedaan yang bisa terjadi berhubungan dengan tingkat pemahaman atau edukasi mengenai tingkat kesadaran keamanan informasi pada mahasiswa. Laki-laki yang memiliki kesadaran keamanan informasi rendah tentang penggunaan internet yang aman dan prosedur pelaporan

insiden ditunjukkan pada angka 62%. Sebaliknya, proporsi perempuan yang lebih kecil dalam kategori ini mencerminkan pendekatan yang berbeda dalam berinteraksi dengan teknologi atau akses yang lebih baik terhadap pelaporan insiden keamanan.

B. Klasifikasi Berdasarkan Umur



Gambar 4. Grafik Klasifikasi berdasarkan umur

Berdasarkan diagram pada gambar 4, dijabarkan bahwa responden yang berusia 22 tahun mendominasi dengan jumlah jawaban yang terbanyak yaitu sebanyak 12 responden, diikuti oleh responden dengan umur 20 tahun sebanyak 7 responden, umur 21 tahun sebanyak 6 responden, dan terakhir yaitu umur 19 tahun sebanyak 1 responden. Klasifikasi ini menggambarkan hasil temuan yang tergolong paling rendah dari keseluruhan data dimensi *behaviour* pada *internet use* dan *incident reporting*.

Wawancara dengan Mahasiswa

Seluruh data kuantitatif yang menggunakan instrumen penelitian yaitu kuisioner telah dianalisis dan didapatkan hasil bahwa tingkat kesadaran keamanan informasi pada mahasiswa menunjukan hasil yang baik, tetapi masih ditemukan poin yang berada dalam kategori "sedang" atau paling rendah dari seluruh hasil data wawancara. Hasil yang paling rendah dari seluruh data yaitu pada fokus area *internet use* dan *incident report*.

5. Wawancara dengan mahasiswa

- ***Internet Use***

Berdasarkan hasil analisis data kuantitatif yang sudah dilaksanakan, peneliti menemukan poin yang perlu di garis bawahi, karena pada hasil ini menunjukkan tingkat kesadaran keamanan informasi mahasiswa pada fokus area *internet use* dalam dimensi *behaviour* menghasilkan nilai yang berada pada kategori sedang dengan persentase 78,21%. Hal ini perlu diteliti lebih dalam untuk mengetahui faktor penyebab rendahnya tingkat kesadaran keamanan pada fokus area ini terutama pada dimensi *behaviour*.

Setelah melaksanakan wawancara dengan lima orang narasumber dengan dipilih secara acak berdasarkan data pada kuisioner yang tingkat kesadarannya pada fokus area *internet use* dan *incident reporting* paling rendah, ditemukan bahwa kelima narasumber mengunduh file berformat *PDF*, aplikasi, dan *game* melalui *website* yang keamanannya tidak terjamin. Seluruh narasumber juga tidak memiliki kriteria khusus untuk memilih *website*, tetapi para narasumber menghindari *website* dengan iklan yang banyak serta peringatan dari *google*. Para narasumber rata-rata memilih mengunduh dari *website* yang kurang meyakinkan karena hendak mendapatkan materi atau aplikasi yang mereka butuhkan dengan cepat dan gratis, maka dari itu mereka cenderung mengabaikan tingkat keamanan dari suatu *website* ketika mereka sedang membutuhkan sesuatu dan harus cepat. Selain itu salah satu narasumber waspada ketika melihat tombol *download* yang banyak dan membingungkan pada suatu *website*, tetapi narasumber tersebut tetap berusaha mencari informasi, file, ataupun aplikasi dari *website* tersebut karena terkadang hal yang dia ingingkan hanya ada pada situs tersebut.

Empat dari lima narasumber mengetahui bahwa mengunduh file dari *website* yang mencurigakan dapat berisiko membuat perangkat menjadi lambat karena terinfeksi virus atau *malware*, kehilangan data penting dan pribadi, dan juga phising, namun para narasumber tetap mengunduh file yang membantu perkuliahannya di *website* yang tidak terjamin keamanannya. Sedangkan salah satu narasumber mengetahui resiko terkena virus dan membuat perangkat menjadi lebih lambat setelah mengunduh file materi yang membantu perkuliahan dari *website* yang tidak terjamin keamanannya, tetapi tidak tahu bahwa hal tersebut juga bisa menjadi resiko pencurian data.

- ***Incident Report***

Pada hasil analisis data kuantitatif, diketahui bahwa tingkat kesadaran mahasiswa dalam berperilaku untuk melaporkan sebuah insiden tergolong sedang, dengan persentase mencapai 75,90%. Hal ini memerlukan penelitian yang lebih mendalam, gunanya untuk memahami faktor-faktor yang memengaruhi tingkat kesadaran dan perilaku mahasiswa dalam melaporkan insiden pada dimensi *behaviour*. Oleh karena itu, peneliti melakukan wawancara mendalam mengenai *incident reporting* kepada narasumber yang telah ditetapkan.

Dalam kasus *incident reporting* terkait pelaporan orang yang mecurigakan di area kampus, ditemukan bahwa kelima narasumber sadar jika mengabaikan atau tidak melaporkan orang yang mencurigakan di dalam kampus beresiko terjadinya kejadian yang tidak diinginkan seperti penipuan, pencurian, kebocoran data, bahkan peretasan. Namun hal tersebut bertolak belakang dengan perilaku para narasumber. Keempat narasumber memiliki niat untuk melaporkan jika ada orang yang mencurigakan di area kampus, namun para narasumber ragu dikarenakan takut hanya berprasangka buruk terhadap orang tersebut, sedangkan satu narasumber lainnya hanya memerhatikan saja jika ada orang yang mencurigakan. Hal ini menunjukan ketidaksesuaian atau kesenjangan antara pengetahuan dan perilaku narasumber.

Jawaban yang telah didapat dari para narasumber tentang menegur teman dan keluarga mengenai hal yang beresiko cukup beragam. Di satu sisi, dua dari lima narasumber merasa perlu menegur teman ketika melihat perilaku yang membahayakan keamanan informasi mereka. Di sisi lain, dua narasumber lainnya memilih untuk tidak menegur dengan alasan kesadaran pribadi masing-masing. Satu narasumber lain memilih untuk tidak menegur secara langsung, tetapi berbagi cerita tentang pengalaman buruk terkait keamanan informasi. Namun para narasumber mempunyai jawaban yang sama saat pertanyaan diganti menjadi ranah keluarga. Kelima narasumber sepakat untuk menegur dan memberi edukasi kepada orang tua mereka. Alasannya, orang tua umumnya memiliki pemahaman teknologi yang lebih terbatas, sehingga lebih rentan terhadap risiko keamanan informasi.

Para narasumber menunjukkan pemahaman yang baik tentang *incident reporting*. Mereka menyadari potensi bahaya yang dapat ditimbulkan jika mereka tidak melaporkan kejadian maupun orang yang mencurigakan, serta resiko jika mereka tidak menegur orang terdekat. Namun para narasumber mempunyai perilaku yang tidak sejalan dan terdapat perbedaan dalam cara menindaklanjuti pemahaman tersebut.

6. Wawancara dengan ahli

- **Ahli satu**

Ahli Satu menyarankan beberapa langkah strategis untuk meningkatkan kesadaran keamanan informasi di lingkungan kampus. Pertama, terkait penggunaan internet, beliau mengusulkan pembatasan akses Wi-Fi kampus pada jam kerja dan pengaturan bandwidth untuk mengoptimalkan penggunaan internet untuk keperluan akademik. Selain itu, pemfilteran situs berbahaya juga perlu dilakukan untuk melindungi mahasiswa dari konten negatif. Kedua, dalam hal incident reporting, Ahli Satu menekankan pentingnya menanamkan budaya peduli keamanan informasi di kalangan mahasiswa. Beliau menyarankan pembentukan agen kesadaran keamanan informasi yang berasal dari himpunan mahasiswa dan asisten laboratorium untuk memberikan edukasi kepada teman-temannya. Kampus juga dapat memberikan penghargaan kepada mahasiswa yang aktif dalam menyebarkan informasi keamanan. Secara keseluruhan, Ahli Satu berpendapat bahwa peningkatan kesadaran keamanan informasi harus menjadi prioritas utama untuk melindungi data mahasiswa dan menjaga keamanan lingkungan kampus.

- **Ahli dua**

Ahli Dua menekankan pentingnya pendekatan komprehensif untuk meningkatkan kesadaran keamanan informasi di kampus. Beliau menyarankan berbagai kegiatan seperti sosialisasi, pelatihan, dan kampanye yang melibatkan seluruh civitas akademika. Selain itu, pemblokiran akses ke situs berbahaya dan evaluasi kebijakan penggunaan Wi-Fi juga perlu dilakukan. Untuk meningkatkan sistem keamanan informasi secara keseluruhan, kampus disarankan mengadopsi standar internasional seperti ISO/IEC 27001 dan 27002. Melalui pelatihan rutin, evaluasi berkala, dan penugasan yang holistik, diharapkan dapat terbentuk budaya keamanan informasi yang kuat di kalangan mahasiswa, dosen, dan staf. Dengan demikian, kampus dapat membangun sistem keamanan informasi yang lebih efektif dan melindungi aset digitalnya.

KESIMPULAN DAN SARAN

A. Kesimpulan

Pada penelitian terdapat tujuan yaitu untuk mengukur tingkat kesadaran keamanan informasi mahasiswa, dengan batasan masalahnya yaitu pada mahasiswa Fakultas S1 Informatika Universitas Telkom. Pada penelitian ini, metode yang digunakan yaitu *mixed method* atau gabungan dari kuantitatif dan kualitatif. Penelitian kuantitatif menggunakan instrumen berupa kuisioner yang berdasarkan pada *HAIS-Q*, pada instrumen ini terdapat tujuh fokus pada penelitian diantaranya *password management, email use, internet use, social media use, mobile devices, information handling, incident reporting*. Kuisioner ini juga berfokus pada tiga dimensi *information security awareness* yang diantaranya *knowledge, attitude,* dan *behaviour,* tujuan dilaksanakannya metode kuantitatif ini yaitu untuk mengetahui sebarapa baik tingkat pengetahuan, sikap, dan kebiasaan mahasiswa terhadap kesadaran keamanan informasi terutama di lingkungan kampusnya. Secara keseluruhan, tingkat kesadaran keamanan informasi mahasiswa Fakultas Informatika Universitas Telkom tergolong baik, dengan nilai rata-rata diangka 85,24%. Angka ini menggambarkan bahwa sebagian besar mahasiswa di fakultas informatika Universitas Telkom memiliki pengetahuan yang baik mengenai pentingnya kesadaran keamanan informasi. Tetapi dengan nilai yang baik itu masih ditemukan dua poin yang perlu ditingkatkan, terutama pada dimensi *behaviour* atau kebiasaan. Pada penelitian ini terlihat temuan pada fokus area *internet use* dan *incident reporting* memiliki persentase tingkat keamanan informasi yang rendah terutama pada dimensi *behaviour*, nilai persentase di fokus area *internet use* pada dimensi *behaviour* berada pada angka 78,21%, sedangkan pada fokus area *incident reporting* pada dimensi *behaviour* mendapatkan nilai 75,90 dan menghasilkan nilai rata-rata 79,94% yang dimana nilai-nilai tersebut masih berada dalam kategori yang sedang, karena berada dibawah 80%.

B. Saran

Pada penelitian ini penulis mengetahui bahwa masih terdapat banyak kekurangan. Diantaranya, dapat dilihat bahwa cakupan penelitian ini hanya berfokus pada mahasiswa dan mahasiswi Fakultas Informatika Universitas Telkom, dan juga total jumlah sampel penelitian yang diambil masih dalam jumlah yang sedikit, hal ini menimbulkan kemungkinan tidak dapat mewakili seluruh mahasiswa di Universitas Telkom Bandung. Pada penelitian ini juga hanya menggunakan framework KAB, yang dimana masih banyak framework lain yang dapat menggali lebih dalam lagi mengenai tingkat kesadaran keamanan informasi di Universitas Telkom Bandung. Dari keseluruhan penelitian terdapat beberapa saran dari peneliti sebagai pengembangan untuk penelitian selanjutnya, diantaranya:

1. Memperluas cakupan penelitian tidak hanya pada satu fakultas tetapi menjadi satu universitas, agar dapat lebih merepresentasikan seluruh mahasiswa.
2. Mencari dan membandingkan beberapa metode atau instrumen penelitian untuk mendapatkan metode dan tools yang terbaik untuk penelitian selanjutnya terutama jika masih dalam topik yang sama.
3. Memperbanyak jumlah sampel dengan memperluas jumlah populasi yang hendak diteliti, agar mendapat data yang lebih detail terkait penelitian yang akan dilaksanakan.

REFERENSI

[1] N. Abdallah, O. Abdullah, H. Alkhazaleh, and A. Ibrahim, “Information Security Awareness Behavior Among Higher Education Students: Case Study,” J Theor Appl Inf Technol, vol. 98, pp. 3825–3836, Sep. 2020.

[2] D. R. Nurfadilah, W. H. N. Putra, and A. Rachmadi, “Analisis Manajemen Risiko Keamanan Sistem Informasi pada BKPSDM Kota Batu menggunakan Kerangka Kerja OCTAVE-S dan ISO 27001: 2013 (Studi Kasus: Aplikasi E-Kinerja),” Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, vol. 4, no. 9, pp. 3014–3020, 2020.

[3] M. S. Mahardika, A. N. Hidayanto, P. A. Paramartha, L. D. Ompusunggu, R. Mahdalina, and F. Affan, “Measurement of employee awareness levels for information security at the center of analysis and information services judicial commission Republic of Indonesia,” Adv. Sci. Technol. Eng. Syst, vol. 5, no. 3, pp. 501–509, 2020.

[4] R. Akraman, C. Candiwan, and Y. Priyadi, “Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia,” Jurnal Sistem Informasi Bisnis, vol. 8, no. 2, p. 115, 2018.

[5] CYPRIANUS ANTO SAPTOWALYONO, “PDN Diretas Berhari-hari, Bagaimana Nasib Data Pribadi Kita?,” https://www.kompas.id/baca/polhuk/2024/06/27/pdn-diretas-bagaimana-nasib-data-pribadi-kita.

[6] A. Qonita, “10 Universitas Swasta Terbaik di Indonesia 2024 Versi Webometrics ,” https://telkomuniversity.ac.id/10-universitas-swasta-terbaik-di-indonesia-2024-versi-webometrics/.

[7] Universitas Telkom, “Berkuliah di Telkom University,” https://telkomuniversity.ac.id/berkuliah-di-tel-u/.

[8] A. Zulfia, R. Adawiyah, A. N. Hidayanto, and N. Fitriah Ayuning Budi, “Measurement of Employee Information Security Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q): Case Study at PT. PQS,” Nov. 2019. doi: 10.1109/ICCED46541.2019.9161120.

[9] P. Potgieter, “The Awareness Behaviour of Students on Cyber Security Awareness by Using Social Media Platforms: A Case Study at Central University of Technology,” Nov. 2019, EasyChair. doi: 10.29007/gprf.

[10] M. Indah, A. Angelina, G. Claudia, D. Sertivia, and J. Jevelin, “Analysis of Factors Affecting Information System Security Behaviour in Employees at IT Company,” Ultima Infosys: Jurnal Ilmu Sistem Informasi, vol. 13, no. 1, pp. 29–36, 2022.

[11] H. Ernita, Y. Ruldeviyani, D. N. Maftuhah, and R. Mulyadi, “Strategy to Improve Employee Security Awareness at Information Technology Directorate Bank XYZ,” Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), vol. 6, no. 4, pp. 577–584, 2022.

[12] M. Fianty, “The Impact of Employees’ Information Security Awareness on Information Security Behaviour,” THE IMPACT OF EMPLOYEES’ INFORMATION SECURITY AWARENESS ON INFORMATION SECURITY BEHAVIOUR, vol. 6, no. 5, pp. 629–636, 2023.

[13] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, “Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness,” MIS quarterly, pp. 523–548, 2010.

[14] A. Al-Omari, A. Deokar, O. El-Gayar, J. Walters, and H. Aleassa, “Information security policy compliance: An empirical study of ethical ideology,” in 2013 46th Hawaii International Conference on System Sciences, IEEE, 2013, pp. 3018–3027.

[15] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, “The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies,” Comput Secur, vol. 66, pp. 40–51, 2017, doi: https://doi.org/10.1016/j.cose.2017.01.004.

[16] M. Utomo, A. H. N. Ali, and I. Affandi, “Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001: 2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I,” Jurnal Teknik ITS, vol. 1, no. 1, pp. A288–A293, 2012.

[17] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, “Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q),” Comput Secur, vol. 42, pp. 165–176, 2014, doi: https://doi.org/10.1016/j.cose.2013.12.003.

[18] J. Heigham and R. Croker, Qualitative research in applied linguistics: A practical introduction. Springer, 2009.

[19] John W. Creswell and Vicki L. Piano Clark, “Designing and Conducting Mixed Methods Research,” Aust N Z J Public Health, vol. 31, no. 4, p. 388, Aug. 2007, doi: https://doi.org/10.1111/j.1753-6405.2007.00096.x.

[20] I. E. Kaban, “Tata Kelola Teknologi Informasi (IT Governance),” CommIT (Communication and Information Technology) Journal, vol. 3, no. 1, pp. 1–5, 2009.