ANALISIS PERBEDAAN TINGKAT KESADARAN KEAMANAN SIBER BERDASARKAN FAKTOR DEMOGRAFI DI KALANGAN MAHASISWA UNIVERSITAS TELKOM BANDUNG

Andra Thio Pangka[1], Puspita Kencana Sari[2],Galuh Sudarawerti[3]
[13]Manajemen Bisnis Telekomunikasi dan Informatika, Fakultas Ekonomi dan Bisnis, Universitas Telkom, Indonesia
[1]andrapanka@student.telkomuniversity.ac.id, [2]puspitakencana@telkomuniversity.ac.id ,
[3]galuh.sudorowerti@telkomuniversity.ac.id

ABSTRAK

Penelitian ini bertujuan untuk menganalisis perbedaan tingkat kesadaran keamanan siber berdasarkan faktor demografi yang terdiri dari jenis kelamin, usia, pengalaman penggunaan internet, dan pendapatan keluarga pada mahasiswa Universitas Telkom di Bandung. Peningkatan aktivitas digital di kalangan mahasiswa menuntut adanya pemahaman yang baik mengenai kesadaran terhadap keamanan siber. Penelitian ini menggunakan pendekatan kuantitatif dengan teknik survei terhadap 397 responden, dengan analisis menggunakan uji One-Way ANOVA melalui SPSS versi 25. Kesadaran keamanan siber diukur melalui tiga dimensi, yaitu pengelolaan password, perilaku aman, dan pengaruh sosial. Hasil penelitian menunjukkan bahwa secara deskriptif seluruh dimensi kesadaran keamanan siber berada pada kategori sangat baik, dengan skor tertinggi pada dimensi pengelolaan password (94,63%). Uji ANOVA mengungkapkan adanya perbedaan signifikan pada tingkat kesadaran keamanan siber berdasarkan jenis kelamin dan pengalaman penggunaan internet (sig. < 0,05), sedangkan usia dan pendapatan keluarga tidak menunjukkan perbedaan signifikan (sig. > 0,05).

Kata Kunci: Kesadaran Keamanan Siber, One-Way ANOVA, Jenis Kelamin, Usia, Pengalaman Penggunaan Internet, Pendapatan Keluarga.

ABSTRACT

This study aims to analyze the differences in the level of cybersecurity awareness based on demographic factors, consisting of gender, age, internet usage experience, and family income, among Telkom University students in Bandung. The increase in digital activities among students requires a good understanding of cybersecurity awareness. This research employed a quantitative approach with a survey method involving 397 respondents, analyzed using the One-Way ANOVA test through SPSS version 25. Cybersecurity awareness was measured through three dimensions: password management, safe behavior, and social influence. The results show that, descriptively, all dimensions of cybersecurity awareness were in the very good category, with the highest score in the password management dimension (94.63%). The ANOVA test revealed significant differences in cybersecurity awareness levels based on gender and internet usage experience (sig. < 0.05), while age and family income showed no significant differences (sig. > 0.05)

Keywords*: Cybersecurity Awareness, One-Way ANOVA, Gender, Age, Internet Usage Experience, Family Income.*

I. PENDAHULUAN

Mihalčová *et al*, (2023) serta Susanto & Maulana (2024) mengungkapkan di era kemajuan pesat dalam sistem informasi dan internet, keamanan sistem informasi menjadi hal yang sangat krusial bagi organisasi maupun perusahaan. Tan et al (2024) menambahkan bahwa berkembangnya teknologi, ancaman terhadap keamanan informasi pun semakin bertambah. Menurut DataReportal (2023), sebanyak 77% dari populasi Indonesia merupakan pengguna internet aktif, dengan mayoritas berada dalam rentang usia produktif, termasuk mahasiswa.

Menurut Nopriadi (2024) kesadaran akan risiko di kalangan anak muda, termasuk mahasiswa, masih tergolong rendah. Sebuah penelitian menunjukkan bahwa meskipun 80% responden peduli terhadap privasi mereka, hanya 25% yang secara aktif mengubah pengaturan privasi di akun media sosial mereka. Temuan ini diperkuat oleh penelitian Puspita Kencana Sari & Candiwan (2020) yang menyatakan bahwa meskipun pengguna memiliki tingkat pengetahuan yang tinggi mengenai keamanan informasi, perilaku nyata mereka dalam menerapkan praktik tersebut masih belum optimal. Sangwan (2024) mengaskan bahwa lingkungan sosial dan budaya juga memainkan peran penting dalam membentuk kesadaran keamanan digital mahasiswa. Diskusi antar teman, pelatihan keamanan siber, dan pengaruh media sosial dapat mendorong perilaku aman dalam penggunaan teknologi. Namun demikian, tidak semua mahasiswa yang terpapar informasi keamanan digital

otomatis menerapkan langkah-langkah pencegahan tersebut. Hal ini menunjukkan bahwa pendekatan untuk meningkatkan kesadaran keamanan siber perlu mempertimbangkan banyak faktor, tidak hanya edukasi formal.

Beberapa perguruan tinggi di Indonesia telah mengadopsi konsep kampus digital sebagai bentuk adaptasi terhadap perkembangan teknologi informasi. Universitas Indonesia, misalnya, mengembangkan *Integrated Academic Information System* (SIAK-NG) yang berfungsi untuk mendukung layanan akademik secara daring, sehingga memudahkan mahasiswa dan dosen dalam mengakses berbagai kebutuhan akademik secara terpadu. Langkah serupa juga diambil oleh Universitas Bina Nusantara melalui pemanfaatan platform *Binusmaya* sebagai sistem pembelajaran dan administrasi berbasis teknologi, yang mengintegrasikan materi perkuliahan, penilaian, dan komunikasi akademik dalam satu sistem terpusat. Sementara itu, Universitas Telkom menerapkan konsep *smart campus* dengan mengintegrasikan teknologi digital ke berbagai aspek kegiatan akademik dan administrasi. Penerapan konsep ini meliputi pemanfaatan *Learning Management System* (LMS), sistem presensi digital, hingga layanan *Microsoft 365* untuk seluruh civitas akademika, sehingga menciptakan ekosistem kampus yang sepenuhnya terhubung secara digital. Tingginya integrasi teknologi ini membuat aktivitas akademik menjadi lebih efisien, namun di sisi lain meningkatkan paparan mahasiswa terhadap potensi risiko siber. Oleh karena itu, mahasiswa Universitas Telkom menjadi objek penelitian yang relevan dan strategis untuk mengukur perbedaan tingkat kesadaran keamanan siber berdasarkan karakteristik demografis.

Salah satu pendekatan yang dapat digunakan untuk memahami perbedaan tingkat kesadaran adalah dengan menelusuri pengaruh faktor demografis. Alsobeh *et al*, (2023) mengatakan bahwa faktor seperti jenis kelamin, usia, pengalaman penggunaan internet, dan pendapatan keluarga dapat memberikan pengaruh yang berbeda terhadap kesadaran keamanan siber. Alsobeh *et al*, (2023) serta Kovacevic *et al*, (2020), menunjukkan bahwa adanya perbedaan tingkat kesadaran keamanan siber di antara kategori demografis tersebut. Di sisi lain, penelitian seperti Ramadhani & Pratama (2020) serta Mahendra *et al*, (2024), melaporkan bahwa tidak semua faktor, seperti jenis kelamin, menunjukkan perbedaan yang berarti. Namun sebaliknya, Sari & Sihotang (2016) menegaskan bahwa terdapat variasi kesadaran keamanan informasi berdasarkan usia, latar belakang pendidikan, dan pendapatan.

II. TINJAUAN PUSTAKA

2.1. Keamanan Siber

Menurut Khoironi (2020), keamanan siber, atau yang dikenal sebagai *cybersecurity*, mencakup berbagai perangkat, kebijakan, konsep perlindungan, panduan, pendekatan dalam manajemen risiko, langkah-langkah, pelatihan, praktik unggulan, jaminan, serta teknologi yang bertujuan melindungi dunia maya dan aset-aset suatu organisasi. Aset tersebut meliputi perangkat komputer yang terhubung, sumber daya manusia, infrastruktur, system telekomunikasi, layanan, aplikasi, hingga informasi yang disimpan atau dikirimkan secara *digital*.

2.2. Kesadaran Keamanan Siber

Ramadhani & Pratama (2020) mengungkapkan bahwa kesadaran keamanan siber merujuk pada pemahaman individu mengenai pentingnya melindungi informasi pribadi dan kemampuan menerapkan praktik keamanan saat berinteraksi di dunia maya. Menurut Afandi dalam Ramadhani & Pratama (2020), kesadaran keamanan siber dapat didefinisikan sebagai pengetahuan atau kemampuan seseorang dalam melakukan praktik keamanan saat menggunakan situs jejaring internet, serta memahami arti penting melindungi data pribadi atau data kelompok dalam sebuah organisasi.

2.3. Budaya Keamanan Siber

Luis Emilio Alvarez (2019), menegaskan bahwa budaya keamanan siber merupakan "pengetahuan, keyakinan, persepsi, sikap, asumsi, norma, serta nilai yang dimiliki oleh masyarakat mengenai keamanan siber dan bagaimana hal tersebut tercermin dalam perilaku masyarakat terhadap teknologi informasi." Secara umum, tujuan utama budaya keamanan siber adalah menciptakan dan menerapkan ekosistem budaya yang mendukung keamanan siber. Selain itu, berbagi pengalaman dalam membangun fondasi sosial dan psikologis yang kuat dapat berkontribusi pada upaya meningkatkan keamanan siber.

2.4. Faktor yang Memengaruhi Kesadaran Keamanan Siber

1. Pengetahuan dan Pendidikan

   Tan *et al,* (2024), mengungkapkan bahwa pengetahuan dan pendidikan memainkan peran krusial dalam meningkatkan kesadaran keamanan siber. Edukasi yang memadai mengenai ancaman siber dan cara mengatasinya dapat membantu individu memahami pentingnya melindungi data pribadi dan organisasi . Namun, perspektif berbeda ditemukan oleh Fatokun *et al,* (2019), yang menemukan bahwa meskipun pendidikan formal mengenai keamanan siber diberikan, hal tersebut tidak selalu berbanding lurus dengan peningkatan kesadaran keamanan siber. Studi ini menunjukkan bahwa beberapa mahasiswa masih melakukan praktik berisiko, seperti menggunakan kata sandi yang lemah atau mengabaikan peringatan keamanan, meskipun mereka telah menerima pelatihan terkait keamanan siber.

2. Pengalaman dan Paparan

   Menurut Humaira (2024), pengalaman serta paparan terhadap insiden keamanan siber dapat meningkatkan kesadaran. Individu yang pernah mengalami atau mengetahui insiden keamanan cenderung lebih waspada dan mengambil tindakan pencegahan. Oleh karena itu, simulasi insiden keamanan siber dalam berbagai konteks dapat menjadi metode yang efektif untuk meningkatkan kesadaran. Namun, beberapa penelitian menemukan bahwa pengalaman tidak selalu membuat seseorang lebih waspada. Studi oleh Kovacevic *et al,* (2020) menunjukkan bahwa individu yang sudah terbiasa menggunakan teknologi dan internet dalam jangka waktu lama terkadang mengalami overconfidence, yang membuat mereka lebih rentan terhadap serangan siber karena merasa terlalu percaya diri dengan praktik keamanan yang mereka gunakan.

3. Lingkungan Sosial dan Budaya

   Menurut Khoironi (2020), diskusi terbuka tentang keamanan siber di lingkungan sosial dapat membantu individu memahami pentingnya melindungi data pribadi mereka. Selain itu, norma budaya yang mendukung privasi dan keamanan informasi juga dapat meningkatkan kesadaran terhadap ancaman siber. Sebaliknya, penelitian oleh Nopriadi (2024) menunjukkan bahwa kesadaran keamanan siber tidak selalu dipengaruhi oleh lingkungan sosial. Dalam beberapa kasus, meskipun mahasiswa berada di lingkungan yang peduli terhadap keamanan digital, tidak semua dari mereka mengadopsi praktik keamanan siber yang baik. Studi ini menemukan bahwa meskipun mereka mendapatkan informasi mengenai keamanan siber dari teman atau dosen, hanya sebagian kecil yang benar-benar menerapkan tindakan pencegahan yang direkomendasikan.

4. Usia

   Alsobeh *et al,* (2023) mengungkapkan bahwa usia adalah salah satu faktor yang mempengaruhi tingkat kesadaran terhadap keamanan siber. Remaja, yang merupakan kelompok pengguna internet terbesar, menunjukkan tingkat kesadaran yang bervariasi tergantung pada usia mereka . Namun, penelitian oleh Ojala Burman (2021) menunjukkan bahwa meskipun remaja adalah pengguna aktif internet, mereka sering kali kurang memahami risiko yang terkait dengan penggunaan teknologi, yang menunjukkan bahwa usia saja tidak cukup untuk menjamin kesadaran yang tinggi.

5. Jenis Kelamin

   Jenis kelamin juga kerap menjadi perhatian dalam studi kesadaran keamanan siber. Zahid *et al,* (2024) menyebutkan bahwa perbedaan dalam pola penggunaan internet serta persepsi risiko antara pria dan wanita menjadikan variabel ini penting untuk dianalisis dalam konteks kesadaran terhadap ancaman siber. Namun, penelitian oleh Alqahtani (2022) menunjukkan bahwa perbedaan ini tidak selalu signifikan, dan dalam beberapa kasus, wanita menunjukkan tingkat kesadaran yang lebih tinggi dibandingkan pria, tergantung pada konteks dan jenis ancaman yang dihadapi.

6. Pendapatan Keluarga

   Pendapatan keluarga merupakan salah satu aspek sosial ekonomi yang dapat memengaruhi tingkat kesadaran individu terhadap keamanan siber. Akses terhadap perangkat digital yang memadai, lingkungan belajar yang mendukung, serta peluang mengikuti pendidikan atau pelatihan mengenai keamanan digital sering kali lebih tersedia bagi mereka yang berasal dari keluarga dengan tingkat pendapatan yang lebih tinggi. Hal ini dapat mendorong individu untuk lebih memahami pentingnya menjaga keamanan informasi pribadi mereka di ruang digital. Alsobeh *et al,* (2023), menyebutkan bahwa pendapatan individu yang berasal dari keluarga dengan pendapatan lebih tinggi umumnya memiliki akses terhadap perangkat yang lebih baik, koneksi internet yang lebih stabil, serta kesempatan mengikuti

pelatihan keamanan digital yang lebih banyak. Akses dan peluang ini berpotensi meningkatkan literasi digital dan kesadaran keamanan. Sebaliknya, keterbatasan sumber daya dapat membatasi kesempatan belajar dan mempraktikkan keamanan siber, sehingga menimbulkan perbedaan tingkat kesadaran antar kelompok pendapatan.

2.5. Cybercrime

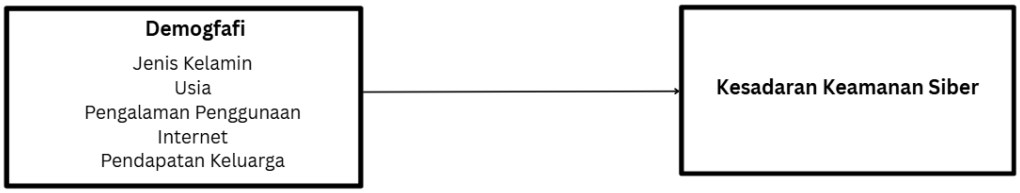
Menurut Willy Kawonal *et al*, (2024), *cybercrime* adalah tindakan kriminal yang melibatkan penggunaan komputer atau jaringan komputer sebagai alat, sasaran, atau tempat terjadinya kejahatan. Jenis-jenis kejahatan siber yang umum di media sosial termasuk penyebaran informasi palsu *(hoaks)*, perundungan daring *(cyberbullying*), ujaran kebencian yang memicu perdebatan SARA, dan lainnya. Kejahatan-kejahatan ini sering kali berdampak pada pengguna media sosial, mengubah pola pikir mereka, terutama akibat kurangnya pemahaman tentang dampak dari konten negatif tersebut.

2.6. Kesadaran Keamanan Siber Di Kalangan Mahasiswa

Mahasiswa merupakan salah satu kelompok yang memiliki intensitas penggunaan teknologi dan internet paling tinggi. Aktivitas seperti mengakses Learning Management System (LMS), mengunduh materi kuliah, mengirim tugas secara daring, hingga berinteraksi di media sosial menjadikan mereka target potensial serangan siber. Garba et al, (2020) menekankan bahwa tingginya paparan teknologi di kalangan mahasiswa menuntut adanya pendidikan keamanan siber yang terintegrasi dalam kurikulum universitas. Namun, Tan et al, (2024) mengungkapkan bahwa meskipun mahasiswa umumnya menyadari adanya ancaman siber, perilaku mereka sering kali tidak mencerminkan tingkat kesadaran tersebut. Menurut Luis Emilio Alvarez (2019) lingkungan sosial, seperti teman sebaya, dosen, dan program edukasi, memiliki peran penting dalam memengaruhi tingkat kesadaran mahasiswa terhadap keamanan siber.

2.7. Kerangka Pemikiran

Berdasarkan tinjauan teori yang telah disampaikan, peneliti merumuskan kerangka pemikiran terkait hubungan antar variabel di penelitian ini sebagai berikut:



Gambar 2. 1 Kerangka Pemikiran

Sumber: Hasil Olahan Peneliti

2.8. Hipotesis Penelitian

Berikut merupakan hipotesis dari penelitian yang dilakukan oleh penulis:

H1: Terdapat perbedaan tingkat kesadaran keamanan siber berdasarkan jenis kelamin pada mahasiswa Universitas Telkom.

H2: Terdapat perbedaan tingkat kesadaran keamanan siber berdasarkan usia pada mahasiswa Universitas Telkom.

H3: Terdapat perbedaan tingkat kesadaran keamanan siber berdasarkan pengalaman penggunaan internet pada mahasiswa Universitas Telkom.

H4: Terdapat perbedaan tingkat kesadaran keamanan siber berdasarkan pendapatan keluarga pada mahasiswa Universitas Telkom.

III. METODE PENELITIAN

Penelitian ini menggunakan metode kuantitatif dengan jenis penelitian deskriptif komparatif. Menurut Sugiyono (2019), penelitian deskriptif bertujuan untuk menggambarkan karakteristik variabel-variabel yang diteliti, sedangkan penelitian komparatif digunakan untuk membandingkan perbedaan variabel pada dua atau lebih kelompok. Dalam konteks ini, penelitian menganalisis perbedaan tingkat kesadaran keamanan siber berdasarkan faktor demografi yang meliputi jenis kelamin, usia, pengalaman

penggunaan internet, dan pendapatan keluarga pada mahasiswa Universitas Telkom di Bandung. Pengumpulan data dilakukan melalui survei menggunakan kuesioner yang dibagikan kepada 397 mahasiswa dengan teknik *purposive sampling*. Skala pengukuran yang digunakan adalah skala Likert lima poin, mulai dari "Sangat Tidak Setuju" hingga "Sangat Setuju". Instrumen penelitian telah diuji validitas dan reliabilitasnya sebelum digunakan pada pengolahan data. Selain itu, analisis regresi linier berganda digunakan untuk menguji pengaruh faktor demografi (jenis kelamin, usia, pengalaman penggunaan internet, dan pendapatan keluarga) terhadap variabel kesadaran keamanan siber. Analisis data dilakukan dengan bantuan perangkat lunak SPSS versi 25. Analisis deskriptif digunakan untuk menggambarkan tingkat kesadaran keamanan siber berdasarkan tiga dimensi utama, yaitu pengelolaan password, perilaku aman, dan pengaruh sosial. Selanjutnya, uji One-Way ANOVA digunakan untuk mengetahui ada atau tidaknya perbedaan yang signifikan pada tingkat kesadaran keamanan siber antara kelompok dalam masing-masing variabel demografi. Keputusan diambil dengan membandingkan nilai signifikansi (*Sig.*) terhadap taraf signifikansi 0,05.

IV. HASIL DAN PEMBAHASAN

4.1 Analisis Deskriptif

Studi deskriptif terhadap 397 responden mahasiswa Universitas Telkom menunjukkan bahwa:

1. Dimensi **Mengatur Password** dinilai sangat tinggi dengan persentase sebesar **94,63%**, yang mencerminkan bahwa mahasiswa memiliki kebiasaan baik dalam mengelola keamanan akses seperti penggunaan password kompleks dan mengganti password secara berkala.
2. Dimensi **Perilaku Aman** menunjukkan tingkat kesadaran yang sangat tinggi pula, dengan skor sebesar **91,12%**, yang menandakan bahwa mayoritas mahasiswa telah menerapkan tindakan preventif dalam aktivitas digital sehari-hari, seperti menghindari login di komputer publik dan tidak membuka tautan mencurigakan.
3. Dimensi **Pengaruh Sosial** juga berada pada kategori sangat tinggi dengan skor sebesar **93,57%**, mengindikasikan bahwa faktor lingkungan, seperti dukungan dari teman dan institusi, turut memengaruhi kesadaran mahasiswa terhadap keamanan siber.

4.2. Uji Normalitas

One-Sample Kolmogorov-Smirnov Test

		Unstandardized Residual
N		397
Normal Parameters[a,b]	Mean	.0000000
	Std. Deviation	14.71767643
Most Extreme Differences	Absolute	.040
	Positive	.040
	Negative	-.023
Test Statistic		.040
Asymp. Sig. (2-tailed)		.126[c]

a. Test distribution is Normal.

b. Calculated from data.

c. Lilliefors Significance Correction.

Gambar 4.1 Uji Normalitas
Sumber: Hasil Olahan Peneliti

Nilai signifikansi dari Kolmogorov smrinov sebesar 0,126 > 0,05. Maka data telah terdistribusi normal.

4.3 Uji Anova

4.3.1 Variabel Jenis Kelamin

Descriptives

Kesadaran Keamanan Siber

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
lak-laki	198	54.5960	15.62272	1.11026	52.4064	56.7855	17.00	85.00
perempuan	199	47.6030	16.25610	1.15236	45.3305	49.8755	17.00	85.00
Total	397	51.0907	16.30352	.81825	49.4820	52.6993	17.00	85.00

Gambar 4.2 Hasil Uji Statistik Deskriptif Jenis Kelamin
Sumber: Hasil Olahan Peneliti

Berdasarkan hasil pengujian terhadap 397 responden, ditemukan bahwa responden laki-laki berjumlah 198 responden dengan nilai rata-rata kesadaran keamanan siber 54,6. Sedangkan responden perempuan dengan jumlah 199 responden memiliki nilai rata-rata keamanan siber sebesar 47,6. Hal tersebut menunjukkan bahwa kesadaran keamanan siber lebih tinggi dimiliki oleh responden dengan jenis kelamin laki-laki.

ANOVA

Kesadaran Keamanan Siber

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	4853.421	1	4853.421	19.094	.000
Within Groups	100405.315	395	254.191		
Total	105258.736	396			

Gambar 4.3 Hasil Uji Anova Jenis Kelamin
Sumber: Hasil Olahan Peneliti

Berdasarkan hasil uji ANOVA, diperoleh nilai signifikansi sebesar 0,000 < 0,05. Maka dapat disimpulkan bahwa terdapat perbedaan yang signifikan kesadaran keamanan siber oleh laki-laki dan perempuan.

4.3.2 Variabel Usia

Descriptives

Kesadaran Keamanan Siber

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
18 tahun	81	48.0000	15.81929	1.75770	44.5021	51.4979	17.00	83.00
19 tahun	75	49.1467	16.81995	1.94220	45.2767	53.0166	18.00	83.00
20 tahun	64	50.1875	16.60644	2.07580	46.0393	54.3357	18.00	85.00
21 tahun	87	53.8736	16.21642	1.73858	50.4174	57.3298	17.00	85.00
22 tahun	90	53.4444	15.73382	1.65849	50.1491	56.7398	17.00	85.00
Total	397	51.0907	16.30352	.81825	49.4820	52.6993	17.00	85.00

Gambar 4.4 Hasil Uji Statistik Deskriptif Usia
Sumber: Hasil Olahan Peneliti

Berdasarkan hasil pengujian terhadap 397 responden, ditemukan bahwa responden dengan usia 18 tahun berjumlah 81 responden dengan nilai rata-rata kesadaran keamanan siber 48. Responden dengan usia 19 tahun berjumlah 75 responden dengan nilai rata-rata kesadaran keamanan siber 49,15. Responden dengan usia 20 tahun berjumlah 64 responden dengan nilai rata-rata kesadaran keamanan siber 50,19. Responden dengan usia 21 tahun berjumlah 87 responden dengan nilai rata-rata kesadaran keamanan siber 53,87. Sedangkan responden dengan usia 22 tahun berjumlah 90 responden dengan nilai rata-rata kesadaran keamanan siber 53,44.

Hal tersebut menunjukkan bahwa kesadaran keamanan siber paling tinggi dimiliki oleh responden dengan usia 21 tahun.

ANOVA

Kesadaran Keamanan Siber

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	2281.767	4	570.442	2.171	.072
Within Groups	102976.968	392	262.696		
Total	105258.736	396			

Gambar 4.5 Hasil Uji Anova Usia
Sumber: Hasil Olahan Peneliti

Berdasarkan hasil uji ANOVA, diperoleh nilai signifikansi sebesar 0,072 > 0,05. Maka dapat disimpulkan bahwa tidak terdapat perbedaan yang signifikan kesadaran keamanan siber oleh usia.

4.3.3 Variabel Pengalaman Penggunaan Internet

Descriptives

Kesadaran Keamanan Siber

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
pemula	39	30.2564	16.95461	2.71491	24.7604	35.7525	17.00	81.00
menengah	149	51.5168	10.72545	.87866	49.7804	53.2531	30.00	77.00
mahir	209	54.6746	16.65110	1.15178	52.4040	56.9453	18.00	85.00
Total	397	51.0907	16.30352	.81825	49.4820	52.6993	17.00	85.00

Gambar 4.6 Hasil Uji Statistik Deskriptif Pengalaman Penggunaan Internet
Sumber: Hasil Olahan Peneliti

Berdasarkan hasil pengujian terhadap 397 responden, ditemukan bahwa responden dengan kategori pengalaman penggunaan internet pemula (≤3 tahun) berjumlah 39 responden, dengan nilai rata-rata kesadaran keamanan siber sebesar 30,26. Responden dalam kategori menengah (3–5 tahun) berjumlah 149 responden, dengan nilai rata-rata sebesar 51,52**.** Sementara itu, responden yang berada dalam kategori mahir (≥5 tahun) berjumlah 209 responden, dengan nilai rata-rata kesadaran keamanan siber sebesar 54,67**.** Hasil ini menunjukkan bahwa semakin lama pengalaman penggunaan internet yang dimiliki responden, maka semakin tinggi pula tingkat kesadaran mereka terhadap keamanan siber. Hal ini terlihat dari perbedaan nilai rata-rata antar kelompok, di mana kelompok mahir memiliki rata-rata paling tinggi, diikuti oleh kelompok menengah, dan yang paling rendah adalah kelompok pemula.

ANOVA

Kesadaran Keamanan Siber

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	19640.216	2	9820.108	45.190	.000
Within Groups	85618.520	394	217.306		
Total	105258.736	396			

Gambar 4.7 Hasil Uji Anova Pengalaman Penggunaan Internet
Sumber: Hasil Olahan Peneliti

Berdasarkan hasil uji ANOVA, diperoleh nilai signifikansi sebesar 0,000 < 0,05. Maka dapat disimpulkan bahwa terdapat perbedaan yang signifikan kesadaran keamanan siber oleh Pengalaman Penggunaan Internet.

4.3.4 Variabel Pendapatan Keluarga

Descriptives

Kesadaran Keamanan Siber

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
2 juta - 4 juta	114	51.7895	15.53840	1.45530	48.9063	54.6727	17.00	85.00
4 juta - 7 juta	172	50.8140	16.09076	1.22691	48.3921	53.2358	17.00	85.00
lebih dari 7 juta	111	50.8018	17.48341	1.65945	47.5132	54.0904	17.00	85.00
Total	397	51.0907	16.30352	.81825	49.4820	52.6993	17.00	85.00

Gambar 4.8 Hasil Uji Statistik Deskriptif Pendapatan Keluarga
Sumber: Hasil Olahan Peneliti

Berdasarkan hasil pengujian terhadap 397 responden, ditemukan bahwa responden dengan pendapatan keluarga 2 juta – 4 juta rupiah berjumlah 114 responden dengan nilai rata-rata kesadaran keamanan siber 51,78. Responden dengan pendapatan keluarga 4 juta – 7 juta rupiah berjumlah 172 responden dengan nilai rata-rata kesadaran keamanan siber 50,81. Responden dengan pendapatan keluarga lebih dari 7 juta rupiah berjumlah 111 responden dengan nilai rata-rata kesadaran keamanan siber 50,80. Hal tersebut menunjukkan bahwa kesadaran keamanan siber paling tinggi dimiliki oleh responden dengan pendapatan keluarga 2 juta – 4 juta rupiah.

ANOVA

Kesadaran Keamanan Siber

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	78.102	2	39.051	.146	.864
Within Groups	105180.634	394	266.956		
Total	105258.736	396			

Gambar 4.9 Hasil Uji Anova Pendapatan Keluarga
Sumber: Hasil Olahan Peneliti

Berdasarkan hasil Uji ANOVA, diperoleh nilai signifikansi sebesar 0,864 > 0,05. Maka dapat disimpulkan bahwa tidak terdapat perbedaan yang signifikan kesadaran keamanan siber oleh pendapatan keluarga.

4.4 Pembahasan Penelitian

Berdasarkan hasil analisis **ANOVA satu arah (One-Way ANOVA)** yang dilakukan pada 397 responden mahasiswa Universitas Telkom di Bandung, diperoleh temuan yang menunjukkan adanya variasi tingkat kesadaran keamanan siber berdasarkan faktor demografi yang dianalisis, yaitu jenis kelamin, usia, pengalaman penggunaan internet, dan pendapatan keluarga. Pada variabel **jenis kelamin**, hasil uji menunjukkan nilai signifikansi sebesar 0,000 < 0,05, yang berarti terdapat perbedaan yang signifikan pada tingkat kesadaran keamanan siber antara laki-laki dan perempuan. Analisis deskriptif memperlihatkan bahwa responden laki-laki memiliki nilai rata-rata kesadaran keamanan siber sebesar 54,60, sedangkan responden perempuan memiliki rata-rata 47,60. Temuan ini menunjukkan bahwa laki-laki memiliki tingkat kesadaran keamanan siber yang lebih tinggi dibandingkan perempuan. Hasil ini sejalan dengan penelitian Hadlington (2017) yang menemukan bahwa perbedaan gender memengaruhi

persepsi risiko keamanan siber, di mana laki-laki cenderung memiliki rasa percaya diri lebih tinggi dalam menjaga keamanan *digital* nya.

Pada variabel **usia**, hasil uji ANOVA menunjukkan nilai signifikansi sebesar 0,072 > 0,05, sehingga dapat disimpulkan bahwa **tidak terdapat perbedaan yang signifikan pada** tingkat kesadaran keamanan siber antar kelompok usia. Meskipun demikian, analisis deskriptif mengindikasikan adanya variasi rata-rata skor kesadaran, di mana responden berusia 21 tahun memiliki skor tertinggi (mean = 53,87), diikuti oleh responden berusia 22 tahun (mean = 53,44), sedangkan skor terendah dimiliki oleh responden berusia 18 tahun (mean = 48,00). Hal ini menunjukkan bahwa meskipun secara statistik perbedaan antar kelompok usia tidak signifikan, terdapat kecenderungan bahwa kelompok usia yang lebih dewasa memiliki tingkat kesadaran keamanan siber yang lebih tinggi. Hasil ini sejalan dengan studi Akhyari (2020) yang menyatakan bahwa semakin bertambah usia, individu cenderung memiliki sikap lebih hati-hati dalam aktivitas *digital*. . Namun, penelitian oleh Hermawansyah & Adam (2022) bahwa kelompok usia muda yang aktif bermedia sosial justru menunjukkan tingkat kesadaran keamanan yang lebih rendah.

Pada variabel **pengalaman penggunaan internet**, hasil uji ANOVA menunjukkan nilai signifikansi sebesar 0,000 < 0,05, yang berarti **terdapat perbedaan yang signifikan** pada tingkat kesadaran keamanan siber antar kelompok pengalaman. Analisis deskriptif memperlihatkan bahwa kelompok dengan pengalaman penggunaan internet ≥ 5 tahun memiliki skor kesadaran tertinggi (mean = 54,67), diikuti oleh kelompok 3–5 tahun (mean = 51,52), sedangkan skor terendah dimiliki oleh kelompok ≤ 3 tahun (mean = 30,26). Hasil ini menunjukkan kecenderungan bahwa semakin lama pengalaman seseorang dalam menggunakan internet, semakin tinggi pula tingkat kesadaran mereka terhadap keamanan siber. Temuan ini konsisten dengan penelitian Tan et al. (2024) yang menegaskan bahwa paparan teknologi dalam jangka waktu yang panjang mampu meningkatkan kewaspadaan terhadap ancaman *digital*, karena individu memiliki lebih banyak kesempatan untuk belajar dari pengalaman dan mengembangkan perilaku aman dalam berinteraksi di dunia maya.

Sementara itu, variabel **pendapatan keluarga** menghasilkan nilai signifikansi sebesar 0,864 > 0,05, yang berarti tidak terdapat perbedaan signifikan pada tingkat kesadaran keamanan siber antar kelompok berdasarkan tingkat pendapatan keluarga. Meskipun analisis deskriptif menunjukkan bahwa kelompok pendapatan 2 juta – 4 juta memiliki rata-rata skor tertinggi (mean = 51,78), diikuti oleh kelompok 4 juta – 7 juta (mean = 50,81) dan kelompok > 7 juta (mean = 50,80), perbedaan tersebut tidak cukup kuat secara statistik untuk dinyatakan signifikan.. Temuan ini konsisten dengan studi Alif (2020), yang menyimpulkan bahwa faktor literasi *digital* dan akses terhadap informasi lebih penting dibanding pendapatan dalam memengaruhi perilaku aman. Hasil ini konsisten dengan studi Alif (2020) yang menyatakan bahwa literasi *digital* dan akses terhadap informasi lebih berperan penting dibanding tingkat pendapatan dalam membentuk perilaku aman di dunia maya. Secara keseluruhan, hasil penelitian ini menunjukkan bahwa faktor demografi yang membedakan tingkat kesadaran keamanan siber secara signifikan adalah **jenis kelamin** dan **pengalaman penggunaan internet**, sedangkan **usia** dan **pendapatan keluarga** tidak menunjukkan perbedaan signifikan.

Sementara itu, hasil analisis deskriptif terhadap **variabel Kesadaran Keamanan Siber (Y)** yang terdiri dari tiga dimensi utama—**Mengatur Password**, **Perilaku Aman**, dan **Pengaruh Sosial**—menunjukkan bahwa responden secara umum memiliki **tingkat kesadaran yang sangat baik**, dengan semua dimensi mencatat skor rata-rata di atas 90%. Dimensi Mengatur Password memperoleh skor 94,63%, mencerminkan pemahaman yang baik terhadap pentingnya password yang kuat dan unik. Dimensi Perilaku Aman mencatat 91,12%, menunjukkan kebiasaan seperti menghindari login di perangkat publik dan menggunakan autentikasi dua faktor telah diterapkan. Dimensi Pengaruh Sosial mencatat skor 93,57%, menunjukkan bahwa lingkungan kampus yang mendukung dan paparan terhadap edukasi digital turut membentuk sikap mahasiswa terhadap keamanan siber. Hasil ini mencerminkan bahwa meskipun masih ada celah dalam praktik tertentu, mahasiswa secara umum telah memiliki kesadaran digital yang bertanggung jawab.

V.KESIMPULAN DAN SARAN

5. 1 Kesimpulan

1. Hasil uji ANOVA pada jenis kelamin menunjukkan nilai signifikansi 0,000 < 0,05, sehingga dapat disimpulkan bahwa terdapat perbedaan yang signifikan pada tingkat kesadaran keamanan siber antara mahasiswa laki-laki dan perempuan.
2. Hasil uji ANOVA pada usia menunjukkan nilai signifikansi 0,072 > 0,05, sehingga tidak terdapat perbedaan yang signifikan pada tingkat kesadaran keamanan siber antar kelompok usia.

3. Hasil uji ANOVA pada variabel pengalaman penggunaan internet menunjukkan nilai signifikansi 0,000 < 0,05, yang berarti terdapat perbedaan yang signifikan pada tingkat kesadaran keamanan siber berdasarkan pengalaman penggunaan internet.
4. Hasil uji ANOVA pada variabel pendapatan keluarga menunjukkan nilai signifikansi 0,864 > 0,05, sehingga tidak terdapat perbedaan yang signifikan tingkat kesadaran keamanan siber berdasarkan kategori pendapatan keluarga.

5.2 Saran

1. Universitas Telkom perlu meningkatkan literasi keamanan siber secara merata di seluruh kelompok mahasiswa, khususnya pada kelompok yang terbukti memiliki kesadaran rendah, seperti mahasiswa dengan pengalaman penggunaan internet ≤ 3 tahun. Upaya ini dapat dilakukan melalui program sosialisasi, pelatihan, workshop keamanan *digital*, dan integrasi materi keamanan siber ke dalam mata kuliah umum atau orientasi mahasiswa baru. Bagi mahasiswa, diharapkan untuk terus meningkatkan kesadaran terhadap praktik keamanan *digital*, termasuk pembaruan *password* secara rutin, penggunaan autentikasi dua faktor, serta penghindaran tautan yang mencurigakan. Meskipun rata-rata kesadaran cukup tinggi, masih ditemukan area-area yang perlu perbaikan, seperti perilaku dalam mengakses akun menggunakan perangkat publik dan membuka lampiran dari sumber tidak dikenal.
2. Mahasiswa disarankan untuk memperkuat praktik keamanan *digital* dalam aktivitas sehari-hari, termasuk pembaruan password secara berkala, penggunaan autentikasi dua faktor, serta kewaspadaan terhadap tautan atau lampiran dari sumber tidak dikenal. Berdasarkan analisis skor sub-variabel, perilaku yang memiliki nilai terendah adalah pada aspek perlindungan data pribadi saat menggunakan perangkat publik. Oleh karena itu, mahasiswa perlu lebih berhati-hati ketika mengakses akun menggunakan perangkat umum dan memastikan selalu melakukan *logout* setelah selesai digunakan.
3. Peneliti selanjutnya disarankan untuk memperluas variabel penelitian, misalnya dengan menambahkan faktor tingkat literasi *digital*, jurusan kuliah, tingkat pendidikan orang tua, atau jenis perangkat yang digunakan. Selain itu, metode pengumpulan data dapat dikombinasikan dengan wawancara mendalam atau observasi langsung, sehingga dapat memberikan gambaran perilaku keamanan siber yang lebih akurat di luar persepsi responden.
4. Pembuat kebijakan perlu merancang program atau kampanye keamanan siber yang menyasar kelompok demografi yang memiliki kesadaran rendah berdasarkan temuan penelitian ini. Misalnya, menyediakan materi edukasi yang lebih interaktif untuk mahasiswa perempuan atau mahasiswa baru yang masih pemula dalam penggunaan internet. Pendekatan yang berbasis segmentasi ini diharapkan dapat meningkatkan efektivitas kampanye dan mendorong terciptanya budaya aman berinternet di lingkungan kampus.

REFERENSI

Alif, M. S. (2020). *Analisis Kesadaran Keamanan Dalam Penggunaan E-Wallet Di Indonesia*. https://dspace.uii.ac.id/handle/123456789/29705

Alqahtani, M. A. (2022). Factors Affecting Cybersecurity Awareness among University Students. *Applied Sciences 2022, Vol. 12, Page 2589*, *12*(5), 2589. https://doi.org/10.3390/APP12052589

Alsobeh, A. M. R., Alazzam, I., Shatnawi, A. M. J., & Khasawneh, I. (2023). Cybersecurity awareness factors among adolescents in Jordan: Mediation effect of cyber scale and personal factors. *Online Journal of Communication and Media Technologies*, *13*(2), e202312. https://doi.org/10.30935/OJCMT/12942

Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019). The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities. Journal of Physics: Conference Series, 1339(1), 012098. https://doi.org/10.1088/1742-6596/1339/1/012098

Garba, A., Maheyzah Binti Sirat, Siti Hajar, & Ibrahim Bukar Dauda. (2020). Cyber Security Awareness Among University Students: A Case Study. Science Proceedings Series, 2(1), 82–86. https://doi.org/10.31580/SPS.V2I1.1320

Hermawansyah, & ADAM. (2022). *Analisis Profil Dan Karakteristik Pengguna Media Sosial Di Indonesia*. https://dspace.uii.ac.id/handle/123456789/42383

Humaira Humaira, S. A. A. A. S. S. (2024). Membangun Kesadaran Mahasiswa Dalam Menghadapi Tantangan Cyber Security di Era Digital. Jurnal Kajian Hukum.

Khoironi, S. C. (2020). Pengaruh Analisis Kebutuhan Pelatihan Budaya Keamanan Siber Sebagai Upaya Pengembangan Kompetensi bagi Aparatur Sipil Negara di Era Digital. *Jurnal Studi Komunikasi Dan Media*, *24*(1), 37–56. https://doi.org/10.31445/JSKM.2020.2945

Kovacevic, A., Putnik, N., & Toskovic, O. (2020). Factors Related to Cyber Security Behavior. *IEEE Access*, *8*, 125140–125148. https://doi.org/10.1109/ACCESS.2020.3007867

Luis Emilio Alvarez-Dionisi, Ph. D. and N. U.-B. (2019). Implementing a Cybersecurity Culture. ISACA.

Mihalčová, B., Korauš, A., Šišulák, S., Gallo, P., & Lukáč, J. (2023). The risks of misusing social networks in the context of hybrid threat. Entrepreneurship and Sustainability Issues, 10(4), 357–371. https://doi.org/10.9770/JESI.2023.10.4(22)

Nopriadi, N. (2024). Menjaga Privasi Digital: Studi Tentang Kesadaran Mahasiswa dalam Perlindungan Data Pribadi di Media Sosial. *Polygon : Jurnal Ilmu Komputer Dan Ilmu Pengetahuan Alam*, *2*(6), 87–97. https://doi.org/10.62383/POLYGON.V2I6.297

Puspita Kencana Sari, Candiwan, N. T. (2020). Confirmatory Factor Analysis. *Measurement Theory in Action, Istmet 2014*, 302–316. https://doi.org/10.4324/9781003127536-19

Ramadhani, M. R., & Pratama, A. R. (2020). Analisis Kesadaran Cyber Security Pada Pengguna Media Sosial Di Indonesia. *AUTOMATA*, *1*(2). https://journal.uii.ac.id/AUTOMATA/article/view/15426

Sangwan, A. (2024). Human Factors in Cybersecurity Awareness. *2024 International Conference on Intelligent Systems for Cybersecurity, ISCS 2024*. https://doi.org/10.1109/ISCS61804.2024.10581139

Sari, P. K., & Sihotang, F. S. (2016). Measurement of Information Security Awareness Among Facebook Users in Indonesia. Asia Pacific Journal of Contemporary Education and Communication Technology, 2(2), 104–113.

Sugiyono. (2019). Metode Penelitian Kuantif Kualitatif R & D. *Universitas Nusantara PGRI Kediri*, *01*, 1–7. https://www.gramedia.com/products/metode-penelitian-kuantitatif-kualitatif-dan-rd-1

Susanto, T. D., & Maulana, M. D. (2024). Evaluating the Influence of Attitude versus Knowledge and Individual Factor versus Intervention Factor on Information Security Awareness in Local Government. Procedia Computer Science, 234, 1428–1434. https://doi.org/10.1016/J.PROCS.2024.03.142

Tan, T., Sama, H., Wibowo, T., Wijaya, G., & Aboagye, O. E. (2024). Kesadaran Keamanan Siber pada Kalangan Mahasiswa Universitas di Kota Batam. *Jurnal Teknologi Dan Informasi*, *14*(2), 163–173. https://doi.org/10.34010/JATI.V14I2.12518

Willy Kawonal, J., Lodwick Dion Bella, E., Rolando Lumasuge, A., Jonathan Pakan, C., Gilqssly Mokalu, M., Kesya Gonta, N., & Negeri Manado, P. (2024). Efforts to Minimize Crime on Social Media. Jurnal Syntax Admiration, 5(11), 4953–4960. https://doi.org/10.46799/JSA.V5I11.1770

Zahid, I. A., Hussein, S. A., & Mahdi, S. M. (2024). Measuring Individuals Cybersecurity Awareness Based on Demographic Features. *Iraqi Journal for Electrical and Electronic Engineering*, *20*(1), 58–67. https://doi.org/10.37917/ijeee.20.1.6