



Perilaku Keamanan Siber Mahasiswa Sosial-Bisnis Berdasarkan Theory of Planned Behavior

Isnawaty, Miqdad Asyraf Rizqullah, Syafiatul Adawiah, L.M Fid Aksara, L.M Bahtiar Aksara, Vyola Cecilia Potto, Abdillah Jumawal Koda, Awaliyah Fadhilatun Nisa, Muh. Yusuf

Informatika, Fakultas Teknik, Universitas Halu Oleo

isna.1711@gmail.com, miqdadwajo@gmail.com, syafiatuladawiah77@gmail.com, fid.laode@yahoo.com,
bahtiar.aksara@uho.ac.id, vyolasesilia@gmail.com, abdillahjk2006@gmail.com, awaliyahfadhilatunnisa@gmail.com,
yusufmuhyusuh@gmail.com

Abstrak

Penggunaan teknologi informasi di perguruan tinggi menjadikan mahasiswa rentan terhadap ancaman kejahatan siber seperti phishing dan pencurian identitas. Penelitian ini bertujuan untuk menganalisis perilaku keamanan siber mahasiswa rumpun Sosial-Bisnis di Universitas Halu Oleo dengan menggunakan pendekatan Theory of Planned Behavior (TPB) yang mencakup dimensi Sikap, Norma Subjektif, Kontrol Perilaku, dan Niat. Pengumpulan data primer dilakukan melalui kuesioner berskala Likert 5 poin kepada 121 responden dari program studi Akuntansi, Manajemen, Administrasi Bisnis, dan Ilmu Komunikasi. Data dianalisis menggunakan metode statistik deskriptif setelah melalui uji validitas dan reliabilitas. Reliabilitas instrumen terbukti andal dengan nilai Cronbach's Alpha sebesar 0,765. Hasil penelitian menunjukkan bahwa secara umum, tingkat kesadaran keamanan siber mahasiswa berada pada kategori sangat tinggi dengan nilai rata-rata 4,22. Dari empat dimensi TPB, dimensi Sikap (Attitude) mendapatkan skor tertinggi yaitu 4,55, yang mengindikasikan pemahaman individu yang sangat baik terkait keamanan data. Sebaliknya, dimensi Norma Subjektif mencatat skor terendah sebesar 3,99. Penelitian ini menyimpulkan bahwa meskipun mahasiswa telah memiliki pemahaman keamanan digital yang baik secara individu, mereka relatif kurang mendapat dorongan dari lingkungan sosialnya. Oleh karena itu, disarankan agar institusi pendidikan menerapkan pendekatan edukasi keamanan siber yang lebih terintegrasi dan melibatkan interaksi sosial antar teman sebaya guna membangun budaya keamanan siber yang komprehensif di kampus.

Kata kunci: Keamanan Siber, Mahasiswa, Skala Likert, Statistik Deskriptif, Theory of Planned Behavior

Abstract

The use of information technology in higher education makes students vulnerable to cybercrime threats such as phishing and identity theft. This research aims to analyze the cybersecurity behavior of Social-Business students at Halu Oleo University by utilizing the Theory of Planned Behavior (TPB) approach, which includes the dimensions of Attitude, Subjective Norm, Perceived Behavioral Control, and Intention. Primary data collection was conducted through a 5-point Likert scale questionnaire distributed to 121 respondents from the Accounting, Management, Business Administration, and Communication Studies study programs. The data was analyzed using descriptive statistical methods after undergoing validity and reliability testing. The instrument's reliability was proven reliable with a Cronbach's Alpha value of 0.765. The research results indicate that, generally, the students' cybersecurity awareness level is in the very high category with an average value of 4.22. Among the four TPB dimensions, the Attitude dimension obtained the highest score of 4.55, indicating an excellent individual understanding of data security. Conversely, the Subjective Norm dimension recorded the lowest score of 3.99. This study concludes that although students already possess a good understanding of digital security individually, they still receive relatively less influence from their social environment. Therefore, it is recommended that educational institutions implement a more integrated cybersecurity education approach involving social interaction among peers to build a comprehensive cybersecurity culture on campus.

Keywords: Cybersecurity, Descriptive Statistics, Likert Scale, Students, Theory of Planned Behavior

1. Pendahuluan

Perkembangan teknologi digital di lingkungan perguruan tinggi tidak hanya memberikan efisiensi administratif, tetapi juga memunculkan risiko kerentanan terhadap eksploitasi data pribadi. Ketergantungan mahasiswa terhadap sistem yang terintegrasi, seperti Sistem Informasi Akademik (SIKAD) maupun infrastruktur *e-learning*, memaksa mereka untuk mengelola berbagai kata sandi dan akun. Laporan dari Badan Siber dan Sandi Negara

(BSSN) menunjukkan bahwa sektor pendidikan kerap menjadi sasaran serangan siber (BSSN, 2024; Creswell & Creswell, 2022). Hal ini menegaskan bahwa kesadaran keamanan siber bukan lagi hal yang hanya perlu dipahami oleh mahasiswa IT, melainkan pengetahuan dasar yang harus dimiliki oleh seluruh mahasiswa untuk mencegah *social engineering*, *phishing*, atau pencurian identitas (Rahmawati & Irawan, 2023; Saputra & Hidayat, 2023; Kusuma, 2022).

Terdapat kekhawatiran bahwa mahasiswa dari rumpun keilmuan Sosial-Bisnis memiliki risiko yang lebih tinggi, mengingat mata kuliah mereka jarang membahas keamanan sistem informasi secara langsung (Utama et al., 2024; Widodo & Hasanah, 2024). Meskipun demikian, aktivitas mereka di dunia digital - mulai dari transaksi keuangan daring hingga penggunaan media sosial - sama aktifnya dengan kelompok mahasiswa lainnya. Oleh karena itu, pemetaan terhadap tingkat kesadaran keamanan siber mahasiswa ini menjadi sangat penting untuk menemukan titik lemah (*blind spot*) yang masih bisa dimanfaatkan oleh pelaku kejahatan siber (Pratama, 2023; Hasanah, 2023).

Pendekatan *Theory of Planned Behavior* (TPB) yang dikemukakan oleh Icek Ajzen digunakan sebagai landasan utama dalam studi ini. Kerangka psikologi sosial ini menganalisis perilaku manusia ke dalam empat variabel pembentuk: Sikap (*attitude*), Norma Subjektif (*subjective norm*), Kontrol Perilaku (*perceived behavioral control*), dan Niat (*intention*). Penelitian terdahulu membuktikan bahwa model TPB dapat digunakan untuk mengukur kepatuhan individu terhadap keamanan informasi, sehingga menjadikannya pendekatan yang tepat untuk konteks akademis (Sommestad et al., 2022; Purwanto & Hakim, 2022; Setiawan, 2023).

Riset ini berfokus pada analisis statistik deskriptif kuantitatif, bukan pada metode teknis seperti keamanan jaringan perangkat lunak. Tujuannya adalah mendeskripsikan tingkat kesadaran dan perilaku keamanan siber mahasiswa rumpun Sosial-Bisnis Universitas Halu Oleo. Diharapkan pemetaan empiris dari riset ini dapat memberikan implikasi manajerial yang konkret bagi otoritas universitas dalam menyusun kurikulum literasi digital masa depan (Sugiyono, 2022; Dewi & Susanto, 2024).

2. Metode Penelitian

Studi ini dirancang menggunakan metode survei kuantitatif dengan pendekatan deskriptif, yang bertujuan menganalisis perilaku kelompok sasaran secara empiris. Pengumpulan data primer dilakukan melalui kuesioner digital (Google Form). Kuesioner tersebut disusun berdasarkan keempat variabel TPB, yang menghasilkan total 16 indikator pertanyaan. Pengukuran jawaban menggunakan Skala Likert 5 poin, mulai dari 'Sangat Tidak Setuju' (skor 1) hingga 'Sangat Setuju' (skor 5) (Arikunto, 2023; Yin, 2024).

TPB atau Theory of Planned Behavior adalah sebuah teori psikologi sosial yang dikembangkan oleh Icek Ajzen untuk menjelaskan perilaku manusia berdasarkan empat dimensi utama, yaitu: Sikap (*Attitude*), Norma Subjektif (*Subjective Norm*), Kontrol Perilaku (*Perceived Behavioral Control*), dan Niat (*Intention*). Jumlah 16 pertanyaan diperoleh dengan membagi masing-masing empat pertanyaan untuk setiap dimensi, sehingga setiap aspek perilaku keamanan siber dapat terukur secara seimbang (Ajzen, 2022; Sommestad et al., 2022).

Populasi dan Sampel. Populasi penelitian ini adalah mahasiswa aktif di rumpun Sosial-Bisnis Universitas Halu Oleo. Penarikan sampel menggunakan teknik *purposive sampling* dengan kriteria pertama yaitu berstatus mahasiswa aktif pada program studi Akuntansi, Manajemen, Administrasi Bisnis, atau Ilmu Komunikasi, dan kriteria kedua adalah merupakan mahasiswa angkatan 2022 hingga 2025. Dari penyebaran kuesioner yang berlangsung selama lima hari, terkumpul 121 responden yang memenuhi kriteria inklusi tersebut (Wulan & Setiawan, 2024; Maulana, 2024).

Variabel Penelitian. Variabel operasional dalam riset ini didasarkan pada kerangka TPB. Dimensi pertama, Sikap (*Attitude*), diukur melalui pertanyaan Q1 hingga Q4. Indikator ini mengukur pemahaman mahasiswa tentang pentingnya kata sandi yang rumit, penggunaan autentikasi dua faktor (2FA), serta sikap waspada terhadap tautan mencurigakan. Dimensi kedua, Norma Subjektif (*Subjective Norm*) yang diukur melalui pertanyaan Q5 sampai Q8, mengukur seberapa besar pengaruh dari lingkungan kampus (dosen dan rekan mahasiswa) dalam membentuk perilaku keamanan individu.

Selanjutnya untuk dimensi ketiga, Kontrol Perilaku (*Perceived Behavioral Control*), diukur melalui Q9 hingga Q12 untuk melihat tingkat kepercayaan diri mahasiswa dalam melakukan tindakan teknis, misalnya membedakan halaman web tiruan (*phishing*) maupun mengatur privasi media sosial. Dimensi terakhir, Niat (*Intention*) yang

diukur melalui Q13 hingga Q16, melihat komitmen responden untuk melakukan pembaruan kata sandi secara rutin, tidak membagikan One-Time Password (OTP), serta disiplin menutup sesi (logout) dari perangkat umum.

Tabel 1. Variabel dan Indikator Penelitian

Dimensi TPB	Item	Jumlah
Sikap (Attitude)	Q1 – Q4	4
Norma Subjektif (Subjective Norm)	Q5 – Q8	4
Kontrol Perilaku (Perceived Beh. Control)	Q9 – Q12	4
Niat (Intention)	Q13 – Q16	4
Total		16

Teknik Analisis Data. Pengolahan data dalam penelitian ini menggunakan metode statistik deskriptif untuk mencari nilai rata-rata (mean), standar deviasi, dan persentase. Sebelum dianalisis, instrumen kuesioner diuji keabsahannya menggunakan korelasi Pearson Product Moment dan diuji keandalannya menggunakan koefisien Cronbach's Alpha (Akbar & Nugraha, 2023). Butir yang dinyatakan tidak valid dikeluarkan dari analisis selanjutnya. Skor rata-rata yang diperoleh dari setiap dimensi TPB kemudian dikelompokkan ke dalam lima kategori tingkat kesadaran berdasarkan rentang interval yang diadaptasi dari skala Likert 5 poin, sebagaimana ditampilkan pada tabel berikut (Sugiyono, 2022; Siregar, 2022; Utami, 2023).

Tabel 2. Kategori Interpretasi Skor Rata-rata

Rentang Skor	Kategori
1,00 – 1,80	Sangat Rendah
1,81 – 2,60	Rendah
2,61 – 3,40	Sedang
3,41 – 4,20	Tinggi
4,21 – 5,00	Sangat Tinggi

Kategori interpretasi tersebut dihitung menggunakan rumus interval kelas, yaitu (nilai maksimum - nilai minimum) / jumlah kelas = $(5 - 1) / 5 = 0,80$. Dengan demikian, setiap kategori memiliki rentang 0,80 poin. Data angka tersebut juga diubah ke dalam bentuk grafik agar hasil penelitian lebih mudah dibaca dan dipahami.

3. Hasil dan Pembahasan

Bab ini membahas hasil pengolahan data yang diperoleh dari 121 responden. Penjelasan hasil penelitian akan dibagi menjadi beberapa bagian secara berurutan, dimulai dari profil demografi responden, hasil uji validitas dan reliabilitas kuesioner, analisis rata-rata skor pada setiap dimensi TPB, hingga penentuan kategori tingkat kesadaran siber secara keseluruhan.

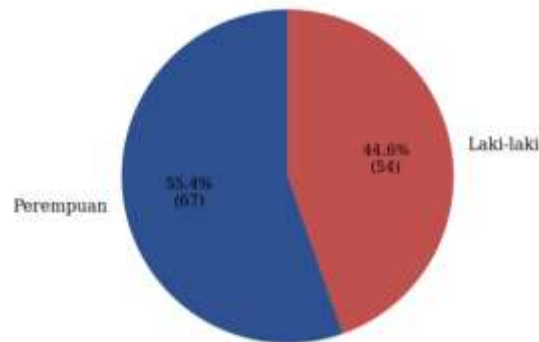
Karakteristik Demografi Responden. Profil demografis responden merupakan data dasar untuk memahami latar belakang responden. Distribusi responden berdasarkan jenis kelamin disajikan pada Tabel 3.

Tabel 3. Distribusi Responden Berdasarkan Jenis Kelamin

Jenis Kelamin	Jumlah	Persentase (%)
Perempuan	67	55,4
Laki-laki	54	44,6
Total	121	100,0

Data pada Tabel 3 menunjukkan bahwa responden lebih banyak didominasi oleh perempuan (55,4%) dibandingkan laki-laki (44,6%). Perbedaan jumlah ini wajar terjadi karena secara umum, program studi yang berada di rumpun Sosial-Bisnis seperti Akuntansi, Manajemen, Administrasi Bisnis, dan Ilmu Komunikasi memang memiliki jumlah

mahasiswi yang lebih banyak dibandingkan mahasiswa laki-laki. Kondisi ini kemungkinan berkaitan dengan komposisi mahasiswa pada rumpun tersebut.

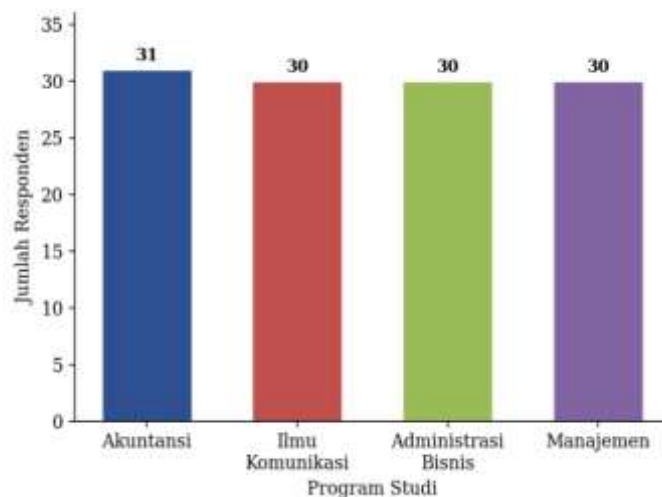


Gambar 1. Distribusi Responden Berdasarkan Jenis Kelamin

Seperti yang ditunjukkan pada Gambar 1, komposisi gender responden yang didominasi perempuan ini mencerminkan populasi aktual mahasiswa di rumpun Sosial-Bisnis. Namun, karena sampel diambil secara purposif, komposisi ini tetap perlu dipertimbangkan sebagai keterbatasan dalam generalisasi hasil (Wulan & Setiawan, 2024). Berdasarkan asal program studi, distribusi responden menunjukkan tingkat keterwakilan yang hampir merata antar program studi, sebagaimana ditunjukkan pada Tabel 4.

Tabel 4. Distribusi Responden Berdasarkan Program Studi

Program Studi	Jumlah	Persentase (%)
Akuntansi	31	25,6
Ilmu Komunikasi	30	24,8
Administrasi Bisnis	30	24,8
Manajemen	30	24,8
Total	121	100,0

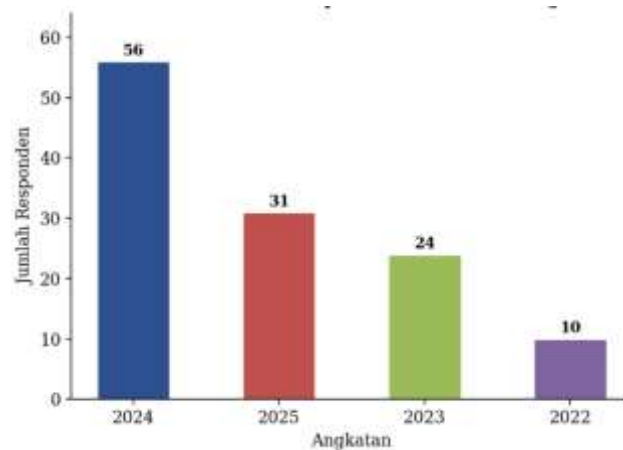


Gambar 2. Distribusi Responden Berdasarkan Program Studi

Berdasarkan Gambar 2, keterwakilan setiap program studi hampir setara, yaitu berada di kisaran 24,8% hingga 25,6%. Keseimbangan jumlah dari keempat program studi ini penting untuk mengurangi kemungkinan bias dari satu jurusan tertentu, sehingga hasil penelitian dapat lebih mewakili kelompok mahasiswa rumpun ilmu Sosial-Bisnis secara keseluruhan. Terakhir, distribusi responden berdasarkan tahun angkatan dapat dilihat pada Tabel 5.

Tabel 5. Distribusi Responden Berdasarkan Angkatan

Angkatan	Jumlah	Persentase (%)
2024	56	46,3
2025	31	25,6
2023	24	19,8
2022	10	8,3
Total	121	100,0



Gambar 3. Distribusi Responden Berdasarkan Angkatan

Berdasarkan Gambar 3, terlihat bahwa partisipasi terbanyak berasal dari angkatan 2024 (46,3%), sedangkan angkatan 2022 paling sedikit (8,3%). Hal ini kemungkinan karena mahasiswa tingkat akhir umumnya memiliki beban akademis yang lebih berat dan sedang fokus pada penyelesaian tugas akhir (Creswell & Creswell, 2022).

Uji Validitas dan Reliabilitas. Sebelum melakukan interpretasi data, kuesioner perlu diuji keabsahannya. Uji validitas dalam penelitian ini menggunakan metode korelasi Pearson Product Moment, yaitu membandingkan nilai r hitung dengan r tabel (0,1786) pada tingkat signifikansi 5%. Hasil pengujian validitas disajikan pada Tabel 6.

Tabel 6. Hasil Uji Validitas Instrumen

Item	r hitung	r tabel	Keterangan
Q1	0,302	0,1786	Valid
Q2	0,042	0,1786	Tidak Valid
Q3	0,201	0,1786	Valid
Q4	0,210	0,1786	Valid
Q5	0,318	0,1786	Valid
Q6	0,386	0,1786	Valid
Q7	0,258	0,1786	Valid
Q8	0,405	0,1786	Valid
Q9	0,178	0,1786	Valid
Q10	0,371	0,1786	Valid
Q11	0,218	0,1786	Valid
Q12	0,314	0,1786	Valid
Q13	0,541	0,1786	Valid
Q14	0,252	0,1786	Valid
Q15	0,407	0,1786	Valid
Q16	0,274	0,1786	Valid

Berdasarkan Tabel 6, terlihat bahwa 15 butir pertanyaan dinyatakan valid (r hitung $>$ 0,1786), dengan catatan bahwa Q9 (r hitung 0,178) berada tepat di batas r tabel dan tetap dipertahankan. Terdapat satu pertanyaan yang

tidak valid yaitu Q2 (terkait fitur autentikasi dua faktor atau 2FA), dengan nilai r hitung sebesar 0,042. Rendahnya nilai r hitung pada Q2 menunjukkan bahwa jawaban responden pada pertanyaan tersebut tidak berkorelasi dengan skor total kuesioner secara keseluruhan. Dengan kata lain, pemahaman responden terhadap konsep 2FA sangat beragam dan tidak sejalan dengan pola jawaban pada pertanyaan lainnya, sehingga pertanyaan ini tidak dapat mengukur apa yang seharusnya diukur. Oleh karena itu, Q2 tidak diikutsertakan dalam pengolahan data selanjutnya.

Meskipun demikian, gugurnya satu pertanyaan ini tidak memengaruhi keseluruhan kerangka Theory of Planned Behavior yang digunakan. Hal ini karena dimensi Sikap masih memiliki tiga pertanyaan valid lainnya (Q1, Q3, dan Q4) yang sudah cukup mewakili pengukuran variabel tersebut. Keempat dimensi TPB yaitu Sikap, Norma Subjektif, Kontrol Perilaku, dan Niat tetap dapat diukur dengan baik menggunakan sisa 15 pertanyaan yang telah terbukti valid (Akbar & Nugraha, 2023; Creswell & Creswell, 2022).

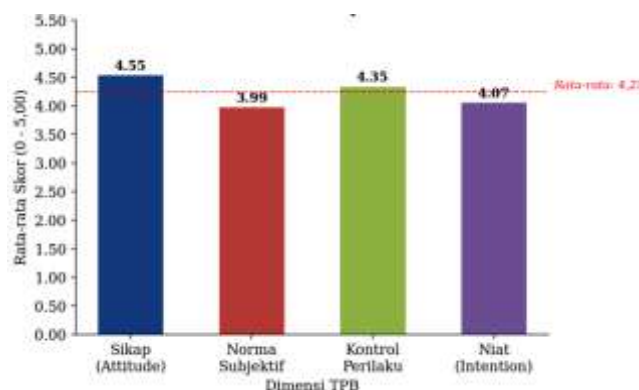
Selain uji validitas, dilakukan juga uji reliabilitas menggunakan Cronbach's Alpha. Nilai Cronbach's Alpha yang didapatkan adalah 0,765, yang mana berada di atas batas minimal 0,60 yang umum digunakan dalam penelitian sosial. Nilai ini menunjukkan bahwa kuesioner yang digunakan sudah andal dan jawaban responden cukup konsisten (Arikunto, 2023; Yin, 2024).

Analisis Statistik Deskriptif per Dimensi TPB. Analisis selanjutnya adalah melihat rata-rata skor dari keempat dimensi utama TPB. Tabel 7 menyajikan nilai rata-rata dari masing-masing dimensi untuk membandingkan tingkat kesadaran keamanan siber mahasiswa pada setiap aspek.

Tabel 7. Statistik Deskriptif per Dimensi TPB

Dimensi	Rata-rata	Standar. Deviasi	Minimum	Maksimum	Kategori
Sikap	4,55	0,39	3,00	5,00	Sangat Tinggi
Norma Subjektif	3,99	0,61	1,75	5,00	
Kontrol Perilaku	4,35	0,49	2,50	5,00	Sangat Tinggi
Niat	4,07	0,54	2,75	5,00	Tinggi
Rata-rata Keseluruhan	4,22				Sangat Tinggi

Berdasarkan Tabel 7 dan Gambar 4, keempat dimensi TPB menunjukkan skor yang beragam. Perlu dicatat bahwa perhitungan skor pada dimensi Sikap tidak lagi memasukkan pertanyaan Q2, karena dinyatakan tidak valid pada pengujian sebelumnya. Dimensi Sikap mendapatkan skor tertinggi yaitu 4,55 yang termasuk kategori Sangat Tinggi berdasarkan tabel interpretasi skor. Angka ini menunjukkan bahwa pemahaman mahasiswa mengenai pentingnya menjaga data pribadi sudah sangat baik (BSSN, 2024; Saputra & Hidayat, 2023; Kusuma, 2022).



Gambar 4. Rata-rata Skor per Dimensi TPB

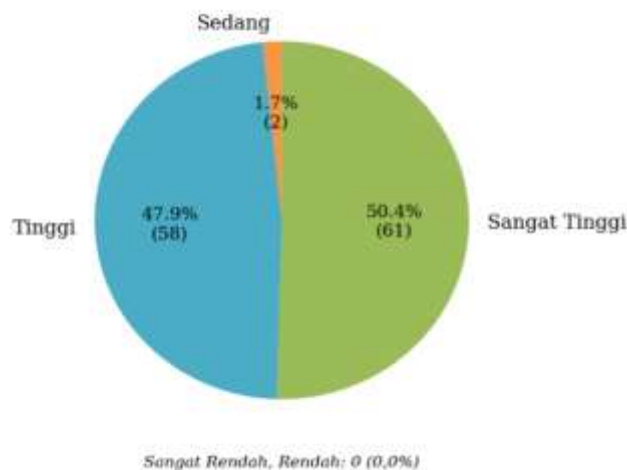
Sebaliknya, dimensi Norma Subjektif mendapatkan skor terendah yaitu 3,99 yang termasuk kategori Tinggi. Perbedaan skor antara kesadaran dari diri sendiri dan pengaruh lingkungan luar ini menggambarkan bahwa isu privasi digital belum menjadi topik perbincangan sehari-hari di kampus (Utama et al., 2024; Hasanah, 2023). Hal ini menunjukkan perlunya pendekatan sosial agar isu keamanan mulai disosialisasikan melalui kegiatan kemahasiswaan dan bimbingan dosen, bukan sekadar imbauan di dalam sistem (Pratama, 2023; Setiawan, 2023; Dewi & Susanto, 2024). Sementara itu, nilai Niat yang berada pada angka 4,07 (kategori Tinggi) mencerminkan bahwa pemahaman keamanan belum sepenuhnya diterapkan menjadi kebiasaan sehari-hari (Somestad et al., 2022; Siregar, 2022).

Distribusi Kategori Tingkat Kesadaran. Selanjutnya, total skor setiap individu dikelompokkan berdasarkan tabel kategori interpretasi skor yang telah ditetapkan pada bagian metode untuk menentukan tingkat kesadaran siber secara keseluruhan. Penentuan kategori dilakukan dengan menghitung rata-rata skor seluruh pertanyaan valid dari setiap responden, kemudian mencocokkannya dengan rentang kategori. Distribusi tingkat kesadaran tersebut dapat dilihat pada Tabel 8.

Tabel 8. Distribusi Kategori Tingkat Kesadaran Keamanan Siber

Kategori	Jumlah	Persentase (%)
Sangat Rendah	0	0,0
Rendah	0	0,0
Sedang	2	1,7
Tinggi	58	47,9
Sangat Tinggi	61	50,4
Total	121	100,0

Tabel 8 dan visualisasinya pada Gambar 5 menunjukkan bahwa mayoritas responden berada pada kategori Sangat Tinggi (50,4%) dan Tinggi (47,9%). Hanya 1,7% responden yang berada pada kategori Sedang, dan tidak ada responden pada kategori Rendah maupun Sangat Rendah. Hal ini menunjukkan bahwa mahasiswa rumpun Sosial-Bisnis secara umum sudah memiliki kesadaran keamanan siber yang baik.



Gambar 5. Distribusi Kategori Tingkat Kesadaran

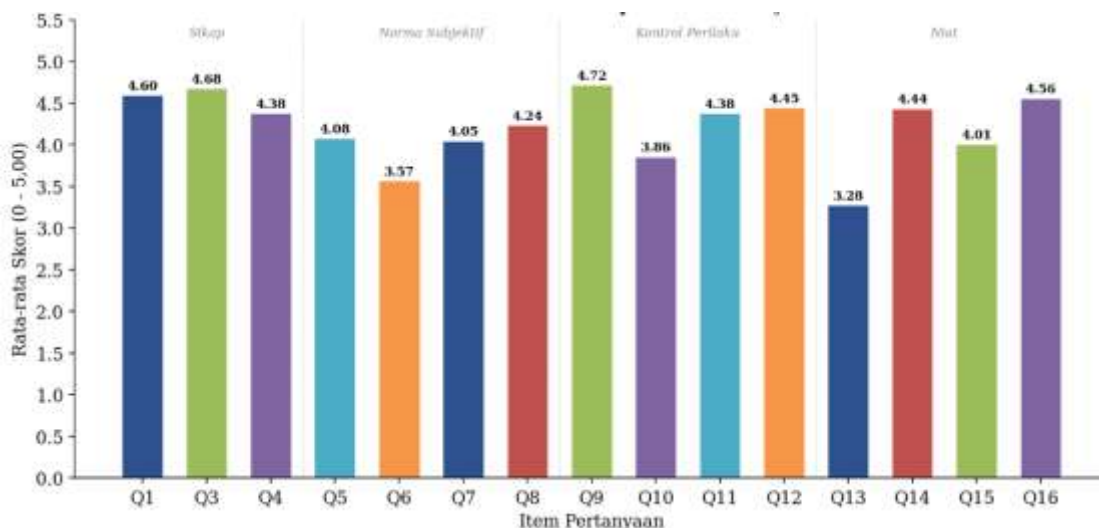
Tidak adanya responden pada kategori Rendah dan Sangat Rendah menunjukkan bahwa seluruh mahasiswa telah memahami dasar-dasar keamanan siber, yang kemungkinan didorong oleh fitur keamanan bawaan di aplikasi media sosial dan perbankan digital (Rahmawati & Irawan, 2023; Widodo & Hasanah, 2024; Utami, 2023).

Analisis Statistik Deskriptif per Item Pertanyaan. Penelitian ini juga melakukan analisis lebih lanjut pada setiap item pertanyaan untuk melihat kebiasaan spesifik responden. Rincian rata-rata dan deviasi standar untuk setiap pernyataan dapat dilihat pada Tabel 9.

Tabel 9. Statistik Deskriptif per Item Pertanyaan

Item	Rata-rata	Standar. Deviasi	Minimum	Maksimum
Q1	4,60	0,79	1	5
Q3	4,68	0,64	2	5
Q4	4,38	0,91	1	5
Q5	4,08	0,93	1	5
Q6	3,57	1,17	1	5
Q7	4,05	1,02	1	5
Q8	4,24	1,08	1	5
Q9	4,72	0,61	2	5
Q10	3,86	1,12	1	5
Q11	4,38	0,93	1	5
Q12	4,45	0,88	1	5
Q13	3,28	1,29	1	5
Q14	4,44	0,97	1	5
Q15	4,01	0,97	2	5
Q16	4,56	0,75	2	5

Berdasarkan data pada Tabel 9 dan diagram pada Gambar 6, terlihat pola perilaku yang saling bertolak belakang. Skor tertinggi terdapat pada Q9 (4,72) pada dimensi Kontrol Perilaku, yang mengukur kepercayaan diri mahasiswa dalam melakukan tindakan keamanan secara teknis. Namun, hal ini berbanding terbalik dengan skor terendah pada Q13 (3,28) yang berkaitan dengan kebiasaan rutin dalam memperbarui kata sandi tersebut.



Gambar 6. Rata-rata Skor per Item Pertanyaan yang Valid

Besarnya nilai standar deviasi pada pertanyaan Q13 (1,29) menunjukkan adanya kemungkinan terjadinya security fatigue atau kelelahan keamanan di kalangan mahasiswa, meskipun dugaan ini perlu dikonfirmasi lebih lanjut. Kondisi ini merupakan situasi psikologis di mana pengguna mulai mengabaikan langkah-langkah pengamanan karena merasa jenuh (Ajzen, 2022; Purwanto & Hakim, 2022; Maulana, 2024). Temuan ini menandakan bahwa kemampuan teknis mahasiswa dalam menjaga keamanan digital masih belum konsisten dan seringkali lebih mengutamakan kepraktisan dibandingkan kedisiplinan.

Keterbatasan Penelitian. Meskipun hasil penelitian ini menunjukkan skor rata-rata keseluruhan sebesar 4,22 yang termasuk kategori Sangat Tinggi, terdapat beberapa keterbatasan dalam penelitian ini yang perlu diakui. Besarnya jumlah responden yang masuk dalam kategori Tinggi dan Sangat Tinggi (98,3%) menunjukkan kemungkinan terjadinya ceiling effect, yaitu kondisi ketika sebagian besar jawaban responden menumpuk di nilai tertinggi skala. Hal ini dapat diketahui dari distribusi skor pada Tabel 8 yang sangat timpang ke sisi kanan. Selain itu, terdapat kemungkinan adanya social desirability bias, yaitu kecenderungan responden memberikan jawaban yang dianggap

baik secara sosial, bukan berdasarkan perilaku mereka yang sesungguhnya. Penggunaan instrumen kuesioner yang mengandalkan self-report (penilaian diri sendiri) juga berpotensi menimbulkan bias, karena tidak ada verifikasi langsung terhadap perilaku nyata responden. Selain itu, butir Q9 memiliki nilai r hitung (0,178) yang berada tepat di batas r tabel (0,1786) dan tetap dipertahankan dalam analisis, sehingga validitas butir tersebut perlu dikonfirmasi pada penelitian selanjutnya.

4. Kesimpulan

Berdasarkan hasil analisis data, studi ini menyimpulkan bahwa mahasiswa rumpun Sosial-Bisnis Universitas Halu Oleo secara umum telah memiliki tingkat kesadaran keamanan siber yang baik, ditunjukkan oleh rata-rata skor keseluruhan yang masuk dalam kategori Sangat Tinggi. Penerapan kerangka Theory of Planned Behavior dalam penelitian ini berhasil mengidentifikasi temuan penting: tingginya pemahaman individu (Sikap) ternyata tidak sejalan dengan pengaruh lingkungan sosial yang relatif lebih rendah (Norma Subjektif). Hal ini menunjukkan bahwa kesadaran yang ada masih bersifat individual dan belum berkembang menjadi kebiasaan atau budaya saling mengingatkan di lingkungan pergaulan kampus. Berdasarkan temuan tersebut, disarankan kepada pihak kampus untuk tidak hanya mengandalkan seminar teknis dalam memberikan edukasi. Kampus perlu menerapkan pendekatan yang lebih terintegrasi, misalnya menyisipkan materi perlindungan data ke dalam tugas perkuliahan, mengadakan simulasi serangan phishing agar mahasiswa berlatih mengenali ancaman nyata, atau membentuk komunitas kesadaran keamanan siber di tingkat fakultas yang melibatkan peran teman sebaya. Bagi peneliti selanjutnya, disarankan untuk beralih dari sekadar statistik deskriptif ke arah model pengujian sebab-akibat (seperti Structural Equation Modeling) untuk mengukur seberapa besar pengaruh budaya saling mengingatkan antar teman dalam mencegah kelelahan keamanan (security fatigue) di kampus.

Referensi

1. Ajzen, I. (2022). The Theory of Planned Behavior: Frequently Asked Questions. *Human Behavior and Emerging Technologies*, 2(4), 314-324.
2. Akbar, F., & Nugraha, R. (2023). Studi Kasus Serangan Phishing dan Strategi Pencegahannya di Lingkungan Akademik. *J. Edukasi Siber*, 6(4), 210-218.
3. Arikunto, S. (2023). *Prosedur Penelitian: Suatu Pendekatan Praktik*, Edisi Revisi. Rineka Cipta.
4. BSSN. (2024). *Laporan Tahunan Monitoring Keamanan Siber 2024*. Badan Siber dan Sandi Negara.
5. Creswell, J. W., & Creswell, J. D. (2022). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (6th ed.). SAGE Publications.
6. Dewi, L. M., & Susanto, P. (2024). Analisis Kesadaran Privasi dan Keamanan Pengguna Media Sosial di Kalangan Gen Z. *J. Komun. Digital*, 6(2), 150-160.
7. Hasanah, N. F. (2023). Peran Norma Subjektif dalam Adopsi Praktik Keamanan Siber: Sebuah Pendekatan TPB. *J. Psikol. Dan Teknol.*, 8(2), 88-97.
8. Kusuma, A. B. (2022). Pengaruh Edukasi Keamanan Kata Sandi terhadap Perilaku Mahasiswa di Ruang Siber. *J. Komput. Dan Keamanan*, 5(1), 23-31.
9. Maulana, M. R. (2024). Tren Ancaman Siber pada Institusi Pendidikan Tinggi di Indonesia Tahun 2023. *J. Ris. Keamanan Jaringan*, 5(3), 180-192.
10. Pratama, A. R. (2023). Analisis Kesadaran Keamanan Siber Mahasiswa Non-TI Menggunakan Pendekatan Kuantitatif. *J. Keamanan Siber Indones.*, 7(2), 45-56.
11. Purwanto, E., & Hakim, L. (2022). Evaluasi Perceived Behavioral Control terhadap Penggunaan Software Antivirus pada Mahasiswa. *J. Teknol. Informasi*, 12(4), 315-322.
12. Rahmawati, S., & Irawan, B. (2023). Pengaruh Latar Belakang Pendidikan terhadap Perilaku Keamanan Informasi Pribadi di Dunia Digital. *J. Sist. Inf. dan Teknol.*, 14(1), 78-89.
13. Saputra, M. A., & Hidayat, R. (2023). Efektivitas Penerapan Two-Factor Authentication (2FA) dalam Mencegah Pengambilalihan Akun Edukasi. *J. Nas. Teknol. dan Sist. Inf.*, 9(2), 112-120.
14. Setiawan, B. (2023). Kerentanan Mahasiswa Terhadap Serangan Social Engineering di Lingkungan Perguruan Tinggi. *J. Sist. Komput.*, 10(1), 45-52.
15. Siregar, Y. A. (2022). Fenomena Security Fatigue: Mengapa Pengguna Mengabaikan Peringatan Keamanan. *J. Interaksi Manusia dan Komputer*, 7(1), 34-45.
16. Somestad, T., Karlzen, H., & Hallberg, J. (2022). A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour. *Int. J. Inf. Secur. Priv.*, 9(1), 26-46.
17. Sugiyono. (2022). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*, Edisi ke-3. Alfabeta.
18. Utama, D. P., Yusuf, M. H., & Wibowo, A. (2024). Evaluasi Keamanan Data Sistem Informasi Akademik Berbasis Perilaku Pengguna. *J. Teknol. Inf. dan Ilmu Komput.*, 10(3), 567-575.
19. Utami, T. P. (2023). Membangun Budaya Keamanan Informasi di Organisasi Non-Profit dan Institusi Pendidikan. *J. Manaj. Sist. Inf.*, 8(4), 290-302.
20. Widodo, R. Y., & Hasanah, S. N. (2024). Pemetaan Kesadaran Keamanan Informasi Mahasiswa Ilmu Sosial di Era Society 5.0. *J. Ilm. Inform.*, 11(3), 201-210.
21. Wulan, K., & Setiawan, A. (2024). Analisis Faktor Demografi terhadap Tingkat Literasi Keamanan Siber Generasi Z. *J. Ilm. Teknol. Inf. Terap.*, 9(1), 34-41.
22. Yin, R. K. (2024). *Case Study Research and Applications: Design and Methods* (7th ed.). SAGE Publications.