

ANALISIS TINGKAT KESADARAN MAHASISWA TERHADAP KEAMANAN AKUN PADA PENGGUNAAN LAYANAN DIGITAL

Muhammad Rafli Daffa Aulia^{1*}, Taufiq²

^{1,2}Universitas Malikussaleh, Indonesia

^{1*}muhammad.240170160@mhs.unimal.ac.id, ²Taufiq.te@unimal.ac.id

ABSTRACT

The use of digital services, such as digital banking, social media, academic portals, and e-commerce platforms, has become an important part of university students' daily activities. However, frequent use of digital services does not always ensure adequate account security practices, leaving accounts potentially vulnerable to phishing, credential theft, and account takeover. This study aims to describe students' awareness of account security and their self-reported account protection behavior when using digital services. A quantitative survey was conducted using 100 questionnaire responses collected from students at Universitas Malikussaleh. The questionnaire consisted of ten statements measured on a five-point scale, comprising five items on account security awareness and five items on self-reported account protection behavior. Data were analyzed using achievement indices, descriptive categorization, and Spearman's rank correlation. The results show that account security awareness reached 81.32% and was categorized as very high, while self-reported account protection behavior reached 77.56% and was categorized as high. The Spearman correlation test showed a positive and significant relationship between the two variables ($\rho = 0.747$, $p < 0.001$). Awareness exceeded self-reported protection behavior by 3.76 percentage points. These findings indicate a descriptive gap between account security awareness and reported protection behavior, although this difference was not tested for statistical significance. The findings can serve as an initial basis for developing account security literacy and education programs in higher education. However, because the data were self-reported and the eligibility of all respondents was not fully confirmed, the results should be interpreted as exploratory and should not be generalized to all undergraduate students at Universitas Malikussaleh.

Keywords:

account security, cybersecurity awareness, security behavior, digital services, university students.

PENDAHULUAN

Transformasi digital mendorong mahasiswa menggunakan berbagai layanan berbasis internet dalam kegiatan akademik maupun kehidupan sehari-hari. Layanan tersebut meliputi Sistem Informasi Akademik (SIKAD), surel institusi, perbankan dan dompet digital, media sosial, serta platform *e-commerce*. Penggunaan layanan tersebut melibatkan akun yang menyimpan kredensial dan informasi pribadi. Oleh karena itu, keamanan akun menjadi penting untuk mencegah akses tanpa izin, penyalahgunaan data pribadi, dan pengambilalihan akun.

Mahasiswa yang akrab dengan teknologi belum tentu selalu menerapkan praktik keamanan yang memadai. Penggunaan kata sandi yang sama pada beberapa akun, kurangnya kewaspadaan terhadap pesan phishing, serta tidak diaktifkannya autentikasi dua faktor (Two-Factor Authentication, 2FA) dapat meningkatkan risiko pengambilalihan akun. Penelitian terhadap mahasiswa menunjukkan bahwa kesadaran keamanan siber dapat berbeda-beda (Alqahtani, 2022; Baraković & Baraković Husić, 2023). Penelitian lain juga menunjukkan bahwa perilaku keamanan mahasiswa dalam menghadapi serangan phishing melalui surel masih perlu diperkuat (Gwenhure, 2025). Temuan tersebut menunjukkan bahwa intensitas penggunaan teknologi tidak otomatis menjamin kesadaran dan praktik keamanan yang memadai.

Kesadaran keamanan akun berkaitan dengan pemahaman dan kepedulian pengguna terhadap ancaman keamanan digital serta pentingnya melindungi akun. Aspek ini mencakup pemahaman mengenai phishing, risiko penggunaan Wi-Fi publik, dampak pengambilalihan akun, pengelolaan kata sandi, dan fungsi autentikasi dua faktor. Sementara itu, perilaku pengamanan akun berkaitan dengan tindakan yang dilaporkan responden dalam penggunaan akun digital sehari-hari, seperti menggunakan kata sandi yang berbeda, menghindari penggunaan informasi pribadi, memperbarui kata sandi, mengaktifkan 2FA, dan menggunakan autentikasi biometrik.

Berdasarkan hal tersebut, penelitian ini mengkaji dua hal utama: bagaimana tingkat kesadaran mahasiswa terhadap keamanan akun dalam penggunaan layanan digital, dan bagaimana perilaku pengamanan akun yang mereka laporkan. Penelitian ini bertujuan menggambarkan kesadaran keamanan akun serta perilaku pengamanan akun mahasiswa Universitas Malikussaleh menggunakan kuesioner berskala Likert. Penelitian juga menelaah hubungan antara kedua skor tersebut menggunakan korelasi Spearman.

Penelitian ini berkontribusi dengan memberikan gambaran mengenai kesadaran dan perilaku pengamanan akun pada mahasiswa Universitas Malikussaleh, khususnya dalam penggunaan layanan akademik, komunikasi, keuangan digital, dan media sosial. Hasil penelitian diharapkan dapat mengidentifikasi aspek yang perlu diperkuat dan menjadi masukan awal bagi penyusunan program edukasi keamanan akun di lingkungan kampus. Namun, karena data diperoleh melalui laporan mandiri dan sampel dipilih secara nonprobabilitas, hasil penelitian tidak dapat digeneralisasikan secara statistik kepada seluruh mahasiswa sarjana Universitas Malikussaleh.

KAJIAN LITERATUR

Kesadaran keamanan akun merupakan pemahaman dan kepedulian pengguna terhadap ancaman keamanan digital serta pentingnya melindungi akun. Aspek ini mencakup pemahaman mengenai phishing, risiko penggunaan Wi-Fi publik, dampak pengambilalihan akun, pengelolaan kata sandi, dan fungsi autentikasi dua faktor (Two-Factor Authentication, 2FA). Kesadaran yang tinggi tidak serta-merta menjamin penerapan praktik keamanan yang memadai, tetapi dapat menjadi dasar bagi pengambilan keputusan pengguna dalam melindungi akunnya.

Perilaku pengamanan akun berkaitan dengan tindakan yang dilaporkan responden dalam penggunaan akun digital sehari-hari. Tindakan tersebut meliputi penggunaan kata sandi yang berbeda pada beberapa layanan, penghindaran penggunaan informasi pribadi, pembaruan kata sandi secara berkala, aktivasi 2FA, dan penggunaan autentikasi biometrik. Dalam penelitian ini, perilaku pengamanan akun diukur melalui laporan mandiri responden, sehingga hasil yang diperoleh menggambarkan perilaku yang dilaporkan, bukan hasil pemeriksaan langsung terhadap akun responden.

Penelitian terdahulu menunjukkan bahwa kesadaran keamanan siber mahasiswa dapat berbeda-beda. Alqahtani (2022) menilai kesadaran keamanan siber mahasiswa berdasarkan keamanan kata sandi, keamanan peramban, dan aktivitas media sosial. Baraković dan Baraković Husić (2023) melaporkan bahwa perilaku kebersihan siber mahasiswa tergolong dapat diterima, tetapi kesadaran dan pengetahuannya belum memuaskan. Guo dan Tinmaz (2023) menelaah kesadaran serta pendidikan keamanan siber mahasiswa di Tiongkok, sedangkan Bognár dan Bottyán (2024) mengembangkan dan memvalidasi skala kesadaran keamanan siber personal untuk mahasiswa.

Praktik pengamanan akun tidak hanya dipengaruhi oleh pemahaman pengguna. Wash dan Rader (2021) menemukan bahwa pengguna mempertimbangkan keseimbangan antara keamanan dan kemudahan penggunaan ketika memilih kata sandi. Temuan tersebut relevan untuk menafsirkan kemungkinan perbedaan antara kesadaran keamanan akun dan perilaku pengamanan akun yang dilaporkan. Namun, faktor keamanan dan kemudahan penggunaan tidak diukur secara langsung dalam penelitian ini, sehingga tidak dapat dinyatakan sebagai penyebab perbedaan tersebut.

Dari sisi teknis, pedoman identitas digital NIST mendefinisikan autentikasi multi-faktor sebagai penggunaan lebih dari satu faktor autentikasi yang berbeda (National Institute of Standards and Technology [NIST], 2025). Penggunaan 2FA atau autentikasi biometrik dapat menjadi salah satu upaya untuk memperkuat perlindungan akun. Namun, efektivitas fitur tersebut tetap bergantung pada kesadaran pengguna, kemudahan penggunaan, proses aktivasi, dan proses pemulihan akun.

METODE PENELITIAN

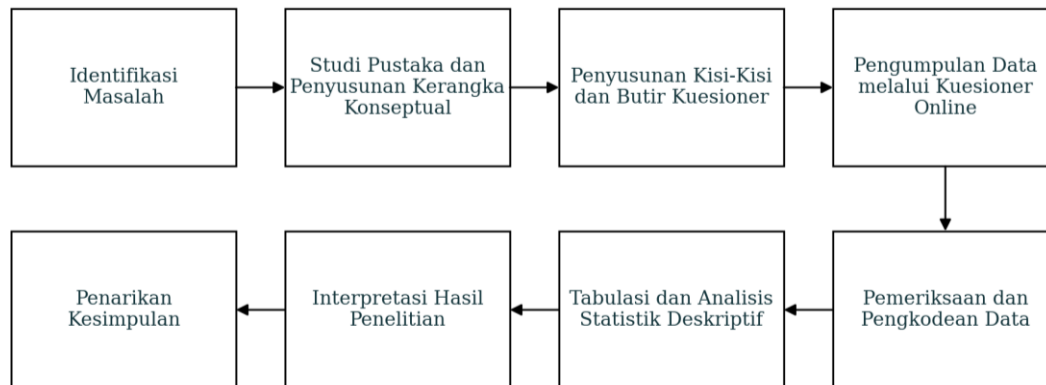
Penelitian ini menggunakan pendekatan kuantitatif dengan desain survei deskriptif. Pendekatan kuantitatif digunakan untuk mengolah data numerik yang diperoleh dari jawaban responden melalui kuesioner. Desain survei deskriptif bertujuan menggambarkan kesadaran mahasiswa terhadap keamanan akun dan perilaku pengamanan akun yang dilaporkan responden dalam penggunaan layanan digital sehari-hari. Penelitian ini tidak memberikan perlakuan atau manipulasi terhadap responden.

Variabel X, yaitu kesadaran keamanan akun, menggambarkan pemahaman dan kepedulian responden terhadap ancaman keamanan digital serta pentingnya melindungi akun. Aspek ini mencakup pemahaman mengenai ancaman seperti phishing dan rekayasa sosial, risiko penggunaan Wi-Fi publik, dampak pengambilalihan akun, pengelolaan kata sandi, serta fungsi autentikasi dua faktor (Two-Factor Authentication, 2FA).

Variabel Y, yaitu perilaku pengamanan akun yang dilaporkan responden, menggambarkan tindakan yang dilaporkan responden dalam penggunaan akun digital sehari-hari. Aspek ini mencakup penggunaan kata sandi yang berbeda, penghindaran penggunaan informasi pribadi, pembaruan kata sandi, aktivasi autentikasi dua faktor, dan penggunaan autentikasi biometrik.

Data penelitian dikumpulkan melalui kuesioner yang diberikan kepada responden sesuai dengan kriteria penelitian. Setelah pengumpulan data, jawaban responden diperiksa kelengkapan dan kesesuaiannya, kemudian ditabulasi untuk dianalisis. Hasil analisis digunakan untuk menggambarkan tingkat kesadaran keamanan akun dan perilaku pengamanan akun yang dilaporkan responden.

Karena data perilaku diperoleh melalui jawaban kuesioner, hasil penelitian menunjukkan perilaku pengamanan akun yang dilaporkan responden dan bukan hasil pemeriksaan langsung terhadap akun mereka. Tahapan pelaksanaan penelitian disajikan pada Gambar 1.



Gambar 1. Tahapan penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan desain survei deskriptif. Pendekatan kuantitatif digunakan untuk mengolah data numerik yang diperoleh dari jawaban responden melalui kuesioner. Desain survei deskriptif bertujuan menggambarkan kesadaran mahasiswa terhadap keamanan akun dan perilaku pengamanan akun yang dilaporkan responden dalam penggunaan layanan digital sehari-hari. Penelitian ini tidak memberikan perlakuan atau manipulasi terhadap responden.

Populasi target dalam penelitian ini adalah mahasiswa aktif program sarjana Universitas Malikussaleh. Responden direkrut dari mahasiswa yang dapat dijangkau peneliti melalui penyebaran kuesioner secara daring di Universitas Malikussaleh selama 7–14 Oktober 2026.

Sampel dipilih menggunakan teknik *non-probability sampling* dengan pendekatan *purposive-convenience sampling*. Pendekatan purposif diterapkan dengan menetapkan karakteristik responden yang sesuai dengan tujuan penelitian, sedangkan pendekatan kemudahan akses berkaitan dengan perekrutan mahasiswa yang dapat dijangkau peneliti. Karena peserta tidak dipilih secara acak, peluang setiap mahasiswa dalam populasi untuk terpilih tidak diketahui.

Responden dapat berpartisipasi apabila memenuhi tiga kriteria, yaitu: (1) berstatus sebagai mahasiswa aktif program sarjana saat pengisian kuesioner; (2) menggunakan sedikitnya tiga jenis platform digital yang relevan dengan penelitian, seperti surel akademik atau SIAKAD, layanan dompet digital atau perbankan, media sosial, dan *e-commerce*; dan (3) bersedia menjadi responden serta mengisi kuesioner sesuai petunjuk.

Target jumlah sampel dalam penelitian ini adalah sekurang-kurangnya 100 responden. Jumlah tersebut ditetapkan sebagai target pengumpulan data untuk analisis deskriptif, bukan sebagai bukti bahwa sampel mewakili seluruh mahasiswa sarjana. Penetapan jumlah tersebut mempertimbangkan keterjangkauan responden dan kebutuhan analisis deskriptif, bukan perhitungan ukuran sampel berdasarkan rumus tertentu.

Data yang dianalisis berasal dari kuesioner responden yang memenuhi kriteria dan memberikan jawaban yang dapat digunakan. Kuesioner yang tidak lengkap atau tidak memenuhi kriteria penelitian dikeluarkan dari analisis. Hasil penelitian ditafsirkan dalam cakupan responden dan konteks perekrutan yang dijelaskan, karena sampel nonprobabilitas tidak mendukung generalisasi statistik secara langsung kepada seluruh mahasiswa sarjana.

Data primer penelitian ini dikumpulkan melalui kuesioner tertutup yang disebar secara daring menggunakan Google Forms. Kuesioner digunakan untuk memperoleh data karakteristik responden serta mengukur kesadaran keamanan akun dan perilaku pengamanan akun yang dilaporkan responden. Sumber data, pengukuran, dan pengkodean setiap variabel dijelaskan pada bagian ini.

Kuesioner terdiri atas dua bagian. Bagian pertama memuat pertanyaan demografis, yaitu program studi, angkatan atau semester, jenis kelamin, dan jenis layanan digital yang paling sering diakses. Bagian kedua memuat 10 butir pernyataan yang mengukur dua variabel, yaitu kesadaran keamanan akun sebagai variabel X dan perilaku pengamanan akun yang dilaporkan sebagai variabel Y.

Masing-masing variabel diukur menggunakan lima butir. Respons untuk setiap pernyataan menggunakan skala Likert lima tingkat, yang umum digunakan untuk mengukur persepsi, sikap, dan perilaku responden (Chyung et al., 2017). Butir kesadaran keamanan akun menggunakan pilihan tingkat persetujuan, sedangkan butir perilaku pengamanan akun menggunakan pilihan frekuensi. Perbedaan tersebut digunakan agar pilihan jawaban sesuai dengan rumusan pernyataan yang dinilai. Skor dan kategori respons disajikan pada Tabel 1.

Tabel 1. Skor dan kategori respons kuesioner

Skor	Tingkat persetujuan	Tingkat frekuensi
5	Sangat Setuju (SS)	Selalu (SL)
4	Setuju (S)	Sering (SR)
3	Netral (N)	Kadang-kadang (KK)
2	Tidak Setuju (TS)	Jarang (JR)
1	Sangat Tidak Setuju (STS)	Tidak Pernah (TP)

Tabel 1 menyajikan skor yang digunakan untuk mengolah jawaban responden pada kuesioner penelitian. Butir pernyataan kesadaran keamanan akun menggunakan kategori tingkat persetujuan, mulai dari sangat tidak setuju hingga sangat setuju. Sementara itu, butir perilaku pengamanan akun menggunakan kategori tingkat frekuensi, mulai dari tidak pernah hingga selalu. Skor tertinggi sebesar 5 diberikan pada jawaban yang menunjukkan kesadaran atau perilaku pengamanan akun yang paling baik, sedangkan skor terendah sebesar 1 diberikan pada jawaban yang menunjukkan kesadaran atau perilaku yang paling rendah. Skor tersebut kemudian dijumlahkan untuk menghitung skor aktual pada masing-masing variabel penelitian.

Skor yang lebih tinggi menunjukkan respons yang lebih positif terhadap aspek yang diukur, setelah memperhatikan arah pernyataan. Apabila terdapat butir negatif, skornya dibalik sebelum penghitungan skor dimensi. Skor tiap dimensi dihitung berdasarkan jawaban pada butir-butir yang mengukurnya. Operasionalisasi dimensi dan indikator instrumen disusun dalam matriks pada Tabel 2.

Tabel 2. Operasionalisasi dimensi dan indikator instrumen

Dimensi	Indikator yang diukur	Jumlah butir	Nomor butir	Jenis respons
Kesadaran keamanan akun	Pemahaman mengenai phishing, risiko Wi-Fi publik, dampak pengambilalihan akun, kata sandi, dan 2FA	5	1-5	Tingkat persetujuan
Perilaku pengamanan akun	Penggunaan kata sandi berbeda, penghindaran informasi pribadi, pembaruan kata sandi, aktivasi 2FA, dan penggunaan biometrik	5	6-10	Tingkat persetujuan

Tabel 2 menjelaskan operasionalisasi dua variabel yang digunakan dalam penelitian ini. Variabel kesadaran keamanan akun sebagai variabel X diukur melalui lima butir pernyataan yang mencakup pemahaman responden terhadap phishing, risiko penggunaan Wi-Fi publik, dampak pengambilalihan akun, pengelolaan kata sandi, serta fungsi autentikasi dua faktor. Variabel perilaku pengamanan akun sebagai variabel Y juga diukur melalui lima butir pernyataan yang mencakup penggunaan kata sandi yang berbeda, penghindaran penggunaan informasi pribadi, pembaruan kata sandi, aktivasi autentikasi dua faktor, dan penggunaan autentikasi biometrik. Butir kesadaran keamanan akun diukur menggunakan tingkat persetujuan, sedangkan butir perilaku pengamanan akun diukur menggunakan tingkat frekuensi. Pembagian tersebut dilakukan agar jenis jawaban responden sesuai dengan karakteristik pernyataan yang dinilai.

Pengumpulan data dilakukan dengan membagikan tautan Google Forms kepada calon responden yang memenuhi kriteria penelitian. Responden mengisi kuesioner secara mandiri. Setelah pengumpulan selesai, jawaban diperiksa untuk memastikan kelengkapan dan kesesuaiannya dengan kriteria responden. Data yang layak dianalisis kemudian diberi kode, ditabulasi, dan diolah menggunakan teknik analisis yang dijelaskan pada bagian teknik pengolahan dan analisis data.

Data kuesioner diolah secara bertahap. Pertama, respons diperiksa untuk memastikan kelengkapan dan kesesuaiannya dengan kriteria responden. Kedua, jawaban diberi kode angka sesuai skala pada instrumen. Ketiga, data ditabulasi dan dianalisis secara deskriptif menggunakan Microsoft Excel. Jumlah respons yang tidak lengkap atau tidak memenuhi kriteria dicatat dan tidak disertakan dalam analisis.

Analisis dilakukan terhadap setiap butir dan setiap variabel, yaitu kesadaran keamanan akun dan perilaku pengamanan akun yang dilaporkan responden. Untuk setiap butir, frekuensi dan persentase jawaban pada masing-masing kategori dilaporkan. Nilai rata-rata digunakan sebagai ringkasan tambahan untuk skor gabungan tiap variabel karena respons Likert bersifat berjenjang (Chyung et al., 2017). Rata-rata skor butir dihitung dengan persamaan (1).

Reliabilitas internal instrumen diuji menggunakan koefisien Cronbach's Alpha untuk menilai konsistensi internal butir-butir dalam setiap variabel. Variabel dinyatakan memiliki konsistensi internal yang dapat diterima apabila nilai Cronbach's Alpha sekurang-kurangnya 0,70 (Taber, 2018). Nilai tersebut merupakan pedoman umum dan ditafsirkan dengan mempertimbangkan jumlah butir pada setiap variabel.

Hasil reliabilitas internal digunakan sebagai informasi tambahan untuk menilai konsistensi jawaban responden pada masing-masing variabel. Nilai alpha tidak membuktikan validitas konstruk atau akurasi jawaban responden. Dalam penelitian ini, reliabilitas internal dihitung pada 100 respons utama, bukan pada uji coba terpisah 30 responden.

$$\bar{x}_i = \frac{\sum_{j=1}^n x_{ij}}{n} \quad (1)$$

dengan $\bar{x}_i$ sebagai rata-rata skor butir ke- i , x_{ij} sebagai skor jawaban responden ke- j pada butir tersebut, dan n sebagai jumlah responden dengan jawaban yang dapat dianalisis. Rata-rata skor dimensi dihitung dari skor seluruh butir dalam dimensi tersebut. Indeks capaian setiap dimensi dihitung menggunakan persamaan (2).

$$\text{Indeks capaian (\%)} = \frac{\text{Skor aktual}}{\text{Skor maksimum}} \times 100\% \quad (2)$$

Skor aktual adalah jumlah skor jawaban responden pada seluruh butir dalam dimensi yang dianalisis. Skor maksimum dihitung dengan mengalikan jumlah butir pada dimensi, jumlah responden yang dianalisis, dan skor tertinggi skala, yaitu 5. Apabila terdapat butir negatif, skornya dibalik terlebih dahulu sebelum skor aktual dihitung. Indeks capaian diinterpretasikan berdasarkan kategori pada Tabel 3.

Tabel 3. Kategori interpretasi indeks capaian

Indeks capaian	Kategori
81,01%–100,00%	Sangat tinggi
61,01%–<81,00%	Tinggi
41,01%–<61,00%	Sedang
21,01%–<41,00%	Rendah
0,00%–<21,00%	Sangat rendah

Tabel 3 digunakan untuk menginterpretasikan hasil indeks capaian pada variabel kesadaran keamanan akun dan perilaku pengamanan akun. Indeks capaian diperoleh dengan membandingkan skor aktual yang diperoleh responden dengan skor maksimum yang dapat dicapai, kemudian dikalikan 100. Indeks capaian sebesar 81,01 hingga 100,00 dikategorikan sebagai sangat tinggi, sedangkan indeks capaian sebesar 61,01 hingga 81,00 dikategorikan sebagai tinggi. Kategori sedang berada pada rentang 41,01 hingga 61,00, kategori rendah berada pada rentang 21,01 hingga 41,00, dan kategori sangat rendah berada pada rentang 0,00 hingga 21,00. Kategori tersebut digunakan untuk menggambarkan tingkat kesadaran dan perilaku pengamanan akun responden secara deskriptif.

Hasil indeks capaian dibandingkan secara deskriptif untuk melihat pola perbedaan antara kesadaran keamanan akun dan perilaku pengamanan akun yang dilaporkan responden. Perbandingan tersebut digunakan untuk membahas kesenjangan deskriptif antarvariabel; tanpa uji statistik komparatif, hasilnya tidak ditafsirkan sebagai perbedaan yang signifikan secara statistik atau sebagai hubungan sebab-akibat.

Selain analisis deskriptif, hubungan antara kesadaran keamanan akun dan perilaku pengamanan akun yang dilaporkan dianalisis menggunakan uji korelasi Spearman dengan taraf signifikansi 5% ($\alpha=0,05$; $\alpha=0,05$). Hasil korelasi digunakan untuk menelaah keterkaitan antara skor kesadaran dan skor perilaku, bukan untuk membuktikan hubungan sebab-akibat.

HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil analisis data kuesioner dan pembahasannya sesuai tujuan penelitian. Hasil disajikan secara deskriptif melalui tabel dan, bila diperlukan, gambar atau grafik. Pembahasan menguraikan makna temuan pada kesadaran keamanan akun dan perilaku pengamanan akun yang dilaporkan responden, menghubungkannya dengan penelitian terdahulu, serta menjelaskan keterbatasan penelitian.

Sebanyak 100 respons dianalisis dalam penelitian ini. Karakteristik responden meliputi jenis kelamin, angkatan atau semester, serta pengalaman insiden keamanan. Rincian karakteristik responden disajikan pada Tabel 1. Mayoritas responden merupakan mahasiswa angkatan 2024 dengan semester 5–6, yaitu sebanyak 59 responden atau 59,00%. Sebanyak 54 responden atau 54,00% berjenis kelamin laki-laki, sedangkan 46 responden atau 46,00% berjenis kelamin perempuan.

Tabel 4. Karakteristik responden

Karakteristik	Kategori	n	%
Jenis Kelamin	Laki-laki	54	54.00
Jenis Kelamin	Perempuan	46	46.00
Angkatan / Semester	2024 / 5-6	59	59.00
Angkatan / Semester	2025 / 3-4	22	22.00
Angkatan / Semester	2026 / 1-2	11	11.00
Angkatan / Semester	2023 / 7-8	8	8.00
Pengalaman Insiden Keamanan: "Pernakah akun digital Anda mengalami upaya peretasan, pembajakan (takeover), atau menerima tautan penipuan (phising)?"	Tidak Pernah	49	49.00
Pengalaman Insiden Keamanan: "Pernakah akun digital Anda mengalami upaya peretasan, pembajakan (takeover), atau menerima tautan penipuan (phising)?"	Pernah	33	33.00
Pengalaman Insiden Keamanan: "Pernakah akun digital Anda mengalami upaya peretasan, pembajakan (takeover), atau menerima tautan penipuan (phising)?"	Ragu-ragu / Tidak Tahu	18	18.00

Tabel 5. Indeks seluruh respons

Variabel	Skor aktual	Skor maksimum	Indeks (%)	Kategori
Kesadaran (X)	2033	2500	81,32	Sangat tinggi
Perilaku (Y)	1939	2500	77,56	Tinggi

Tabel 5 menyajikan hasil perhitungan indeks capaian untuk variabel kesadaran keamanan akun dan perilaku pengamanan akun berdasarkan 100 respons yang dianalisis. Variabel kesadaran keamanan akun memperoleh skor aktual sebesar 2.033 dari skor maksimum 2.500, sehingga menghasilkan indeks capaian sebesar 81,32 dan berada pada kategori sangat tinggi. Sementara itu, variabel perilaku pengamanan akun memperoleh skor aktual sebesar 1.939 dari skor maksimum 2.500, sehingga menghasilkan indeks capaian sebesar 77,56 dan berada pada kategori tinggi. Hasil tersebut menunjukkan bahwa responden memiliki tingkat kesadaran keamanan akun yang sangat tinggi, tetapi perilaku pengamanan akun yang dilaporkan berada pada kategori tinggi. Indeks kesadaran lebih tinggi daripada indeks perilaku dengan selisih sebesar 3,76 poin persentase. Perbedaan tersebut mengindikasikan adanya kesenjangan deskriptif antara kesadaran keamanan akun dan perilaku pengamanan akun yang dilaporkan responden, meskipun perbedaan tersebut belum diuji secara statistik.

Tabel 6. Hasil uji reliabilitas per dimensi

Butir	Indikator ringkas	Indeks (%)
1	Phishing	80.80
2	Wi-Fi publik	77.40
3	Dampak pengambilalihan	85.00
4	Komposisi kata sandi	85.20
5	Fungsi 2FA	78.20
6	Kata sandi berbeda	76.00
7	Menghindari informasi pribadi	78.60
8	Pembaruan kata sandi	73.80
9	Aktivasi 2FA	78.20
10	Biometrik	81.20

Tabel 6 menyajikan indeks capaian untuk setiap butir pernyataan pada kuesioner penelitian. Berdasarkan hasil analisis, butir dengan indeks tertinggi adalah komposisi kata sandi sebesar 85,20, diikuti oleh dampak pengambilalihan akun sebesar 85,00. Hasil tersebut menunjukkan bahwa responden memiliki pemahaman yang baik mengenai pentingnya menyusun kata sandi yang kuat serta dampak yang dapat terjadi apabila akun mengalami pengambilalihan. Sementara itu, butir dengan indeks terendah adalah pembaruan kata sandi sebesar 73,80, diikuti oleh penggunaan kata sandi yang berbeda sebesar 76,00. Temuan tersebut mengindikasikan bahwa aspek pengelolaan kata sandi masih menjadi area yang perlu diperkuat melalui edukasi keamanan akun. Secara keseluruhan, seluruh butir pernyataan

memiliki indeks capaian di atas 70, sehingga menunjukkan bahwa responden memiliki tingkat kesadaran dan perilaku pengamanan akun yang relatif baik. Namun, hasil pada butir terkait pembaruan kata sandi dan penggunaan kata sandi yang berbeda menunjukkan bahwa praktik pengamanan akun masih dapat ditingkatkan.

Tabel 7. Analisis korelasi dan reliabilitas

Statistik	Nilai	Cakupan
Spearman rho	0,747	100 respons
p	<0,001	100 respons
Alpha X	0.931	100 respons utama
Alpha Y	0.899	100 respons utama

Tabel 7 menyajikan hasil uji korelasi Spearman dan uji reliabilitas Cronbach's Alpha terhadap 100 respons yang dianalisis. Hasil uji korelasi Spearman menunjukkan nilai koefisien korelasi sebesar 0,747 dengan nilai signifikansi 0,001. Nilai tersebut menunjukkan adanya hubungan positif dan kuat antara kesadaran keamanan akun dan perilaku pengamanan akun yang dilaporkan responden. Artinya, semakin tinggi kesadaran keamanan akun responden, semakin tinggi pula kecenderungan mereka melaporkan perilaku pengamanan akun yang baik. Namun, hubungan tersebut bersifat korelasional dan tidak dapat ditafsirkan sebagai hubungan sebab-akibat. Hasil uji reliabilitas menunjukkan nilai Cronbach's Alpha sebesar 0,931 untuk variabel kesadaran keamanan akun dan sebesar 0,899 untuk variabel perilaku pengamanan akun. Nilai tersebut berada di atas 0,70 sehingga menunjukkan bahwa butir pernyataan pada masing-masing variabel memiliki konsistensi internal yang sangat tinggi. Meskipun demikian, nilai Cronbach's Alpha hanya menilai konsistensi internal instrumen dan tidak membuktikan validitas konstruk maupun akurasi jawaban responden.

Berdasarkan Tabel 7, hasil uji korelasi Spearman menunjukkan hubungan positif yang kuat antara kesadaran keamanan akun dan perilaku pengamanan akun yang dilaporkan responden, dengan nilai $\rho=0,747$; $\rho=0,747$ dan $p<0,001$ $p<0,001$. Hasil tersebut menunjukkan bahwa responden dengan tingkat kesadaran keamanan akun yang lebih tinggi cenderung melaporkan perilaku pengamanan akun yang lebih tinggi. Hubungan ini bersifat korelasional dan tidak dapat ditafsirkan sebagai hubungan sebab-akibat.

Nilai koefisien alpha untuk kesadaran keamanan akun sebesar 0,931, sedangkan nilai koefisien alpha untuk perilaku pengamanan akun yang dilaporkan sebesar 0,899. Nilai tersebut menunjukkan konsistensi internal yang tinggi pada masing-masing kelompok pernyataan. Namun, nilai alpha hanya menilai konsistensi internal dan tidak membuktikan validitas konstruk atau akurasi jawaban responden.

Temuan ini perlu ditafsirkan secara hati-hati karena data perilaku diperoleh melalui laporan mandiri dan belum sepenuhnya dikonfirmasi kesesuaiannya dengan kriteria mahasiswa aktif program sarjana Universitas Malikussaleh. Oleh karena itu, hasil korelasi menggambarkan hubungan antara skor kesadaran dan skor perilaku yang dilaporkan pada 100 respons yang tersedia, bukan bukti bahwa perilaku keamanan akun telah dilakukan secara langsung atau diverifikasi.

KESIMPULAN

Berdasarkan analisis terhadap 100 respons, kesadaran keamanan akun dalam penggunaan layanan digital mencapai indeks sebesar 81,32% dan berada pada kategori sangat tinggi, sedangkan perilaku pengamanan akun yang dilaporkan responden mencapai 77,56% dan berada pada kategori tinggi berdasarkan kriteria interpretasi penelitian. Indeks kesadaran lebih tinggi daripada indeks perilaku dengan selisih 3,76 poin persentase. Selisih tersebut menunjukkan perbedaan deskriptif antara pemahaman yang dilaporkan dan praktik pengamanan akun, tetapi belum membuktikan adanya perbedaan yang signifikan secara statistik.

Uji korelasi Spearman menunjukkan hubungan positif antara kesadaran keamanan akun dan perilaku pengamanan akun ($\rho=0,747$; $\rho=0,747$; $p<0,001$ $p<0,001$). Hasil tersebut menunjukkan bahwa responden dengan skor kesadaran yang lebih tinggi cenderung memiliki skor perilaku pengamanan yang lebih tinggi. Namun, hubungan ini tidak membuktikan bahwa peningkatan kesadaran menyebabkan perubahan perilaku.

Temuan tersebut dapat menjadi masukan awal bagi penyusunan edukasi keamanan akun yang menggabungkan pemahaman tentang ancaman digital dengan praktik pengamanan akun. Program edukasi dapat mencakup pengelolaan kata sandi yang unik, pengenalan *phishing*, serta penggunaan autentikasi dua faktor. Rekomendasi ini merupakan implikasi praktis yang dapat dipertimbangkan, bukan bukti efektivitas program yang telah diuji dalam penelitian.

Hasil penelitian masih bersifat eksploratif karena kesesuaian seluruh respons dengan kriteria mahasiswa aktif program sarjana Universitas Malikussaleh dan penggunaan minimal tiga kelompok layanan digital belum sepenuhnya dikonfirmasi. Selain itu, data diperoleh melalui laporan mandiri dan bukan pemeriksaan langsung terhadap keamanan akun. Oleh karena itu, hasil belum dapat digeneralisasikan kepada seluruh mahasiswa Universitas Malikussaleh. Penelitian selanjutnya perlu memastikan kelayakan responden, memperluas cakupan sampel, dan mengevaluasi efektivitas program edukasi keamanan akun.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada seluruh mahasiswa Universitas Malikussaleh yang telah bersedia menjadi responden dan memberikan jawaban dalam kuesioner penelitian ini. Penulis juga mengucapkan terima kasih kepada Universitas Malikussaleh atas dukungan akademik dan fasilitas yang diberikan selama proses penelitian.

REFERENSI

- Adeshola, I., & Oluwajana, D. I. (2025). Assessing cybersecurity awareness among university students: Implications for educational interventions. *Journal of Computers in Education*, 12(4), 1283–1305. <https://doi.org/10.1007/s40692-024-00346-7>
- Ahamed, B., Polas, M. R. H., Kabir, A. I., Sohel-Uz-Zaman, A. S. M., Fahad, A. A., Chowdhury, S., & Dey, M. R. (2024). Empowering students for cybersecurity awareness management in the emerging digital era: The role of cybersecurity attitude in the 4.0 industrial revolution era. *SAGE Open*, 14(1), 21582440241228920. <https://doi.org/10.1177/21582440241228920>
- Al Zaidy, A. (2025). Measuring cybersecurity awareness of students: A study of state college students. *Journal of Information Technology, Cybersecurity, and Artificial Intelligence*, 2(3), 17–40. <https://doi.org/10.70715/jitcai.2025.v2.i3.030>
- Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences*, 12(5), 2589. <https://doi.org/10.3390/app12052589>
- Baraković, S., & Baraković Husić, J. (2023). Cyber hygiene knowledge, awareness, and behavioral practices of university students. *Information Security Journal: A Global Perspective*, 32(5), 347–370. <https://doi.org/10.1080/19393555.2022.2088428>
- Bognár, L., & Bottyán, L. (2024). Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. *Education Sciences*, 14(6), 588. <https://doi.org/10.3390/educsci14060588>
- Bottyán, L. (2023). Cybersecurity awareness among university students. *Journal of Applied Technical and Educational Sciences*, 13(3), 363. <https://doi.org/10.24368/jates.363>
- Chyung, S. Y., Roberts, K., Swanson, I., & Hankinson, A. (2017). Evidence-based survey design: The use of a midpoint on the Likert scale. *Performance Improvement*, 56(10), 15–23. <https://doi.org/10.1002/pfi.21727>
- Du, J., Kalafut, A., & Schymik, G. (2024). The health belief model and phishing: Determinants of preventative security behaviors. *Journal of Cybersecurity*, 10(1), 1–17. <https://doi.org/10.1093/cybsec/tyae012>
- Gwenhure, A. K. (2025). University students' security behavior against email phishing attacks: Insights from the health belief model. *Journal of Cybersecurity*, 11(1), tyaf034. <https://doi.org/10.1093/cybsec/tyaf034>
- Guo, H., & Tınmaz, H. (2023). A survey on college students' cybersecurity awareness and education from the perspective of China. *Journal for the Education of Gifted Young Scientists*, 11(3), 351–367.
- Mai, P. T., & Tick, A. (2021). Cyber security awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam. *Acta Polytechnica Hungarica*, 18(2), 67–89.
- National Institute of Standards and Technology. (2025). Digital identity guidelines (NIST Special Publication 800-63-4). <https://csrc.nist.gov/pubs/sp/800/63/4/final>
- Okokpujie, K., Ariyo, M. A., Moninuola, F. S., & Akanle, M. B. (2025). Evaluating students' vulnerability and awareness to phishing attacks. *International Journal of Safety and Security Engineering*, 15(3), 1–10.
- Parsons, K., Calic, D., Pattinson, M., Butavicius, A., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, 66, 40–51. <https://doi.org/10.1016/j.cose.2017.01.004>
- Sivakumar, S., & Venkataraman, S. (2025). Cracks in digital defense: A study on password security awareness and behavior in college students. *ICTACT Journal on Soft Computing*, 16(3), 4030–4035. <https://doi.org/10.21917/ijsc.2025.0557>
- Taber, K. S. (2018). The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in Science Education*, 48(6), 1273–1296. <https://doi.org/10.1007/s11165-016-9602-2>
- Wash, R., & Rader, E. (2021). Prioritizing security over usability: Strategies for how people choose passwords. *Journal of Cybersecurity*, 7(1), tyab012. <https://doi.org/10.1093/cybsec/tyab012>
- Xu, X., Hong, W. C. H., Kolletar-Zhu, K., Zhang, Y., & Chi, C. (2024). Validation and application of the Human Aspects of Information Security Questionnaire for undergraduates: Effects of gender, discipline and grade level. *Behaviour & Information Technology*, 43(12), 2799–2820. <https://doi.org/10.1080/0144929X.2023.2260876>