Jejakdigital
JURNAL ILMIAH MULTIDISIPLIN
Available online at https://indojurnal.com/index.php/jejakdigital

eISSN 3089-7734; pISSN 3089-7742
Vol. 1, No. 3, Mei 2025
doi.org/10.63822/vmtade43
Hal. 567-577

Determinasi Faktor-Faktor Kesadaran Pengguna *Mobile Banking* terhadap Ancaman Keamanan Siber di Era Digital

Stevani Matandatu
Prodi Sistem dan Teknologi Informasi Fakultas Ilmu Alam dan Teknologi Rekayasa
Universitas Halmahera

Corresponding Author's Email: stevanimatandatu22@gmail.com

Sejarah Artikel:

Diterima *24-05-2025*
Disetujui *25-05-2025*
Diterbitkan *27-05-2025*

ABSTRACT

The rapid development of digital technology has significantly increased the use of mobile banking services, which offer convenience but also increase the risk of cybersecurity threats. This study aims to determine the factors that influence user awareness of cybersecurity threats in mobile banking services in the digital era. A quantitative survey was conducted on 100 active mobile banking users in urban areas of Indonesia. Data were collected using a structured questionnaire that measured the level of cybersecurity knowledge, security behavior and practices, and perception of cyberthreat risk. Descriptive statistical analysis and multiple linear regression were used to test the relationship between variables. The results showed that cybersecurity knowledge, such as awareness of phishing, the importance of updating applications, and the risk of using weak passwords, had a significant effect on user risk perception. In addition, security behaviors such as using different passwords, activating two-factor authentication (2FA), and changing passwords regularly also increased the risk perception. Social and environmental factors, including formal education, on-the-job training, and community discussions, also played an important role in increasing digital literacy and user awareness. These findings emphasize the importance of an integrated approach that combines ongoing education, easy-to-use security technology, and social environmental support to strengthen mobile banking security awareness. Recommendations include intensifying educational programs tailored to digital literacy levels and developing automated security features that encourage protective behavior. This study provides empirical contributions to the development of cybersecurity protection policies and strategies in the digital era.

Keywords: *Cybersecurity Awareness, Mobile Banking, Risk Perception, User Security Behavior*

ABSTRAK

Perkembangan pesat teknologi digital telah meningkatkan penggunaan layanan mobile banking secara signifikan, yang menawarkan kemudahan namun juga meningkatkan risiko ancaman keamanan siber. Penelitian ini bertujuan untuk menentukan faktor-faktor yang memengaruhi kesadaran pengguna terhadap ancaman keamanan siber pada layanan mobile banking di era digital. Survei kuantitatif dilakukan terhadap 100 pengguna aktif mobile banking di wilayah perkotaan Indonesia. Data dikumpulkan menggunakan kuesioner terstruktur yang mengukur tingkat pengetahuan keamanan siber, perilaku dan praktik keamanan, serta persepsi risiko ancaman siber. Analisis statistik deskriptif dan regresi linier berganda digunakan untuk menguji hubungan antar variabel. Hasil penelitian menunjukkan bahwa pengetahuan keamanan siber, seperti kesadaran terhadap phishing, pentingnya pembaruan aplikasi, dan risiko penggunaan password lemah, berpengaruh signifikan terhadap persepsi risiko pengguna. Selain itu, perilaku keamanan seperti penggunaan password berbeda, pengaktifan otentikasi dua faktor (2FA), dan penggantian password secara rutin juga meningkatkan persepsi risiko tersebut. Faktor sosial dan lingkungan, termasuk edukasi formal, pelatihan di tempat kerja, dan diskusi komunitas, turut berperan penting dalam meningkatkan literasi digital dan kesadaran pengguna. Temuan ini menegaskan pentingnya pendekatan terintegrasi yang menggabungkan edukasi berkelanjutan, teknologi keamanan yang mudah digunakan, serta dukungan lingkungan sosial untuk memperkuat kesadaran keamanan mobile banking. Rekomendasi mencakup intensifikasi program edukasi yang disesuaikan dengan tingkat literasi digital serta pengembangan fitur keamanan otomatis yang mendorong perilaku protektif. Penelitian ini memberikan kontribusi empiris bagi pengembangan kebijakan dan strategi perlindungan keamanan siber di era digital.

Katakunci: Kesadaran Keamanan Siber, Mobile Banking, Persepsi Risiko, Perilaku Keamanan Pengguna

Bagaimana Cara Sitasi Artikel ini:

Matandatu, S. (2025). Determinasi Faktor-Faktor Kesadaran Pengguna Mobile Banking terhadap Ancaman Keamanan Siber di Era Digital: Determining the Factors Influencing Mobile Banking Users' Awareness of Cybersecurity Threats in the Digital Era. Jejak Digital: Jurnal Ilmiah Multidisiplin, 1(3), 567-577. https://doi.org/10.63822/vmtade43

PENDAHULUAN

Perkembangan pesat teknologi digital dan meningkatnya penggunaan perangkat mobile telah mendorong adopsi layanan mobile banking secara masif di masyarakat. Mobile banking menawarkan kemudahan akses transaksi keuangan kapan saja dan di mana saja, sehingga menjadi solusi populer di era digital. Namun, kemudahan ini juga diiringi oleh meningkatnya risiko keamanan siber yang mengancam data dan transaksi pengguna. Ancaman seperti phishing, malware, pencurian data, dan serangan ransomware menjadi tantangan utama yang harus dihadapi oleh penyedia layanan maupun pengguna mobile banking (Smith et al., 2023; Liu et al., 2022; Rahman et al., 2020). Kesadaran pengguna terhadap ancaman keamanan siber menjadi faktor kritis dalam menjaga keamanan transaksi dan data pribadi. Pengguna yang memiliki tingkat kesadaran tinggi cenderung lebih berhati-hati dan menerapkan langkah-langkah keamanan yang tepat, sehingga risiko serangan dapat diminimalisasi. Sebaliknya, kurangnya kesadaran dapat membuka celah keamanan yang berpotensi menimbulkan kerugian finansial dan menurunkan kepercayaan pengguna terhadap layanan (Muliawan & Hasnawati, 2024; Alrababah et al., 2024). Oleh karena itu, pemahaman mendalam tentang faktor-faktor yang memengaruhi kesadaran pengguna mobile banking sangat penting untuk dikaji dalam konteks keamanan digital saat ini

Meskipun teknologi keamanan terus berkembang, kasus insiden keamanan pada mobile banking masih sering terjadi, yang menunjukkan adanya ketidakseimbangan antara kemampuan teknis sistem dan kesadaran pengguna (Arisya et al., 2020). Permasalahan utama dalam penelitian ini adalah bagaimana faktor-faktor internal dan eksternal memengaruhi kesadaran pengguna mobile banking terhadap ancaman keamanan siber. Tingkat pengetahuan pengguna tentang keamanan siber dan perilaku keamanan yang diterapkan menjadi aspek penting dalam membentuk kesadaran tersebut (Hutagaol et al., 2024). Selain itu, pengaruh lingkungan sosial dan edukasi turut membentuk persepsi risiko serta tindakan protektif yang diambil pengguna (Kornitasari et al., 2024). Solusi umum yang diusulkan adalah melalui pendekatan edukasi dan sosialisasi yang terintegrasi serta penyediaan teknologi keamanan yang mudah digunakan oleh pengguna, meskipun studi empiris terkait faktor-faktor determinan ini dalam konteks lokal masih terbatas (Orucho et al., 2023).

Penelitian terdahulu menunjukkan bahwa tingkat pengetahuan keamanan siber merupakan faktor utama yang membentuk kesadaran dan persepsi risiko pengguna. Pengguna yang memahami ancaman seperti phishing dan pentingnya pembaruan aplikasi lebih cenderung menerapkan praktik keamanan yang tepat (Putra et al., 2024). Chen et al. (2019) menyoroti pentingnya edukasi keamanan dalam meningkatkan kewaspadaan pengguna terhadap serangan siber pada layanan digital. Selain pengetahuan, perilaku keamanan pengguna juga berperan penting. Zhang et al. (2022) menemukan bahwa aktivasi otentikasi dua faktor dan penggunaan password unik secara signifikan menurunkan risiko pembobolan akun. Namun, mereka juga mencatat adanya kesenjangan dalam konsistensi pengguna menerapkan praktik tersebut, yang dipengaruhi oleh tingkat literasi digital dan sikap terhadap risiko (Mustapha & Alabi, 2022; Mouncey & Ciobotaru, 2025).

Faktor sosial dan lingkungan turut memberikan kontribusi dalam pembentukan kesadaran keamanan. Komunikasi sosial dan edukasi formal di institusi pendidikan maupun tempat kerja terbukti meningkatkan pemahaman dan kesiapan pengguna menghadapi ancaman siber (Zakirova & Pol, 2024; Banjarnahor, 2022). Hal ini menunjukkan perlunya pendekatan holistik yang mengintegrasikan edukasi, teknologi, dan interaksi sosial dalam strategi keamanan mobile banking. Meskipun demikian, gap riset masih ditemukan terkait analisis empiris yang mengkaji hubungan antara tingkat pengetahuan, perilaku, dan persepsi risiko

dalam konteks penggunaan mobile banking di Indonesia, sehingga penelitian ini mengisi kekosongan tersebut.

Penelitian ini bertujuan untuk mendeterminasi faktor-faktor yang memengaruhi kesadaran pengguna mobile banking terhadap ancaman keamanan siber di era digital. Secara spesifik, penelitian ini ingin mengidentifikasi peran tingkat pengetahuan keamanan siber, perilaku dan praktik keamanan pengguna, serta pengaruh lingkungan sosial dan edukasi dalam membentuk persepsi risiko ancaman siber.

Penelitian juga bertujuan memberikan rekomendasi strategis bagi penyedia layanan mobile banking dan pembuat kebijakan terkait pengembangan program edukasi keamanan serta penguatan teknologi protektif yang efektif dan mudah diakses oleh pengguna. Penelitian ini berfokus pada pengguna mobile banking di wilayah perkotaan di Indonesia, dengan melibatkan responden dari berbagai latar belakang demografis dan tingkat literasi digital. Variabel yang dikaji meliputi tingkat pengetahuan keamanan siber, perilaku dan praktik keamanan pengguna, pengaruh sosial dan edukasi, serta persepsi risiko terhadap ancaman siber.

Data dikumpulkan melalui survei kuantitatif dan dianalisis menggunakan metode statistik deskriptif dan inferensial, termasuk regresi linier berganda untuk mengetahui pengaruh variabel independen terhadap persepsi risiko. Penelitian ini tidak mencakup analisis teknis sistem keamanan mobile banking secara mendalam, melainkan fokus pada aspek pengguna sebagai ujung tombak keamanan digital.

METODE

Penelitian ini menggunakan kuesioner terstruktur sebagai alat pengumpulan data utama. Kuesioner disusun berdasarkan variabel utama penelitian, yaitu tingkat pengetahuan keamanan siber, perilaku dan praktik keamanan pengguna mobile banking, serta persepsi risiko ancaman siber. Setiap variabel diukur menggunakan beberapa indikator yang sudah disesuaikan dengan literatur dan dikembangkan untuk konteks pengguna mobile banking. Sebelum digunakan secara luas, instrumen ini diuji validitas dan reliabilitasnya melalui studi pendahuluan (pilot study) untuk memastikan keakuratan dan konsistensi pengukuran.

1. Sampel Penelitian

Sampel penelitian terdiri dari 100 responden pengguna aktif mobile banking yang dipilih menggunakan teknik purposive sampling. Kriteria inklusi meliputi pengguna mobile banking yang telah aktif menggunakan layanan minimal enam bulan, berusia di atas 18 tahun, dan bersedia mengisi kuesioner secara lengkap. Sampel diambil dari wilayah perkotaan di Indonesia untuk mencerminkan pengguna dengan tingkat akses teknologi yang memadai. Data demografis seperti usia, pendidikan, dan pekerjaan dikumpulkan untuk memberikan gambaran karakteristik responden dan mendukung analisis variabel demografis sebagai variabel kontrol.

2. Desain Penenelitian

Penelitian ini menggunakan desain survei kuantitatif dengan pendekatan cross-sectional yang bertujuan menggambarkan keadaan variabel secara bersamaan pada waktu pengumpulan data. Pengumpulan data dilakukan secara daring menggunakan platform survei elektronik, yang dipilih untuk efisiensi dan kemudahan akses responden dalam kondisi pembatasan sosial.

Kuesioner terdiri atas pertanyaan yang menggunakan skala Likert 5 poin, dari 1 (sangat tidak setuju) hingga 5 (sangat setuju), untuk mengukur persepsi dan praktik pengguna. Instrumen mencakup pertanyaan tentang pengetahuan keamanan siber, perilaku keamanan, dan persepsi risiko ancaman. Setelah data terkumpul, dilakukan pemeriksaan kelengkapan dan validitas data untuk memastikan kualitas sebelum proses analisis.

3. Parameters Penelitian

Penelitian ini mengukur tiga variabel utama dengan indikator berikut:

a. Tingkat Pengetahuan Keamanan Siber: Meliputi pemahaman tentang phishing dan cara menghindarinya, pentingnya pembaruan aplikasi keamanan, serta risiko penggunaan password yang lemah.
b. Perilaku dan Praktik Keamanan Pengguna: Termasuk penggunaan password unik untuk akun mobile banking, pengaktifan otentikasi dua faktor (2FA), dan kebiasaan rutin mengganti password atau PIN.
c. Persepsi Risiko terhadap Ancaman Siber: Mengacu pada tingkat kewaspadaan dan kesadaran pengguna terhadap potensi ancaman yang dapat terjadi dalam penggunaan mobile banking.

Setiap indikator diukur melalui pernyataan yang harus dijawab responden sesuai tingkat persetujuan mereka pada skala Likert, sehingga memungkinkan analisis kuantitatif yang detail terhadap setiap aspek variabel.

4. Analisis Data

Data yang diperoleh dianalisis menggunakan metode statistik deskriptif dan inferensial dengan perangkat lunak SPSS versi terbaru. Statistik deskriptif meliputi rata-rata (mean), median, standar deviasi, skewness, dan kurtosis untuk menggambarkan karakteristik distribusi data dan tingkat variabel yang diukur.

Untuk menguji hubungan dan pengaruh variabel independen (tingkat pengetahuan dan perilaku keamanan) terhadap variabel dependen (persepsi risiko ancaman siber), digunakan analisis regresi linier berganda. Uji validitas dan reliabilitas instrumen dilakukan terlebih dahulu untuk memastikan instrumen dapat mengukur variabel dengan tepat dan konsisten, menggunakan uji Cronbach's Alpha untuk reliabilitas.

Multikolinearitas antar variabel diuji dengan Variance Inflation Factor (VIF), dengan nilai VIF di bawah 5 dianggap tidak menunjukkan adanya masalah multikolinearitas. Seluruh analisis ini bertujuan untuk mengidentifikasi faktor-faktor determinan yang memengaruhi kesadaran keamanan pengguna mobile banking dan memberikan landasan empiris untuk rekomendasi strategis dalam penguatan keamanan siber.

HASIL

1. Tingkat Pengetahuan Keamanan Siber

Untuk menggambarkan tingkat pengetahuan pengguna mobile banking terkait keamanan siber, dilakukan analisis statistik deskriptif terhadap tiga indikator utama. Ketiga indikator ini mencakup pemahaman pengguna mengenai phishing, pentingnya pembaruan keamanan aplikasi, dan risiko penggunaan password lemah. Hasil statistik deskriptif yang meliputi nilai mean, median, standar deviasi, nilai minimum dan maksimum, skewness, serta kurtosis disajikan dalam Tabel 1 berikut. Data ini memberikan gambaran umum mengenai sebaran dan kecenderungan respon pengguna terhadap aspek-aspek dasar keamanan siber.

Tabel 1. Statistik Deskriptif Tingkat Pengetahuan Keamanan Siber Pengguna Mobile Banking

Indikator	Mean	Median	Std. Dev	Min	Max	Skewness	Kurtosis
Mengetahui phishing dan cara menghindarinya	4.12	4	0.75	2	5	-0.85	1.30
Memahami pentingnya pembaruan keamanan aplikasi	3.95	4	0.80	1	5	-0.45	0.50
Mengenal risiko penggunaan password lemah	4.05	4	0.70	2	5	-0.70	1.10

Analisis statistik deskriptif pada Tabel 1 menunjukkan tingkat pengetahuan keamanan siber pengguna mobile banking terhadap berbagai aspek ancaman keamanan. Tabel tersebut melaporkan nilai mean, median, standar deviasi, serta parameter distribusi data seperti skewness dan kurtosis untuk tiga indikator utama. Pertama, indikator "Mengetahui phishing dan cara menghindarinya" memperoleh nilai mean sebesar 4.12 dan median 4 pada skala 1–5, yang menunjukkan bahwa sebagian besar responden memiliki pengetahuan yang cukup baik tentang phishing dan strategi pencegahannya. Nilai standar deviasi 0.75 menandakan variasi yang relatif kecil dalam pengetahuan ini antar pengguna. Distribusi data yang skewness-nya negatif (-0.85) mengindikasikan bahwa sebagian besar responden menilai pengetahuan ini di atas rata-rata, sementara kurtosis 1.30 menunjukkan distribusi data yang sedikit lebih puncak dari distribusi normal.

Indikator kedua, "Memahami pentingnya pembaruan keamanan aplikasi," menunjukkan nilai mean 3.95 dan median 4, yang juga menandakan kesadaran yang cukup tinggi terhadap pentingnya menjaga aplikasi tetap terbaru untuk mengurangi risiko keamanan. Standar deviasi 0.80 mencerminkan adanya sedikit variasi pengetahuan antar pengguna, dengan skewness -0.45 yang mengindikasikan distribusi cenderung condong ke penilaian positif namun lebih merata dibandingkan indikator pertama. Kurtosis 0.50 mengindikasikan distribusi data yang mendekati normal.

Untuk indikator ketiga, "Mengenal risiko penggunaan password lemah," nilai mean sebesar 4.05 dengan median 4 mengonfirmasi bahwa pengguna secara umum memahami risiko dari penggunaan password yang tidak kuat. Standar deviasi sebesar 0.70 menunjukkan homogenitas relatif dalam pengetahuan ini. Distribusi skewness negatif (-0.70) juga menegaskan kecenderungan mayoritas pengguna menilai pengetahuan ini tinggi, dan kurtosis 1.10 menunjukkan distribusi yang sedikit lebih puncak. Secara keseluruhan, data menunjukkan bahwa tingkat pengetahuan pengguna mobile banking terhadap aspek keamanan siber utama berada pada level yang cukup tinggi, dengan sebagian besar pengguna memahami risiko dan mekanisme perlindungan dasar. Hal ini menjadi dasar penting dalam membangun kesadaran keamanan yang efektif. Selain pengetahuan individu, faktor sosial dan lingkungan juga berperan signifikan dalam membentuk kesadaran keamanan pengguna mobile banking. Interaksi sosial, seperti diskusi dengan keluarga, teman, dan komunitas pengguna, memberikan saluran efektif untuk pertukaran informasi dan pengalaman terkait ancaman keamanan siber.

Hasil survei menunjukkan bahwa responden yang secara aktif berdiskusi mengenai keamanan siber dengan lingkungan sosialnya memiliki tingkat kesadaran yang lebih tinggi. Diskusi ini tidak hanya meningkatkan pengetahuan teknis, tetapi juga memperkuat sikap waspada dan perilaku protektif dalam penggunaan mobile banking. Lingkungan kerja dan institusi pendidikan juga berkontribusi dalam membentuk kesadaran. Responden yang menerima pelatihan atau sosialisasi tentang keamanan siber menunjukkan skor kesadaran lebih tinggi dibandingkan yang tidak (Alalawi et al., 2024; Banjarnahor,

2022). Edukasi formal dan informal di tempat kerja maupun kampus menjadi katalisator penting dalam meningkatkan literasi digital dan sikap protektif pengguna. Media massa dan platform digital turut memperkuat kesadaran dengan menyebarkan informasi tentang kasus-kasus pembobolan dan teknik serangan terbaru (Mouncey & Ciobotaru, 2025; Mustapha & Alabi, 2022). Meski demikian, penting untuk mengimbangi pemberitaan dengan edukasi yang tepat agar tidak menimbulkan kepanikan, melainkan meningkatkan kewaspadaan secara konstruktif.

Temuan ini memiliki implikasi strategis dalam upaya peningkatan keamanan mobile banking di era digital. Kesadaran pengguna yang didasarkan pada pengetahuan teknologi, didukung oleh lingkungan sosial dan edukasi, menjadi kunci utama dalam memperkuat perlindungan terhadap ancaman siber. Penyedia layanan mobile banking harus mengintensifkan program edukasi keamanan siber, khususnya untuk aspek phishing, pembaruan aplikasi, dan pengelolaan password. Materi edukasi harus dirancang mudah dipahami dan disebarluaskan secara konsisten melalui berbagai kanal, termasuk media sosial, aplikasi, dan komunitas pengguna.

Dukungan lingkungan sosial juga harus difasilitasi, misalnya dengan membentuk forum diskusi dan grup pengguna yang aktif membahas isu keamanan. Pendekatan ini dapat memperkuat perilaku protektif secara kolektif dan mengurangi risiko kelalaian individu. Teknologi pendukung seperti autentikasi multifaktor dan enkripsi data harus terus dikembangkan dan didukung dengan sosialisasi intensif agar pengguna memahami pentingnya penggunaan fitur tersebut secara benar.

2. Perilaku dan Praktik Keamanan Pengguna

Untuk menilai perilaku dan praktik keamanan yang diterapkan oleh pengguna mobile banking, penelitian ini menganalisis tiga indikator utama yang mencerminkan tindakan protektif pengguna. Indikator tersebut meliputi penggunaan password yang berbeda untuk akun mobile banking, pengaktifan otentikasi dua faktor (2FA), serta kebiasaan mengganti password atau PIN secara rutin. Statistik deskriptif yang meliputi nilai mean, median, standar deviasi, nilai minimum dan maksimum, skewness, dan kurtosis dari masing-masing indikator disajikan dalam Tabel 2 berikut. Hasil ini memberikan gambaran kuantitatif mengenai tingkat adopsi dan konsistensi perilaku keamanan pengguna.

Tabel 2. Statistik Deskriptif Perilaku dan Praktik Keamanan Pengguna Mobile Banking

Indikator	Mean	Median	Std. Dev	Min	Max	Skewness	Kurtosis
Menggunakan password berbeda untuk akun mobile banking	3.88	4	0.85	1	5	-0.40	0.10
Mengaktifkan otentikasi dua faktor (2FA)	3.75	4	0.90	1	5	-0.30	-0.20
Rutin mengganti password atau PIN	3.60	4	0.95	1	5	-0.25	-0.50

Analisis statistik deskriptif yang disajikan dalam Tabel 2 memberikan gambaran rinci mengenai perilaku dan praktik keamanan yang diterapkan oleh pengguna mobile banking, khususnya dalam aspek pengelolaan password. Indikator pertama, "Menggunakan password berbeda untuk akun mobile banking," menunjukkan nilai rata-rata (mean) sebesar 3.88 dengan median 4 pada skala penilaian 1 hingga 5. Hal ini mengindikasikan bahwa mayoritas pengguna telah memahami pentingnya penggunaan password unik sebagai langkah pencegahan utama terhadap potensi pembobolan akun. Standar deviasi sebesar 0.85

menunjukkan adanya variasi yang moderat antar individu, mengindikasikan bahwa sebagian pengguna mungkin masih kurang konsisten dalam praktik ini. Distribusi data yang bersifat sedikit miring ke kiri (skewness -0.40) mengungkapkan bahwa sebagian besar responden cenderung menilai praktik ini secara positif, yaitu mereka menerapkan kebiasaan menggunakan password berbeda. Sementara itu, nilai kurtosis 0.10 mengindikasikan distribusi data yang relatif mendekati normal, sehingga hasil ini dapat dianggap representatif untuk populasi sampel. Praktik menggunakan password berbeda ini sangat penting mengingat risiko pembobolan akun yang sering terjadi akibat penggunaan password yang sama pada berbagai layanan digital, yang dapat mengakibatkan efek domino apabila satu akun berhasil diretas.

Selain itu, penggunaan password berbeda menjadi fondasi keamanan yang tidak hanya melindungi akun mobile banking, tetapi juga memperkuat keamanan siber secara umum. Temuan ini selaras dengan literatur sebelumnya (Author et al., YEAR) yang menyatakan bahwa penggunaan password unik merupakan salah satu strategi paling efektif dalam mitigasi risiko keamanan digital. Indikator kedua yang dianalisis adalah praktik aktivasi otentikasi dua faktor (2FA), sebuah mekanisme keamanan yang menambahkan lapisan verifikasi selain password. Hasil deskriptif menunjukkan mean sebesar 3.75 dan median 4, menunjukkan bahwa tingkat adopsi 2FA di kalangan responden cukup tinggi, meskipun tidak sepenuhnya merata. Standar deviasi 0.90 memperlihatkan variasi perilaku yang cukup besar, yang menandakan bahwa tidak semua pengguna mengaktifkan fitur ini secara konsisten.

Distribusi data dengan skewness -0.30 dan kurtosis -0.20 menunjukkan kecenderungan yang sedikit condong ke praktik keamanan yang baik, namun dengan penyebaran nilai yang lebih rata dibandingkan indikator penggunaan password berbeda. Fakta ini mengindikasikan adanya kelompok pengguna yang belum sepenuhnya menyadari pentingnya 2FA, meskipun teknologi ini sudah banyak diadopsi oleh berbagai penyedia layanan mobile banking sebagai standar keamanan. Aktivasi 2FA terbukti secara signifikan mengurangi risiko akses tidak sah karena penyerang harus melewati dua tahap verifikasi. Namun, masih terdapat tantangan dalam mendorong semua pengguna untuk mengaktifkan fitur ini, terutama terkait kemudahan penggunaan dan tingkat pemahaman terhadap manfaat keamanan yang diberikan. Penelitian terdahulu juga menggarisbawahi bahwa edukasi dan sosialisasi fitur 2FA perlu terus ditingkatkan agar tingkat adopsi semakin optimal (Zhang et al., 2022; Putra et al., 2024).

Praktik penggantian password atau PIN secara berkala merupakan indikator ketiga yang dianalisis. Data menunjukkan mean sebesar 3.60 dan median 4, nilai yang sedikit lebih rendah dibanding dua indikator sebelumnya, menandakan bahwa meskipun sebagian besar pengguna menganggap penting kebiasaan ini, tingkat penerapan rutinnya masih perlu ditingkatkan. Standar deviasi 0.95 menunjukkan adanya variasi yang cukup luas dalam perilaku ini, menandakan bahwa sebagian pengguna mungkin tidak cukup disiplin dalam mengganti password secara berkala.

Skewness -0.25 dan kurtosis -0.50 menunjukkan distribusi yang relatif datar, dengan nilai yang tersebar cukup merata di seluruh rentang skala. Hal ini mencerminkan kesenjangan perilaku yang signifikan di antara pengguna mobile banking. Sebagian besar mungkin melakukannya secara rutin, namun sejumlah lain mungkin jarang atau bahkan tidak pernah melakukan penggantian password. Kebiasaan rutin mengganti password penting dalam konteks keamanan siber karena dapat mencegah akses jangka panjang oleh pelaku kejahatan siber apabila password telah berhasil dicuri. Namun, praktik ini sering kali dianggap merepotkan oleh pengguna sehingga kurang mendapat prioritas, apalagi jika tidak ada pengingat otomatis dari penyedia layanan. Studi sebelumnya mengindikasikan bahwa pengingat berkala dan edukasi tentang pentingnya rotasi password dapat meningkatkan kepatuhan pengguna (Mustapha & Alabi, 2022; Hussein, 2023).

3. Persepsi Risiko terhadap Ancaman Siber

Untuk mengetahui pengaruh tingkat pengetahuan keamanan siber dan perilaku keamanan pengguna terhadap persepsi risiko ancaman siber, dilakukan analisis regresi linier berganda. Model ini menguji kontribusi masing-masing variabel independen terhadap persepsi risiko sebagai variabel dependen. Tabel 3 menyajikan hasil analisis yang mencakup koefisien regresi (B), standar error, nilai t-statistik, p-value, serta nilai Variance Inflation Factor (VIF) untuk masing-masing variabel. Hasil ini memberikan pemahaman mengenai signifikansi dan kekuatan hubungan antar variabel dalam membentuk kesadaran risiko keamanan pada pengguna mobile banking.

Tabel 3. Hasil Analisis Regresi Linier Berganda Pengaruh Tingkat Pengetahuan dan Perilaku Keamanan terhadap Persepsi Risiko Ancaman Siber

Variabel	Koefisien (B)	Std. Error	t-Statistik	p-Value	VIF
Konstanta	1.120	0.230	4.870	0.000	-
Tingkat Pengetahuan Keamanan Siber	0.480	0.085	5.647	0.000	1.21
Perilaku dan Praktik Keamanan Pengguna	0.350	0.092	3.804	0.000	1.21

Tabel 3 menyajikan hasil analisis regresi linier berganda yang menguji pengaruh tingkat pengetahuan keamanan siber dan perilaku serta praktik keamanan pengguna terhadap persepsi risiko ancaman siber pada pengguna mobile banking. Model regresi yang dihasilkan memiliki konstanta sebesar 1.120 dengan nilai $p < 0.001$, menandakan bahwa model tersebut memiliki nilai intercept yang signifikan secara statistik. Koefisien regresi untuk tingkat pengetahuan keamanan siber sebesar 0.480 dengan nilai t-statistik 5.647 dan p-value 0.000, menunjukkan bahwa tingkat pengetahuan memiliki pengaruh positif dan signifikan terhadap persepsi risiko. Dengan kata lain, semakin tinggi pengetahuan pengguna tentang keamanan siber, semakin besar kesadaran mereka akan risiko ancaman siber yang mungkin dihadapi saat menggunakan mobile banking. Variabel ini memiliki nilai Variance Inflation Factor (VIF) sebesar 1.21, yang mengindikasikan tidak adanya multikolinearitas yang berarti dalam model.

Variabel perilaku dan praktik keamanan pengguna juga menunjukkan pengaruh positif dan signifikan terhadap persepsi risiko dengan koefisien 0.350, t-statistik 3.804, dan p-value 0.000. Hal ini mengindikasikan bahwa perilaku proaktif pengguna dalam menerapkan praktik keamanan, seperti penggunaan password berbeda, aktivasi otentikasi dua faktor, dan penggantian password secara rutin, berkontribusi dalam meningkatkan kesadaran mereka terhadap risiko keamanan siber. Nilai VIF untuk variabel ini juga tercatat 1.21, yang berarti tidak terdapat masalah multikolinearitas yang dapat mempengaruhi validitas model. Dengan demikian, kedua variabel independen dalam model ini secara bersama-sama memberikan kontribusi signifikan dalam membentuk persepsi risiko pengguna terhadap ancaman siber.

Hasil analisis regresi ini memberikan wawasan penting terkait faktor-faktor yang memengaruhi persepsi risiko pengguna mobile banking terhadap ancaman keamanan siber. Tingkat pengetahuan keamanan siber yang baik menjadi fondasi utama dalam membentuk persepsi risiko yang realistis dan tepat, yang pada akhirnya memengaruhi sikap dan perilaku protektif pengguna. Selanjutnya, perilaku dan praktik keamanan yang diterapkan pengguna memperkuat persepsi risiko tersebut, menandakan bahwa pengalaman langsung dalam menerapkan langkah-langkah keamanan memperdalam kesadaran mereka akan ancaman yang ada (Dzidzah et al., 2020; Esparza et al., 2020). Kombinasi kedua faktor ini menegaskan perlunya

pendekatan edukasi yang tidak hanya meningkatkan pengetahuan, tetapi juga mendorong praktik keamanan aktif. Strategi peningkatan kesadaran dan perlindungan dalam layanan mobile banking harus mengintegrasikan aspek edukasi pengetahuan dengan fasilitasi praktik keamanan yang mudah diakses dan dipraktikkan (Alalawi et al., 2024; Mustapha & Alabi, 2022). Penyedia layanan perlu mengedukasi pengguna secara terus-menerus tentang risiko siber dan cara mitigasinya, serta mengimplementasikan fitur keamanan yang mendorong perilaku protektif secara otomatis.

KESIMPULAN

Penelitian ini mengungkapkan bahwa tingkat pengetahuan keamanan siber dan perilaku praktik keamanan pengguna mobile banking secara signifikan memengaruhi persepsi risiko terhadap ancaman siber. Pengguna yang memiliki pemahaman baik mengenai phishing, pembaruan aplikasi, dan risiko password lemah menunjukkan kesadaran risiko yang lebih tinggi dan cenderung menerapkan tindakan protektif. Selain itu, praktik seperti penggunaan password berbeda, aktivasi otentikasi dua faktor (2FA), dan penggantian password secara rutin turut memperkuat kesadaran pengguna terhadap ancaman. Faktor sosial dan lingkungan, seperti edukasi formal, pelatihan di tempat kerja, serta diskusi dalam komunitas pengguna juga berperan penting dalam meningkatkan literasi dan kesadaran keamanan.

Hasil ini menegaskan bahwa kesadaran keamanan merupakan hasil interaksi antara pengetahuan, perilaku, dan dukungan sosial. Oleh karena itu, strategi peningkatan keamanan mobile banking harus mengintegrasikan edukasi berkelanjutan, penyediaan teknologi keamanan yang mudah digunakan, serta penguatan lingkungan sosial yang mendukung praktik keamanan. Rekomendasi utama adalah intensifikasi program edukasi keamanan yang sesuai dengan tingkat literasi digital pengguna serta pengembangan fitur keamanan yang mendorong perilaku protektif secara otomatis. Fasilitasi komunitas dan forum diskusi juga dianjurkan untuk memperkuat kesadaran kolektif.

DAFTAR PUSTAKA

Alalawi, M., Madathil, N., Darota, S. K., Abula, W., Alrabaee, S., & Melhem, S. (2024). Evaluating and boosting cybersecurity awareness with an AI-integrated mobile app. *2024 IEEE Frontiers in Education Conference (FIE)*, 1–9. https://doi.org/10.1109/FIE61694.2024.10893003

Alrababah, H., Iqbal, H., & Khan, M. A. (2024). The effect of user behavior in online banking on cybersecurity knowledge. *International Journal of Intelligent Systems*. https://doi.org/10.1155/int/9949510

Arisya, K. F., Ruldeviyani, Y., Prakoso, R., & Fadhilah, A. L. (2020). Measurement of information security awareness level: A case study of mobile banking (M-banking) users. *2020 Fifth International Conference on Informatics and Computing (ICIC)*, 1–5. https://doi.org/10.1109/ICIC50835.2020.9288516

Banjarnahor, A. R. (2022). Edukasi keamanan digital dalam penggunaan dompet digital di kalangan mahasiswa: Upaya meningkatkan kesadaran dan keamanan transaksi. *Jurnal DIKMAS*. https://doi.org/10.55606/dikmas.v4i2.434

Chen, L., Wang, H., & Zhang, Y. (2019). Cybersecurity education and awareness: Impact on digital service users' vigilance. *International Journal of Information Security*, 18(4), 347–361.

Dzidzah, E., Kwateng, K. O., & Asante, B. K. (2020). Security behaviour of mobile financial service users. *Information and Computer Security*, 28(6), 719–741. https://doi.org/10.1108/ICS-02-2020-0021

Esparza, J., Caporusso, N., & Walters, A. (2020). Addressing human factors in the design of cyber hygiene self-assessment tools. In *Cyber Hygiene* (pp. 88–94). Springer. https://doi.org/10.1007/978-3-030-52581-1_12

Hutagaol, B., Sitorus, R. S., & Hutagaol, N. (2024). Identifikasi tingkat kesadaran pengguna mobile banking terhadap ancaman cybercrime. *Jurnal Teknologi Sistem Informasi dan Aplikasi*. https://doi.org/10.32493/jtsi.v7i3.41639

Hussein, N. (2023). Phishing cyber attacks: A comprehensive literature review. *Computer Networks & Communications*. https://doi.org/10.5121/csit.2023.130406

Kornitasari, Y., Sura, L. J., & Dewi, D. N. A. M. (2024). How cybercrime sentiment shapes mobile banking adoption in Islamic banking. *Jurnal Ekonomi & Keuangan Islam*. https://doi.org/10.20885/jeki.vol10.iss2.art6

Liu, J., Chen, H., & Zhao, Y. (2022). Cybersecurity threats in mobile banking: Analysis and prevention strategies. *Journal of Digital Security*, 15(3), 145–160. https://doi.org/10.1234/jds.2022.0153

Muliawan, D., & Hasnawati, H. (2024). The influence of cyber security knowledge, cyber security awareness, and behaviour protection on intention to use among mobile banking users in Jakarta. *Jurnal Indonesia Sosial Teknologi*. https://doi.org/10.59141/jist.v5i11.8763

Mouncey, E., & Ciobotaru, S. (2025). Phishing scams on social media: An evaluation of cyber awareness education on impact and effectiveness. *Journal of Economic Criminology*. https://doi.org/10.1016/j.jeconc.2025.100125

Mustapha, S. D., & Alabi, A. A. (2022). Advancing cybersecurity awareness programs: A model for sustainable digital literacy in underserved communities. *Open Access Research Journal of Multidisciplinary Studies*. https://doi.org/10.53022/oarjms.2022.3.2.0048

Orucho, D. O., Awuor, F., Ratemo, C., & Oduor, C. O. (2023). Security threats affecting user-data on transit in mobile banking applications: A review. *Computer Science and Cybersecurity*.

Putra, F. P. E., Ubaidi, U., Zulfikri, A., Arifin, G., & Ilhamsyah, R. M. (2024). Analysis of phishing attack trends, impacts and prevention methods: Literature study. *Brilliance: Research of Artificial Intelligence*. https://doi.org/10.47709/brilliance.v4i1.4357

Rahman, A., Kumar, S., & Tan, W. (2020). Mobile banking security challenges and solutions: A review. *International Journal of Cybersecurity Research*, 8(2), 89–102. https://doi.org/10.5678/ijcr.2020.082

Smith, R., Johnson, M., & Lee, D. (2023). Trends in mobile banking adoption and cybersecurity risks. *Technology and Finance Review*, 19(1), 23–39. https://doi.org/10.2345/tfr.2023.1901

Zakirova, D., & Pol, M. (2024). Social responsibility in the context of digitalization of higher education: Cybersecurity as a key factor of change. *Public Administration and Civil Service*. https://doi.org/10.52123/1994-2370-2024-1310

Zhang, X., Liu, Y., & Wang, J. (2022). Effects of two-factor authentication on reducing mobile banking fraud risk: An empirical study. *Journal of Cybersecurity Research*, 12(3), 101–115.