Jurnal Teknologi Sistem Informasi dan Aplikasi **ISSN: 2654-3788**
Penerbit: Program Studi Teknik Informatika Universitas Pamulang **e-ISSN: 2654-4229**
Vol. 7, No. 3, Juli 2024 (1043-1054) **DOI: 10.32493/jtsi.v7i3.41639**

Identifikasi Tingkat Kesadaran Pengguna Mobile Banking terhadap Ancaman Cybercrime

B. Junedi Hutagaol [1], Riama Santy Sitorus[2], Nindya Hutagaol[3]

Fakultas Ilmu Komputer, Universitas ASA Indonesia, Jl Raya Kalimalang No.2A Jakarta Timur, Indonesia, 031076
e-mail: [1]junedi@asaindo.ac.id, [2]riama@asaindo.ac.id, [3]nindya@asaindo.ac.id

Submitted Date: July 03rd, 2024 Reviewed Date: July 18th, 2024
Revised Date: July 20th, 2024 Accepted Date: July 24th, 2024

Abstract

The development of information technology has brought about a significant increase in the number of people connected to and using the internet. However, this phenomenon also poses serious risks regarding the security of valuable information such as passwords, financial information, and other sensitive data, making them attractive targets for attackers. Attacks on this infrastructure not only have the potential to cause data breaches but also significant financial impacts and even threats to lives. Protecting oneself from these threats, and considering the crucial role of humans in the technology ecosystem, emphasizes the importance of enhancing cybersecurity awareness. This study aims to explore the awareness levels of mobile banking users regarding cybercrime threats, involving the participation of 403 respondents. Questionnaire data processing results showed that 51% of the total respondents have experienced cybercrime attempts, and 21% have been victims. Respondents' awareness levels varied between 3.49 and 4.05 on a Likert scale (1-5). Several factors significantly influence respondents' awareness levels, such as age, occupation, personal experience as a victim of cybercrime attempts, and interactions between variables.

Keywords: Information Security; Cybercrime; Cybercrime Prevention; Cybercrime Awareness Level; Mobile Banking

Abstrak

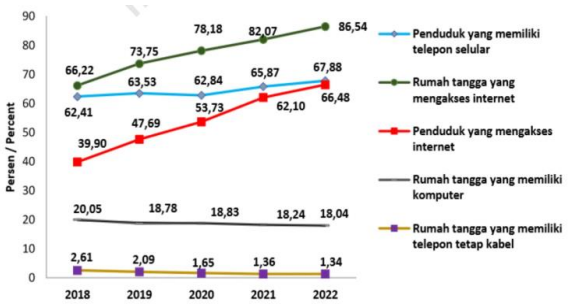
Perkembangan teknologi informasi telah menghadirkan lonjakan jumlah orang yang terhubung dan menggunakan internet secara signifikan. Namun, fenomena ini juga membawa risiko serius terkait keamanan informasi berharga seperti kata sandi, informasi keuangan, dan data rahasia lainnya menjadi sasaran yang menarik bagi penyerang. Serangan terhadap infrastruktur ini tidak hanya berpotensi menyebabkan kebocoran data, tetapi juga dapat menimbulkan dampak finansial yang signifikan bahkan ancaman terhadap nyawa. Untuk melindungi diri dari ancaman ini dan mengingat peran krusial manusia dalam ekosistem teknologi, meningkatkan kesadaran akan keamanan siber menjadi sangat penting. Penelitian ini bertujuan untuk mengeksplorasi tingkat kesadaran pengguna *mobile banking* terhadap ancaman kejahatan siber, melibatkan partisipasi dari 403 responden. Hasil pengolahan data kuesioner menunjukkan bahwa 51% dari total responden pernah mengalami percobaan kejahatan siber dan 21% dari total responden pernah menjadi korban kejahatan. Tingkat kesadaran responden bervariasi ada di antara 3.49 sampai 4.05 mengacu pada skala Likert (1-5). Terdapat beberapa faktor yang memengaruhi secara signifikan tingkat kesadaran responden seperti usia, pekerjaan dan pengalaman pribadi sebagai korban percobaan kejahatan siber, serta beberapa interaksi antar variabel.

Keywords: Keamanan Informasi; Kejahatan Siber; Pencegahan Kejahatan Siber; Tingkat Kesadaran Kejahatan Siber; Mobile Banking.

Jurnal Teknologi Sistem Informasi dan Aplikasi **ISSN: 2654-3788**
Penerbit: Program Studi Teknik Informatika Universitas Pamulang **e-ISSN: 2654-4229**
Vol. 7, No. 3, Juli 2024 (1043-1054) **DOI: 10.32493/jtsi.v7i3.41639**

1 Pendahuluan

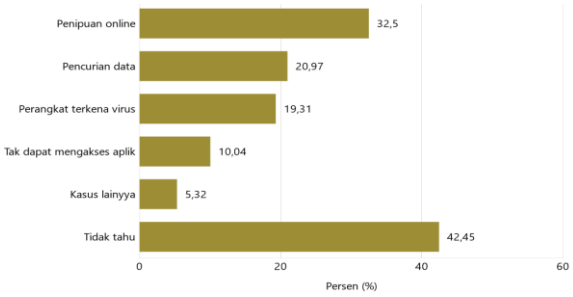
Pertumbuhan pesat teknologi informasi dan komunikasi (TIK) telah menciptakan transformasi yang signifikan dalam berbagai aspek kehidupan masyarakat, termasuk di Indonesia. Dalam beberapa tahun terakhir, Indonesia telah menjadi saksi perkembangan pesat dalam ranah digital. Menurut data dari Badan Pusat Statistik (BPS), dalam 5 tahun (2018 - 2022) penggunaan TIK di Indonesia menunjukkan perkembangan yang pesat. Ada tiga kategori yang mengalami pertumbuhan yang sangat pesat, yaitu penduduk yang memiliki telepon seluler, rumah tangga yang mengakses internet, dan penduduk yang mengakses internet. Kategori tersebut dapat dilihat pada Gambar 1.



Gambar 1. Pengguna TIK di Indonesia Tahun 2018-2022 (*Badan Pusat Statistikmiskin*, n.d.)

Dalam era digital yang berkembang pesat, penggunaan layanan *mobile banking* telah menjadi bagian integral dari kehidupan sehari-hari masyarakat. Kemudahan akses dan fleksibilitas yang ditawarkan oleh *mobile banking* telah mendorong peningkatan signifikan dalam jumlah pengguna di seluruh dunia, termasuk di Indonesia. Perkembangan era digital di Indonesia mencakup berbagai hal, seperti peningkatan akses internet, adopsi perangkat seluler, pertumbuhan *e-commerce*, dan munculnya layanan finansial digital seperti *mobile banking*. Fenomena ini memberikan dampak yang besar terhadap pola perilaku masyarakat, baik dalam hal interaksi sosial, bisnis, hingga akses terhadap layanan umum (Tantrinesia et al., 2023). Peningkatan adopsi teknologi *mobile banking* telah membuka pintu kemudahan akses ke layanan perbankan, memungkinkan pengguna untuk melakukan berbagai transaksi keuangan melalui perangkat seluler mereka. Namun, seiring dengan meningkatnya adopsi teknologi ini, muncul pula tantangan baru berupa ancaman *cybercrime* yang semakin kompleks dan canggih. Keamanan dalam penggunaan *mobile banking* menjadi perhatian utama bagi pengguna, bank, dan regulator (Nur Rohmah, 2022). Tantangan besar terkait keamanan sistem di era digital ini mengakibatkan semakin banyak penelitian terkait *cyber security* terutama yang berkaitan dengan *mobile banking* yang merupakan salah satu produk digital perbankan yang digunakan untuk melayani nasabah dan memperkuat kinerja beserta stabilitas perusahaan perbankan (Herlina & Ainun, 2023).

Indonesia sendiri merupakan negara dengan serangan *cybercrime* tertinggi (termasuk 10 besar) sehingga menjadi negara dengan risiko tinggi terkait keamanan siber (Delvyan Putri Surya Ningrum & Jamiatur Robekha, 2023). Dalam beberapa tahun terakhir, serangan *cybercrime* terhadap pengguna *mobile banking* semakin canggih dan merugikan. Menurut NCSI (*National Cyber Security Index*), pada tahun 2022 Indonesia menduduki peringkat ke-tiga terendah dalam penanganan keamanan siber di antara negara-negara G20. Pada tahun 2024, terdapat banyak kasus kejahatan yang melibatkan internet yang terjadi di Indonesia (Tropika, 2023). Menurut survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) terhadap pengguna internet mulai dari usia 13 tahun keatas yang dilaporkan pada Laporan Survei Penetrasi Internet Indonesia 2024, kasus terbesar yang terjadi adalah penipuan online disusul kasus pencurian data dan perangkat terkena virus seperti pada Gambar 2.



Gambar 2. Kasus Serangan Siber 2023 (Tropika, 2023)

Meskipun telah ada upaya dari pihak penyedia layanan keuangan dan pemerintah melalui kebijakan-kebijakan yang dikeluarkan dalam hal penerapan digital (Ginting et al., 2016), namun upaya yang dilakukan tersebut belum sepenuhnya bisa menyelesaikan masalah, terbukti dengan masih banyaknya kejadian *cybercrime* yang merugikan nasabah dan masyarakat Indonesia. Dalam mencegah semakin banyaknya korban *cybercrime* dalam penggunaan *mobile banking*, semua pihak harus bekerja sama, baik dari

sisi perbankan sebagai penyedia jasa, pemerintah, dan juga masyarakat khususnya nasabah pengguna *mobile banking*. Baik pemerintah maupun institusi perbankan diharapkan bisa memberikan pengawasa dari sisi teknologi, memberikan edukasi terkait pengetahuan *cybercrime,* tindakan tegas terhadap pelaku *cybercrime* (Alhakim & Sofia, 2021). Di sisi lain perlu juga kesadaran pengguna *mobile banking* untuk meningkatkan tingkat kesadaran dalam memahami perkembangan pengetahuan *cybercrime* dan resiko yang kemungkinan terjadi (Nur Rohmah, 2022).

Untuk melindungi diri dari ancaman ini dan mengingat peran krusial manusia dalam ekosistem teknologi, meningkatkan kesadaran akan keamanan siber menjadi sangat penting. Peneliti mencoba untuk mengidentifikasi tingkat kesadaran pengguna *mobile banking* terhadap ancaman *cybercrime*. Tingkat kesadaran akan ancaman *cybercrime* ini dapat dipengaruhi oleh berbagai faktor yang mencerminkan karakteristik demografis, perilaku penggunaan, dan persepsi individu terhadap risiko. Oleh karena itu, penelitian ini menggunakan beberapa indikator untuk mengukur tingkat kesadaran tersebut. Indikator pertama adalah sosiodemografi, yang terdiri dari usia, jenis kelamin, tingkat pendidikan, dan pekerjaan dapat memengaruhi kesadaran dan pemahaman seseorang terhadap ancaman *cybercrime*. Studi sebelumnya menunjukkan bahwa kelompok usia tertentu dan tingkat pendidikan yang lebih tinggi cenderung lebih sadar akan risiko keamanan siber (Senol et al., 2021). Yang kedua adalah tingkat penggunaan *mobile banking*, di mana frekuensi dan intensitas penggunaan *mobile banking* dapat memengaruhi kesadaran pengguna terhadap ancaman *cybercrime*. Pengguna yang lebih sering menggunakan layanan ini akan lebih sadar akan praktik keamanan yang diperlukan (Apaua & Lallie, 2022).

Indikator ketiga adalah kepuasan terhadap keamanan *mobile banking*, kepuasan pengguna terhadap fitur keamanan yang disediakan oleh bank dapat mencerminkan kesadaran mereka terhadap pentingnya perlindungan data pribadi dan transaksi finansial (Herzallah et al., 2018). Indikator keempat adalah persepsi risiko, yang merupakan persepsi individu mengenai risiko yang terkait dengan penggunaan *mobile banking* sangat penting dalam menentukan tingkat kewaspadaan mereka terhadap ancaman *cybercrime*. Pengguna yang merasa bahwa risiko *cybercrime* tinggi cenderung lebih berhati-hati dalam menggunakan layanan ini (Kota & Kusumastuti, 2022). Indikator kelima adalah pengalaman pribadi nasabah. Pengalaman pribadi dengan insiden keamanan, seperti penipuan atau pelanggaran data, dapat meningkatkan kesadaran dan pengetahuan pengguna tentang ancaman *cybercrime* dan langkah-langkah yang perlu diambil untuk mencegahnya (Petru-cristian, 2023). Kepatuhan terhadap praktik keamanan menjadi indikator keenam. Kepatuhan pengguna terhadap praktik keamanan yang direkomendasikan, seperti penggunaan kata sandi yang kuat dan otentikasi dua faktor, merupakan indikator penting dari kesadaran mereka terhadap ancaman *cybercrime* (Zwilling et al., 2022). Indikator ketujuh adalah bagaimana kesiapan nasabah dalam menghadapi ancaman *cybercrime*. Kesiapan dan kemampuan pengguna dalam menghadapi ancaman, seperti pengetahuan tentang cara melaporkan insiden keamanan dan mengatasi serangan siber, menunjukkan tingkat kesadaran yang lebih tinggi (Alzubaidi, 2021). Indikator kedelapan adalah tingkat pengetahuan pengguna tentang *cybercrime*. Pengetahuan umum pengguna tentang jenis-jenis *cybercrime* dan metode perlindungan adalah kunci dalam menilai kesadaran mereka terhadap ancaman ini. Pendidikan dan informasi yang tepat dapat meningkatkan tingkat pengetahuan dan kesadaran pengguna (Zwilling et al., 2022).

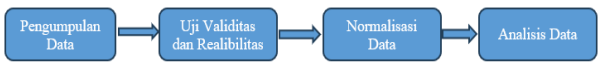
Selain melakukan analisis tingkat kesadaran dan pemahaman pengguna *mobile banking* terhadap ancaman *cybercrime* melalui indikator-indikator yang telah diidentifikasi, penelitian ini juga menganalisis dan mampu memberikan wawasan mendalam tentang faktor-faktor apa saja yang memengaruhi kesadaran keamanan di kalangan pengguna *mobile banking* saat ini. Dengan mengetahui tingkat kesadaran pengguna dan faktor-faktor apa saja yang memengaruhi kesadaran tersebut, diharapkan dapat mengidentifikasi kelemahan yang memengaruhi kurangnya kesadaran mereka akan bahaya *cybercrime* dan akan memudahkan pemangku kepentingan dalam merumuskan strategi edukasi yang efektif untuk meningkatkan tingkat keamanan pengguna *mobile banking* secara keseluruhan. Hasil penelitian ini akan bermanfaat bagi penyedia layanan perbankan untuk meningkatkan strategi keamanan dan edukasi, serta bagi regulator untuk merumuskan kebijakan yang lebih efektif dalam melindungi konsumen dari ancaman *cybercrime* dan juga sebagai pengetahuan umum masyarakat

khususnya pengguna *mobile banking* dalam meningkatkan kewaspadaan akan ancaman yang kemungkinan terjadi. Dengan demikian, penelitian ini akan memberikan kontribusi signifikan untuk merancang langkah-langkah pencegahan yang lebih baik, referensi untuk meningkatkan keamanan transaksi *mobile banking*, dan membangun kepercayaan pengguna terhadap teknologi ini di masa depan.

Dalam penelitian sebelumnya, terdapat berbagai jenis penelitian yang membahas terkait definisi dan jenis-jenis *cyber security* serta risiko yang akan terjadi pada pengguna teknologi. Terdapat juga penelitian terkait pengukuran kesadaran pengguna teknologi akan *cybercrime* dan risiko yang kemungkinan terjadi untuk studi kasus tertentu di berbagai negara. Namun belum ditemukan penelitian yang menghasilkan informasi tingkat kesadaran para pengguna *mobile banking* di Indonesia terhadap ancaman dan risiko dari *cybercrime*. Penelitian ini mencoba untuk identifikasi hal tersebut dengan memperhitungkan beberapa indikator seperti sosiodemografi, tingkat penggunaan *mobile banking*, kepuasan terhadap keamanan *mobile banking*, persepsi risiko, pengalaman pribadi, tingkat kepatuhan terhadap praktik keamanan, kesiapan dalam menghadapi ancaman *cybercrime*, dan tingkat pengetahuan pengguna tentang *cybercrime*. Dengan demikian, penelitian ini akan menjadi pengetahuan yang baru dan menjadi landasan teori baru untuk menindaklanjuti cara penanganan *cybercrime* yang lebih tepat oleh pemangku kepentingan, baik perbankan sebagai penyedia jasa, pemerintah sebagai regulatori dan penegak hukum, beserta masyarakat sebagai nasabah pengguna *mobile banking*.

2 Metodologi

Untuk mencapai tujuan penelitian, penelitian ini dilakukan melalui beberapa langkah metodologi yang sistematis, yaitu pengumpulan data, uji validitas dan reliabilitas, normalisasi data, dan analisis data seperti pada Gambar 3 di bawah.



Gambar 3. Metodologi Penelitian

Data yang digunakan pada penelitian ini berupa data primer yang diperoleh melalui survei dengan menyebarkan kuesioner kepada para responden. Kuesioner tersebut terdiri dari pertanyaan-pertanyaan dengan pilihan jawaban menggunakan skala Likert 1-5, di mana 1 berarti sangat tidak setuju (*strongly disagree*) dan 5 berarti sangat setuju (*strongly agree*) (Joshi et al., 2015). Kuesioner disebarkan melalui *google form* dan didistribusikan melalui media sosial. Penelitian ini menggunakan teknik *Simple Random Sampling* untuk memilih sampel dari populasi pengguna *mobile banking*. *Simple Random Sampling* dipilih karena untuk memastikan setiap anggota populasi memiliki peluang yang sama untuk terpilih, sehingga hasil yang diperoleh lebih representatif terhadap populasi secara keseluruhan. Pemilihan teknik ini dilakukan untuk menghindari bias seleksi dan memastikan bahwa setiap nasabah memiliki kesempatan yang sama untuk menjadi responden dalam penelitian ini. Hal ini diharapkan dapat menghasilkan data yang valid dan dapat dilakukan generalisasi ke seluruh populasi pengguna *mobile banking*.

Setelah data dikumpulkan, tahap selanjutnya adalah melakukan uji validitas dan reliabilitas data. Uji validitas dilakukan untuk menilai seberapa baik pertanyaan kuesioner mencerminkan konstruksi yang diukur, sedangkan uji reliabilitas dilakukan untuk menilai konsistensi internal dari item-item kuesioner. Analisis data dilakukan dengan menggunakan *software* IBM SPSS versi 29.0.2. Untuk uji validitas, digunakan korelasi *Pearson Product Moment* untuk menilai sejauh mana setiap item dalam kuesioner berkorelasi dengan skor total, sehingga memastikan bahwa item-item tersebut benar-benar mengukur konstruk yang dimaksud (Utami, 2023). Selanjutnya, untuk uji reliabilitas, digunakan *Alpha Cronbach* untuk menilai konsistensi internal dari item-item kuesioner, memastikan bahwa instrumen yang digunakan memiliki tingkat keandalan yang tinggi (Kaloka et al., 2023). Pengujian akan menghasilkan status item kuesioner valid atau tidak. Item yang valid akan digunakan untuk pengolahan data sedangkan item yang tidak valid akan dieliminasi.

Setelah uji validitas dan reliabilitas data dilakukan, langkah berikutnya adalah normalisasi data. Normalisasi dilakukan untuk menggabungkan berbagai indikator menjadi satu variabel tunggal, yaitu tingkat kesadaran pengguna. Proses normalisasi dilakukan dengan mencari nilai rata-rata dari indikator-indikator berikut: kepuasan terhadap keamanan *mobile banking*, persepsi risiko, kepatuhan terhadap praktik keamanan, kesiapan dalam menghadapi ancaman *cybercrime*,

dan tingkat pengetahuan pengguna tentang *cybercrime*.

Data yang sudah diuji validitas dan realibilitasnya serta variabel baru hasil normalisasi data kemudian diolah dan dianalisis. Analisis data dibedakan menjadi dua bagian, yang pertama adalah penghitungan nilai rata-rata tingkat kesadaran responden (sesuai skala Likert 1-5) berdasarkan data sosiodemografi (usia, jenis kelamin, pendidikan, dan pekerjaan). Analisis data yang kedua adalah untuk mencari faktor-faktor apa saja yang secara signifikan memengaruhi tingkat kesadaran responden. Analisis dilakukan dengan menggunakan ANOVA (*Analysis of Variance*) melalui *software* IBM SPSS versi 29.0.2. ANOVA dipilih karena memungkinkan peneliti untuk menentukan apakah terdapat perbedaan yang signifikan dalam rata-rata tingkat kesadaran antara beberapa kelompok yang diperoleh dari indikator yang sudah ditentukan (Anggraini & Arif, 2024).

3 Hasil dan Pembahasan

Bagian ini menjelaskan hasil dan pembahasan penelitian yang terdiri dari enam bagian, yaitu pengelompokan instrumen penelitian, uji validitas data, uji reliabilitas data, analisis profil responden, normalisasi data, dan proses analisis dan pengolahan data.

3.1 Pengelompokan Instrumen Penelitian

Penelitian ini terdiri dari beberapa indikator yang akan diuji. Setiap indikator memiliki berbagai pertanyaan yang akan diolah. Jumlah pertanyaan yang ada pada kuesioner ini adalah sebanyak 31. Pengelompokan instrumen penelitian dapat dilihat pada Tabel 1 berikut ini:

Tabel 1. Pengelompokan Instrumen Penelitian

Kode	Indikator	Jumlah
X1	Sosiodemografi (umur, jenis kelamin, pekerjaan, dan pendidikan)	4
X2	Tingkat penggunaan *mobile banking*	1
X3	Kepuasan terhadap keamanan mobile banking	3
X4	Persepsi risiko	3
X5	Pengalaman pribadi sebagai percobaan dan korban *cybercrime*	2
X6	Kepatuhan terhadap praktik keamanan	7
X7	Kesiapan dalam menghadapi ancaman *cybercrime*	5
X8	Tingkat pengetahuan pengguna tentang *cybercrime*	6

3.2 Uji Validitas Data

Uji validitas dilakukan untuk memastikan bahwa kuesioner yang disusun mampu mengukur tingkat kesadaran pengguna *mobile banking* terhadap ancaman *cybercrime* secara akurat dan terpercaya. Uji validitas merupakan langkah krusial dalam penelitian ini, karena hanya melalui instrumen yang valid, data yang dikumpulkan dapat memberikan gambaran yang tepat mengenai tingkat kesadaran pengguna. Sama seperti yang dilakukan oleh (Utami, 2023) dalam penelitiannya untuk mengukur validitas instrumen penilaian kinerja dosen dengan menggunakan korelasi *Pearson* dengan *software* IBM SPSS. Peneliti juga menguji validitas data pada penelitian ini menggunakan korelasi *Pearson* dengan taraf signifikan 5% dan sampel data 50 responden. Hasil validitas data yang telah dilakukan dapat dilihat pada Tabel 2.

Tabel 2. Uji Validitas Korelasi Pearson

Kode Pertanyaan	Pearson Correlation	Sig. (2-tailed)	N
X3.1	.436**	0.002	50
X3.2	.335*	0.017	50
X3.3	0.092	0.524	50
X4.1	.707**	0.000	50
X4.2	.562**	0.000	50
X4.3	.504**	0.000	50
X6.1	.602**	0.000	50
X6.2	.368**	0.009	50
X6.3	0.216	0.131	50
X6.4	.646**	0.000	50
X6.5	.730**	0.000	50
X6.6	.439**	0.001	50
X6.7	.630**	0.000	50
X7.1	.620**	0.000	50
X7.2	.755**	0.000	50
X7.3	.750**	0.000	50
X7.4	.733**	0.000	50
X7.5	.723**	0.000	50
X8.1	.475**	0.000	50
X8.2	.744**	0.000	50
X8.3	.764**	0.000	50
X8.4	.601**	0.000	50
X8.5	.749**	0.000	50
X8.6	.759**	0.000	50
X3.1	.436**	0.002	50
X3.2	.335*	0.017	50
X3.3	0.092	0.524	50
X4.1	.707**	0.000	50
X4.2	.562**	0.000	50
X4.3	.504**	0.000	50
X6.1	.602**	0.000	50
X6.2	.368**	0.009	50

Kode Pertanyaan	Pearson Correlation	Sig. (2-tailed)	N
X6.3	0.216	0.131	50
X6.4	.646**	0.000	50
X6.5	.730**	0.000	50
X6.6	.439**	0.001	50
X6.7	.630**	0.000	50
X7.1	.620**	0.000	50
X7.2	.755**	0.000	50
X7.3	.750**	0.000	50
X7.4	.733**	0.000	50
X7.5	.723**	0.000	50
X8.1	.475**	0.000	50
X8.2	.744**	0.000	50
X8.3	.764**	0.000	50
X8.4	.601**	0.000	50
X8.5	.749**	0.000	50
X8.6	.759**	0.000	50

Penjelasan kolom pada Tabel 2 adalah sebagai berikut:

1. Kolom Kode Pertanyaan merupakan daftar pertanyaan yang diisi oleh responden. Pertanyaan tersebut berisi profil nasabah dengan tingkat kesadaran pengguna *mobile banking* terhadap ancaman *cybercrime*.
2. Kolom Pearson Correlation menunjukkan koefisien korelasi *Pearson* antar variabel untuk mendapatkan tingkat signifikansi tabel. Apabila nilainya > 0.279 dengan tingkat signifikansi 5% maka dinyatakan valid.
3. Kolom Sig. (2-tailed) menunjukkan nilai signifikansi (p-*value*) dari uji korelasi Pearson. Jika p-*value* < 0.05 maka pertanyaan dinyatakan valid dan jika p-*value* > 0.05 maka pertanyaan tersebut dinyatakan tidak valid.
4. Kolom N merupakan jumlah sampel data yang dilakukan untuk pengujian.

Dari Tabel 2 terdapat 22 pertanyaan yang valid, yaitu X3.1, X3.2, X4.1, X4.2, X4.3, X6.1, X6.2, X6.4, X6.5, X6.6, X6.7, X7.1, X7.2, X7.3, X7.4, X7.5, X8.1, X8.2, X8.3, X8.4, X8.5, dan X8.6. Namun ada 2 pertanyaan (X3.3 dan X6.3) yang tidak valid. Data pertanyaan yang tidak valid dieliminasi dari kuesioner sehingga tidak menjadi bahan untuk pengolahan data.

3.3 Uji Reliabilitas Data

Uji reliabilitas dilakukan untuk mengetahui tingkat konsistensi instrumen penelitian yang diukur menggunakan *Cronbach's Alpha*. Hasil uji reliablitas pada penelitian ini dapat dilihat pada Tabel 3.

Tabel 3. Uji Reliabilitas Data

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.917	0.917	24

Penjelasan kolom pada Tabel 3 adalah sebagai berikut:

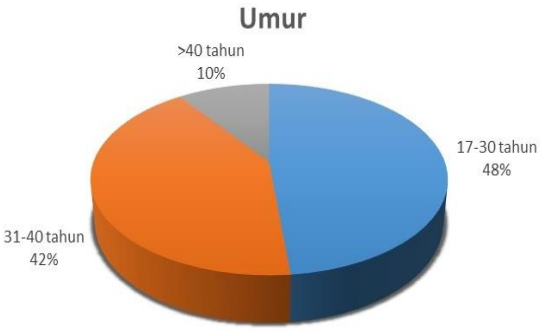
1. Kolom Cronbach's Alpha: merupakan koefisien reliabilitas yang digunakan untuk mengukur konsistensi internal dari sebuah item dalam kuesioner. Nilai *Cronbach's Alpha* berkisar antara 0 hingga 1 (Kaloka *et al*., 2023).
2. Kolom Cronbach's Alpha Based on Standardized Items: merupakan nilai *Cronbach's Alpha* yang dihitung berdasarkan item yang telah dilakukan standardisasi.
3. Kolom N of Items: Menunjukkan jumlah item (pertanyaan) dalam skala yang digunakan untuk menghitung nilai *Cronbach's Alpha*.

Secara umum, nilai *Cronbach's Alpha* di atas 0.7 dianggap memadai untuk penelitian eksploratif, sementara nilai di atas 0.8 dianggap baik untuk penelitian konfirmatori (Kennedy, 2022). Nilai 0.917 berada jauh di atas ambang batas ini, menunjukkan reliabilitas yang sangat baik.

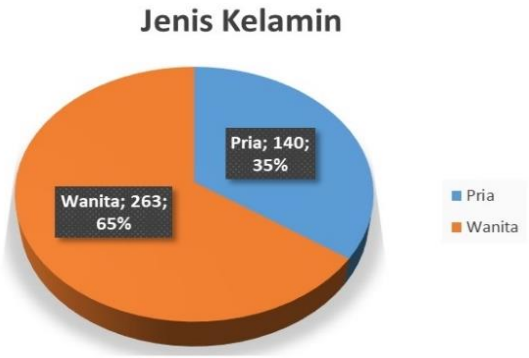
3.4 Uji Analisis Profil responden

Profil responden terdiri dari beberapa kategori, yaitu sosiodemografi, tingkat penggunaan *mobile banking* dan pengalaman pribadi sebagai korban *cybercrime*. Penyebaran data responden berdasarkan jenis sosiodemografi dapat dilihat pada Gambar 4, Gambar 5, Gambar 6, dan Gambar 7.

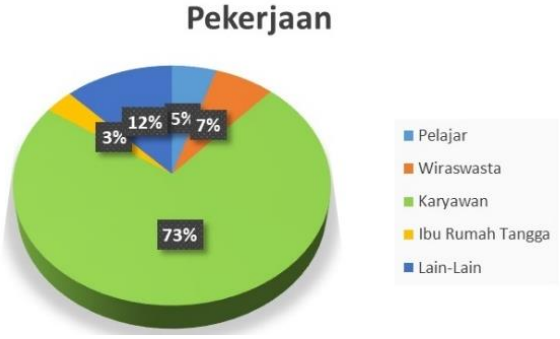
Jurnal Teknologi Sistem Informasi dan Aplikasi **ISSN: 2654-3788**
Penerbit: Program Studi Teknik Informatika Universitas Pamulang **e-ISSN: 2654-4229**
Vol. 7, No. 3, Juli 2024 (1043-1054) **DOI: 10.32493/jtsi.v7i3.41639**



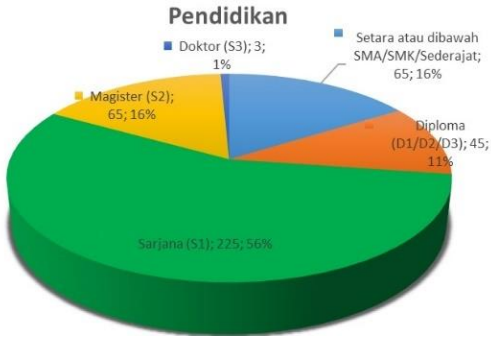
Gambar 4. Persentasi Responden Berdasarkan Umur



Gambar 5. Persentasi Responden Berdasarkan Jenis Kelamin



Gambar 6. Persentasi Responden Berdasarkan Pekerjaan



Gambar 7. Persentasi Responden Berdasarkan Pendidikan

Dari total 403 responden yang sudah dikumpulkan, seperti yang ada pada Gambar 4 didapatkan data sebanyak 48% adalah pengguna *mobile banking* berusia 17-30 tahun, 42% berusia 31-40% dan sisanya di atas 40 tahun atau 10% dari total responden. Untuk penyebaran responden sesuai jenis kelamin, terdiri dari 65% laki-laki dan 35% wanita seperti yang tercantum pada Gambar 5. Mayoritas responden bekerja sebagai karyawan yaitu sebanyak 73%, 7% merupakan wirawasta, 5% merupakan pelajar, 3% merupakan ibu rumah tangga dan sisanya sebanyak 7% merupakan pekerja di luar yang disebutkan (lain-lain) seperti yang tercantum pada Gambar 6. Sedangkan Gambar 7 merupakan pengelompokan responden berdasarkan jenjang pendidikan tertinggi dari responden. Mayoritas responden yang dimiliki memiliki jenjang pendidikan tertinggi S1 yaitu sebanyak 56%, jenjang pendidikan magister (S2) dan setara atau di bawah SMA/SMK/Sederajat sama-sama sebanyak 16% dari total responden, jenjang pendidikan diploma baik D1, D2 dan D3 sebanyak 11% dari total responden kemudian jenjang pendidikan S3 sebanyak 1% dari total responden.

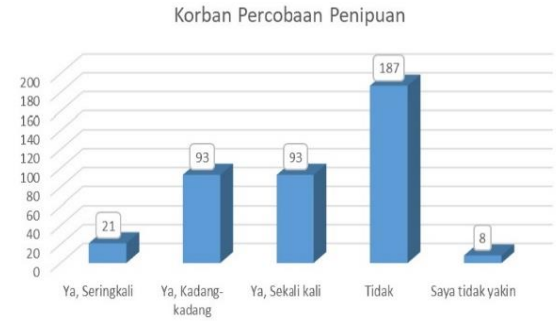
Frekuensi nasabah menggunakan layanan *mobile banking* untuk melakukan transaksi keuangan merupakan salah satu indikator yang diuji apakah memengaruhi tingkat kesadaran mereka dalam memahami ancaman *cybercrime*. Semua responden merupakan pengguna *mobile banking*. Sebanyak 213 atau sebanyak 53% dari total responden merupakan pengguna aktif atau menggunakan *mobile banking* setiap hari, 115 orang atau 29% dari total responden merupakan menggunakan *mobile banking* beberapa kali dalam seminggu, 49 orang atau 12% dari total responden menggunakannya beberapa kali dalam sebulan, dan 26 orang atau 6% dari total responden menggunakan *mobile banking* jika dibutuhkan saja seperti yang tercantum pada Gambar 8 dan Tabel 4.

Gambar 8. Frekuensi Penggunaan Mobile Banking

Tabel 4. Frekuensi Penggunaan Mobile Banking

Frekuensi Penggunaan Mobile Banking	Jumlah	Persentasi
Setiap hari	213	53%
Beberapa kali seminggu	115	29%
Beberapa kali sebulan	49	12%
Jarang, hanya dalam keadaan tertentu	26	6%
Tidak Pernah	0	0%
Total	403	100%

Dari data kuesioner yang diperoleh, 51% dari total responden pernah mengalami percobaan kejahatan *cybercrime* seperti menerima pesan atau email yang mencurigakan yang mengklaim berasal dari layanan *mobile banking* yang digunakan, dan 21 orang diantaranya sering mengalami percobaan *cybercrime*. Sedangkan 49% dari total responden tidak pernah mengalami percobaan *cybercrime*, di mana 187 orang diantaranya tidak pernah mengalami dan 8 orang diantaranya tidak yakin seperti yang tercantum pada Gambar 9. Ditemukan juga bahwa 21% dari total responden pernah menjadi korban *cybercrime* berupa penipuan dan pencurian data, dan 79% dari total responden belum pernah menjadi korban penipuan seperti yang dicantumkan pada Gambar 10.



Gambar 9. Persentasi Responden Sebagai Korban Percobaan Cybercrime

Gambar 10. Persentasi Responden Sebagai Korban Cybercrime

3.5 Normalisasi Data

Untuk memperoleh pemahaman yang komprehensif mengenai kesadaran pengguna, lima indikator utama telah dinormalisasi dan digabungkan menjadi satu variabel tunggal yaitu tingkat kesadaran pengguna yang diberikan kode X9. Indikator-indikator tersebut meliputi:

1. Kepuasan terhadap Keamanan *Mobile Banking* (X3)
2. Persepsi Risiko (X4)
3. Kepatuhan terhadap Praktik Keamanan (X6)
4. Kesiapan dalam Menghadapi Ancaman *Cybercrime* (X7)
5. Tingkat Pengetahuan Pengguna tentang *Cybercrime* (X8)

Proses normalisasi ini bertujuan untuk menyederhanakan kompleksitas data dan memungkinkan analisis yang lebih mendalam mengenai bagaimana pengguna *mobile banking* menyadari dan menanggapi berbagai ancaman *cybercrime*. Hasil analisis ini diharapkan dapat memberikan wawasan yang lebih jelas tentang profil kesadaran pengguna dan faktor-faktor yang memengaruhinya. Proses normalisasi dilakukan dengan cara mencari nilai rata-rata dari semua indikator tersebut. Rumus yang digunakan untuk menghitung rata-rata dari kelima indikator (X3, X4, X6, X7, dan X8) adalah sebagai berikut :

$$X9 = \frac{X3 + X4 + X6 + X7 + X8}{5}$$

3.6 Pengolahan Data

Secara garis besar, hasil pengolahan data responden yang sudah dilakukan normalisasi dibagi menjadi dua pokok utama, yaitu pemaparan hasil rata-rata tingkat kesadaran responden terhadap ancaman dan identifikasi faktor-faktor yang memengaruhi tingkat kesadaran tersebut. Setelah proses normalisasi, maka variabel yang diolah dan analisis untuk tahap pengolahan data ini adalah X1.1, X1.2, X1.3, X1.4, X2.1, X5.1, X5.2 dan X9 dengan detil informasi yang dicantumkan pada Tabel 5.

Tabel 5. Variabel Setelah Normalisasi

Kode Variabel	Deskripsi
X1.1	Usia
X1.2	Jenis kelamin
X1.3	Pekerjaan
X1.4	Pendidikan

Kode Variabel	Deskripsi
X2.1	Frekuensi penggunaan *mobile banking*
X5.1	Pengalaman korban percobaan *cybercrime*
X5.2	Pengalaman korban *cybercrime*
X9	Tingkat kesadaran responden terhadap *cybercrime*

Untuk menganalisis tingkat kesadaran responden terhadap ancaman *cybercrime* berdasarkan sosiodemografi, peneliti menghitung nilai rata-rata Likert dari jawaban responden pada kelima indikator yang disebutkan pada sub bab 4.5. Nilai rata-rata ini kemudian dianalisis berdasarkan indikator sosiodemografi, yaitu usia, jenis kelamin, pendidikan, dan pekerjaan. Dengan demikian, peneliti dapat mengidentifikasi variasi tingkat kesadaran di antara kelompok-kelompok sosiodemografi yang berbeda. Pendekatan ini memungkinkan peneliti untuk memahami bagaimana faktor-faktor sosiodemografi memengaruhi persepsi dan kesadaran pengguna terhadap ancaman *cybercrime* dalam konteks penggunaan *mobile banking*. Rata-rata tingkat kesadaran pengguna *mobile banking* terhadap ancaman *cybercrime* berdasarkan jenis sosiodemografi dapat dilihat di Tabel 6.

Tabel 6. Rata-Rata Tingkat Kesadaran Responden Berdasarkan Sosiodemografi

Sosiodemografi	Nilai	Rata-Rata Tingkat Kesadaran (Skala likert 1-5)
Usia	17 – 30 tahun	3,89
	30 – 40 tahun	3,96
	>=40 tahun	3,81
Jenis Kelamin	Pria	3,98
	Wanita	3,87
Pekerjaan	Pelajar	3,81
	Wiraswasta	4,05
	Karyawan	3,92
	Ibu Rumah Tangga	3,98
	Lain-Lain	3,81
Pendidikan	Setara atau di bawah SMA/SMK/Sederajat	3,91
	Diploma (D1/D2/D3)	3,90
	Sarjana (S1)	3,93
	Magister (S2)	3,87
	Doktor (S3)	3,49

Penjelasan dan interpretasi dari Tabel 6 adalah sebagai berikut:

1. Usia (X1.1): Pengguna *mobile banking* berusia 30-40 tahun memiliki tingkat kesadaran tertinggi terhadap ancaman *cybercrime* dengan rata-rata nilai 3,96. Pengguna berusia 17-30 tahun memiliki rata-rata tingkat kesadaran 3,89. Pengguna yang berusia 40 tahun ke atas memiliki tingkat kesadaran terendah di antara kelompok usia dengan nilai rata-rata 3,81.
2. Jenis Kelamin (X1.2): Pria menunjukkan tingkat kesadaran yang lebih tinggi terhadap ancaman *cybercrime* dibandingkan wanita, dengan nilai rata-rata 3,98 sedangkan wanita 3,87.
3. Pekerjaan (X1.3): Pengguna yang berprofesi sebagai wiraswasta memiliki tingkat kesadaran tertinggi dengan nilai rata-rata 4,05. Ibu rumah tangga juga menunjukkan tingkat kesadaran yang tinggi dengan rata-rata 3,98. Pelajar dan kelompok pekerjaan lainnya memiliki tingkat kesadaran yang sama, yaitu 3,81.
4. Pendidikan (X1.4): Pengguna dengan tingkat pendidikan Sarjana (S1) memiliki tingkat kesadaran tertinggi dengan nilai rata-rata 3,93. Pengguna dengan pendidikan Doktor (S3) memiliki tingkat kesadaran terendah dengan nilai rata-rata 3,49. Secara umum, tingkat kesadaran tidak meningkat secara signifikan dengan tingkat pendidikan yang lebih tinggi.

Dari hasil analisis ini, peneliti dapat menyimpulkan bahwa tingkat kesadaran pengguna *mobile banking* terhadap ancaman *cybercrime* bervariasi berdasarkan faktor sosiodemografi. Kelompok usia 30-40 tahun dan mereka yang berprofesi sebagai wiraswasta memiliki tingkat kesadaran yang lebih tinggi.

Peneliti mengevaluasi hubungan dan interaksi antara berbagai variabel independen dan variabel dependen menggunakan analisis varians (ANOVA) dengan *software* IBM SPSS. Teknik ini dipilih karena kemampuannya dalam mengidentifikasi pengaruh masing-masing variabel independen, serta interaksinya terhadap variabel dependen. ANOVA digunakan dalam penelitian ini untuk mengevaluasi pengaruh variabel independen (dan interaksinya) terhadap variabel dependen (X9), sedangkan variabel independen adalah X1.1, X1.2, X1.3, X1.4, X2.1, X5.1, dan X5.2. Hasil ini berasal dari "*Tests of Between-Subjects Effects*" yang menampilkan nilai Type III Sum of Squares,

degrees of freedom (df), Mean Square, F-value, dan nilai signifikansi (Sig.)

Setelah melakukan pengolahan data dengan menggunakan ANOVA, diperoleh sebanyak 127 jenis kombinasi antar variabel independen. Terdiri dari 11 kombinasi memiliki Sig. <= 0.05 dan sebanyak 116 memiliki Sig. <0.05. Dari hasil pengolahan data ditemukan juga R Squared = 0.680 yang berarti 68% dari variabilitas variabel dependen (X9) dapat dijelaskan oleh variabel independen dalam model. Ini menunjukkan bahwa model memiliki kemampuan penjelasan yang cukup baik, karena sebagian besar variabilitas dalam data dapat dijelaskan oleh model.

Tabel 7. Hasil Uji Anova Dengan Sig. <=0.05

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
X1.1	335,624	2	167,812	3,783	0,024
X1.3	444,216	4	111,054	2,504	0,043
X5.1	429,553	4	107,388	2,421	0,050
X1.2*X5.1	343,198	2	171,599	3,869	0,022
X1.3*X1.4	998,300	8	124,788	2,813	0,006
X1.4*X5.1	711,329	5	142,266	3,207	0,008
X1.4*X5.2	293,745	2	146,872	3,311	0,038
X1.1*X1.2 * X2.1	276,602	1	276,602	6,236	0,013
X1.1*X1.2 * X5.1	373,072	1	373,072	8,411	0,004
X1.1*X1.4 * X5.1	214,798	1	214,798	4,843	0,029
X1.1*X2.1 * X5.1	340,390	2	170,195	3,837	0,023

Berikut adalah ringkasan hasil analisis ANOVA yang dicantumkan pada Tabel 7:

1. Usia (X1.1) menunjukkan pengaruh signifikan terhadap variabel dependen dengan nilai F sebesar 3,783 dan nilai signifikansi (Sig.) 0,024.
2. Pekerjaan (X1.3) memiliki nilai F sebesar 2,504 dan nilai signifikansi 0,043, yang menunjukkan adanya pengaruh signifikan terhadap variabel dependen.
3. Pengalaman korban percobaan *cybercrime* (X5.1) menunjukkan pengaruh signifikan dengan nilai F sebesar 2,421 dan nilai signifikansi 0,050.
4. Interaksi jenis kelamin (X1.2) dengan pengalaman korban percobaan *cybercrime* (X5.1) memiliki nilai F sebesar 3,869 dan nilai signifikansi 0,022, menunjukkan adanya interaksi signifikan antara kedua variabel tersebut.
5. Interaksi pekerjaan (X1.3) dengan pendidikan (X1.4) menunjukkan pengaruh signifikan dengan nilai F sebesar 2,813 dan nilai signifikansi 0,006.
6. Interaksi pendidikan (X1.4) dengan pengalaman korban percobaan *cybercrime* (X5.1) menunjukkan nilai F sebesar 3,207 dan nilai signifikansi 0,008, interaksi ini juga signifikan.
7. Interaksi pendidikan (X1.4) dengan pengalaman korban cybercrime (X5.1) menunjukkan nilai F sebesar 3,311 dan nilai signifikansi 0,038, menunjukkan adanya interaksi signifikan.
8. Interaksi usia (X1.1), jenis kelamin (X1.2) dan frekuensi penggunaan *mobile banking* (X2.1) memiliki nilai F sebesar 6,236 dan nilai signifikansi 0,013, menunjukkan adanya interaksi signifikan di antara ketiga variabel.
9. Interaksi usia (X1.1), jenis kelamin (X1.2) dan pengalaman korban cybercrime (X5.1) menunjukkan pengaruh signifikan dengan nilai F sebesar 8,411 dan nilai signifikansi 0,004.
10. Interaksi usia (X1.1), pendidikan (X1.4) dan pengalaman korban cybercrime (X5.1) memiliki nilai F sebesar 4,843 dan nilai signifikansi 0,029, menunjukkan interaksi signifikan.
11. Interaksi usia (X1.1), frekuensi penggunaan *mobile banking* (X2.1) dan pengalaman korban cybercrime (X5.1) menunjukkan nilai F sebesar 3,837 dan nilai signifikansi 0,023, menunjukkan interaksi signifikan.

Dari hasil tersebut dapat dilihat bahwa terdapat beberapa interaksi antar variabel memiliki pengaruh yang signifikan terhadap variabel dependen seperti yang tercantum di tabel 7. Sedangkan X1.2, X1.4, X2.1, X5.2 dan beberapa kombinasi lainnya tidak memiliki pengaruh yang signifikan terhadap variabel dependen X9. Ini mengindikasikan adanya hubungan yang kuat antara variabel-variabel tersebut dalam konteks penelitian ini. Temuan ini memberikan wawasan yang berharga untuk memahami dinamika dan interaksi antar variabel yang diuji, serta kontribusi masing-masing variabel terhadap hasil penelitian.

4 Kesimpulan

Secara garis besar dari hasil analisis rata-rata tingkat kesadaran responden terhadap ancaman *cybercrime*, dapat disimpulkan bahwa saat ini tingkat kesadaran pengguna *mobile banking* terhadap ancaman *cybercrime* berdasarkan faktor sosiodemografi seperti usia, jenis kelamin, pendidikan, dan pekerjaan bervariasi. Rentang tingkat kesadaran ada diantara 3.49 sampai 4.05 mengacu pada skala Likert (1-5) sehingga bisa disimpulkan bahwa rata-rata responden memiliki tingkat kesadaran yang lumayan bagus. Kelompok usia 30-40 tahun, pria, serta wiraswasta dan ibu rumah tangga menunjukkan tingkat kesadaran yang lebih tinggi. Analisis ini penting untuk mengarahkan strategi pendidikan dan kesadaran yang lebih efektif di masa depan terkait dengan keamanan *cyber* dalam penggunaan layanan perbankan digital.

Berdasarkan hasil analisis pemetaan profil yang ditemukan dari data responden yang berhasil dikumpulkan, ditemukan dari 403 responden yang dipilih secara acak dengan usia 17 tahun ke atas dan menggunakan *mobile banking* dalam mendukung kegiatan keuangan merekan bahwa ancaman *cybercrime* masih terjadi bahkan setengah responden memiliki pengalaman percobaan *cybercrime* dan 21% dari total responden pernah menjadi korban *cybercrime* yang mengakibatkan kerugian baik secara finansial dan bocornya data pribadi.

Berdasarkan hasil analisis yang sudah dipaparkan, ditarik beberapa kesimpulan seperti adanya variabel yang signifikan. Beberapa variabel dan interaksi antara variabel menunjukkan pengaruh yang signifikan terhadap tingkat kesadaran pengguna terhadap ancaman *cybercrime*. Secara khusus, usia, pekerjaan dan pengalaman pribadi sebagai korban percobaan *cybercrime*, serta interaksi antara beberapa variabel yang dicantumkan pada bab pembahasan, memiliki nilai p-*value* yang kurang dari 0.05. Hal ini mengindikasikan bahwa variabel-variabel ini secara statistik signifikan dalam memengaruhi tingkat kesadaran pengguna terhadap ancaman *cybercrime* dalam konteks *mobile banking*.

Variabel yang tidak signifikan: Di sisi lain, beberapa variabel seperti jenis kelamin, pendidikan, dan beberapa kombinasi interaksi yang melibatkan variabel-variabel lainnya tidak menunjukkan pengaruh yang signifikan, karena nilai p-*value* mereka lebih besar dari 0.05. Ini menandakan bahwa faktor-faktor ini mungkin tidak secara signifikan memengaruhi tingkat kesadaran pengguna terhadap ancaman *cybercrime* dalam penggunaan *mobile banking*. Hasil pengolahan data menghasilkan R Squared yang tinggi (0.680), yang menunjukkan bahwa model yang digunakan mampu menjelaskan sebagian besar variasi dalam tingkat kesadaran pengguna terhadap ancaman *cybercrime*. Artinya, variabel-variabel yang dimasukkan ke dalam model cukup kuat untuk menjelaskan variasi dalam tingkat kesadaran ini.

Dalam konteks penelitian ini, temuan bahwa beberapa variabel dan interaksi signifikan secara statistik dapat memberikan wawasan berharga kepada penyedia layanan *mobile banking*, pemerintah ataupun pengguna *mobile banking* untuk meningkatkan kesadaran pengguna terhadap ancaman *cybercrime*. Hal ini dapat mencakup pengembangan kebijakan keamanan yang lebih efektif, pelatihan atau edukasi yang ditargetkan, atau peningkatan fitur keamanan dalam aplikasi *mobile banking*. Dengan demikian, penelitian ini dapat memberikan kontribusi yang signifikan dalam memperkuat strategi keamanan digital, khususnya dalam konteks penggunaan *mobile banking* di era yang semakin terhubung secara digital dan rentan terhadap ancaman *cybercrime*.

References

Alhakim, A., & Sofia, S. (2021). Kajian Normatif Penanganan Cyber Crime Di Sektor Perbankan Di Indonesia. *Jurnal Komunitas Yustisia*, *4*(2), 377–385. https://doi.org/10.23887/jatayu.v4i2.38089

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, *7*(1), e06016. https://doi.org/10.1016/j.heliyon.2021.e06016

Anggraini, I. N., & Arif, S. (2024). The effect of game-based learning model with STEM approach in reducing learning anxiety and enhancing science learning motivation among students. *Indonesian Journal of Science and …*, *07*(March), 105–117. https://doi.org/10.24042/ijsme.v5i1.20424

Apaua, R., & Lallie, H. S. (2022). *Measuring User Perceived Security of Mobile Banking Applications*. 1–36. http://arxiv.org/abs/2201.03052

Badan Pusat Statistikmiskin. (n.d.).

Delvyan Putri Surya Ningrum, & Jamiatur Robekha. (2023). Analisa Yuridis Dalam Kasus Kejahatan Siber Terhadap Internet Banking di Indonesia. *PESHUM : Jurnal Pendidikan, Sosial Dan Humaniora*, *2*(4), 765–776. https://doi.org/10.56799/peshum.v2i4.2115

Ginting, V. S., Benna, E., Manurung, P., Crime, C., & Crime, C. (2016). *PENERAPAN KEBIJAKAN DIGITAL DALAM RANGKA*. 249–253.

Herlina, B., & Ainun, A. A. (2023). Penggunaan Aplikasi Taspen Otentikasi Dalam Meningkatkan Efektifitas Pelayanan Pembayaran Pensiun Di Kantor Pos Sengkang. *Journal Of Social Science Research*, *3*, 10514–10526. https://j-innovative.org/index.php/Innovative

Herzallah, F., Al-Sharafi, M. A., & Arshah, R. A. (2018). *The Impact of Customer Trust and Perception of Security and Privacy on The Acceptance of Online Banking Services: Structural Equation Modeling Approach Internet Banking View project The Continuous Use of Cloud Computing Services and Its Impact On SMEs Per*. *September*. https://www.researchgate.net/publication/327671731

Joshi, A., Kale, S., Chandel, S., & Pal, D. (2015). Likert Scale: Explored and Explained. *British Journal of Applied Science & Technology*, *7*(4), 396–403. https://doi.org/10.9734/bjast/2015/14975

Kaloka, P. T., Yuliarto, H., & Wulandari, P. P. (2023). *Validity and Reliability of a Nonlinear Pedagogy Assessment Test (GPAI) in Invasion Games* (Issue 1). Atlantis Press International BV. https://doi.org/10.2991/978-94-6463-356-6_12

Kennedy, I. (2022). Sample Size Determination in Test-Retest and Cronbach Alpha Reliability Estimates. *British Journal of Contemporary Education*, *2*(1), 17–29. https://doi.org/10.52589/bjce-fy266hk9

Kota, T. P., & Kusumastuti, S. Y. (2022). Analisis Pengaruh Minat Nasabah Dalam Menggunakan Mobile Banking Dengan Menggunakan Kerangka Technology Acceptance Model (Tam). *Jurnal Apresiasi Ekonomi*, *10*(3), 276–288. https://doi.org/10.31846/jae.v10i3.515

Nur Rohmah, R. (2022). Upaya Membangun Kesadaran Keamanan Siber pada Konsumen E-commerce di Indonesia. *Cendekia Niaga*, *6*(1), 1–11. https://doi.org/10.52391/jcn.v6i1.629

Petru-cristian, N. (2023). *Conflict Analysis and Management Master Thesis Supervisor*. *October*. https://doi.org/10.13140/RG.2.2.17461.65763

Şenol, A., Talan, T., & Aktürk, C. (2021). *A Research on University Students' Awareness of Cyber Security: Case Study of Password Usage*. . *March*, 46–56.

Tantrinesia, M., Amelia, L. F., & Sidarwaya, H. A. (2023). Pengaruh M-banking Terhadap Pola Belanja Masyarakat di Surabaya. *Seminar Nasional Universitas Negeri Surabaya*, 24–38.

Tropika, B. (2023). *Ringkasan*. *5*(2).

Utami, Y. (2023). Uji Validitas dan Uji Reliabilitas Instrument Penilaian Kinerja Dosen. *Jurnal Sains Dan Teknologi*, *4*(2), 21–24. https://doi.org/10.55338/saintek.v4i2.730

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269