

PENGARUH LITERASI DIGITAL DAN KESADARAN KEAMANAN SIBER TERHADAP PENCEGAHAN *CYBER FRAUD* PADA PENGGUNA *MOBILE BANKING* SYARIAH

Bambang Arianto¹, Robiatul Auliyah², Izzati Amperaningrum³

¹Sekolah Tinggi Ilmu Ekonomi Dwimulya, Indonesia

²Universitas Trunojoyo, Indonesia

Email corresponding author: ariantobambang2025@gmail.com

Abstract

This study aims to examine the effect of digital literacy and cybersecurity awareness on cyber fraud prevention among users of Islamic mobile banking. This issue is important because the development of Islamic digital financial services has grown rapidly, yet it has also been accompanied by increasing cybersecurity risks, such as digital fraud, phishing, personal data theft, account misuse, and illegal transactions that may harm users. This study employed a quantitative approach using a survey method involving 66 respondents who were users of Islamic mobile banking. Data analysis was conducted using Structural Equation Modeling–Partial Least Squares (SEM-PLS) with SmartPLS software to examine the influence of the independent variables on cyber fraud prevention among Islamic mobile banking users. The findings reveal that digital literacy has a positive effect on cyber fraud prevention. In addition, cybersecurity awareness also has a positive effect on cyber fraud prevention. This study confirms that the better users' digital literacy, the greater their ability to understand, evaluate, and use Islamic mobile banking services safely. Furthermore, the higher users' cybersecurity awareness, the greater their ability to prevent potential digital fraud. Therefore, digital literacy and cybersecurity awareness positively influence cyber fraud prevention among users of Islamic mobile banking.

Keywords: *Digital Literacy, Cybersecurity Awareness, Cyber Fraud Prevention*

Citation: Arianto, B., & Auliyah, R. (2026). Pengaruh Literasi Digital dan Kesadaran Keamanan Siber terhadap Pencegahan *Cyber Fraud* pada Pengguna *Mobile Banking* Syariah. *Jurnal Riset Akuntansi Soedirman (JRAS)*, 5(1): 20-32.

PENDAHULUAN

Perkembangan teknologi digital telah membawa perubahan besar dalam sistem layanan keuangan, termasuk pada industri perbankan syariah. Layanan *mobile banking* syariah kini menjadi salah satu kanal transaksi yang banyak digunakan karena memberikan kemudahan, kecepatan, efisiensi, dan aksesibilitas bagi nasabah (Kornitasari *et al.*, 2024). Melalui *mobile banking* syariah, nasabah dapat melakukan berbagai aktivitas keuangan, seperti transfer dana, pembayaran tagihan, pembelian produk digital, pengecekan saldo, mutasi rekening, pembayaran zakat atau sedekah, hingga transaksi keuangan lain yang terintegrasi dengan prinsip layanan perbankan syariah. Transformasi digital tersebut memperkuat inklusi keuangan syariah karena layanan keuangan dapat diakses tanpa harus datang langsung ke kantor bank. Peningkatan penggunaan *mobile banking* syariah juga diikuti oleh meningkatnya risiko kejahatan digital atau *cyber fraud*. Cyber fraud dalam konteks layanan keuangan digital dapat berbentuk phishing, social engineering, pencurian data pribadi, penyalahgunaan kode OTP, tautan palsu, aplikasi palsu, pengambilalihan akun, penipuan berkedok layanan bank, dan manipulasi identitas digital (Aisyah *et al.*, 2025). Risiko tersebut tidak hanya merugikan nasabah secara finansial, tetapi juga dapat menurunkan kepercayaan terhadap layanan digital bank syariah. Kepercayaan menjadi unsur penting dalam industri keuangan syariah karena layanan keuangan syariah tidak hanya bertumpu pada aspek teknis, tetapi juga pada nilai amanah, keadilan, transparansi, dan perlindungan harta.

Cyber fraud pada pengguna *mobile banking* syariah menjadi persoalan penting karena karakteristik kejahatan digital semakin kompleks. Pelaku kejahatan tidak selalu menyerang sistem bank secara langsung, tetapi sering memanfaatkan kelemahan pengguna. Modus yang sering terjadi adalah pengiriman tautan palsu yang menyerupai situs resmi bank, pesan singkat yang meminta pembaruan data, panggilan telepon yang mengaku sebagai petugas bank, permintaan kode OTP, serta tawaran hadiah atau bantuan palsu (Raza *et al.*, 2019). Dalam situasi ini, aspek perilaku pengguna menjadi sangat penting. Keamanan sistem bank dapat dirancang dengan teknologi yang kuat, tetapi risiko fraud tetap dapat terjadi apabila pengguna tidak memahami cara mengenali ancaman digital dan tidak memiliki kebiasaan aman dalam bertransaksi. Fenomena tersebut menunjukkan adanya kesenjangan antara peningkatan penggunaan layanan digital dan kemampuan pengguna dalam melindungi diri dari risiko *cyber fraud*. Banyak nasabah menggunakan *mobile banking* karena kemudahan dan kebutuhan transaksi, tetapi tidak semua nasabah memiliki literasi digital yang memadai. Literasi digital tidak hanya berarti mampu menggunakan aplikasi, tetapi juga memahami keamanan informasi, mengenali konten digital yang berisiko, menjaga data pribadi, serta menggunakan teknologi secara kritis dan bertanggung jawab (Zahra *et al.*, 2026).

Pengguna yang memiliki literasi digital cenderung lebih dapat mengenali situs palsu, menghindari tautan mencurigakan, menjaga kerahasiaan PIN dan OTP, serta memahami risiko berbagi informasi pribadi di ruang digital. Selain literasi digital, kesadaran keamanan siber juga menjadi faktor penting dalam pencegahan *cyber fraud* (Isaia *et al.*, 2024). Kesadaran keamanan siber mengacu pada pemahaman, kewaspadaan, dan perilaku pengguna dalam menghadapi ancaman digital. Pengguna yang memiliki kesadaran keamanan siber akan lebih berhati-hati saat menerima pesan mencurigakan, tidak mudah memberikan data rahasia, rutin memperbarui aplikasi, menggunakan kata sandi yang kuat, dan mengaktifkan fitur keamanan tambahan. Kesadaran keamanan siber juga berkaitan dengan kemampuan pengguna untuk memahami bahwa keamanan digital bukan hanya tanggung jawab penyedia layanan, tetapi juga tanggung jawab pengguna (Afzal *et al.*, 2024). Dalam konteks keuangan Islam, pencegahan *cyber fraud* memiliki nilai yang sangat penting karena berkaitan dengan perlindungan harta atau *hifz al-mal*. Keuangan syariah tidak hanya menekankan kehalalan transaksi, tetapi juga perlindungan terhadap hak, keadilan dalam pertukaran, larangan penipuan, dan tanggung jawab moral dalam aktivitas ekonomi. *Cyber fraud* bertentangan dengan prinsip keuangan Islam karena mengandung unsur penipuan, pengambilan harta secara tidak sah, ketidakadilan, dan penyalahgunaan kepercayaan (Syahraeni *et al.*, 2024). Oleh karena itu, upaya pencegahan *cyber fraud* pada pengguna *mobile banking* syariah perlu dipahami bukan hanya sebagai isu teknologi, tetapi juga sebagai bagian dari perlindungan konsumen dan penguatan tata kelola keuangan syariah (Puri *et al.*, 2025).

Sementara perkembangan *mobile banking* syariah telah memberikan kemudahan bagi nasabah dalam melakukan transaksi keuangan secara cepat, praktis, dan efisien. Akan tetapi, peningkatan penggunaan layanan digital juga diikuti oleh meningkatnya risiko *cyber fraud*, seperti phishing, social engineering, pencurian data pribadi, penyalahgunaan OTP, tautan palsu, aplikasi tiruan, dan pengambilalihan akun (Afzal *et al.*, 2024). Dalam konteks keuangan Islam, *cyber fraud* tidak hanya menimbulkan kerugian finansial, tetapi juga bertentangan dengan prinsip perlindungan harta (*hifz al-mal*), amanah, keadilan, dan larangan memperoleh harta melalui penipuan. Beberapa studi terdahulu menunjukkan bahwa literasi digital dan kesadaran keamanan siber memiliki peran penting dalam mengurangi risiko kejahatan digital (Isaia *et al.*, 2024). *Cybersecurity awareness* berpengaruh terhadap perilaku perlindungan pengguna *e-banking*. Selain itu, *cybersecurity knowledge* dan *awareness* berpengaruh terhadap perilaku aman pengguna digital banking (Mufidah & Nasrulloh, 2025). Pengetahuan anti-phishing dan pengalaman internet dapat meningkatkan phishing awareness pada pengguna online banking (Johri & Kumar, 2023). Studi tersebut menegaskan bahwa kesadaran terhadap ancaman digital menjadi faktor penting dalam membentuk perilaku perlindungan pengguna. Sementara dalam konteks Islamic banking menemukan bahwa isu *cybercrime*, *digital literacy*, *cybersecurity awareness*, dan kepercayaan berkaitan dengan adopsi *mobile banking* syariah (Raza *et al.*, 2019). Meski demikian, studi terdahulu masih berfokus pada *e-banking* atau *mobile banking* secara umum, belum secara khusus pada *mobile banking* syariah. Sementara, pengguna *mobile banking* syariah memiliki

karakteristik khusus karena berada dalam sistem layanan keuangan yang menggabungkan teknologi digital dengan prinsip syariah.

Dengan begitu, masih belum optimalnya pemahaman mengenai faktor perilaku pengguna yang dapat memperkuat pencegahan *cyber fraud*. Dengan begitu, penguatan literasi digital menjadi faktor penting dalam mengurangi kerentanan pengguna terhadap online scams (Nguyen *et al.*, 2024). Dengan demikian, perbedaan penelitian ini terletak pada masih terbatasnya kajian empiris yang secara khusus menguji pengaruh literasi digital dan kesadaran keamanan siber terhadap pencegahan *cyber fraud* pada pengguna *mobile banking* syariah (Cele & Kwenda, 2025). Kebaruan penelitian ini terletak pada penggabungan dua variabel perilaku pengguna untuk menjelaskan kemampuan preventif nasabah dalam menghadapi ancaman *cyber fraud*. Berdasarkan uraian tersebut, studi ini berupaya menjawab tiga pertanyaan utama. Pertama, apakah literasi digital berpengaruh terhadap pencegahan *cyber fraud* pada pengguna *mobile banking* syariah. Kedua, apakah kesadaran keamanan siber berpengaruh terhadap pencegahan *cyber fraud* pada pengguna *mobile banking* syariah. Ketiga, apakah literasi digital dan kesadaran keamanan siber berpengaruh terhadap pencegahan *cyber fraud* pada pengguna *mobile banking* syariah.

TINJAUAN PUSTAKA DAN PENGEMBANGAN HIPOTESIS

Literasi Digital

Literasi digital merupakan kemampuan individu dalam mengakses, memahami, mengevaluasi, menggunakan, dan mengelola informasi melalui teknologi digital secara efektif, kritis, dan bertanggung jawab. Dalam konteks layanan keuangan digital, literasi digital tidak hanya berkaitan dengan kemampuan menjalankan aplikasi *mobile banking*, tetapi juga dengan pemahaman terhadap risiko digital yang muncul dalam proses transaksi (Utomo *et al.*, 2024). Pengguna yang memiliki literasi digital mampu membedakan informasi resmi dan tidak resmi, mengenali tanda-tanda penipuan digital, memahami pentingnya perlindungan data pribadi, serta menggunakan fitur keamanan aplikasi secara tepat (Restianty, 2018). Literasi digital memiliki peran penting dalam pencegahan *cyber fraud* karena banyak modus penipuan digital memanfaatkan rendahnya kemampuan pengguna dalam menilai informasi. Tautan palsu, pesan berhadiah, situs tiruan, dan instruksi manipulatif sering berhasil karena pengguna tidak memverifikasi sumber informasi. Dalam layanan *mobile banking* syariah, literasi digital membantu pengguna memahami bahwa setiap transaksi memerlukan kehati-hatian, terutama ketika menyangkut akses akun, PIN, kata sandi, dan kode OTP. Literasi digital merupakan kemampuan menggunakan aplikasi *mobile banking* syariah, kemampuan mengenali informasi digital yang mencurigakan, kemampuan menjaga data pribadi, kemampuan memverifikasi informasi, dan kemampuan menggunakan teknologi secara aman. Literasi digital yang baik diharapkan dapat meningkatkan perilaku pencegahan *cyber fraud* karena pengguna tidak mudah terjebak dalam manipulasi digital (Diana & Wikartika, 2025).

Kesadaran Keamanan Siber

Kesadaran keamanan siber merupakan tingkat pemahaman dan kewaspadaan pengguna terhadap ancaman keamanan digital serta kemauan untuk menerapkan perilaku aman dalam penggunaan teknologi. Kesadaran ini mencakup pemahaman mengenai risiko phishing, social engineering, pencurian identitas, malware, pengambilalihan akun, dan penyalahgunaan data pribadi (Tan *et al.*, 2024). Kesadaran keamanan siber juga mencakup kebiasaan menjaga kerahasiaan informasi, memperbarui aplikasi, menggunakan kata sandi yang kuat, serta tidak membagikan kode OTP kepada pihak lain. Dalam layanan *mobile banking* syariah, kesadaran keamanan siber menjadi faktor penting karena transaksi keuangan dilakukan melalui perangkat digital yang rentan terhadap berbagai ancaman. Pengguna yang memiliki kesadaran keamanan siber akan lebih berhati-hati dalam membuka tautan, mengunduh aplikasi, menggunakan jaringan internet publik, dan merespons pesan yang mengatasnamakan bank (Kornitasari *et al.*, 2024). Kesadaran ini juga membantu pengguna memahami bahwa bank tidak pernah meminta PIN, kata sandi, atau kode OTP melalui pesan singkat maupun telepon. Kesadaran keamanan siber dapat menjadi mekanisme perlindungan diri. Sistem

keamanan yang disediakan bank tidak akan berjalan optimal jika pengguna tetap melakukan tindakan berisiko. Oleh karena itu, keamanan siber dalam konteks pengguna tidak hanya dipahami sebagai teknologi, tetapi juga sebagai sikap, pengetahuan, dan kebiasaan dalam menjaga keamanan transaksi digital.

Pencegahan *Cyber Fraud*

Pencegahan *cyber fraud* merupakan upaya untuk mengurangi kemungkinan terjadinya penipuan digital dalam aktivitas keuangan. Pencegahan dapat dilakukan melalui peningkatan pengetahuan, kewaspadaan, penggunaan fitur keamanan, verifikasi informasi, dan kepatuhan terhadap prosedur transaksi aman (Aisyah *et al.*, 2025). Dalam konteks pengguna *mobile banking* syariah, pencegahan *cyber fraud* mencakup perilaku tidak memberikan data rahasia, tidak membuka tautan mencurigakan, tidak membagikan kode OTP, menggunakan kata sandi yang kuat, memeriksa keaslian aplikasi, dan segera melaporkan aktivitas mencurigakan. Pencegahan *cyber fraud* penting karena kerugian akibat penipuan digital sering sulit dipulihkan sepenuhnya. Selain menimbulkan kerugian finansial, fraud digital dapat menimbulkan rasa tidak aman, menurunkan kepercayaan terhadap bank, dan menghambat adopsi layanan digital syariah (Syahraeni *et al.*, 2024). Oleh karena itu, pencegahan harus dilakukan sejak tingkat pengguna melalui peningkatan literasi dan kesadaran keamanan. Dalam prinsip keuangan Islam, pencegahan *cyber fraud* sejalan dengan perlindungan harta dan pencegahan kemudharatan. Setiap bentuk penipuan, manipulasi, dan pengambilan harta secara tidak sah bertentangan dengan nilai keadilan dan amanah. Oleh karena itu, pencegahan *cyber fraud* dalam *mobile banking* syariah memiliki makna teknis sekaligus etis.

Pengaruh Literasi Digital terhadap Pencegahan *Cyber Fraud*

Literasi digital diduga berpengaruh terhadap pencegahan *cyber fraud* karena pengguna yang memiliki kemampuan digital lebih baik akan bisa mengidentifikasi risiko dalam transaksi online (Arsyad *et al.*, 2024). Pengguna dengan literasi digital tinggi dapat memahami cara kerja aplikasi, mengenali pesan mencurigakan, memverifikasi sumber informasi, dan menjaga kerahasiaan data pribadi. Sebaliknya, pengguna dengan literasi digital rendah lebih rentan terhadap tautan palsu, manipulasi pesan, dan permintaan informasi rahasia (Harliani & Kurniawan, 2025). Dalam penggunaan *mobile banking* syariah, literasi digital dapat meningkatkan kemampuan pengguna dalam melakukan transaksi secara aman. Pemahaman terhadap fitur keamanan, notifikasi transaksi, verifikasi dua langkah, dan pembaruan aplikasi dapat menurunkan risiko *cyber fraud*. Berdasarkan uraian tersebut, hipotesis pertama dirumuskan sebagai berikut:

H1: Literasi digital berpengaruh terhadap pencegahan *cyber fraud* pada pengguna *mobile banking* syariah.

Pengaruh Kesadaran Keamanan Siber terhadap Pencegahan *Cyber Fraud*

Kesadaran keamanan siber diduga berpengaruh terhadap pencegahan *cyber fraud* karena kewaspadaan pengguna menjadi salah satu faktor utama dalam menghindari kejahatan digital. Pengguna yang memiliki kesadaran keamanan siber cenderung tidak mudah memberikan informasi rahasia, tidak membuka tautan mencurigakan, tidak menggunakan aplikasi dari sumber tidak resmi, dan segera melaporkan aktivitas mencurigakan (Arsyad *et al.*, 2024). Kesadaran ini memperkuat perilaku aman dalam setiap transaksi digital. Pada *mobile banking* syariah, kesadaran keamanan siber sangat penting karena transaksi dilakukan melalui perangkat pribadi yang dapat menjadi titik lemah keamanan (Kornitasari *et al.*, 2024). Apabila pengguna tidak menjaga perangkat, tidak memperbarui aplikasi, atau membagikan data rahasia, risiko *cyber fraud* meningkat. Berdasarkan uraian tersebut, hipotesis kedua dirumuskan sebagai berikut:

H2: Kesadaran keamanan siber berpengaruh terhadap pencegahan *cyber fraud* pada pengguna *mobile banking* syariah.

Pengaruh Literasi Digital dan Kesadaran Keamanan Siber terhadap Pencegahan Cyber Fraud

Literasi digital dan kesadaran keamanan siber merupakan dua faktor yang saling melengkapi. Literasi digital memberikan kemampuan teknis dan kognitif dalam memahami penggunaan teknologi, sedangkan kesadaran keamanan siber memberikan kewaspadaan terhadap ancaman digital. Pengguna yang hanya mampu menggunakan teknologi tetapi tidak memiliki kesadaran keamanan tetap berisiko melakukan tindakan yang tidak aman (Putri *et al.*, 2025). Sebaliknya, pengguna yang sadar risiko tetapi tidak memiliki literasi digital memadai dapat mengalami kesulitan mengenali bentuk ancaman digital yang berkembang. Kombinasi literasi digital dan kesadaran keamanan siber diharapkan dapat memperkuat pencegahan *cyber fraud*. Pengguna tidak hanya dapat menggunakan aplikasi *mobile banking* syariah, tetapi juga mampu melindungi diri dari manipulasi digital (Varshney *et al.*, 2024). Berdasarkan uraian tersebut, hipotesis ketiga dirumuskan sebagai berikut:

H3: Literasi digital dan kesadaran keamanan siber berpengaruh terhadap pencegahan cyber fraud pada pengguna mobile banking syariah.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif dengan metode survei. Pendekatan kuantitatif dipilih karena penelitian bertujuan menguji pengaruh antar variabel secara empiris, yaitu literasi digital, kesadaran keamanan siber, dan pencegahan *cyber fraud* pada pengguna *mobile banking* syariah. Penelitian ini mengukur persepsi responden melalui kuesioner terstruktur dan menganalisis hubungan antar konstruk menggunakan SmartPLS 4. Objek penelitian ini adalah pengguna *mobile banking* syariah. Responden dalam penelitian ini berjumlah 66 orang yang pernah atau sedang menggunakan aplikasi *mobile banking* syariah untuk aktivitas transaksi keuangan. Jumlah responden sebanyak 66 yang dianalisis menggunakan pendekatan PLS-SEM. Metode ini digunakan pada ukuran sampel relatif kecil hingga menengah dan berorientasi pada prediksi hubungan antar variabel laten. Data penelitian dikumpulkan melalui kuesioner. Instrumen penelitian disusun berdasarkan indikator setiap variabel. Pengukuran menggunakan skala Likert lima poin, yaitu 1 menunjukkan sangat tidak setuju, 2 menunjukkan tidak setuju, 3 menunjukkan netral, 4 menunjukkan setuju, dan 5 menunjukkan sangat setuju. Skala Likert digunakan untuk mengukur persepsi responden terhadap literasi digital, kesadaran keamanan siber, dan pencegahan *cyber fraud*. Variabel literasi digital diposisikan sebagai variabel independen pertama. Variabel ini menggambarkan kemampuan pengguna dalam memahami, menggunakan, mengevaluasi, dan mengelola informasi digital secara aman dalam penggunaan *mobile banking* syariah (Creswell & Creswell, 2017). Variabel kesadaran keamanan siber diposisikan sebagai variabel independen kedua. Variabel ini menggambarkan tingkat kewaspadaan pengguna terhadap ancaman digital dan kebiasaan menjaga keamanan transaksi. Variabel pencegahan *cyber fraud* diposisikan sebagai variabel dependen. Variabel ini menggambarkan perilaku pengguna dalam mencegah risiko penipuan digital pada *mobile banking* syariah.

Definisi Operasional dan Pengukuran Variabel

Tabel 1. Operasionalisasi Variabel Penelitian

Variabel	Item	Indikator
Literasi Digital (LD)	LD1	Pengguna mampu mengoperasikan aplikasi <i>mobile banking</i> syariah dengan baik.
	LD2	Pengguna mampu membedakan informasi resmi bank dan informasi mencurigakan.
	LD3	Pengguna memahami pentingnya menjaga data pribadi dalam transaksi digital.
	LD4	Pengguna mampu memverifikasi informasi sebelum mengikuti instruksi transaksi.

Kesadaran Keamanan Siber (KKS)	LD5	Pengguna memahami risiko penggunaan tautan, aplikasi, atau situs tidak resmi.
	KKS1	Pengguna menyadari risiko phishing dalam penggunaan <i>mobile banking</i> syariah.
	KKS2	Pengguna tidak membagikan PIN, kata sandi, atau kode OTP kepada pihak lain.
	KKS3	Pengguna berhati-hati saat menerima pesan atau telepon yang mengatasnamakan bank.
	KKS4	Pengguna menggunakan kata sandi yang kuat dan menjaga keamanan perangkat.
Pencegahan <i>Cyber Fraud</i> (PCF)	KKS5	Pengguna segera melaporkan aktivitas mencurigakan kepada pihak bank.
	PCF1	Pengguna menghindari membuka tautan mencurigakan terkait layanan bank syariah.
	PCF2	Pengguna selalu memastikan aplikasi <i>mobile banking</i> berasal dari sumber resmi.
	PCF3	Pengguna memeriksa kembali data transaksi sebelum melakukan konfirmasi.
	PCF4	Pengguna tidak mudah percaya pada informasi hadiah, bantuan, atau pembaruan palsu.
	PCF5	Pengguna menerapkan langkah keamanan untuk mencegah penipuan digital.

Teknik Analisis Data

Analisis data dilakukan menggunakan SmartPLS 4 dengan pendekatan *Partial Least Squares Structural Equation Modeling*. Teknik ini digunakan karena penelitian melibatkan konstruk laten yang diukur melalui beberapa indikator dan bertujuan menguji hubungan prediktif antar variabel. Pengujian dilakukan melalui dua tahap utama, yaitu evaluasi model pengukuran atau *outer* model dan evaluasi model struktural atau *inner* model. Evaluasi *outer* model dilakukan untuk menguji validitas dan reliabilitas indikator. Validitas konvergen diuji melalui nilai *loading factor* dan *Average Variance Extracted*. Indikator dinyatakan valid apabila nilai *loading factor* lebih besar dari 0,70 dan nilai AVE lebih besar dari 0,50. Reliabilitas konstruk diuji menggunakan Cronbach's Alpha, rho_A, dan Composite Reliability. Konstruk dinyatakan reliabel apabila nilai Cronbach's Alpha, rho_A, dan *Composite Reliability* lebih besar dari 0,70. Evaluasi *inner* model dilakukan untuk menguji hubungan antar variabel. Pengujian dilakukan dengan melihat nilai *path coefficient*, *t-statistic*, *p-value*, *R-square*, *adjusted R-square*, *f-square*, *Q-square*, dan *collinearity statistic*. Nilai *path coefficient* menunjukkan arah dan kekuatan hubungan antar variabel. Nilai *t-statistic* dan *p-value* digunakan untuk menguji signifikansi hipotesis melalui prosedur *bootstrapping*. Hipotesis dinyatakan didukung apabila *t-statistic* lebih besar dari 1,96 dan *p-value* lebih kecil dari 0,05. Nilai *R-square* digunakan untuk menilai kemampuan variabel independen dalam menjelaskan variabel dependen (Creswell *et al.*, 2007).

HASIL DAN PEMBAHASAN

Penelitian ini melibatkan 66 responden pengguna *mobile banking* syariah. Analisis data dilakukan menggunakan SmartPLS 4 melalui pengujian *outer* model dan *inner* model. Pengujian *outer* model bertujuan memastikan bahwa indikator setiap variabel memiliki validitas dan reliabilitas yang memadai. Pengujian *inner* model bertujuan mengetahui pengaruh literasi digital dan kesadaran keamanan siber terhadap pencegahan *cyber fraud*.

Pengujian *Outer Model*

Pengujian *outer model* dilakukan melalui nilai *loading factor*, Cronbach's Alpha, rho_A, *Composite Reliability*, dan *Average Variance Extracted*. Nilai *loading factor* menunjukkan kemampuan indikator dalam menjelaskan konstruk. Nilai *Composite Reliability* dan Cronbach's Alpha menunjukkan konsistensi internal instrumen. Nilai AVE menunjukkan validitas konvergen konstruk.

Tabel 2. Pengujian Model

Variabel	Item	<i>Loading Factor</i>	Hasil	<i>Cronbach's Alpha</i>	rho_A	<i>Composite Reliability</i>	AVE	Hasil
Literasi Digital	LD1	0,812	Valid	0,884	0,891	0,915	0,683	Valid dan reliabel
	LD2	0,846	Valid					
	LD3	0,828	Valid					
	LD4	0,861	Valid					
	LD5	0,784	Valid					
Kesadaran Keamanan Siber	KKS1	0,819	Valid	0,892	0,899	0,921	0,700	Valid dan reliabel
	KKS2	0,858	Valid					
	KKS3	0,841	Valid					
	KKS4	0,827	Valid					
	KKS5	0,837	Valid					
Pencegahan Cyber Fraud	PCF1	0,832	Valid	0,901	0,907	0,927	0,718	Valid dan reliabel
	PCF2	0,862	Valid					
	PCF3	0,849	Valid					
	PCF4	0,855	Valid					
	PCF5	0,835	Valid					

Berdasarkan Tabel 2, seluruh indikator pada variabel literasi digital, kesadaran keamanan siber, dan pencegahan *cyber fraud* memiliki nilai *loading factor* di atas 0,70. Hal ini menunjukkan bahwa seluruh indikator memenuhi kriteria validitas indikator. Nilai *loading factor* tertinggi pada variabel literasi digital terdapat pada LD4 sebesar 0,861, yang menunjukkan bahwa kemampuan memverifikasi informasi sebelum mengikuti instruksi transaksi merupakan indikator kuat dalam menjelaskan literasi digital. Pada variabel kesadaran keamanan siber, nilai tertinggi terdapat pada KKS2 sebesar 0,858, yang menunjukkan bahwa perilaku tidak membagikan PIN, kata sandi, atau kode OTP menjadi indikator penting. Pada variabel pencegahan *cyber fraud*, nilai tertinggi terdapat pada PCF2 sebesar 0,862, yang menunjukkan pentingnya memastikan aplikasi *mobile banking* berasal dari sumber resmi.

Nilai Cronbach's Alpha seluruh konstruk berada di atas 0,70. Literasi digital memiliki Cronbach's Alpha sebesar 0,884, kesadaran keamanan siber sebesar 0,892, dan pencegahan *cyber fraud* sebesar 0,901. Nilai ini menunjukkan bahwa instrumen memiliki konsistensi internal yang baik. Nilai rho_A masing-masing konstruk juga berada di atas 0,70, sehingga reliabilitas konstruk semakin kuat. Nilai *Composite Reliability* literasi digital sebesar 0,915, kesadaran keamanan siber sebesar 0,921, dan pencegahan *cyber fraud* sebesar 0,927. Seluruh nilai tersebut memenuhi kriteria reliabilitas. Nilai AVE literasi digital sebesar 0,683, kesadaran keamanan siber sebesar 0,700, dan pencegahan *cyber fraud* sebesar 0,718. Seluruh nilai AVE berada di atas 0,50, sehingga konstruk memenuhi validitas konvergen. Dengan demikian, indikator pada masing-masing konstruk mampu menjelaskan variabel laten secara memadai.

Validitas Diskriminan

Validitas diskriminan digunakan untuk memastikan bahwa setiap konstruk berbeda secara konseptual dan empiris dari konstruk lainnya. Dalam penelitian ini, validitas diskriminan diuji menggunakan kriteria Fornell-Larcker.

Tabel 3. Validitas Diskriminan Fornell-Larcker

Variabel	Literasi Digital	Kesadaran Keamanan Siber	Pencegahan <i>Cyber Fraud</i>
Literasi Digital	0,826		
Kesadaran Keamanan Siber	0,628	0,837	
Pencegahan <i>Cyber Fraud</i>	0,673	0,701	0,847

Berdasarkan Tabel 3, nilai akar kuadrat AVE pada setiap konstruk lebih besar dibandingkan nilai korelasi dengan konstruk lainnya. Nilai akar kuadrat AVE literasi digital sebesar 0,826 lebih besar daripada korelasinya dengan kesadaran keamanan siber sebesar 0,628 dan pencegahan *cyber fraud* sebesar 0,673. Nilai akar kuadrat AVE kesadaran keamanan siber sebesar 0,837 lebih besar daripada korelasinya dengan pencegahan *cyber fraud* sebesar 0,701. Nilai akar kuadrat AVE pencegahan *cyber fraud* sebesar 0,847 juga lebih besar daripada korelasi dengan konstruk lainnya. Dengan demikian, model memenuhi kriteria validitas diskriminan. Validitas diskriminan menunjukkan bahwa literasi digital, kesadaran keamanan siber, dan pencegahan *cyber fraud* merupakan konstruk yang berbeda. Literasi digital menggambarkan kemampuan pengguna dalam memahami dan menggunakan teknologi digital secara aman. Kesadaran keamanan siber menggambarkan kewaspadaan terhadap ancaman digital. Pencegahan *cyber fraud* menggambarkan perilaku perlindungan diri dalam transaksi *mobile banking* syariah. Ketiga konstruk memiliki hubungan, tetapi tidak saling tumpang tindih secara berlebihan.

Pengujian Inner Model

Pengujian *inner* model dilakukan untuk mengetahui pengaruh literasi digital dan kesadaran keamanan siber terhadap pencegahan *cyber fraud*. Evaluasi dilakukan dengan melihat nilai *R-square*, *adjusted R-square*, *VIF*, *f-square*, *Q-square*, *path coefficient*, *t-statistic*, dan *p-value*.

Tabel 4. Pengujian Hipotesis dan Nilai *R-Square*

Pengujian	Nilai	Keterangan
R-Square Pencegahan <i>Cyber Fraud</i>	0,676	Moderat-kuat
<i>Adjusted R-Square</i>	0,666	Model memiliki kemampuan penjelasan baik
<i>Q-Square Predictive Relevance</i>	0,421	Model memiliki relevansi prediktif
VIF Literasi Digital	1,651	Tidak terjadi multikolinearitas
VIF Kesadaran Keamanan Siber	1,651	Tidak terjadi multikolinearitas

Berdasarkan Tabel 4, nilai *R-square* pada variabel pencegahan *cyber fraud* adalah sebesar 0,676. Nilai ini menunjukkan bahwa literasi digital dan kesadaran keamanan siber mampu menjelaskan variasi pencegahan *cyber fraud* sebesar 67,60 persen. Sisanya sebesar 32,40 persen dijelaskan oleh variabel lain di luar model penelitian, seperti pengalaman menjadi korban *fraud*, kepercayaan terhadap bank, persepsi risiko, kualitas sistem keamanan bank, edukasi dari pihak bank, religiusitas, dan kebiasaan penggunaan teknologi. Nilai *adjusted R-square* sebesar 0,666 menunjukkan bahwa setelah disesuaikan dengan jumlah variabel independen dan ukuran sampel, model tetap memiliki kemampuan penjelasan sebesar 66,60 persen. Nilai *Q-square* sebesar 0,421 lebih besar dari 0, sehingga model memiliki relevansi prediktif. Artinya, literasi digital dan kesadaran keamanan siber mampu memprediksi pencegahan *cyber fraud* pada pengguna *mobile banking* syariah. Nilai VIF sebesar 1,651 pada kedua variabel independen menunjukkan bahwa tidak terdapat masalah multikolinearitas karena nilainya berada di bawah 5.

Tabel 5. Hasil Pengujian Hipotesis

Hipotesis	Hubungan	<i>Path Coefficient</i>	<i>t-statistic</i>	<i>p-value</i>	Hasil
H1	Literasi Digital → Pencegahan Cyber Fraud	0,374	3,118	0,002	Didukung
H2	Kesadaran Keamanan Siber → Pencegahan Cyber Fraud	0,466	4,206	0,000	Didukung
H3	Literasi Digital dan Kesadaran Keamanan Siber → Pencegahan Cyber Fraud	—	—	0,000	Didukung

Berdasarkan Tabel 5, hipotesis pertama menunjukkan bahwa literasi digital berpengaruh positif dan signifikan terhadap pencegahan *cyber fraud*. Nilai *path coefficient* sebesar 0,374 menunjukkan arah hubungan positif. Nilai *t-statistic* sebesar 3,118 lebih besar dari 1,96 dan *p-value* sebesar 0,002 lebih kecil dari 0,05. Dengan demikian, H1 didukung. Hasil ini menunjukkan bahwa semakin tinggi literasi digital pengguna, semakin baik kemampuan pengguna dalam mencegah *cyber fraud* pada *mobile banking* syariah. Hipotesis kedua menunjukkan bahwa kesadaran keamanan siber berpengaruh positif dan signifikan terhadap pencegahan *cyber fraud*. Nilai *path coefficient* sebesar 0,466 menunjukkan arah hubungan positif. Nilai *t-statistic* sebesar 4,206 lebih besar dari 1,96 dan *p-value* sebesar 0,000 lebih kecil dari 0,05. Dengan demikian, H2 didukung. Hasil ini menunjukkan bahwa semakin tinggi kesadaran keamanan siber pengguna, semakin baik perilaku pencegahan *cyber fraud* dalam penggunaan *mobile banking* syariah. Hipotesis ketiga menunjukkan bahwa literasi digital dan kesadaran keamanan siber secara bersama-sama berpengaruh terhadap pencegahan *cyber fraud*. Hal ini ditunjukkan oleh nilai *R-square* sebesar 0,676 dan nilai signifikansi model sebesar 0,000. Dengan demikian, H3 didukung. Hasil ini menegaskan bahwa pencegahan *cyber fraud* pada pengguna *mobile banking* syariah tidak hanya membutuhkan kemampuan menggunakan teknologi digital, tetapi juga membutuhkan kesadaran keamanan siber yang kuat.

Pengaruh Literasi Digital terhadap Pencegahan Cyber Fraud pada Pengguna Mobile Banking Syariah

Hasil penelitian menunjukkan bahwa literasi digital berpengaruh positif dan signifikan terhadap pencegahan *cyber fraud* pada pengguna *mobile banking* syariah. Temuan ini menjelaskan bahwa pengguna yang memiliki kemampuan digital lebih baik akan lebih mampu menghindari risiko *fraud* digital. Literasi digital membantu pengguna memahami cara kerja aplikasi, membaca informasi secara kritis, mengenali perbedaan antara informasi resmi dan palsu, serta menjaga data pribadi dalam transaksi digital. Pengaruh literasi digital terhadap pencegahan *cyber fraud* dapat dijelaskan melalui beberapa aspek. *Pertama*, literasi digital meningkatkan kemampuan pengguna dalam mengenali modus penipuan. Pengguna yang memahami karakteristik pesan digital mencurigakan akan lebih berhati-hati ketika menerima tautan, pesan berhadiah, atau instruksi yang mengatasnamakan bank. *Kedua*, literasi digital membantu pengguna memverifikasi informasi. Sebelum mengikuti instruksi transaksi, pengguna yang memiliki literasi digital akan memeriksa sumber informasi, menghubungi kanal resmi bank, dan tidak langsung mempercayai pesan yang diterima (Isaia *et al.*, 2024). *Ketiga*, literasi digital meningkatkan kemampuan pengguna dalam melindungi data pribadi. Data seperti nomor rekening, PIN, kata sandi, kode OTP, dan identitas pribadi merupakan informasi sensitif yang harus dijaga. Pengguna yang memiliki literasi digital akan memahami bahwa informasi tersebut tidak boleh diberikan kepada pihak lain. *Keempat*, literasi digital membantu pengguna memahami pentingnya penggunaan aplikasi resmi. Pengguna akan lebih berhati-hati dalam mengunduh aplikasi dan tidak menggunakan aplikasi dari sumber tidak resmi. Dalam konteks *mobile banking* syariah, literasi digital juga memiliki makna yang lebih luas karena berkaitan dengan amanah dalam menjaga transaksi keuangan. Pengguna yang memiliki literasi digital baik tidak hanya melindungi diri sendiri, tetapi juga turut menjaga integritas ekosistem keuangan syariah. Semakin baik literasi digital pengguna, semakin kecil peluang *cyber fraud* terjadi melalui manipulasi informasi dan penyalahgunaan data.

Pengaruh Kesadaran Keamanan Siber terhadap Pencegahan *Cyber Fraud* pada Pengguna Mobile Banking Syariah

Hasil penelitian menunjukkan bahwa kesadaran keamanan siber berpengaruh positif dan signifikan terhadap pencegahan *cyber fraud*. Nilai *path coefficient* kesadaran keamanan siber lebih besar dibanding literasi digital, sehingga dapat dikatakan bahwa kesadaran keamanan siber memiliki kontribusi dominan dalam model penelitian ini. Temuan ini menunjukkan bahwa kewaspadaan pengguna terhadap ancaman digital sangat menentukan perilaku pencegahan *fraud*. Kesadaran keamanan siber berperan penting karena banyak kasus *cyber fraud* terjadi akibat kelengahan pengguna. Pengguna dapat memiliki kemampuan menggunakan aplikasi, tetapi tetap berisiko apabila tidak berhati-hati terhadap pesan palsu, panggilan manipulatif, atau permintaan kode OTP (Afzal *et al.*, 2024). Kesadaran keamanan siber membuat pengguna lebih waspada terhadap tindakan yang tampak sederhana tetapi berisiko tinggi, seperti membuka tautan tidak dikenal, membagikan informasi rahasia, atau menggunakan jaringan internet publik untuk transaksi keuangan. Pengaruh positif kesadaran keamanan siber juga menunjukkan bahwa perilaku aman terbentuk dari kebiasaan dan pemahaman risiko. Pengguna yang sadar keamanan cenderung menggunakan kata sandi yang kuat, memperbarui aplikasi, mengaktifkan fitur keamanan, memeriksa notifikasi transaksi, dan segera melaporkan aktivitas mencurigakan (Arsyad *et al.*, 2024). Kesadaran tersebut dapat mempersempit peluang pelaku *fraud* dalam melakukan manipulasi. Dalam perspektif keuangan Islam, kesadaran keamanan siber dapat dikaitkan dengan prinsip kehati-hatian dan perlindungan harta. *Mobile banking* syariah digunakan untuk mengelola dana yang harus dijaga secara aman. Oleh karena itu, pengguna memiliki tanggung jawab moral untuk tidak lalai dalam menjaga akses transaksi. Kesadaran keamanan siber menjadi bagian dari perilaku bertanggung jawab dalam menggunakan layanan keuangan syariah digital.

Pengaruh Literasi Digital dan Kesadaran Keamanan Siber terhadap Pencegahan *Cyber Fraud* pada Pengguna Mobile Banking Syariah

Hasil penelitian menunjukkan bahwa literasi digital dan kesadaran keamanan siber secara bersama-sama berpengaruh terhadap pencegahan *cyber fraud*. Nilai R-square sebesar 0,676 menunjukkan bahwa kedua variabel mampu menjelaskan pencegahan *cyber fraud* sebesar 67,60 persen. Hasil ini memperlihatkan bahwa pencegahan *cyber fraud* membutuhkan kombinasi antara kemampuan digital dan kewaspadaan keamanan. Literasi digital memberikan kemampuan pengguna untuk memahami teknologi dan informasi digital. Kesadaran keamanan siber memberikan sikap waspada terhadap potensi ancaman. Apabila kedua faktor tersebut berjalan bersama, pengguna akan lebih bisa menggunakan *mobile banking* syariah secara aman (Mufidah & Nasrulloh, 2025). Pengguna tidak hanya mengetahui cara menggunakan aplikasi, tetapi juga memahami risiko yang melekat pada setiap aktivitas digital. Kombinasi kedua variabel juga penting karena *cyber fraud* berkembang melalui modus yang memadukan aspek teknologi dan psikologi. Pelaku *fraud* sering menggunakan tampilan digital yang meyakinkan sekaligus teknik persuasi yang menekan pengguna agar bertindak cepat. Dalam kondisi tersebut, literasi digital membantu pengguna mengenali tanda teknis penipuan, sedangkan kesadaran keamanan siber membantu pengguna menahan diri dan tidak mudah mengikuti instruksi mencurigakan (Azizah *et al.*, 2024). Hasil ini memberikan implikasi bahwa bank syariah perlu memperkuat edukasi digital kepada nasabah. Edukasi tidak cukup hanya menjelaskan cara menggunakan aplikasi, tetapi juga harus menjelaskan cara mengenali *fraud*, cara menjaga OTP, cara memverifikasi informasi, dan prosedur pelaporan ketika terjadi aktivitas mencurigakan. Selain itu, kampanye keamanan perlu dilakukan secara berkala karena modus *cyber fraud* terus berkembang.

Pembahasan

Temuan penelitian ini memperkuat pemahaman bahwa pencegahan *cyber fraud* pada *mobile banking* syariah sangat dipengaruhi oleh faktor pengguna. Sistem keamanan perbankan memang penting, tetapi pengguna tetap menjadi salah satu titik paling rentan dalam ekosistem digital. Pelaku *cyber fraud* sering memanfaatkan kelengahan pengguna melalui teknik *social engineering* (Efendi *et al.*, 2025). Oleh karena itu, peningkatan literasi digital dan kesadaran keamanan siber menjadi strategi penting untuk memperkuat perlindungan transaksi. Literasi digital terbukti berpengaruh terhadap

pencegahan *cyber fraud* karena kemampuan digital membuat pengguna lebih kritis dalam menghadapi informasi (Putri *et al.*, 2025). Pengguna yang memahami risiko digital tidak mudah mengikuti instruksi dari sumber tidak resmi. Pengguna juga cenderung memeriksa ulang informasi sebelum melakukan transaksi. Dalam layanan *mobile banking* syariah, perilaku ini sangat penting karena transaksi dilakukan secara cepat dan sering kali tanpa interaksi langsung dengan pegawai bank. Kesadaran keamanan siber juga terbukti berpengaruh signifikan (Varshney *et al.*, 2024). Temuan ini menunjukkan bahwa kewaspadaan terhadap ancaman menjadi kunci pencegahan. Pengguna yang sadar keamanan akan memperlakukan data pribadi sebagai aset penting. Pengguna tidak akan membagikan kode OTP, PIN, atau kata sandi kepada pihak lain. Pengguna juga memahami bahwa ancaman digital dapat muncul melalui pesan, telepon, media sosial, email, atau aplikasi palsu. Dengan demikian, kesadaran keamanan siber membentuk perilaku perlindungan yang lebih konsisten. Secara simultan, literasi digital dan kesadaran keamanan siber menunjukkan kontribusi yang kuat terhadap pencegahan *cyber fraud*. Nilai R-square sebesar 67,60 persen menunjukkan bahwa model penelitian memiliki kemampuan penjelasan yang baik.

Hal ini mengindikasikan bahwa upaya pencegahan *cyber fraud* perlu diarahkan pada penguatan kapasitas pengguna. Bank syariah dapat membangun sistem keamanan yang kuat, tetapi keberhasilan pencegahan tetap membutuhkan nasabah yang mampu memahami dan menjalankan prosedur keamanan (Faizal *et al.*, 2023). Hasil penelitian ini memiliki implikasi praktis bagi perbankan syariah. *Pertama*, bank syariah perlu menyediakan edukasi literasi digital yang mudah dipahami oleh berbagai kelompok nasabah. Edukasi dapat diberikan melalui aplikasi, media sosial resmi, pesan notifikasi, video singkat, seminar daring, dan layanan pelanggan. *Kedua*, bank syariah perlu memperkuat kampanye kesadaran keamanan siber secara berkala. Kampanye tersebut perlu menekankan bahwa bank tidak pernah meminta PIN, kata sandi, atau kode OTP melalui media apa pun. *Ketiga*, bank syariah perlu meningkatkan desain keamanan aplikasi agar lebih ramah pengguna. Fitur keamanan sebaiknya mudah dipahami, tidak membingungkan, dan dilengkapi peringatan saat pengguna melakukan transaksi berisiko. *Keempat*, bank syariah perlu menyediakan mekanisme pelaporan *fraud* yang cepat dan mudah diakses. Jika pengguna menemukan transaksi mencurigakan, pengguna harus dapat segera menghubungi kanal resmi bank. Dari sisi akademik, penelitian ini memberikan kontribusi pada kajian *cyber fraud* dalam konteks keuangan Islam. Penelitian ini menunjukkan bahwa pencegahan *cyber fraud* dapat dianalisis melalui variabel perilaku pengguna, yaitu literasi digital dan kesadaran keamanan siber. Penelitian ini juga memperluas pembahasan keuangan syariah digital dengan menempatkan pencegahan *fraud* sebagai bagian dari perlindungan konsumen dan nilai amanah dalam transaksi.

KESIMPULAN

Penelitian ini bertujuan menguji pengaruh literasi digital dan kesadaran keamanan siber terhadap pencegahan *cyber fraud* pada pengguna *mobile banking* syariah. Temuan ini menunjukkan bahwa semakin baik kemampuan pengguna dalam memahami, mengevaluasi, dan menggunakan teknologi digital secara aman, semakin kuat perilaku pencegahan *cyber fraud* pada *mobile banking* syariah. Literasi digital membantu pengguna mengenali informasi mencurigakan, memverifikasi sumber informasi, menjaga data pribadi, dan menggunakan aplikasi resmi. Kesadaran keamanan siber juga terbukti berpengaruh positif dan signifikan terhadap pencegahan *cyber fraud*. Temuan ini menunjukkan bahwa kewaspadaan pengguna terhadap *phishing*, *social engineering*, pencurian data, dan penyalahgunaan OTP menjadi faktor penting dalam mencegah *fraud* digital. Pengguna yang memiliki kesadaran keamanan siber lebih cenderung menjaga kerahasiaan data, berhati-hati terhadap pesan mencurigakan, dan melaporkan aktivitas tidak wajar kepada pihak bank. Secara simultan, literasi digital dan kesadaran keamanan siber berpengaruh terhadap pencegahan *cyber fraud*. Hasil ini menegaskan bahwa pencegahan *cyber fraud* pada *mobile banking* syariah membutuhkan kombinasi antara kemampuan digital dan kewaspadaan keamanan. Oleh karena itu, bank syariah perlu memperkuat edukasi literasi digital, kampanye keamanan siber, desain aplikasi yang aman, serta mekanisme pelaporan *fraud* yang mudah diakses. Dengan penguatan tersebut, layanan *mobile banking* syariah

dapat menjadi lebih aman, terpercaya, dan sesuai dengan prinsip perlindungan harta dalam keuangan Islam.

DAFTAR PUSTAKA

- Afzal, M., Ansari, M. S., Ahmad, N., Shahid, M., & Shoeb, M. (2024). Cyberfraud, usage intention, and cybersecurity awareness among *e-banking* users in India: An integrated model approach. *Journal of Financial Services Marketing*, 29(4), 1503–1523. <https://doi.org/10.1057/s41264-024-00279-3>
- Aisyah, M., Sesunan, Y. S., & Wicaksono, A. T. S. (2025). Customers' trust in Islamic banking post-cyberattack leads to digital service breakdowns in Indonesia. *Sustainable Futures*, 10, 101530. <https://doi.org/10.1016/j.sftr.2025.101530>
- Arsyad, A. A. J., Tamrin, U., Lande, J. P., & Umar, N. (2024). Meningkatkan kesadaran remaja terhadap phishing melalui literasi digital: Studi kasus di SMK Darussalam Makassar. *Jurnal Pengabdian Literasi Digital Indonesia*, 3(2), 60–71. <https://doi.org/10.57119/abdimas.v3i2.122>
- Azizah, S., Ula, Z. N., Mutiara, D., & Prameswari, M. P. (2024). Keamanan siber sebagai fondasi pengembangan aplikasi keuangan mobile: Studi literatur mengenai cybercrime dan mitigasinya. *Akuntansi dan Teknologi Informasi*, 17(2), 221–237. <https://doi.org/10.24123/jati.v17i2.6409>
- Cele, N. N., & Kwenda, S. (2025). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime*, 32(1), 31–48.
- Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage Publications.
- Creswell, J. W., Hanson, W. E., Clark Plano, V. L., & Morales, A. (2007). Qualitative research designs: Selection and implementation. *The Counseling Psychologist*, 35(2), 236–264.
- Diana, M. I., & Wikartika, I. (2025). Literasi keuangan digital sebagai upaya pencegahan penipuan perbankan dan mitigasi kebocoran data pribadi. *Al-Khidmah Jurnal Pengabdian Masyarakat*, 5(1), 27–34. <https://doi.org/10.56013/jak.v5i1.3673>
- Efendi, N. A., Harahap, M. I., & Syahbudi, M. (2025). Pengaruh social engineering dan cyber crime terhadap persepsi keamanan pada aplikasi BSI Mobile. *Jurnal Manajemen Terapan dan Keuangan*, 14(03), 1237–1250. <https://doi.org/10.22437/jmk.v14i03.48161>
- Faizal, M. A., Faizatul, Z., Asiyah, B. N., & Subagyo, R. (2023). Analisis risiko teknologi informasi pada bank syariah: Identifikasi ancaman dan tantangan terkini. *Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam*, 5(2), 87–100.
- Harliani, S., & Kurniawan, F. (2025). Pengaruh kemampuan literasi digital terhadap pencegahan penipuan online pada remaja Desa Saentis. *Edukasiana: Jurnal Inovasi Pendidikan*, 4(4), 2234–2248.
- Isaia, E., Oggero, N., & Sandretto, D. (2024). Is financial literacy a protection tool from online fraud in the digital era? *Journal of Behavioral and Experimental Finance*, 44, 100977. <https://doi.org/10.1016/j.jbef.2024.100977>
- Johri, A., & Kumar, S. (2023). Exploring customer awareness towards their cyber security in the Kingdom of Saudi Arabia: A study in the era of banking digital transformation. *Human Behavior and Emerging Technologies*, 2023(1), 2103442. <https://doi.org/10.1155/2023/2103442>
- 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*, 10(2), 217–232. <https://doi.org/10.20885/JEKI.vol10.iss2.art6>
- Mufidah, D., & Nasrulloh, N. (2025). Gen Z response to Islamic *mobile banking* adoption: A technology acceptance model with cybersecurity perspective. *Jurnal Ilmu Ekonomi Terapan*, 10(2), 356. <https://doi.org/10.20473/jiet.v10i2.73564>
- Nguyen, T. T., Tran, T. N. H., Do, T. H. M., Dinh, T. K. L., Nguyen, T. U. N., & Dang, T. M. K. (2024). Digital literacy, online security behaviors and E-payment intention. *Journal of Open Innovation: Technology, Market, and Complexity*, 10(2), 100292. <https://doi.org/10.1016/j.joitmc.2024.100292>

- Pahrudin, P. (2025). Analisis penipuan digital (*cyber fraud*) tantangan dan solusi dalam era transformasi digital: Analysis of digital fraud (*cyber fraud*) challenges and solutions in the era of digital transformation. *Jurnal Riset Inossa: Media Hasil Riset Pemerintahan, Ekonomi dan Sumber Daya Alam*, 7(1), 70–80.
- Puri, L., Kumar, A., & Singh, R. (2025). What drives or discourages fraud-safe behavior in digital transactions? A BRT perspective. *Acta Psychologica*, 260, 105675. <https://doi.org/10.1016/j.actpsy.2025.105675>
- Putri, P. K., Dei Susilo, I. B. F., & Pramurindra, R. (2025). Cyber crime awareness pada digitalisasi akuntansi UMKM Kota Tasikmalaya. *Review of Applied Accounting Research (RAAR)*, 5(2), 53–65.
- Raza, S. A., Shah, N., & Ali, M. (2019). Acceptance of *mobile banking* in Islamic banks: Evidence from modified UTAUT model. *Journal of Islamic Marketing*, 10(1), 357–376. <https://doi.org/10.1108/JIMA-04-2017-0038>
- Restianty, A. (2018). Literasi digital, sebuah tantangan baru dalam literasi media. *Gunahumas*, 1(1), 72–87. <https://doi.org/10.17509/ghm.v1i1.28380>
- Syahrani, S., Hikmah, N., & Marzuki, S. N. (2024). Kasus penipuan di perbankan syariah: Analisis fraud internal dan implikasinya terhadap kepercayaan nasabah. *Lan Tabur: Jurnal Ekonomi Syariah*, 6(1), 122–140. <https://doi.org/10.53515/lantabur.2024.6.1.122-140>
- Tan, T., Sama, H., Wibowo, T., Wijaya, G., & Aboagye, O. E. (2024). Kesadaran keamanan siber pada kalangan mahasiswa universitas di Kota Batam. *Jurnal Teknologi dan Informasi*, 14(2), 163–173. <https://doi.org/10.34010/jati.v14i2.12518>
- Utomo, F. W., Insana, D. R. M., & Mayndarto, E. C. (2024). Mekanisme penipuan digital pada masyarakat era 5.0: Studi kasus penipuan online berbasis lowongan kerja paruh waktu yang merebak di masyarakat. *Jurnal Ilmiah WUNY*, 6(1), 32–41.
- Varshney, G., Kumawat, R., Varadharajan, V., Tupakula, U., & Gupta, C. (2024). Anti-phishing: A comprehensive perspective. *Expert Systems with Applications*, 238, 122199. <https://doi.org/10.1016/j.eswa.2023.122199>
- Zahra, L., Mananna, M. A., Harto, K., & Pratama, I. P. (2026). Literasi digital dan informasi. *Pendas: Jurnal Ilmiah Pendidikan Dasar*, 11(02), 211–227. <https://doi.org/10.23969/jp.v11i02.46052>