**Comit: Communication, Information and Technology Journal**
**Volume 3 Nomor 2 (2025) 313 – 323 E-ISSN 2986-5395**
**DOI: 10.47467/comit.v3i2.8965**

# Analisis Persepsi Mahasiswa Terhadap Ancaman *Phishing* Sebagai Tindak Pidana Perbankan: Studi Kasus pada Mahasiswa Perbankan Syariah UNISNU Jepara

**Nevy dia sanadyanta[1], Sheftiyani fazrina[2], Rizka laili amelia[3], Sri wulandari[4], Faridlotun Ni'mah[5], Wahidullah[6]**
Universitas Nahdatul Ulama Jepara[123456]
nevydiasanadyanta@gmail.com sheftiyanifz@gmail.com
Rizkaamel2270@gmail.com wulandarii02112@gmail.com
nimahfaridatun486@gmail.com

***ABSTRACT***

*This study analyzes the perception of students of the Islamic Banking Study Program of Nahdlatul Ulama Jepara Islamic University towards the threat of phishing as a banking crime. In the digital era, students have the potential to become agents of change in creating a safe Islamic banking ecosystem, but low digital literacy and education about data security make them vulnerable to online fraud. This study aims to explore students' understanding of the mechanism of phishing attacks, their level of awareness of cyber risks, and the factors that influence their perceptions and responses. The method used is qualitative with literature studies and interviews to obtain in-depth data. The results of the study show that the level of student understanding varies, some already understand this threat well, while others are still less familiar. Education from the campus is needed to increase students' awareness and understanding of the dangers of phishing, so that it can strengthen digital literacy and personal data protection among them.*

***Keywords:*** *Perception, Phishing, Banking Crime, Education*

**ABSTRAK**

Penelitian ini menganalisis persepsi mahasiswa Program Studi Perbankan Syariah Universitas Islam Nahdlatul Ulama Jepara terhadap ancaman *phishing* sebagai tindak pidana perbankan. Pada era digital, mahasiswa berpotensi menjadi agen perubahan dalam menciptakan ekosistem perbankan syariah yang aman, namun rendahnya literasi digital dan kurangnya edukasi mengenai keamanan data membuat mereka rentan terhadap penipuan *online*. Penelitian ini bertujuan mengeksplorasi pemahaman mahasiswa tentang mekanisme serangan *phishing*, tingkat kewaspadaan mereka terhadap risiko siber, serta faktor-faktor yang memengaruhi persepsi dan respons mereka. Metode yang digunakan kualitatif dengan studi literatur dan wawancara untuk mendapatkan data yang mendalam. Hasil penelitian menunjukkan tingkat pemahaman mahasiswa bervariasi, beberapa sudah memahami ancaman ini dengan baik, sementara lainnya masih kurang familiar. Edukasi dari kampus sangat diperlukan untuk meningkatkan kesadaran dan pemahaman mahasiswa tentang bahaya *phishing*, sehingga dapat memperkuat literasi digital dan perlindungan data pribadi di kalangan mereka.

**Kata Kunci:** Persepsi, *Phising,* Tindak Pidana Perbankan, Edukasi

**Comit: Communication, Information and Technology Journal**
**Volume 3 Nomor 2 (2025) 313 – 323 E-ISSN 2986-5395**
**DOI: 10.47467/comit.v3i2.8965**

## PENDAHULUAN

Mahasiswa program studi Perbankan Syariah pada Universitas Islam Nahdlatul Ulama Jepara, merupakan kelompok strategis yang relevan untuk diteliti persepsinya terhadap ancaman *phishing* sebagai tindak pidana perbankan. Nusaibah, (2023) menyatakan bahwa sebagai generasi muda yang tumbuh dalam era digital dan aktif menggunakan layanan keuangan berbasis teknologi, mereka memiliki potensi besar untuk menjadi agen perubahan dalam menciptakan ekosistem perbankan syariah yang aman dan berintegritas. Selain itu, mereka juga calon praktisi di industri keuangan syariah yang akan menghadapi secara langsung tantangan dunia digital termasuk ancaman kejahatan siber.

Namun menurut Budiarti et al., (2023) rendahnya literasi digital, kurangnya edukasi terkait keamanan data, serta minimnya pengalaman menghadapi situasi berisiko digital menjadikan mahasiswa maupun masyarakat umum rentan terhadap upaya penipuan daring. Tingginya ketergantungan terhadap teknologi digital dalam kegiatan sehari-hari seperti melakukan transaksi keuangan menggunakan berbagai aplikasi finansial turut memperburuk situasi. Aktivitas tersebut kerap dilakukan tanpa memperhatikan aspek keamanan data pribadi yang menyebabkan kejahatan digital mudah dilakukan (Agustin, 2024).

Kejadian nyata yang menimpa Bank Syariah Indonesia (BSI) menjadi salah satu bukti bagaimana *phishing* dapat menyerang institusi keuangan besar dan bereputasi, sekaligus membuktikan bahwa sistem keamanan digital masih memiliki celah yang perlu diperkuat (Tirta & Lie 2024). Dari insiden di atas tentunya akan menyadarkan mahasiswa bahwa siapa saja dapat menjadi korban *phishing* termasuk mereka yang memiliki akses layanan keuangan yang dianggap terkesan aman. Oleh karena itu, penting bagi setiap pihak yang terlibat dalam industri perbankan untuk memahami dengan baik bagaimana cara serangan *phishing* bekerja dan bagaimana upaya mencegahnya agar sistem perbankan yang sudah dibangun tidak lengah terhadap kejahatan siber (Njatrijani, 2022).

Penggunaan teknologi digital pada sistem keuangan yang semakin masif tentunya akan memicu peningkatan ancaman kejahatan siber. Menurut Wibowo & Fatimah, (2017) kejahatan siber yang paling meresahkan saat ini adalah *phishing*. Penipuan berbasis internet yang dikenal sebagai *phishing* melibatkan penggunaan situs web palsu atau sistem email untuk mendapatkan informasi pribadi atau data sensitif dari korban seperti nomor rekening, Pin, atau kata sandi. Fenomena ini dapat menjadi ancaman serius karena akan menimbulkan kerugian secara langsung kepada nasabah sekaligus merusak citra terhadap lembaga keuangan, termasuk bank syariah yang mengusung prinsip kejujuran dan Amanah (Anjheli, 2024).

Perkembangan teknologi digital yang begitu cepat dalam dunia perbankan telah membawa perubahan signifikan terhadap layanan keuangan menjadi lebih praktis, efisien, dan mudah diakses (Mutiasari, 2020). Namun di balik semua kemudahan ini, terdapat juga sisi gelap yang membuka peluang bagi pelaku kejahatan siber untuk mengeksploitasi sistem digital dengan berbagai macam cara yang merugikan melalui praktik *phishing*. Modus *phishing* yang semakin canggih memanfaatkan kelemahan keamanan serta kelalaian pengguna untuk mendapatkan

data pribadi secara ilegal, terutama melalui situs web palsu dan surat elektronik penipuan yang seolah-olah berasal dari lembaga resmi (Wahyu Hidayat M et al., 2023).

Penelitian yang dilakukan Ginting et al., (2023) telah memberikan gambaran mengenai ragam ancaman *phishing* yang mengincar layanan perbankan digital. Namun, kajian tersebut masih memiliki keterbatasan karena bersifat konseptual-deskriptif dan hanya mengandalkan data sekunder dari literatur, tanpa menyertakan temuan empiris berdasarkan pengalaman nyata pengguna. Hal ini menyebabkan aspek praktis terkait interaksi langsung nasabah dengan sistem perbankan belum tergali secara mendalam. Padahal, rendahnya tingkat pemahaman pengguna terhadap keamanan digital menjadi salah satu faktor dominan yang memperbesar peluang terjadinya serangan *phishing*.

Melihat urgensi yang telah dipaparkan, penelitian ini menjadi hal yang krusial untuk memperoleh pemahaman secara langsung kepada mahasiswa Program Studi Perbankan Syariah terhadap ancaman *phishing* yang terus berkembang. Penelitian ini bertujuan untuk mengeksplorasi sejauh mana mahasiswa memahami mekanisme serangan *phishing*, tingkat kewaspadaan mereka terhadap risiko siber, serta faktor-faktor yang memengaruhi persepsi dan respons mereka terhadap potensi ancaman tersebut. Temuan dari penelitian ini diharapkan mampu memberikan kontribusi dalam bentuk rekomendasi edukatif dan strategi pencegahan yang dapat diterapkan di lingkungan perguruan tinggi maupun masyarakat luas, sebagai upaya meningkatkan literasi digital dan kesadaran pentingnya perlindungan data pribadi dalam menghadapi tantangan era digital.

## TINJAUAN LITERATUR

1. Persepsi

   Persepsi adalah proses di mana seseorang mengorganisasikan, menginterpretasikan, dan memberi makna terhadap rangsang atau stimulus yang diterima dari lingkungan melalui panca indra. Persepsi melibatkan cara pandang atau tanggapan individu terhadap sesuatu, yang dapat berbeda antara satu orang dengan yang lain meskipun objek yang dipersepsi sama. Dengan kata lain, persepsi adalah kesan atau gambaran yang diperoleh seseorang setelah mengolah informasi sensorik sehingga individu tersebut dapat memahami dan menilai lingkungan sekitarnya (Lawotjo, 2013). Persepsi didefinisikan sebagai proses individu dalam mengorganisasikan dan menginterpretasikan kesan-kesan sensorik untuk memberi makna pada lingkungannya. Persepsi dipengaruhi oleh karakteristik pribadi, faktor situasional, dan atribut target (Simbolon, 2007).

2. Ancaman *Phising*

   *Phishing* merupakan salah satu bentuk penipuan daring yang dilakukan oleh penyerang dengan mengelabui korbannya agar mengungkapkan informasi sensitif seperti nama pengguna dan kata sandi (Irawan, 2020; Wiranata et al., 2024). *Phishing* merupakan ancaman yang

signifikan terhadap layanan perbankan daring, dengan memanfaatkan kurangnya pengetahuan dan kerentanan psikologis pengguna. Kejahatan dunia maya ini menargetkan berbagai industri, dengan perbankan menjadi yang paling terpengaruh, Untuk memerangi *phishing*, bank harus menerapkan langkah-langkah keamanan yang kuat dan mendidik nasabah tentang potensi risiko (Muftiadi et al., 2022; Wibowo Noor Fikri et al., 2023).

*Phishing* sering kali dilakukan dengan membuat situs web atau email palsu yang menyerupai entitas yang sah, khususnya lembaga keuangan (Ananta Kumala Sari & Hwihanus Hwihanus, 2022; Pratama Erdiyanto, 2023). Pelaku *phishing*, yang dianggap sebagai peretas topi hitam, memanfaatkan kerentanan keamanan untuk menyusup ke dalam sistem dan menimbulkan kerugian. Pesatnya perkembangan teknologi dan penggunaan internet turut memicu maraknya kejahatan dunia maya, termasuk *phishing* Serangan *phishing* dapat mengakibatkan pengambilalihan akun, kerugian finansial, dan pencurian identitas. Untuk menanggulangi ancaman ini, kesadaran dan edukasi masyarakat sangatlah penting, terutama di daerah pedesaan yang pengetahuan tentang kejahatan siber tersebut mungkin masih terbatas (Ananta Kumala Sari & Hwihanus Hwihanus, 2022; Wiranata et al., 2024)

3. Serangan *Cyber*

Serangan siber telah menjadi perhatian penting di era digital, khususnya bagi lembaga keuangan dan infrastruktur penting. Bank-bank di Indonesia mempertahankan tingkat keamanan tertentu, meskipun beberapa pengguna tetap berhati-hati tentang perbankan daring karena kerentanan akses internet publik (Dermawan et al., 2023). Serangan *cyber* adalah upaya ilegal atau tidak sah untuk mengakses, mencuri, mengubah, merusak, atau mengganggu sistem komputer, jaringan, atau data digital. Tujuannya bisa berupa pencurian informasi, pengendalian sistem, penghancuran data, atau mengganggu operasional suatu sistem baik untuk keuntungan finansial, politik, atau tujuan kriminal lainnya.

4. Tindak Pidana

Tindak pidana perbankan adalah perilaku atau tindakan yang melanggar hukum yang terkait langsung dengan kegiatan perbankan dan diatur secara khusus dalam Undang-Undang Perbankan. Dalam pengertian sempit, tindak pidana perbankan mencakup perbuatan yang dilakukan atau tidak dilakukan yang telah ditetapkan sebagai kejahatan berdasarkan Undang-Undang Perbankan, seperti yang tercantum dalam Pasal 46 sampai Pasal 50A Undang-Undang Perbankan (Lestari, 2019). Secara lebih luas, tindak pidana di bidang perbankan mencakup segala jenis perbuatan melanggar hukum yang berhubungan dengan kegiatan menjalankan usaha bank, baik bank sebagai sasaran maupun sebagai sarana, termasuk tindak pidana lain seperti penipuan, penggelapan, pemalsuan, dan tindak pidana lain sepanjang berkaitan dengan lembaga perbankan yang mungkin tidak hanya diatur dalam

Undang-Undang Perbankan saja, tetapi juga dalam peraturan hukum pidana umum atau khusus lainnya (Faridah, 2018)

## METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur (*literature review*) dan wawancara sebagai teknik pengumpulan data. Studi literatur dilakukan dengan menelaah berbagai jurnal, artikel ilmiah, serta dokumen relevan yang berkaitan dengan topik penelitian untuk memperoleh pemahaman teoritis dan hasil-hasil penelitian sebelumnya. Selain itu, peneliti juga melakukan wawancara secara langsung kepada narasumber yang dianggap memiliki pengetahuan dan pengalaman terkait permasalahan yang diteliti. Tujuan dari wawancara ini adalah untuk memperoleh data yang lebih mendalam, aktual, dan kontekstual guna melengkapi hasil dari kajian literatur. Pendekatan ini dipilih agar penelitian dapat menggambarkan fenomena yang diteliti secara komprehensif, mendalam, dan sesuai dengan konteks di lapangan

## HASIL DAN PEMBAHASAN

*Phising* merupakan jenis penipuan di mana pelaku berusaha memperoleh data pribadi korban, seperti kata sandi, nomor rekening atau informasi penting lainnya, dengan cara menipu korban agar secara sukarela menyerahkan data tersebut. Pelaku biasanya menggunakan Teknik yang sangat meyakinkan sehingga korban tidak menyadari bahwa mereka sedang menjadi korban penipuan (Reyhan & Gultom, 2025).

Para pelaku *phising* mengasah kemampuan teknis mereka melalui interaksi dengan kelompok kriminal, yang menandakan Tindakan ini bukan dilakukan secara spontan oleh individu, melainkan hasil dari proses pembelajaran yang terstruktur. Faktor teknis seperti koneksi jaringan dan ketimpangan penyebaran teknologi mempermudah aktivitas pelaku. Selain itu, faktor ekonomi juga menjadi pendorong, memberikan motivasi baik dalam bentuk kepuasan intelektual maupun keuntungan materi. Dampak yang dialami korban sangat beragam (Bantara et al., 2025).

Keamanan siber memiliki peranan krusial dalam menjaga data pelanggan agar tetap terlindungi dari berbagai ancaman digital. Hal ini sangat penting terutama di sektor perbankan, yang sangat mengandalkan kepercayaan nasabah serta keandalan sistem informasi yang digunakan. Bank mengelola banyak data sensitif, seperti informasi pribadi pelanggan, catatan transaksi, dan data keuangan, yang sering menjadi sasaran utama bagi pelaku kejahatan siber. Untuk meminimalkan risiko tersebut, bank dapat menerapkan kebijakan manajemen data yang ketat dan menyelenggarakan pelatihan keamanan informasi secara rutin untuk karyawan mereka. Salah satu langkah penting yang dapat diterapkan adalah penggunaan mekanisme autentikasi dua faktor (2FA) untuk akses internal guna menghindari kehilangan data (Novarianti et al., 2025).

Selain menerapkan strategi-strategi ini, tindakan pencegahan juga sangat penting untuk menjaga keamanan dunia maya. Ini adalah tindakan proaktif yang

bertujuan untuk melindungi sistem dan data pelanggan dari ancaman. Hal ini mencakup, misalnya, memastikan bahwa data sensitif disimpan dengan aman dan akses yang tidak sah dicegah. Keamanan dipastikan melalui berbagai kontrol seperti penggunaan *firewall*, enkripsi data, dan pembatasan akses yang ketat. Selain itu, teknologi keamanan juga digunakan untuk pemantauan secara *real-time* sehingga ancaman siber dapat dikenali dan diblokir dengan segera. Tata kelola keamanan yang efektif juga penting. Selain itu, audit keamanan secara berkala, termasuk tes penetrasi, dilakukan untuk mengidentifikasi dan menghilangkan kerentanan dalam sistem keamanan siber (Ashidiq et al., 2025).

Di lingkungan mahasiswa perbankan syariah di UNISNU, penting bagi mereka untuk memahami betul ancaman *phishing*. Hal ini dikarenakan mereka adalah calon-calon profesional masa depan yang nantinya akan berperan aktif di dunia perbankan. Kesadaran dan pemahaman mahasiswa akan bahaya *phishing* sangat berpengaruh terhadap bagaimana mereka melindungi diri mereka sendiri dan bagaimana mereka menyebarluaskan informasi tersebut kepada masyarakat umum. Akibatnya, risiko serangan *phishing* yang berhasil meningkat, yang dapat menyebabkan kerugian finansial dan melemahkan kepercayaan masyarakat terhadap sistem perbankan berbasis digital.

Guna mendapatkan perspektif yang lebih luas terkait tingkat pemahaman mahasiswa terhadap mekanisme serangan *phishing* dan kesadaran mereka terhadap ancaman siber, peneliti melakukan serangkaian wawancara terhadap sejumlah mahasiswa yang secara rutin memanfaatkan layanan keuangan berbasis teknologi. Melalui pendekatan studi empiris ini, diharapkan informasi yang diperoleh dapat memberikan data yang valid mengenai sejauh mana pemahaman mahasiswa terhadap serangan *phishing*. Penelitian ini bertujuan memberikan saran edukasi dan langkah-langkah pencegahan yang bisa diterapkan di lingkungan akademik maupun masyarakat luas. Fokusnya adalah meningkatkan pemahaman digital serta kesadaran akan pentingnya melindungi data pribadi agar dapat menghadapi berbagai tantangan di era digital dengan lebih baik.

Berikut ini adalah rangkuman hasil wawancara dengan mahasiswa yang aktif menggunakan layanan keuangan berbasis teknologi.

**Tabel 1. Hasil Wawancara**

| Informan | Hasil Wawancara |
|---|---|
| A | "Saya memahami bahwa *phishing* adalah metode penipuan yang bertujuan untuk mencuri data-data penting, seperti *password* dan PIN. Biasanya, para pelaku menggunakan tautan palsu untuk mengelabui korban. Saya pernah hampir menjadi korban, tapi untungnya saya mengecek ulang alamat email dan situsnya sebelum bertindak." Ia juga menekankan bahwa edukasi dari pihak kampus sangat penting agar mahasiswa tidak mudah tertipu. Apalagi mahasiswa yang belajar di bidang perbankan harus memiliki pemahaman yang kuat mengenai hal ini karena berkaitan erat dengan keamanan nasabah. |

| | |
|---|---|
| B | "Saya tahu *phising* adalah salah satu bentuk penipuan, meskipun saya tidak mengerti secara detail. Saya pernah mendengar bahwa *phishing* terjadi melalui internet, tapi saya belum pernah mengalami langsung." Ia berharap pihak kampus dapat mengadakan pelatihan atau sosialisasi mengenai ancaman digital agar mahasiswa lebih sadar akan bahaya *phishing*. |
| C | "Saya belum familiar dengan istilah *phishing*. Biasanya jika saya menerima pesan yang mencurigakan, saya cenderung mengabaikannya. Namun, saya tidak menyadari bahwa pesan tersebut bisa berbahaya. Selama ini, saya beranggapan bahwa semua pesan dari bank itu aman selama menggunakan aplikasi resmi." Namun, ia menyadari bahwa pengetahuan mahasiswa tentang risiko kejahatan digital masih sangat terbatas. Oleh karena itu, ia menyarankan agar universitas memberikan edukasi yang lebih sederhana dan mudah dipahami mengenai hal ini. |

Berdasarkan hasil wawancara, ditemukan bahwa tingkat pemahaman mahasiswa sangat bervariasi. Dari informan A menunjukkan pemahaman yang cukup baik mengenai *phishing*. Ia mengetahui bahwa *phishing* merupakan metode penipuan yang bertujuan mencuri data penting, dan mampu mengenali taktik umum seperti tautan palsu. Sebaliknya, informan B dan C menunjukkan tingkat pemahaman yang lebih rendah. Informan B mengetahui *phishing* sebagai bentuk penipuan namun mengaku tidak mengerti mekanisme secara rinci. Sementara itu, informan C sama sekali belum familiar dengan istilah *phishing*, meskipun ia secara intuitif mengabaikan pesan mencurigakan. Ini menunjukkan bahwa belum semua mahasiswa memiliki pemahaman konseptual maupun teknis terkait ancaman *phishing*. Perbedaan tingkat pemahaman ini menunjukkan bahwa tidak semua mahasiswa, bahkan di era digital, memiliki pengetahuan kritis terhadap ancaman keamanan siber. Hal ini menjadi dasar penting untuk merancang intervensi pendidikan yang disesuaikan dengan latar belakang dan kebutuhan mahasiswa dari berbagai disiplin ilmu. Temuan ini mempertegas pentingnya peningkatan literasi digital yang tidak hanya bersifat definisional, tetapi juga aplikatif, terutama di kalangan mahasiswa non-teknis yang rentan terhadap manipulasi digital.

Dari ketiga informan tersebut menunjukkan respons yang beragam terhadap potensi risiko siber. Informan A memiliki tingkat kewaspadaan yang relatif tinggi. Berdasarkan dari pengalaman yang dia alami, ia memiliki kesadaran akan risiko sehingga memverifikasi sumber email. Ini menunjukkan pemahaman pentingnya kehati-hatian dalam dunia digital. Namun, informan B dan C masih menunjukkan kewaspadaan yang terbatas. Meski mereka berhati-hati dalam menggunakan internet, tetapi mereka belum memahami bahwa pesan mencurigakan bisa menjadi bagian dari serangan *phishing* yang terorganisir. Ini menunjukkan bahwa sebagian mahasiswa masih memiliki kesenjangan dalam pengetahuan mendasar mengenai ancaman digital yang umum. Ia bahkan beranggapan bahwa pesan dari bank akan selalu aman jika melalui aplikasi resmi, sebuah asumsi seperti ini yang berpotensi berbahaya mengingat banyak *phishing* yang memanfaatkan *brand* atau nama lembaga

terpercaya. Tingginya ketergantungan pada intuisi dan asumsi yang selalu percaya bahwa aplikasi resmi pasti aman akan dapat menjadi titik lemah dalam sistem pertahanan pribadi terhadap serangan siber.

Beberapa faktor yang memengaruhi persepsi dan respons mahasiswa terhadap *phising* yang diidentifikasi dari hasil wawancara sebagai berikut:

1. Tingkat pengetahuan dan pemahaman: Informan A menunjukkan pemahaman yang baik tentang *phishing* dan dampaknya, serta memiliki pengalaman hampir menjadi korban. Hal ini membuatnya lebih waspada dan proaktif dalam memeriksa keaslian tautan. Informan B memiliki pengetahuan dasar tentang *phishing*, tetapi tidak memahami detailnya. Ini menunjukkan bahwa meskipun ia menyadari adanya ancaman, kurangnya pemahaman mendalam dapat mengurangi kewaspadaan. Informan C tidak familiar dengan istilah *phishing* dan cenderung mengabaikan pesan mencurigakan. Ini menunjukkan bahwa kurangnya pengetahuan dapat membuat individu lebih rentan terhadap serangan *phishing*.
2. Pengalaman pribadi: Pengalaman informan A yang hampir menjadi korban *phishing* membuatnya lebih berhati-hati dan menyadari pentingnya memeriksa informasi sebelum bertindak. Sementara itu, Informan B dan C tidak memiliki pengalaman langsung, yang dapat memengaruhi tingkat kewaspadaan mereka.
3. Ketersediaan edukasi dari kampus: Semua informan secara eksplisit menyatakan pentingnya peran kampus dalam memberikan sosialisasi dan pelatihan. Informan C yang tidak familiar dengan *phishing* menyarankan edukasi yang lebih sederhana dan mudah dipahami.
4. Asumsi keamanan dari sumber resmi: Informan C menganggap bahwa pesan dari bank pasti aman jika disampaikan melalui aplikasi resmi. Ini menunjukkan yang berlebihan terhadap otoritas digital, yang bias menjadi celah eksploitasi jika tidak diimbangi dengan pemahaman kritis.
5. Latar belakang akademik: Mahasiswa dengan latar belakang akademi bidang keuangan seperti informan A merasa lebih bertanggung jawab dan relevan dengan isu keamanan digital karena menyangkut transaksi dan data sensitif. Ini mengindikasikan bahwa program studi turut memengaruhi kesadaran terhadap isu ini.

## KESIMPULAN

*Phishing* adalah metode pencurian data dengan cara mengelabui korban agar memberikan informasi pribadi secara sukarela. Para pelaku biasanya memiliki kemampuan teknis yang baik karena belajar dari kelompok terorganisir. Ancaman ini semakin mudah dilakukan karena dukungan teknologi dan motivasi keuntungan finansial. Sektor perbankan yang mengelola data sensitif menjadi sasaran utama, sehingga memerlukan sistem keamanan yang ketat seperti autentikasi dua faktor dan pelatihan karyawan.

Berdasarkan wawancara dengan mahasiswa perbankan syariah, ditemukan perbedaan tingkat pemahaman tentang *phishing*. Sebagian mahasiswa sudah paham

dan waspada, sementara lainnya masih kurang mengerti bahkan belum familiar dengan istilah *phishing*. Hal ini menunjukkan perlunya peningkatan edukasi di kampus, terutama karena mahasiswa ini akan menjadi tenaga profesional di bidang perbankan. Oleh karena itu, universitas perlu memberikan pemahaman yang lebih praktis tentang bahaya *phishing*, tidak hanya teori tetapi juga contoh kasus nyata. Edukasi ini penting untuk membangun kewaspadaan digital mahasiswa sebagai calon profesional di industri perbankan.

**DAFTAR PUSTAKA**

Agustin, S. (2024). Dampak Kemajuan Teknologi Informasi Era Digital Terhadap Keamanan Data Pribadi Tantangan Dan Penanggulangan Terhadap Kejahatan Cyber. 1(6), 500–504.

Ananta Kumala Sari, & Hwihanus Hwihanus. (2022). Peranan Sistem Informasi Akuntansi Dan Implementasi Menghadapi Pemalsuan Data Di Era Digital Pada Masyarakat Desa. Jurnal Manajemen Riset Inovasi, 1(1), 186–196. https://doi.org/10.55606/mri.v1i1.648

Anjheli, D. (2024). Privasi Digital dan Kejahatan Phishing di Indonesia : Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP Berdasarkan laporan Asosiasi Penyelenggara Jasa Internet Indonesia ( APJII ) tahun 2023 , lebih dari 215 juta penduduk telah terhubung. 4(1).

Ashidiq, A. R., Kurniawan, L. D., & Ronaldi. (2025). Kajian Kriminologi: Mitigasi Cyber Security Sebagai Penanggulangan Serangan Cyber Crime Dan Upaya Recovery (Studi Bank Sumsel Babel Syari'ah). Jurnal ISO: Jurnal Ilmu Sosial, Politik Dan Humaniora, 5(1), 1–9. https://doi.org/10.53697/iso.v5i1.2315

Bantara, F., Simatupang, M. T., Terangta, M., Nicholine, & Behuku, R. D. P. (2025). Analisis Kriminologi atas Kejahatan Dunia Maya Phising di Era Pandemi Covid-19. Birokrasi: JURNAL ILMU HUKUM DAN TATA NEGARA, 3(1), 10–20. https://doi.org/10.55606/birokrasi.v3i1.1801

Budiarti, R. P. N., Magfira, D. B., Meutia, N. S., & Rulyansah, A. (2023). Peningkatan Literasi Digital Mahasiswa UNUSA Untuk Pengamanan Data Pribadi. Journal of Dedicators Community, 7(1), 79–94. https://doi.org/10.34001/jdc.v7i1.3775

Dermawan, I., Baidawi, A., Iksan, & Mellyana Dewi, S. (2023). Serangan Cyber dan Kesiapan Keamanan Cyber Terhadap Bank Indonesia. Jurnal Informasi Dan Teknologi, 5(3), 20–25. https://doi.org/10.60083/jidt.v5i3.364

Faridah, H. (2018). Jenis-jenis Tindak Pidana Perbankan dan Perbandingan Undang-undang Perbankan. Jurnal Hukum Positum, 3(2), 106. https://doi.org/10.35706/positum.v3i2.2896

Ginting, E., Sinaga, M. P., Nurdin, M. R., & Putra, M. D. (2023). Analisis Ancaman Phising Terhadap Layanan Online Perbankan (Studi Kasus Pada Bank BRI). UNES Journal of Scientech Research, 8(1), 41–47.

Irawan, D. (2020). Mencuri Informasi Penting Dengan Mengambil Alih Akun Facebook Dengan Metode Phising. JIKI (Jurnal Llmu Komputer & Lnformatika), 1(1), 43–46. https://doi.org/10.24127/jiki.v1i1.671

Lawotjo, S. (2013). Kajian Persepsi Hukum Pada Masyarakat Tentang Rencana Umum Tata Ruang Kota. Kajian Persepsi Hukum, 2, 81–93.

Lestari, A. J. (2019). Kajian Yuridis Tindak Pidana Perbankan Terhadap Penghimpunan Dana MAsyarakat Berdasarkan Undang-Undang Nomor 10 Tahun 1998. Lex Crimen, VII(3), 41–51.

Muftiadi, A., Agustina, T. P. M., & Evi, M. (2022). Studi kasus keamanan jaringan komputer: analisis ancaman phising terhadap layanan online banking. Hexatech: Jurnal Ilmiah Teknik. https://api.semanticscholar.org/CorpusID:270346969

Mutiasari, A. I. (2020). Perkembangan Industri Perbankan Di Era Digital. Jurnal Ekonomi Bisnis Dan Kewirausahaan, 9(2), 32–41. https://doi.org/10.47942/iab.v9i2.541

Njatrijani, R. (2022). Upaya Menghadapi Kejahatan Terhadap Sistem Keamanan Perbankan Indonesia di Era Cyberspace. Law, Development & Justice Review, 3(2), 1–9.

Novarianti, W. D., Meliala, A. P. P. S., Yusuf, N. A. S., & Melati, B. N. C. (2025). Kerahasiaan Bank vs Hak Atas Informasi: Mengurai Konflik Kepentingan dalam Perlindungan Data Pribadi. Jurnal Multidisiplin Ilmu Akademik, 2(1), 103–114. https://doi.org/10.61722/jmia.v2i1.3180

Nusaibah, U. (2023). Digitalisasi Ekonomi Syariah di Kalangan Generasi Z Untuk Peningkatan Literasi Keuangan Syariah (Studi Kasus Mbanking BSI). Musyarakah: Journal of Sharia Economic (MJSE), 12(1), 12–22. https://doi.org/10.24269/mjse.v12i1.6695

Pratama Erdiyanto, R. (2023). Penipuan Mengatasnamakan Bank Berbentuk Phising. Jurnal Inovasi Global, 1(2), 71–79. https://doi.org/10.58344/jig.v1i2.11

Reyhan, E., & Gultom, P. (2025). PERLINDUNGAN HUKUM TERHADAP PENGGUNA SOSIAL MEDIA TERKAIT CYBER CRIME PHISING BERDASARKAN UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK. Lex Laguens: Jurnal Kajian Hukum Dan Keadilan, 3(1), 111–124. https://jurnal.dokterlaw.com/index.php/lexlaguens

Simbolon, M. (2007). Persepsi dan kepribadian. Jurnal Ekonomis, 1(1), 52–66

Tirta, G. A., & Lie, G. (2024). Tinjauan Hukum Terhadap Tindak Pidana Cybercrime dan Upaya Pencegahannya (Studi Kasus Peretasan Data Pengguna Bank BSI). MANTAP: Journal of Management Accounting, Tax and Production, 2(1), 240–249. https://doi.org/10.57235/mantap.v2i1.1634

Wahyu Hidayat M, Hartini Ramli, Ikhram, P. M. B., Sidrayanti, Ridhawi, A. R., Mukhtar, N. A., & Renaldy Junedy. (2023). Analisa Clustering Phising Untuk Meningkatkan Kesadaran Mahasiswa Terhadap Keamanan Data Pribadi Mahasiswa Universitas Negeri Makassar. Vokatek : Jurnal Pengabdian Masyarakat, 1(1), 28–33. https://doi.org/10.61255/vokatekjpm.v1i1.29

Wibowo Noor Fikri, A., Fauzi, A., Alfathur Rachman, A., Khaerunisa, A., Puspita Sari, D., Vernanda, P., Hikmah, R., & Putri Fadyanti, T. (2023). Analisis Keamanan Sistem Operasi dalam Menghadapi Ancaman Phishing dalam Layanan Online Banking. Jurnal Ilmu Multidisplin, 2(1), 84–91. https://doi.org/10.38035/jim.v2i1.228

Wibowo, M. H., & Fatimah, N. (2017). Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime. JoEICT (Journal of Education And ICT), 1(1), 1–5.

Wiranata, G. A., Ucuk, Y., Subekti, & Sidarta, D. D. (2024). PERTANGGUNGJAWABAN PIDANA TERHADAP PELAKU TINDAK PIDANA PHISHING. COURT REVIEW: Jurnal Penelitian Hukum (e-ISSN: 2776-1916). https://api.semanticscholar.org/CorpusID:271237318