ANALISIS YURIDIS TERHADAP KEJAHATAN PHISING DALAM SISTEM PERBANKAN DIGITAL MELALUI SCAM LINK BERBAHAYA

¹Clara Nervia¹, ²Kresentia Aiko Wardhana², ³Pricilia Angel Sie³, ⁴Talitha Livia Talim⁴,
⁵Waynehard Brayne Hizkia⁵,

¹Ilmu Hukum, UNiversitas Pelita Harapan, Jakarta

²Ilmu Hukum, UNiversitas Pelita Harapan, Jakarta

³Ilmu Hukum, UNiversitas Pelita Harapan, Jakarta

⁴Ilmu Hukum, UNiversitas Pelita Harapan, Jakarta

⁵Ilmu Hukum, UNiversitas Pelita Harapan, Jakarta

E-mail: ¹Clara Nervia (01051220078@student.uph.edu), ²Kresentia Aiko
Wardhana (01051220175@student.uph.edu), ³Pricilia Angel Sie
(01051220056@student.uph.edu), ⁴Talitha Livia Talim
(01051220042@student.uph.edu), ⁵Waynehard Brayne Hizkia
(01051220073@student.uph.edu)

ABSTRAK

sekaligus meningkatkan risiko kejahatan siber, salah satunya adalah phishing melalui scam link berbahaya. Modus kejahatan ini dilakukan dengan cara mengelabui nasabah melalui tautan palsu yang menyerupai situs resmi bank, sehingga nasabah tanpa sadar memasukkan data pribadi dan kredensial perbankan yang kemudian disalahgunakan oleh pelaku. Penelitian ini bertujuan untuk menganalisis secara yuridis tindak kejahatan phishing dalam sistem perbankan digital melalui scam link berbahaya serta implikasi hukumnya terhadap perlindungan nasabah. Metode penelitian yang digunakan adalah pendekatan normatif dengan menelaah berbagai peraturan perundang-undangan yang relevan, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Otoritas Jasa Keuangan (OJK), serta ketentuan dalam hukum pidana yang mengatur kejahatan siber. Hasil penelitian menunjukkan bahwa meskipun regulasi di Indonesia telah mengatur sanksi bagi pelaku phishing, masih terdapat tantangan dalam implementasi hukum, terutama dalam aspek pencegahan dan perlindungan nasabah. Oleh karena itu, diperlukan peningkatan kesadaran masyarakat, penguatan sistem keamanan perbankan digital, serta optimalisasi penegakan hukum guna meminimalisir dampak kejahatan phishing melalui scam link berbahaya.

Kata kunci: *Phishing*; Kejahatan Siber; Scam Link; Perlindungan Nasabah; Analisis Yuridis.

ABSTRACT

The rapid development of digital technology in the banking system brings numerous benefits while also increasing the risk of cybercrime, one of which is phishing through dangerous scam links. This crime is committed by deceiving bank customers through fraudulent links that mimic official banking websites, leading them to unknowingly enter personal data and banking credentials, which are then exploited by perpetrators. This study aims to conduct a juridical analysis of phishing crimes in digital banking systems through dangerous scam links and examine their legal implications for customer protection. The research employs a normative approach by analyzing relevant legal regulations, such as the Electronic Information and Transactions Law (UU ITE), regulations issued by the Financial Services Authority (OJK), and provisions in criminal law governing cybercrimes. The findings indicate that although Indonesian regulations impose sanctions on phishing perpetrators, challenges remain in legal enforcement, particularly in prevention efforts and customer protection. Therefore, enhancing public awareness, strengthening digital banking security systems, and optimizing law enforcement are crucial to minimizing the impact of phishing crimes through dangerous scam links.

Keywords: Phishing,;Cybercrime; Scam Links, Customer Protection, Juridical Analysis.

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam berbagai aspek kehidupan manusia, termasuk dalam dunia perbankan. Digitalisasi perbankan yang berkembang pesat memberikan berbagai keuntungan bagi masyarakat, seperti kemudahan dalam melakukan transaksi, aksesibilitas yang lebih luas, serta efisiensi dalam pengelolaan keuangan tanpa harus mengunjungi kantor cabang bank secara langsung (Danuri, 2019). Namun, di balik manfaat tersebut, transformasi digital juga membuka celah bagi berbagai ancaman kejahatan siber (cybercrime), salah satunya adalah kejahatan phishing yang sering dilakukan melalui scam link berbahaya. Kejahatan ini menjadi salah satu modus yang paling sering digunakan oleh pelaku kejahatan siber untuk

mencuri data pribadi dan informasi perbankan nasabah dengan cara yang sangat meyakinkan dan sulit dideteksi (Budyanto, 2025).

Phishing adalah bentuk penipuan daring yang bertujuan untuk memperoleh informasi sensitif korban, seperti nama pengguna (username), kata sandi (password), dan data finansial lainnya, dengan menyamarkan sebagai entitas tepercaya dalam komunikasi elektronik. Salah satu metode yang paling umum digunakan dalam phishing adalah pengiriman tautan (scam link) melalui email, pesan singkat, atau media sosial yang mengarahkan korban ke situs web palsu yang menyerupai situs asli bank atau lembaga keuangan lainnya (Tabrani dkk, 2024). Situs tersebut dirancang sedemikian rupa agar terlihat autentik sehingga nasabah yang kurang waspada akan tanpa sadar memasukkan informasi pribadi mereka. Data yang telah

diperoleh kemudian digunakan oleh pelaku untuk mengakses rekening bank korban dan melakukan transaksi ilegal, yang sering kali menyebabkan kerugian finansial yang sangat besar bagi nasabah. (Pearson, 2017)

Di Indonesia, fenomena kejahatan phishing dalam sistem perbankan digital semakin meningkat seiring dengan meningkatnya penggunaan layanan perbankan berbasis internet dan aplikasi mobile banking. Berdasarkan laporan dari Kementerian Komunikasi dan Informatika (Kominfo), jumlah kasus kejahatan siber di Indonesia meningkat secara signifikan dalam beberapa tahun terakhir, dengan phishing sebagai salah satu modus yang paling banyak digunakan oleh pelaku kejahatan. (Kominfo, 2023) Menurut data dari Otoritas Jasa Keuangan (OJK), sepanjang tahun 2023 terjadi peningkatan lebih dari 50% dalam jumlah kasus penipuan digital di sektor perbankan, dengan sebagian besar kasus melibatkan penggunaan scam link berbahaya. (OJK, 2024)

Meningkatnya kasus phishing ini tidak hanya menimbulkan dampak finansial bagi individu yang menjadi korban, tetapi juga dapat merusak kepercayaan masyarakat terhadap sistem perbankan digital secara keseluruhan. Keamanan dalam transaksi perbankan merupakan salah satu faktor utama yang mempengaruhi adopsi layanan perbankan digital oleh masyarakat. Jika tingkat kejahatan siber terus meningkat dan tidak diimbangi dengan langkah-langkah perlindungan yang memadai, maka potensi pertumbuhan sektor keuangan digital di Indonesia dapat terhambat. (Bank Indonesia, 2023) Oleh karena itu, analisis mendalam mengenai aspek hukum dan perlindungan nasabah dalam menghadapi ancaman phishing sangat diperlukan guna menemukan solusi yang efektif dalam menanggulangi kejahatan ini.

Dalam konteks regulasi, Indonesia telah memiliki berbagai aturan hukum yang mengatur kejahatan siber, termasuk kejahatan phishing yang dilakukan melalui scam link berbahaya. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya dalam Undang-Undang Nomor 19 Tahun 2016 telah mengatur berbagai tindak pidana siber, termasuk akses ilegal, penipuan berbasis teknologi informasi, dan pencurian data pribadi. (Undang-Undang Nomor 19, 2016) Selain itu, Bank Indonesia dan OJK juga telah menerbitkan berbagai regulasi terkait keamanan sistem pembayaran digital serta perlindungan konsumen dalam transaksi elektronik. (Peraturan OJK, 2018) Namun, meskipun regulasi telah tersedia, masih terdapat berbagai tantangan dalam implementasinya, terutama dalam hal penegakan hukum dan perlindungan bagi korban phishing.

Salah satu tantangan utama dalam menangani kejahatan phishing adalah kesulitan dalam mengidentifikasi dan menangkap pelaku. Pelaku kejahatan siber sering kali beroperasi secara anonim dengan menggunakan jaringan yang terenkripsi dan teknik penyamaran yang canggih untuk menghindari pelacakan oleh pihak berwenang. Selain itu, banyak kasus phishing yang melibatkan jaringan kejahatan lintas negara, sehingga proses hukum menjadi semakin kompleks karena melibatkan yurisdiksi hukum yang berbeda. (Europol, 2023) Hal ini mengakibatkan banyak kasus phishing yang tidak dapat diselesaikan secara efektif, dan korban sering kali tidak mendapatkan penggantian atas kerugian yang mereka alami.

Selain aspek penegakan hukum, aspek edukasi dan kesadaran masyarakat juga menjadi faktor penting dalam pencegahan phishing. Banyak korban phishing yang tertipu karena kurangnya pemahaman mengenai tanda-tanda scam link

berbahaya dan cara menghindarinya. Beberapa studi menunjukkan bahwa banyak nasabah masih mudah mempercayai pesan yang mengatasnamakan bank tanpa melakukan verifikasi lebih lanjut (Ventures, 2024). Oleh karena itu, upaya sosialisasi dan edukasi kepada masyarakat mengenai keamanan siber dan cara melindungi diri dari phishing perlu terus ditingkatkan.

Negara-negara lain telah menerapkan berbagai kebijakan untuk mengatasi kejahatan phishing secara lebih efektif. Misalnya, Uni Eropa telah memberlakukan General Data Protection Regulation (GDPR), yang memberikan perlindungan ketat terhadap data pribadi pengguna dan mewajibkan lembaga keuangan untuk memiliki sistem keamanan yang kuat dalam melindungi data nasabah. (GDPR, 2018) Sementara itu, di Amerika Serikat, terdapat undang-undang Cybersecurity Information Sharing Act (CISA) yang memungkinkan berbagai lembaga untuk berbagi informasi mengenai ancaman siber secara lebih luas guna meningkatkan deteksi dan respons terhadap kejahatan siber (CISA, 2015). Indonesia perlu belajar dari praktik-praktik terbaik yang telah diterapkan di negara lain untuk memperkuat regulasi dan kebijakan dalam menangani kejahatan phishing.

Selain regulasi dan edukasi, peningkatan teknologi keamanan juga menjadi langkah penting dalam menangani phishing. Bank dan lembaga keuangan perlu terus mengembangkan sistem deteksi dan pencegahan yang lebih canggih untuk mengidentifikasi dan memblokir scam link sebelum mencapai nasabah (Rahmadani dkk, 2024). Beberapa teknologi yang dapat digunakan antara lain autentikasi multi-faktor (MFA), enkripsi tingkat tinggi, serta penggunaan kecerdasan buatan (artificial intelligence) untuk menganalisis pola transaksi yang mencurigakan (IBM, 2024). Dengan

mengadopsi teknologi yang lebih maju, risiko kejahatan phishing dapat diminimalisir secara lebih efektif.

Dari berbagai permasalahan yang telah diuraikan, jelas bahwa kejahatan phishing dalam sistem perbankan digital melalui scam link berbahaya merupakan ancaman yang semakin serius dan membutuhkan penanganan yang komprehensif. Regulasi yang ada di Indonesia perlu terus diperkuat dan diimplementasikan secara lebih efektif, sementara upaya pencegahan melalui edukasi masyarakat dan peningkatan teknologi keamanan juga harus dioptimalkan (Rahmadani dkk, 2024). Oleh karena itu, penelitian ini akan mengkaji secara mendalam aspek yuridis dari kejahatan phishing, termasuk efektivitas regulasi yang ada serta langkah-langkah yang dapat dilakukan untuk meningkatkan perlindungan hukum bagi nasabah.

2. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian yuridis normatif yang berfokus pada analisis terhadap peraturan perundang-undangan yang berlaku dalam mengatasi kejahatan phishing dalam sistem perbankan digital melalui scam link berbahaya. Pendekatan yuridis normatif dipilih karena penelitian ini bertujuan untuk mengkaji aspek hukum, baik dari segi peraturan yang telah ada maupun efektivitas penerapannya dalam perlindungan nasabah perbankan digital di Indonesia (Marzuki, 2005). Selain itu, penelitian ini juga akan menganalisis berbagai doktrin hukum, prinsip-prinsip yang berkembang, serta studi kasus yang relevan guna mendapatkan pemahaman yang komprehensif mengenai permasalahan yang diteliti. Dalam penelitian ini, sumber data yang digunakan terdiri dari bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi peraturan

perundang-undangan yang berkaitan dengan kejahatan siber dan perlindungan data pribadi, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya dalam Undang-Undang Nomor 19 Tahun 2016, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta berbagai peraturan yang diterbitkan oleh Otoritas Jasa Keuangan (OJK) dan Bank Indonesia terkait keamanan perbankan digital. Bahan hukum sekunder meliputi buku, jurnal ilmiah, laporan penelitian, serta berbagai artikel yang membahas aspek hukum dan teknis terkait dengan kejahatan phishing. Sementara itu, bahan hukum tersier digunakan sebagai pendukung dalam memahami konsep-konsep dasar yang berkaitan dengan penelitian ini, seperti kamus hukum, ensiklopedia, serta referensi lain yang relevan.

3. HASIL DAN PEMBAHASAN

a. Bentuk dan Modus Operandi Kejahatan Phishing Melalui Scam Link Berbahaya dalam Sistem Perbankan Digital

1. Pengertian dan Karakteristik Kejahatan Phising
Kejahatan phishing merupakan salah satu bentuk kejahatan siber yang bertujuan untuk memperoleh informasi pribadi korban, seperti nama pengguna (username), kata sandi (password), dan data finansial lainnya, dengan cara menipu korban agar memberikan informasi tersebut secara sukarela (Tabrani dkk, 2024). Kejahatan ini biasanya dilakukan dengan mengelabui korban melalui komunikasi yang tampak seolah-olah berasal dari entitas resmi, seperti bank atau institusi keuangan lainnya. Istilah phishing sendiri berasal dari kata

"fishing" yang berarti memancing, menggambarkan upaya pelaku untuk memancing informasi sensitif dari korban melalui metode penipuan daring yang terlihat meyakinkan (Sitorus, 2020).

Dalam konteks perbankan digital, phishing sering kali dilakukan melalui tautan palsu (scam link), yang mengarahkan korban ke situs web tiruan yang menyerupai halaman login asli dari layanan perbankan. Tautan ini dapat disebarkan melalui berbagai saluran komunikasi, seperti email, pesan teks (SMS), aplikasi pesan instan, dan media sosial. Setelah korban memasukkan informasi mereka ke dalam situs palsu tersebut, data yang telah dikumpulkan oleh pelaku akan digunakan untuk mengakses rekening bank korban dan melakukan transaksi ilegal (Sitorus, 2020).

2. Bentuk-bentuk Kejahatan Phising dalam Perbankan Digital

Dalam praktiknya, kejahatan phishing dapat dikategorikan ke dalam beberapa bentuk utama berdasarkan metode yang digunakan oleh pelaku, yaitu: (Akbar & Rahdian, 2024)

a. Email Phishing

Modus ini melibatkan pengiriman email yang tampak resmi dari bank atau institusi keuangan. Email tersebut biasanya berisi peringatan palsu mengenai akun yang bermasalah, permintaan verifikasi data, atau tawaran promosi yang mengarahkan korban untuk mengklik tautan tertentu. Setelah korban mengklik

tautan tersebut, mereka akan diarahkan ke situs palsu yang menyerupai situs resmi bank, di mana mereka akan diminta untuk memasukkan informasi pribadi mereka (Petelka dkk, 2019).

b. SMS dan WhatsApp Phishing (Smishing)

Modus ini menggunakan pesan singkat (SMS) atau aplikasi perpesanan seperti WhatsApp untuk mengirim tautan berbahaya. Pesan tersebut sering kali mengatasnamakan bank dan menginformasikan bahwa akun korban telah diblokir atau ada transaksi mencurigakan yang harus segera dikonfirmasi melalui tautan yang diberikan. Setelah korban mengklik tautan tersebut, mereka akan diarahkan ke situs web palsu yang meminta data login dan informasi pribadi lainnya.

c. Voice Phishing (Vishing)

Dalam modus ini, pelaku melakukan panggilan telepon kepada korban dengan berpura-pura sebagai petugas bank atau otoritas keuangan lainnya. Pelaku akan berusaha meyakinkan korban untuk memberikan informasi penting seperti nomor kartu kredit, kode OTP (One-Time Password), atau data pribadi lainnya. Teknik ini sering kali dilakukan dengan nada mendesak agar korban panik dan segera memberikan informasi yang diminta tanpa berpikir lebih jauh. (Petelka dkk, 2019).

d. Situs Web Tiruan

Pelaku kejahatan sering kali membuat situs web palsu yang meniru tampilan situs resmi bank atau aplikasi perbankan. Situs tersebut dapat muncul dalam hasil pencarian Google, disebarkan melalui iklan daring, atau dikirimkan melalui email dan SMS. Jika korban tidak teliti dan memasukkan informasi mereka, data tersebut akan langsung masuk ke tangan pelaku untuk disalahgunakan.

e. Social Media Phishing

Kejahatan phishing juga sering terjadi di media sosial, di mana pelaku membuat akun palsu yang menyerupai akun resmi bank. Akun ini kemudian digunakan untuk menghubungi korban, menawarkan bantuan, atau mengarahkan mereka untuk mengunjungi tautan tertentu yang sebenarnya adalah situs phishing.

3. Modus Operandi Kejahatan Phishing Melalui Scam Link

Modus operandi kejahatan phishing melalui scam link dalam sistem perbankan digital umumnya mengikuti tahapan berikut: (Prastya dkk, 2024)

a. Pengiriman Tautan Berbahaya

Pelaku menyebarkan tautan palsu melalui email, SMS, media sosial, atau aplikasi pesan instan. Tautan ini dibuat sedemikian rupa agar terlihat sah, misalnya dengan menggunakan nama domain yang mirip dengan situs asli bank, seperti

- "bri-login.com" yang meniru "bri.co.id".
- b. Pemalsuan Identitas dan Manipulasi Psikologis
Agar korban percaya, pelaku sering kali menggunakan teknik rekayasa sosial (social engineering), seperti mengaku sebagai pegawai bank atau petugas keamanan. Mereka menciptakan situasi mendesak, misalnya dengan menginformasikan bahwa akun korban telah diblokir atau ada transaksi mencurigakan yang perlu dikonfirmasi segera.
- c. Pengalihan ke Situs Palsu
Ketika korban mengklik tautan yang diberikan, mereka akan diarahkan ke situs web palsu yang dirancang untuk menyerupai situs resmi bank. Situs ini biasanya meminta korban untuk memasukkan nama pengguna, kata sandi, serta kode OTP yang dikirimkan ke ponsel mereka.
- d. Pencurian Data dan Penggunaan Informasi
Setelah korban memasukkan data mereka, informasi tersebut akan langsung dikirim ke server milik pelaku. Dengan data tersebut, pelaku dapat masuk ke akun perbankan korban, mengurus saldo, atau melakukan transaksi ilegal lainnya.
- e. Penyamaran dan Penghapusan Jejak
Setelah berhasil mencuri dana korban, pelaku biasanya akan segera menarik uang melalui rekening perantara atau mengonversinya ke mata uang kripto untuk menghilangkan jejak. Pelaku juga dapat menggunakan layanan pencucian uang digital untuk menyamarkan aliran dana hasil kejahatan mereka.
4. Dampak Kejahatan Phishing terhadap Nasabah dan Perbankan
Kejahatan phishing dalam sistem perbankan digital memiliki dampak yang luas, baik bagi nasabah maupun industri perbankan secara keseluruhan (Radiansyah, 2016).
- a. Kerugian Finansial
Nasabah yang menjadi korban phishing dapat kehilangan dana mereka akibat transaksi ilegal yang dilakukan oleh pelaku. Dalam beberapa kasus, korban bahkan kehilangan seluruh saldo rekening mereka sebelum mereka menyadari bahwa mereka telah tertipu.
- b. Penyalahgunaan Data Pribadi
Selain digunakan untuk mencuri uang, informasi yang diperoleh dari phishing dapat dijual di pasar gelap (dark web) atau digunakan untuk kejahatan lain, seperti pencurian identitas dan pemerasan (Muftiadi dkk, 2022)
- c. Menurunnya Kepercayaan terhadap Perbankan Digital
Meningkatnya kasus phishing dapat menyebabkan nasabah menjadi enggan untuk menggunakan layanan perbankan digital karena khawatir akan risiko kejahatan siber. Hal ini dapat menghambat pertumbuhan

sektor keuangan digital dan memperlambat inklusi keuangan.

- d. Kerugian Reputasi bagi Bank
Ketika nasabah mengalami penipuan phishing, mereka sering kali menyalahkan bank karena dianggap tidak memberikan perlindungan yang cukup terhadap keamanan akun mereka. Akibatnya, reputasi bank dapat tercoreng, dan kepercayaan publik terhadap layanan yang mereka tawarkan dapat menurun.
 - e. Biaya Tambahan untuk Keamanan dan Investigasi
Bank harus menginvestasikan lebih banyak sumber daya untuk meningkatkan sistem keamanan, melakukan investigasi terhadap kasus phishing, serta menangani keluhan nasabah yang menjadi korban. Biaya ini dapat membebani institusi perbankan dan mengurangi efisiensi operasional mereka.
- b. Pengaturan Hukum di Indonesia Terkait Kejahatan Phishing dalam Sistem Perbankan Digital Melalui Scam Link Berbahaya**
1. Landasan Hukum Kejahatan Phishing dalam Sistem Perbankan Digital
Kejahatan phishing dalam sistem perbankan digital melalui scam link berbahaya telah menjadi salah satu ancaman siber yang semakin marak terjadi di Indonesia. Pemerintah telah mengatur berbagai ketentuan hukum untuk menanggulangi tindak kejahatan ini, baik melalui undang-undang yang secara

khusus mengatur transaksi elektronik maupun regulasi terkait perlindungan konsumen di sektor perbankan digital. Beberapa peraturan yang relevan dalam menangani kejahatan phishing antara lain adalah: (Yustitiana, 2021)

- a. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Perubahannya dalam Undang-Undang Nomor 19 Tahun 2016
UU ITE merupakan dasar hukum utama dalam mengatur aktivitas di dunia siber, termasuk kejahatan phishing. Dalam Pasal 28 ayat (1) UU ITE, disebutkan bahwa setiap orang dilarang dengan sengaja dan tanpa hak menyebarkan informasi elektronik yang bersifat menyesatkan dan dapat merugikan konsumen dalam transaksi elektronik. Selain itu, Pasal 35 UU ITE mengatur bahwa setiap orang yang dengan sengaja dan tanpa hak memanipulasi, mengubah, atau menciptakan informasi elektronik atau dokumen elektronik dengan tujuan agar dianggap seolah-olah data yang asli dapat dikenakan sanksi pidana.
- b. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)
UU PDP mengatur perlindungan data pribadi masyarakat agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab. Kejahatan phishing sering kali melibatkan

- pencurian data pribadi, seperti nama, nomor rekening, serta kredensial login nasabah perbankan. Dalam undang-undang ini, pihak yang menyalahgunakan atau mengakses data pribadi seseorang tanpa izin dapat dikenakan sanksi pidana.
- c. Kitab Undang-Undang Hukum Pidana (KUHP)
Meskipun KUHP tidak secara eksplisit mengatur kejahatan siber, beberapa pasalnya dapat diterapkan dalam kasus phishing. Pasal 378 KUHP tentang penipuan, misalnya, dapat digunakan untuk menjerat pelaku yang dengan sengaja mengelabui korban guna mendapatkan keuntungan yang tidak sah. Selain itu, Pasal 362 KUHP tentang pencurian juga dapat diterapkan apabila kejahatan phishing menyebabkan hilangnya uang atau aset korban.
- d. Peraturan Bank Indonesia (PBI) dan Peraturan Otoritas Jasa Keuangan (OJK)
Dalam konteks perbankan digital, Bank Indonesia (BI) dan Otoritas Jasa Keuangan (OJK) memiliki peraturan yang bertujuan untuk melindungi konsumen dan menjaga keamanan transaksi elektronik. Salah satu regulasi yang relevan adalah:
- PBI Nomor 22/20/PBI/2020 tentang Keamanan Sistem Pembayaran, yang mewajibkan bank dan penyedia layanan keuangan digital untuk menerapkan sistem keamanan yang ketat guna mencegah penyalahgunaan data nasabah.
 - POJK Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan, yang mengatur kewajiban lembaga keuangan untuk memberikan edukasi serta perlindungan kepada nasabah terkait risiko kejahatan digital.
 - e. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UU PK)
UU PK memberikan landasan hukum bagi nasabah yang mengalami kerugian akibat tindak kejahatan phishing. Bank sebagai penyedia layanan perbankan digital memiliki tanggung jawab untuk memastikan keamanan sistem mereka dan memberikan informasi yang jelas mengenai risiko transaksi daring. Jika bank tidak memberikan perlindungan yang memadai, maka nasabah yang dirugikan dapat menuntut ganti rugi berdasarkan ketentuan dalam UU PK.
2. Sanksi Hukum bagi Pelaku Kejahatan Phishing di Indonesia
Sanksi yang dikenakan terhadap pelaku phishing dalam sistem perbankan digital melalui scam link berbahaya dapat berupa sanksi pidana maupun perdata, tergantung pada dampak yang ditimbulkan terhadap korban dan bagaimana kejahatan tersebut dilakukan. Beberapa ketentuan

- sanksi yang dapat diterapkan antara lain: (Wiranata dkk, 2024)
- a. Sanksi Pidana Berdasarkan UU ITE
 - Pasal 28 ayat (1): Pelaku yang menyebarkan informasi elektronik yang menyesatkan dan merugikan konsumen dapat dipidana dengan hukuman penjara paling lama 6 tahun dan/atau denda maksimal Rp1 miliar.
 - Pasal 35 dan Pasal 51 ayat (1): Pelaku yang dengan sengaja memanipulasi data elektronik agar dianggap sebagai data yang sah dapat dipidana dengan hukuman penjara maksimal 12 tahun dan/atau denda maksimal Rp12 miliar.
 - b. Sanksi Pidana Berdasarkan UU PDP
 - Pasal 67 dan Pasal 68: Setiap orang yang secara ilegal memperoleh, mengungkapkan, atau menggunakan data pribadi seseorang tanpa izin dapat dipidana dengan hukuman penjara maksimal 6 tahun dan/atau denda hingga Rp6 miliar.
 - c. Sanksi Pidana Berdasarkan KUHP
 - Pasal 378 (Penipuan): Pelaku phishing yang terbukti melakukan penipuan dapat dikenakan pidana penjara maksimal 4 tahun.
 - Pasal 362 (Pencurian): Jika phishing menyebabkan kerugian finansial, pelaku dapat dijerat dengan pasal pencurian dengan ancaman pidana penjara maksimal 5 tahun.
 - d. Sanksi Perdata Berdasarkan UU Perlindungan Konsumen
 - Konsumen atau nasabah yang dirugikan akibat kelalaian bank dalam melindungi sistem perbankan digitalnya dapat mengajukan gugatan ganti rugi berdasarkan Pasal 19 UU PK.
 - Bank juga dapat dituntut jika terbukti tidak memberikan informasi yang cukup kepada nasabah terkait keamanan perbankan digital atau tidak menyediakan langkah mitigasi yang memadai terhadap risiko kejahatan phishing.
3. Evaluasi dan Tantangan dalam Penegakan Hukum terhadap Phishing
- Meskipun regulasi di Indonesia telah cukup jelas dalam mengatur kejahatan phishing, terdapat beberapa tantangan dalam implementasi hukum yang perlu diperhatikan, antara lain: (Hariyono & Simangunsong, 2023)
- a. Kurangnya Kesadaran dan Literasi Digital
- Banyak nasabah perbankan digital yang masih belum sepenuhnya memahami ancaman kejahatan siber dan cara melindungi diri dari serangan phishing. Hal ini menyebabkan korban lebih mudah tertipu oleh modus kejahatan yang semakin canggih.

- b. Kesulitan Identifikasi dan Penangkapan Pelaku
Pelaku phishing sering kali menggunakan identitas palsu dan teknologi canggih untuk menyembunyikan jejak mereka. Selain itu, banyak dari mereka yang beroperasi dari luar negeri, sehingga menyulitkan aparat penegak hukum dalam menangkap dan memproses mereka secara hukum.
- c. Perlunya Harmonisasi Regulasi
Regulasi mengenai kejahatan siber di Indonesia masih tersebar dalam berbagai undang-undang, sehingga diperlukan harmonisasi hukum yang lebih baik agar penegakan hukum dapat berjalan lebih efektif.
- d. Kurangnya Koordinasi antara Institusi Keuangan dan Aparat Penegak Hukum
Bank dan lembaga keuangan sering kali memiliki data yang dapat membantu investigasi kejahatan phishing, namun koordinasi dengan pihak kepolisian dan lembaga penegak hukum lainnya masih belum optimal.
- c. Upaya Perlindungan Hukum bagi Nasabah yang Menjadi Korban Phishing melalui Scam Link dalam Sistem Perbankan Digital**
1. Perlindungan Hukum bagi Nasabah dalam Sistem Perbankan Digital
Kejahatan phishing yang dilakukan melalui scam link dalam sistem perbankan digital sering kali menyebabkan kerugian finansial yang signifikan bagi nasabah. Oleh karena itu, perlindungan hukum bagi korban kejahatan ini menjadi aspek yang sangat penting dalam sistem hukum di Indonesia. Perlindungan hukum terhadap nasabah yang menjadi korban phishing dapat dibedakan menjadi dua jenis, yaitu perlindungan hukum preventif dan perlindungan hukum represif. (Tanonggi dkk, 2024)
- a. Perlindungan Hukum Preventif
Perlindungan hukum preventif merupakan upaya yang dilakukan sebelum kejahatan terjadi guna mencegah atau meminimalisir risiko yang dihadapi oleh nasabah. Upaya ini melibatkan regulasi ketat, edukasi kepada masyarakat, serta peningkatan sistem keamanan digital oleh lembaga keuangan. Bank Indonesia (BI) dan Otoritas Jasa Keuangan (OJK) telah mengeluarkan berbagai peraturan terkait keamanan transaksi digital untuk melindungi nasabah dari serangan siber, termasuk phishing.
- Peraturan Bank Indonesia (PBI) No. 22/20/PBI/2020 tentang Keamanan Sistem Pembayaran mengatur bahwa penyedia layanan pembayaran digital wajib menerapkan standar keamanan yang tinggi guna melindungi data nasabah.
 - POJK No. 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan mewajibkan lembaga

keuangan untuk menyediakan edukasi kepada nasabah mengenai risiko kejahatan siber, termasuk bagaimana mengidentifikasi scam link berbahaya.

Upaya preventif lainnya adalah peningkatan literasi digital di kalangan nasabah perbankan. Banyak korban phishing tertipu karena kurangnya pemahaman tentang modus kejahatan siber. Oleh karena itu, bank dan regulator perbankan diwajibkan untuk melakukan sosialisasi tentang pentingnya menjaga kerahasiaan data pribadi serta mengenali tanda-tanda phishing. Bank memiliki peran krusial dalam melindungi nasabah dari serangan phishing. Beberapa langkah yang telah diterapkan oleh bank dalam sistem keamanannya antara lain: (Hariyono, 2023)

- Implementasi autentikasi dua faktor (2FA) untuk transaksi perbankan digital guna memastikan bahwa hanya nasabah yang berwenang yang dapat mengakses akun mereka.
- Penerapan teknologi enkripsi dan deteksi anomali transaksi untuk mengidentifikasi aktivitas mencurigakan dalam akun nasabah.
- Peringatan dini melalui SMS atau email jika terdapat aktivitas yang mencurigakan di rekening nasabah.

b. Perlindungan Hukum Represif

Perlindungan hukum represif merupakan upaya yang dilakukan setelah kejahatan terjadi, dengan tujuan untuk memberikan keadilan bagi korban dan menindak pelaku kejahatan. Bentuk perlindungan ini meliputi:

- Pelaporan dan Investigasi oleh Aparat Penegak Hukum

Jika seorang nasabah menjadi korban phishing, ia dapat melaporkan kejadian tersebut kepada kepolisian, OJK, atau Bank Indonesia. Polisi siber (Cyber Crime Unit) akan melakukan investigasi untuk mengidentifikasi pelaku dan melakukan pemrosesan hukum berdasarkan UU ITE, KUHP, dan UU Perlindungan Data Pribadi.

- Tuntutan Ganti Rugi oleh Nasabah

Jika bank terbukti lalai dalam memberikan perlindungan terhadap sistem perbankan digitalnya, nasabah dapat mengajukan gugatan perdata berdasarkan:

1. Pasal 19 Undang-Undang Perlindungan Konsumen (UU No. 8 Tahun 1999), yang menyatakan bahwa pelaku usaha wajib memberikan ganti rugi kepada konsumen yang mengalami kerugian akibat kelalaiannya.

2. Pasal 1365 KUH Perdata tentang Perbuatan Melawan Hukum, yang memungkinkan nasabah untuk menuntut ganti rugi jika terbukti ada unsur kesalahan atau kelalaian dari pihak bank.
 - Pengembalian Dana oleh Bank
Beberapa bank telah menerapkan kebijakan kompensasi bagi nasabah yang menjadi korban phishing, terutama jika terbukti bahwa kejahatan terjadi akibat kelemahan dalam sistem keamanan bank. Namun, kebijakan ini biasanya bergantung pada hasil investigasi internal dan kepatuhan nasabah terhadap prosedur keamanan yang telah ditetapkan oleh bank.
 2. Tantangan dalam Perlindungan Hukum bagi Korban Phishing
Meskipun regulasi mengenai perlindungan nasabah telah ada, terdapat beberapa tantangan yang dihadapi dalam implementasinya, antara lain:
 - a. Kurangnya Kesadaran Hukum di Kalangan Nasabah
Banyak nasabah yang tidak mengetahui hak-haknya sebagai konsumen jasa keuangan, termasuk mekanisme pelaporan dan proses hukum yang dapat ditempuh jika menjadi korban kejahatan phishing.
 - b. Kesulitan Identifikasi dan Penindakan terhadap Pelaku
Para pelaku kejahatan phishing sering kali menggunakan server luar negeri dan identitas palsu, sehingga menyulitkan aparat penegak hukum dalam melacak serta menangkap mereka. Selain itu, kerja sama internasional dalam penanganan kejahatan siber masih memiliki keterbatasan.
 - c. Belum Adanya Regulasi yang Mengatur Pengembalian Dana secara Pasti
Meskipun beberapa bank telah memberikan kompensasi kepada korban phishing, tidak ada regulasi khusus yang mewajibkan bank untuk mengembalikan dana yang hilang akibat serangan phishing. Hal ini menyebabkan ketidakpastian bagi nasabah mengenai apakah mereka akan mendapatkan ganti rugi atau tidak.
 - d. Kurangnya Kerja Sama antara Bank, Regulator, dan Penegak Hukum
Masih terdapat kelemahan dalam koordinasi antara perbankan, regulator keuangan (OJK dan BI), serta aparat penegak hukum dalam menangani kasus phishing. Proses investigasi yang lambat sering kali menyebabkan pelaku sulit ditindak sebelum mereka menghilangkan jejaknya.
3. Rekomendasi untuk Meningkatkan Perlindungan Hukum bagi Nasabah
Untuk meningkatkan efektivitas perlindungan hukum bagi nasabah yang menjadi korban

phishing, beberapa rekomendasi yang dapat diterapkan adalah:

- a. Meningkatkan Literasi Keuangan Digital
Pemerintah dan lembaga perbankan perlu terus mengedukasi masyarakat mengenai risiko phishing, tanda-tanda scam link, serta langkah-langkah yang harus dilakukan jika menjadi korban.
- b. Peningkatan Pengawasan oleh Regulator
OJK dan BI perlu meningkatkan pengawasan terhadap penerapan sistem keamanan perbankan digital serta memastikan bahwa bank memberikan perlindungan yang optimal bagi nasabahnya.
- c. Pembuatan Regulasi yang Lebih Ketat mengenai Pengembalian Dana bagi Korban
Perlu adanya regulasi yang mewajibkan bank untuk mengganti kerugian nasabah dalam kondisi tertentu, misalnya jika terbukti ada kelemahan dalam sistem keamanan bank yang dimanfaatkan oleh pelaku phishing.
- d. Penguatan Kerja Sama Internasional dalam Penegakan Hukum terhadap Kejahatan Siber
Mengingat banyaknya kejahatan phishing yang dilakukan oleh sindikat internasional, pemerintah Indonesia perlu memperkuat kerja sama dengan negara lain dalam rangka ekstradisi pelaku serta pertukaran informasi intelijen terkait kejahatan siber.

d. Kendala dalam Penegakan Hukum terhadap Kejahatan Phishing melalui Scam Link Berbahaya di Indonesia

Penegakan hukum terhadap kejahatan phishing dalam sistem perbankan digital melalui scam link berbahaya menghadapi berbagai tantangan, baik dari aspek hukum, teknis, maupun kelembagaan. Beberapa kendala utama yang menghambat efektivitas penindakan terhadap kejahatan ini di Indonesia antara lain: (Ekayani dkk, 2023)

1. Keterbatasan Regulasi yang Spesifik terhadap Kejahatan Phishing
Meskipun Indonesia telah memiliki beberapa regulasi terkait kejahatan siber, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 11 Tahun 2008, Undang-Undang Perlindungan Data Pribadi No. 27 Tahun 2022, serta berbagai peraturan dari Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI), regulasi yang secara khusus mengatur kejahatan phishing masih terbatas. UU ITE memang mengatur tentang kejahatan siber secara umum, tetapi tidak secara rinci menjelaskan tentang phishing melalui scam link berbahaya. Akibatnya, dalam praktiknya, aparat penegak hukum sering kali mengalami kesulitan dalam menjerat pelaku dengan pasal yang tepat.
2. Kesulitan dalam Identifikasi dan Pelacakan Pelaku
Pelaku phishing sering menggunakan berbagai metode canggih untuk menyembunyikan identitas

dan lokasinya. Beberapa tantangan dalam identifikasi dan pelacakan pelaku kejahatan ini antara lain:

- Penggunaan server luar negeri: Banyak pelaku phishing yang menggunakan server atau domain yang berbasis di luar negeri, sehingga menyulitkan otoritas Indonesia dalam melacak dan menangkap mereka.
 - Teknik anonimitas digital: Pelaku sering kali menggunakan VPN, proxy server, atau identitas palsu untuk menghindari deteksi.
 - Perpindahan dana yang cepat: Dana hasil kejahatan biasanya langsung dipindahkan ke beberapa rekening, termasuk melalui cryptocurrency, sehingga menyulitkan proses pelacakan dan pemulihan dana.
3. Kurangnya Sumber Daya dan Kapasitas Aparat Penegak Hukum
- Aparat penegak hukum di Indonesia, termasuk kepolisian dan penyidik siber, masih menghadapi kendala dalam hal kapasitas dan sumber daya yang memadai untuk menangani kejahatan siber yang semakin kompleks. Beberapa permasalahan yang dihadapi antara lain:
- Kurangnya tenaga ahli dalam bidang forensik digital: Tidak semua aparat penegak hukum memiliki keahlian yang cukup dalam menganalisis bukti digital dan melacak transaksi elektronik yang dilakukan oleh pelaku.
 - Terbatasnya fasilitas teknologi untuk investigasi siber: Dalam beberapa kasus, keterbatasan perangkat lunak dan perangkat keras dalam investigasi siber membuat proses penegakan hukum menjadi lebih lambat dan tidak efektif.
4. Rendahnya Kesadaran Hukum dan Literasi Digital Masyarakat
- Salah satu faktor utama yang membuat kejahatan phishing terus berkembang adalah rendahnya literasi digital di kalangan masyarakat. Banyak korban tidak memahami cara kerja scam link dan mudah tertipu oleh modus operandi yang digunakan oleh pelaku. Selain itu, kesadaran masyarakat untuk melaporkan kasus phishing juga masih rendah, yang menyebabkan banyak kasus tidak tertangani dengan baik oleh aparat hukum.
5. Kurangnya Kerja Sama Internasional dalam Menangani Kejahatan Siber
- Kejahatan phishing sering kali dilakukan oleh sindikat internasional yang beroperasi lintas negara. Namun, kerja sama antarnegara dalam hal ekstradisi pelaku dan pertukaran data intelijen masih terbatas. Hal ini membuat penegakan hukum terhadap pelaku yang berada di luar yurisdiksi Indonesia menjadi lebih sulit.

4. KESIMPULAN

Kejahatan phishing dalam sistem perbankan digital melalui scam link berbahaya merupakan salah satu bentuk kejahatan siber yang terus berkembang seiring dengan meningkatnya digitalisasi layanan keuangan. Phishing dilakukan dengan cara mengelabui nasabah melalui tautan palsu yang menyerupai situs resmi bank, sehingga pelaku dapat mencuri data pribadi dan kredensial perbankan korban untuk melakukan transaksi ilegal. Dari analisis yuridis yang dilakukan, ditemukan bahwa regulasi di Indonesia, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Data Pribadi (UU PDP), serta berbagai regulasi dari Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI), telah mengatur mengenai kejahatan siber termasuk phishing. Namun, masih terdapat berbagai tantangan dalam implementasi regulasi tersebut, terutama dalam aspek pencegahan, penegakan hukum, serta perlindungan nasabah. Salah satu kendala utama adalah kesulitan dalam mengidentifikasi dan menangkap pelaku yang sering kali beroperasi secara anonim dan lintas negara. Selain itu, rendahnya literasi digital masyarakat menyebabkan banyak nasabah masih mudah tertipu oleh modus phishing yang semakin canggih. Bank dan lembaga keuangan memiliki peran penting dalam meningkatkan sistem keamanan perbankan digital dengan menerapkan teknologi deteksi dini, autentikasi berlapis, serta melakukan edukasi kepada nasabah. Di sisi lain, aparat penegak hukum harus lebih proaktif dalam menangani kasus phishing dengan memperkuat koordinasi antarinstansi, baik di tingkat nasional maupun internasional. Untuk mengatasi ancaman phishing secara efektif, diperlukan pendekatan yang komprehensif, mulai dari penguatan

regulasi, peningkatan kesadaran masyarakat, hingga optimalisasi strategi penegakan hukum. Perlindungan hukum bagi nasabah harus diperkuat dengan mekanisme pemulihan dana yang jelas serta kebijakan yang memastikan tanggung jawab bank dalam melindungi data dan transaksi nasabah. Dengan demikian, upaya pencegahan dan penanggulangan kejahatan phishing melalui scam link berbahaya dapat lebih efektif dalam menciptakan sistem perbankan digital yang aman, terpercaya, dan berkelanjutan di Indonesia.

DAFTAR PUSTAKA

Peraturan Perundang-Undangan

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. (2016). Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251.

Buku

- Bahri, I. S. (2023). *Cyber Crime dalam Sorotan Hukum Pidana* (Edisi 2023). Bahasa Rakyat.
- Dharani, L. I. C., Idayanti, S., & Rahayu, K. (2024). *Perlindungan Hukum terhadap Tindakan Phishing di Media Sosial*. Penerbit NEM.
- Mansur, D. M. A. (2005). *Cyber law: aspek hukum teknologi informasi*. Tiga Serangkai.
- Marzuki, P. M. (2005). *Penelitian hukum*.
- Situmeang, S. M. T. (2020). *Cyber law*.
- Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson.

Jurnal

- Akbar, D. A., & Rahdian, M. (2024). Analisis Web Phishing Menggunakan Metode OSCAR Forensic (Studi Kasus: Follower Instagram Gratis). *JTINFO: Jurnal Teknik Informatika*, 3(1), 18-24.
- Ansyafa, K. Z., Fajarudin, M., Fadhil, M., & Neyman, S. N. (2024). Analisis Keamanan Media Sosial terhadap Serangan Phising Online menggunakan Metode Zphisher dan Social Engineering Toolkit. *Journal of Internet and Software Engineering*, 1(4), 10-10.
- Arisandy, Y. O. (2020). Penegakan Hukum terhadap Cyber Crime Hacker. *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, 1(3), 162-169.
- Danuri, M. (2019). Perkembangan dan transformasi teknologi digital. *Jurnal ilmiah infokam*, 15(2).
- Ekayani, L., Djanggih, H., & Suong, M. A. A. (2023). Perlindungan Hukum Nasabah Terhadap Kejahatan Pencurian Data Pribadi (Phising) Di Lingkungan Perbankan. *Journal of Lex Philosophy (JLP)*, 4(1), 22-40.
- Ersya, M. P. (2017). Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. *Journal of Moral and Civic Education*, 1(1), 50-62.
- Gupta, S., Singhal, A., & Kapoor, A. (2016, April). A literature survey on social engineering attacks: Phishing attack. In 2016 international conference on computing, communication and automation (ICCCA) (pp. 537-540). IEEE.
- Hariyono, A. G. (2023). Perlindungan Hukum terhadap Korban Phishing Cyber Crime dalam Perspektif Kriminologi.(Protection of The Victims of Phishing Cyber Crime in A Criminal Perspective) (Doctoral dissertation, Universitas 17 Agustus 1945 Surabaya).
- Hariyono, A. G., & Simangunsong, F. (2023). Perlindungan Hukum Korban Pencurian Data Pribadi (Phishing cybercrime) Dalam Perspektif Kriminologi. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, 3(1), 428-439.
- Hariyono, A. G., & Simangunsong, F. (2023). Perlindungan Hukum Korban Pencurian Data Pribadi (Phishing cybercrime) Dalam Perspektif Kriminologi. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, 3(1), 428-439.
- 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*, 1(2), 60-65.
- Petelka, J., Zou, Y., & Schaub, F. (2019, May). Put your warning where your link is: Improving and evaluating email phishing warnings. In Proceedings of the 2019 CHI conference on human factors in computing systems (pp. 1-15).

- Prastya, M. W. A., Tahir, M., Ningrum, A. A., Zaibintoro, A. P., Sa'adah, L., Mutmainnah, U., & Sa'diah, S. K. (2024). Analisis Ancaman Pishing melalui Aplikasi WhatsApp: Review Metode Studi Literatur. *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, 7(3), 190-197.
- Radiansyah, I., Rusdjan, C., & Priyadi, Y. (2016). Analisis Ancaman Phishing Dalam Layanan Online Banking. *Journal of Innovation in Business and Economics*, 7(1), 1-14.
- Rahmadani, A. E., Pangestu, Y., & Halizhah, N. (2024). Perlindungan Data Pribadi di Era Digital: Tantangan dan Solusi Dalam Sistem Perbankan. *Media Hukum Indonesia (MHI)*, 2(4), 180-186.
- Sitorus, N. T. Urgensi Penegakan Hukum Terhadap Perbuatan Phising Sebagai Upaya Pencegahan Kejahatan Siber. *Riau Law Journal*, 8(1), 83-94.
- Tabrani, S., Safitri, V., & Hosnah, A. U. (2024). KEJAHATAN PHISHING DITINJAU DARI PERSPEKTIF HUKUM DAN KEJAHATAN SIBER. *Civilia: Jurnal Kajian Hukum dan Pendidikan Kewarganegaraan*, 3(1), 1-13.
- Wiranata, G. A., Ucuq, Y., & Sidarta, D. D. (2024). PERTANGGUNGJAWABAN PIDANA TERHADAP PELAKU TINDAK PIDANA PHISHING. *COURT REVIEW: Jurnal Penelitian Hukum* (e-ISSN: 2776-1916), 4(02), 13-25.
- Yustitiana, R. (2021). Pelaksanaan Pengaturan Hukum Tindak Kejahatan Fraud Phishing Transaksi Elektronik Sebagai Bagian dari Upaya Penegakan Hukum di Indonesia Dikaitkan Dengan Teori Efektivitas Hukum. *Jurnal Hukum Visio Justisia*, 1(1), 98-126.

Laporan

- Bank Indonesia. (2024). Laporan keuangan dan keamanan digital perbankan 2023. Bank Indonesia.
- Kementerian Komunikasi dan Informatika. (2025) Laporan kejahatan siber di Indonesia tahun 2023.
- Otoritas Jasa Keuangan. (2018). Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018 tentang penyelenggaraan layanan perbankan digital. Otoritas Jasa Keuangan.

Internet

- United States. (2015). Cybersecurity Information Sharing Act (CISA).
- European Union. (2018). General Data Protection Regulation (GDPR).