Deposisi: Jurnal Publikasi Ilmu Hukum
Volume. 2, Nomor. 4 Tahun 2024
e-ISSN: 2987-4211; p-ISSN: 2987-5188, Hal 132-148
DOI: https://doi.org/10.59581/deposisi.v2i4.4214
Available Online at: https://ifrelresearch.org/index.php/Deposisi-widyakarya

Perlindungan Hukum Nasabah dari Kejahatan *Phising* dalam Layanan Perbankan Digital di Indonesia

Imelia Damai Agusthin[1] , Dinda Christy Nada[2] , Nadia Ananda Putri[3]
[1-3] Program Studi Ilmu Hukum, Universitas Negeri Semarang, Indonesia
Email: imeliadamai@students.unnes.ac.id, dindachristy10@students.unnes.ac.id, nadiaaaputrii3@students.unnes.ac.id

Abstract. *The digitalization of the banking sector, driven by the Fourth Industrial Revolution, has significantly impacted the ease of financial transactions through digital banking services. However, this progress also creates vulnerabilities to cybercrimes, particularly phishing, which aims to steal customers' personal data via fake websites or messages. This article examines relevant legal frameworks, including Law No. 19 of 2016 on Electronic Information and Transactions (EIT Law), the Indonesian Criminal Code (KUHP), and regulations issued by the Financial Services Authority (OJK), such as POJK No. 12/POJK.03/2018 on Digital Banking Services. Employing a normative qualitative approach, the study explores the legal protection available to customers as phishing victims and the responsibilities of banks in preventing and addressing such threats. This article recommends strengthening banks' technological security systems, enhancing customers' digital literacy, and enforcing laws more effectively to establish secure and reliable digital banking services.*

Keywords: *phishing, legal protection, digital banking*

Abstrak. Digitalisasi sektor perbankan yang dipicu oleh Revolusi Industri 4.0 telah membawa dampak signifikan terhadap kemudahan transaksi keuangan melalui layanan perbankan digital. Namun, kemajuan ini juga membuka celah terhadap ancaman kejahatan siber, khususnya phishing, yang bertujuan mencuri data pribadi nasabah melalui situs atau pesan palsu. Artikel ini menganalisis ketentuan hukum yang relevan, termasuk UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE), KUHP, serta peraturan OJK seperti POJK No. 12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital. Metode penelitian normatif kualitatif digunakan untuk mengkaji perlindungan hukum terhadap nasabah sebagai korban phishing dan tanggung jawab perbankan dalam mencegah serta menangani ancaman ini. Artikel ini merekomendasikan penguatan keamanan sistem teknologi bank, edukasi literasi digital nasabah, serta penegakan hukum yang lebih efektif guna menciptakan layanan perbankan digital yang aman dan terpercaya.

Kata kunci : phishing, perlindungan hukum, perbankan digital

1. PENDAHULUAN

Revolusi Industri 4.0 menandai era baru dalam perkembangan teknologi dan industri global. Peran manusia dalam proses operasional semakin diminimalisir karena teknologi otomatisasi mengambil alih sebagian besar fungsi kerja. Dukungan teknologi informasi dalam proses ini meningkatkan efisiensi dan efektivitas kerja di berbagai sektor, menciptakan lingkungan kerja yang lebih terorganisasi dan produktif. Dengan kemajuan ini, berbagai industri mulai mengubah cara mereka beroperasi untuk mengikuti tren digitalisasi, termasuk dengan memanfaatkan teknologi inovatif untuk mempermudah aktivitas sehari-hari, terutama di sektor keuangan.

Sektor keuangan, khususnya perbankan, menjadi salah satu bidang yang mengalami dampak signifikan dari peralihan menuju era Revolusi Industri 4.0. Industri perbankan di Indonesia memiliki peran penting dalam mendukung pertumbuhan ekonomi, tidak hanya

Received: September 16,2024; Revised: Oktober 30, 2024; Accepted: November 17, 2024; Online Available: November 19, 2024

melalui kontribusinya terhadap pendapatan nasional tetapi juga dengan berfungsi sebagai lembaga perantara yang mengelola dana masyarakat dan menyalurkannya kembali untuk mendukung kegiatan produktif. Dalam rangka mempercepat proses digitalisasi perbankan, Otoritas Jasa Keuangan (OJK) mengeluarkan Peraturan OJK No. 12/POJK.03/2018 yang mengatur penyelenggaraan layanan perbankan digital oleh bank umum. Peraturan ini menjelaskan bahwa layanan perbankan digital adalah layanan berbasis elektronik yang dirancang untuk mengoptimalkan pemanfaatan data nasabah sehingga dapat memberikan pengalaman layanan yang cepat, mudah, dan sesuai kebutuhan. Layanan ini juga memungkinkan nasabah untuk mengaksesnya secara mandiri dengan tetap memperhatikan aspek keamanan yang ketat. Langkah ini menunjukkan bagaimana transformasi digital menjadi prioritas utama dalam meningkatkan kualitas layanan perbankan.

Transformasi digital yang diterapkan dalam sektor perbankan tidak hanya terbatas pada pengembangan layanan *online* dan *mobile banking*. Transformasi ini juga mencakup penggabungan teknologi canggih dengan interaksi nasabah secara langsung untuk menciptakan pengalaman yang lebih nyaman dan efisien. Sejumlah bank di Indonesia telah mulai memperluas digitalisasi ini dengan menyediakan berbagai fitur yang mempermudah akses nasabah, seperti aplikasi untuk memesan nomor antrian, mesin otomatis untuk mencetak transaksi tabungan, hingga pembukaan rekening secara mandiri tanpa perlu datang langsung ke kantor cabang. Selain itu, kantor-kantor cabang perbankan juga mulai dioptimalkan melalui teknologi modern, yang tidak hanya meningkatkan kecepatan pelayanan tetapi juga mengurangi waktu tunggu nasabah. Digitalisasi perbankan ini diharapkan dapat menjadi solusi jangka panjang untuk menyelesaikan berbagai permasalahan operasional yang sering terjadi, sekaligus menunjukkan komitmen industri perbankan dalam berinvestasi pada inovasi teknologi demi masa depan yang lebih cerah. Dengan strategi ini, perbankan berupaya untuk terus relevan di tengah perubahan teknologi yang semakin cepat.[1]

Seiring dengan perluasan transformasi digital di sektor perbankan yang mencakup berbagai inovasi teknologi, tantangan baru berupa ancaman keamanan siber juga terus meningkat. Salah satu ancaman yang paling sering terjadi adalah *phishing*, sebuah kejahatan siber yang berkembang pesat di sektor perbankan. Dalam metode ini, data pribadi yang bersifat rahasia seringkali dicuri melalui penyamaran pelaku sebagai individu atau entitas tepercaya dalam pesan elektronik. Aktivitas phishing umumnya dikaitkan dengan teknik rekayasa sosial

[1] Mutiasari, A. I. (2020). PERKEMBANGAN INDUSTRI PERBANKAN DI ERA DIGITAL. JURNAL EKONOMI BISNIS DAN KEWIRAUSAHAAN, 9(2), 32–41.

yang dirancang untuk mengecoh korban agar secara tidak sengaja memberikan informasi penting. Praktik semacam ini telah diidentifikasi sebagai bentuk pelanggaran hukum berdasarkan Undang-Undang No. 19 Tahun 2016, yang merupakan revisi atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Dengan adanya regulasi tersebut, perlindungan terhadap sistem elektronik terus diperketat untuk menjaga integritas serta keamanan data dari ancaman seperti phishing.

Dampak yang ditimbulkan oleh phishing terhadap sektor perbankan dan nasabah tidak dapat dianggap remeh, mengingat kerugian yang bisa terjadi sangatlah signifikan. Dari sisi nasabah, serangan ini dapat menyebabkan hilangnya dana secara langsung, terutama jika data perbankan yang rahasia berhasil dicuri dan disalahgunakan. Sementara itu, bagi bank sebagai lembaga keuangan, kerugian reputasi menjadi ancaman serius yang dapat mengurangi tingkat kepercayaan masyarakat terhadap layanan yang disediakan. Ketika nasabah merasa tidak aman menggunakan layanan perbankan digital akibat risiko *phishing*, kepercayaan terhadap transformasi digital yang sedang dikembangkan pun dapat terganggu. Oleh karena itu, langkah-langkah preventif yang komprehensif sangat dibutuhkan untuk mengurangi risiko tersebut, baik dengan meningkatkan keamanan sistem elektronik maupun melalui edukasi kepada nasabah terkait praktik keamanan digital.[2]

Upaya perlindungan terhadap nasabah dan sistem perbankan dari ancaman *phishing* menjadi prioritas utama dalam era digitalisasi ini. Sistem keamanan berbasis teknologi terus dikembangkan oleh bank untuk mendeteksi dan mencegah serangan siber secara lebih efektif. Selain itu, edukasi kepada masyarakat menjadi bagian yang tidak kalah penting dalam menghadapi ancaman ini. Nasabah perlu diberikan pemahaman tentang cara mengenali potensi ancaman *phishing*, seperti kewaspadaan terhadap tautan atau pesan elektronik mencurigakan yang meminta informasi pribadi. Di sisi lain, regulasi yang diterapkan oleh pemerintah, termasuk sanksi tegas terhadap pelaku kejahatan siber, menunjukkan komitmen dalam melindungi sektor perbankan dari kejahatan berbasis teknologi. Dengan kombinasi langkah-langkah keamanan teknologi, edukasi, dan penegakan hukum yang kuat, diharapkan industri perbankan dapat terus berkembang tanpa mengabaikan aspek perlindungan terhadap ancaman *phishing* yang semakin kompleks. Oleh karena itu, penelitian ini akan berfokus pada analisis mengenai bagaimana ketentuan hukum terkait kejahatan *phishing* dalam sistem perbankan digital di Indonesia serta bagaimana bentuk perlindungan hukum yang diberikan kepada

[2] Akhmad Fery Hasanudin, & A Basuki Babussalam. (2024). Perlindungan Hukum Bagi Korban Kejahatan Phising Yang Menguras Saldo M-Banking. Jurnal Gagasan Hukum, 6(01), 16-29.

nasabah sebagai korban dari kejahatan tersebut dalam konteks layanan perbankan digital di Indonesia.

2. METODE PENELITIAN

Dalam penelitian ini, metode normatif kualitatif diterapkan dengan memanfaatkan bahan hukum primer, yaitu berbagai peraturan perundang-undangan yang memiliki relevansi langsung dengan topik penelitian. Selain itu, bahan hukum sekunder turut dimanfaatkan, termasuk berbagai literatur, buku-buku yang membahas ilmu hukum, artikel dari surat kabar, hasil penelusuran informasi melalui internet, serta jurnal ilmiah yang mendukung analisis.[3] Dengan memadukan metode analisis yang terstruktur dan sumber data yang relevan, penelitian ini diharapkan mampu menghasilkan kajian yang bersifat mendalam, terperinci, dan menyeluruh dalam menjawab permasalahan yang berkaitan dengan perkembangan perbankan digital.

3. HASIL DAN PEMBAHASAN

A. Ketentuan Hukum Kejahatan *Phishing* dalam Sistem Perbankan Digital di Indonesia

Dalam era perkembangan teknologi yang semakin pesat, digitalisasi telah menjadi bagian tak terpisahkan dari berbagai sektor, termasuk perbankan. Sistem perbankan digital, yang mengandalkan teknologi informasi untuk memberikan layanan perbankan secara online, dirancang untuk mempermudah transaksi finansial, mulai dari transfer uang hingga pengelolaan investasi. Namun, di balik kemudahan ini, ancaman kejahatan siber seperti *phishing* semakin marak terjadi. *Phishing* adalah upaya penipuan yang dilakukan dengan cara mengelabui korban agar memberikan informasi pribadi atau data sensitif, seperti nomor kartu kredit, kata sandi, atau identitas pribadi lainnya. Tindakan ini sering kali dilakukan melalui email, situs palsu, atau pesan yang tampak meyakinkan.

Fenomena *phishing* di sektor perbankan digital erat kaitannya dengan meningkatnya ketergantungan pada teknologi dan data elektronik. Ketika sistem digital menjadi tulang punggung transaksi keuangan, risiko kebocoran data pribadi pun meningkat. Pelaku *phishing* memanfaatkan celah keamanan atau kurangnya kesadaran pengguna untuk mencuri informasi yang kemudian disalahgunakan untuk keuntungan pribadi. Dalam konteks perbankan digital,

[3] Maulana, R. A., & Apriani, R. (2021). Perlindungan Yuridis Terhadap Data Pribadi Nasabah Dalam Penggunaan Elektronik Banking (E-Banking). Jurnal Hukum De'rechtsstaat, 7(2), 163–172.

data yang dicuri dapat berupa kredensial akun, informasi rekening, hingga data keuangan lainnya yang bersifat sangat sensitif. *Phising* bisa terjadi akibat dari perilaku transaksi ekonomi yang didasari dengan niat yang tidak baik serta lembaga perbankan yang belum bisa menjamin dan menjaga kerahasiaan pemilik dan terkait kepemilikan dana yang tersimpan di bank tersebut.

Dalam menghadapi ancaman phishing dan kejahatan siber lainnya, bank digital memiliki tanggung jawab besar untuk memastikan keamanan sistem mereka. Berdasarkan Peraturan Otoritas Jasa Keuangan (POJK) Nomor 11 Tahun 2022 tentang Penyelenggaraan Teknologi Informasi, bank digital diwajibkan untuk menerapkan tata kelola teknologi informasi yang baik dan menjaga ketahanan siber. Ketentuan Pasal 2 dan Pasal 21 dalam peraturan ini menegaskan bahwa bank digital harus menyediakan layanan yang aman, andal, dan bertanggung jawab sebagai langkah preventif terhadap risiko kejahatan seperti phishing dan peretasan. Jika bank melanggar ketentuan tersebut, sanksi administratif dapat dikenakan, mulai dari teguran tertulis hingga pembekuan kegiatan usaha tertentu, atau bahkan penurunan nilai tata kelola yang memengaruhi tingkat kesehatan bank.

Selain menjaga keamanan teknis, bank digital juga memiliki tanggung jawab untuk melindungi konsumen, sebagaimana diatur dalam POJK tentang Perlindungan Konsumen dan Masyarakat Sektor Jasa Keuangan. Pasal 21 ayat (1) POJK Penyelenggaraan Layanan Perbankan Digital mengharuskan bank digital menerapkan prinsip perlindungan konsumen, termasuk menangani pertanyaan dan pengaduan nasabah selama 24 jam. Ketika nasabah mengalami kerugian akibat layanan bank, tanggung jawab bank tidak hanya bersifat materiil, tetapi juga mencakup edukasi keuangan kepada nasabah.

Dalam upaya meningkatkan literasi keuangan, bank digital diwajibkan untuk melaksanakan program edukasi sebagaimana diatur dalam POJK Nomor 3 Tahun 2023 tentang Peningkatan Literasi dan Inklusi Keuangan. Bank harus mengintegrasikan program literasi keuangan ke dalam rencana tahunan mereka, bertujuan untuk meningkatkan pemahaman nasabah terhadap produk dan layanan perbankan digital. Bentuk edukasi ini dapat berupa sosialisasi yang melibatkan kerja sama dengan instansi pemerintah, akademisi, organisasi non-pemerintah, atau pihak lain yang memiliki visi serupa. Melalui langkah-langkah ini, bank digital tidak hanya memperkuat sistem keamanan mereka, tetapi juga membangun kesadaran masyarakat terhadap risiko dan perlindungan dalam layanan perbankan digital.[4]

[4] Chairunnisa, S., Murwadji, T., & Harrieti, N. (2024). Perlindungan Hukum Terhadap Nasabah atas Kejahatan Phising dan Hacking pada Layanan Bank Digital Ditinjau Berdasarkan Hukum Positif Indonesia. *Hakim: Jurnal Ilmu Hukum dan Sosial*, *2*(1), 01-16.

Tindakan yang dilakukan oleh pelaku *phising* tidak hanya sebatas memanipulasi situs web atau surel untuk menyesatkan korban, tetapi juga melibatkan penggunaan kebohongan dengan maksud menipu korban, yang pada akhirnya menyebabkan kerugian bagi korban. Kejahatan phishing dalam sistem perbankan digital dapat dianalisis melalui berbagai ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), mengingat karakteristik kejahatan ini yang melibatkan manipulasi dan penyalahgunaan sistem elektronik. Pasal 28 ayat (1) UU ITE menjerat tindakan distribusi atau transmisi informasi elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan yang mengakibatkan kerugian materiil bagi konsumen dalam transaksi elektronik. Tindak pidana ini dipidana sebagaimana diatur dalam Pasal 45A ayat (1), dengan ancaman pidana penjara maksimal enam tahun dan/atau denda maksimal satu miliar rupiah. Dalam konteks phishing, pelaku sering kali mengirimkan email atau pesan elektronik yang menyesatkan, seperti berpura-pura menjadi lembaga resmi untuk mengelabui korban agar memberikan data sensitif, seperti kredensial akun bank.

Jika pelaku melakukan manipulasi terhadap informasi elektronik agar data yang digunakan tampak otentik, maka tindakannya dapat dikenakan Pasal 35 jo. Pasal 51 UU ITE. Ancaman hukuman bagi tindakan ini mencapai 12 tahun penjara dan/atau denda maksimal Rp12 miliar, menunjukkan beratnya pelanggaran hukum karena mengancam kepercayaan terhadap sistem elektronik. Selain itu, apabila pelaku phishing menerobos sistem elektronik, seperti menggunakan identitas dan kata sandi korban tanpa izin, maka ia dapat dijerat Pasal 30 ayat (3) jo. Pasal 46 ayat (3) UU ITE. Ketentuan ini menegaskan bahwa tindakan ilegal terhadap sistem keamanan elektronik memiliki ancaman pidana maksimal delapan tahun penjara dan/atau denda hingga Rp 800 juta. Lebih lanjut, pelaku yang memindahkan atau mentransfer informasi elektronik, seperti mentransfer isi rekening korban ke akun lain tanpa hak, dapat dijerat Pasal 32 ayat (2) jo. Pasal 48 ayat (2). Tindakan ini merupakan bentuk lanjutan dari phishing yang bertujuan untuk memanfaatkan data korban secara ilegal, dengan ancaman pidana sembilan tahun penjara dan/atau denda maksimal Rp3 miliar.[5]

Dalam menangani kejahatan fraud phishing, Kitab Undang-Undang Hukum Pidana (KUHP) mengakomodasi kriminalisasi tindakan tersebut melalui pendekatan interpretasi ekstensif. Metode ini memungkinkan pasal-pasal dalam KUHP yang tidak secara eksplisit mengatur tentang kejahatan berbasis elektronik tetap dapat diterapkan dengan mengidentifikasi kesamaan unsur atau karakteristik tindak pidana yang relevan. Sebagai contoh, tindakan

[5] Ramadhanti, A. N., Tias, T. A., Lestari, E. D., & Hosnah, A. U. (2024). Cara Operasi Kejahatan Phising di Ranah Siber yang Diatur Oleh Hukum Positif Indonesia. *Jurnal Pendidikan Tambusai*, *8*(1), 1299-1305.

phishing yang terkait dengan pencurian data kartu kredit dapat dikualifikasikan sebagai tindak pidana pencurian sebagaimana diatur dalam Pasal 362 KUHP. Selain itu, tindak phishing yang dilakukan melalui pembuatan situs palsu untuk menipu korban dapat diproses sebagai tindak pidana penipuan berdasarkan Pasal 378 KUHP, yang mengatur tindakan memanfaatkan tipu muslihat untuk memperoleh keuntungan secara tidak sah. Kejahatan fraud phishing sering kali melibatkan lebih dari satu pelaku. Biasanya, tindak pidana ini dilakukan secara terorganisasi, di mana beberapa individu bekerja sama untuk melancarkan aksinya. Dalam situasi ini, KUHP juga menerapkan Pasal 363 ayat (4) yang memberikan pemberatan hukuman jika pencurian dilakukan oleh dua orang atau lebih secara bersama-sama. Selain itu, Pasal 55 KUHP tentang penyertaan dapat digunakan untuk menjerat semua pihak yang terlibat, baik mereka yang secara langsung melakukan tindakan, memberikan bantuan, atau memiliki peran lain yang mendukung pelaksanaan kejahatan tersebut.

Kemudian pasal 263 KUHP menegaskan sanksi hukum bagi tindak pidana pemalsuan surat, di mana pelaku memalsukan atau membuat surat palsu yang seolah-olah asli dan dapat digunakan untuk menimbulkan hak, kewajiban, atau pembebasan utang. Pasal ini juga mencakup penggunaan surat palsu tersebut dengan maksud untuk menipu orang lain, terutama jika tindakan itu mengakibatkan kerugian bagi pihak tertentu. Ancaman hukuman untuk tindak pidana ini adalah pidana penjara maksimal enam tahun, menunjukkan bahwa pemalsuan surat dipandang sebagai kejahatan serius yang merugikan aspek kepercayaan dalam hubungan hukum dan sosial. Dalam konteks kejahatan fraud phishing, Pasal 263 KUHP dapat diterapkan ketika pelaku membuat dokumen elektronik palsu, seperti email yang menyerupai komunikasi resmi dari bank atau institusi tertentu, dengan tujuan untuk menipu korban. Dokumen elektronik palsu ini dapat memuat informasi yang mengarahkan korban untuk menyerahkan data sensitif, seperti nomor rekening atau kata sandi, yang kemudian disalahgunakan oleh pelaku untuk mendapatkan keuntungan pribadi. Pasal ini relevan karena pemalsuan dalam bentuk dokumen fisik maupun elektronik memiliki dampak yang sama, yaitu menciptakan kerugian bagi korban dan mengganggu kepercayaan terhadap sistem administrasi, baik di ranah pribadi maupun institusional. Oleh karena itu, pelaku phishing yang membuat dan menggunakan dokumen elektronik palsu dapat dijerat dengan Pasal 263 KUHP, selain ketentuan dalam UU ITE. Dengan mengkombinasikan pasal-pasal ini, penegak hukum dapat

memberikan sanksi yang lebih komprehensif dan memastikan pelaku phishing bertanggung jawab atas seluruh tindakannya. [6]

Kejahatan pencurian data melalui layanan *online banking*, *mobile banking*, dan informasi nomor kartu kredit merupakan contoh kejahatan *fraud phishing* yang sering menargetkan lembaga perbankan. Bank menjadi sasaran utama para pelaku *phishing* (phisher) karena akses terhadap data nasabah dapat memberikan keuntungan finansial yang signifikan. Dalam menghadapi risiko ini, peraturan perundang-undangan di Indonesia telah menetapkan kewajiban bagi bank untuk melindungi data nasabahnya.

Salah satu ketentuan penting tercantum dalam Pasal 29 ayat (4) Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan yang telah diubah menjadi Undang-Undang Nomor 10 Tahun 1998. Pasal ini mewajibkan bank untuk memberikan informasi kepada nasabah mengenai potensi risiko kerugian yang dapat timbul akibat transaksi yang dilakukan melalui bank. Ketentuan ini bertujuan untuk melindungi kepentingan nasabah dan memastikan mereka memahami risiko yang mungkin terjadi, terutama karena hubungan antara bank dan nasabah didasarkan pada prinsip kepercayaan.

Selain itu, perlindungan terhadap data nasabah juga diatur dalam Pasal 40 ayat (1) dan (2) dari undang-undang yang sama, yang mewajibkan bank menjaga kerahasiaan informasi nasabah, termasuk data penyimpanan dan simpanannya. Kewajiban ini mencerminkan pentingnya menjaga privasi nasabah, mengingat bank memegang peran sebagai institusi yang dipercaya untuk mengelola dana masyarakat. Dengan adanya ketentuan ini, bank diharapkan dapat memastikan bahwa data nasabah tidak disalahgunakan atau diakses oleh pihak yang tidak berwenang, sehingga kepercayaan terhadap sistem perbankan tetap terjaga.[7]

Kejahatan *phishing* tidak hanya menjadi ancaman terhadap individu, tetapi juga terhadap kepercayaan masyarakat terhadap sistem perbankan digital secara keseluruhan. Oleh karena itu, penerapan hukum yang tegas, disertai dengan tata kelola teknologi informasi yang baik dan literasi keuangan yang memadai, menjadi kunci dalam mencegah dan menangani kasus phishing. Dengan landasan hukum yang ada, bank digital diharapkan mampu melindungi nasabah dari risiko kejahatan siber sekaligus memperkuat keandalan layanan mereka.

---

[6] 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.

[7] Tanonggi, J. T., Pusparini, I., Limbong, C. P., Thiffani, G., & Siagan, S. N. (2024). Tinjauan Hukum Terhadap Pertanggungjawaban Bank Kepada Data Nasabah Dalam Serangan Phishing. Indonesian Journal of Law, 1(6), 186-194.

B. Perlindungan Hukum Nasabah dari Kejahatan *Phishing* dalam Layanan Perbankan Digital di Indonesia

Transformasi menuju era digital dalam perkembangan industri telah membawa pengaruh signifikan di berbagai bidang yang berdampak pada kehidupan sehari-hari. Salah satu sektor industri yang mengalami perubahan besar adalah sektor perbankan. Sektor perbankan mencakup berbagai elemen penting, termasuk aspek kelembagaan, aktivitas bisnis, serta metode dan proses yang digunakan dalam pelaksanaan kegiatan bank. Hal ini sebagaimana diatur dalam Pasal 1 Ayat (1) Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan. Peraturan ini memberikan dasar hukum yang kuat bagi perbankan untuk menjalankan fungsi-fungsi mereka secara efisien dan adaptif terhadap perkembangan teknologi yang pesat. Bank merupakan lembaga yang dibangun atas dasar kepercayaan, sehingga dalam melaksanakan kegiatan *electronic banking (e-banking)* maupun layanan perbankan non-elektronik, bank harus senantiasa mematuhi ketentuan yang berlaku serta menerapkan prinsip kehati-hatian dan manajemen risiko.

Layanan *e-banking* memberikan kemudahan akses yang sangat besar bagi nasabah, memungkinkan mereka untuk melakukan transaksi keuangan tanpa perlu datang ke kantor bank secara langsung. Hal ini sangat bermanfaat, khususnya bagi pelaku usaha besar yang membutuhkan sistem yang efisien, mudah disesuaikan, aman, otomatis, terintegrasi, dan dapat diandalkan tanpa terikat oleh kendala ruang dan waktu. Namun demikian, hingga saat ini belum ada undang-undang yang secara eksplisit mengatur mengenai *e-banking*. Sebagai solusinya, UU No. 10 Tahun 1998 tentang Perubahan atas UU No. 7 Tahun 1992 tentang Perbankan dijadikan dasar hukum untuk penerapan e-banking. Pasal 5 Ayat (2) undang-undang ini menyatakan bahwa bank umum memiliki kewenangan untuk fokus pada kegiatan tertentu atau memberikan perhatian lebih pada sektor tertentu. Di samping itu, Pasal 6 huruf a juga mengatur bahwa bank umum diperbolehkan melakukan kegiatan lain yang pada umumnya dilakukan oleh bank, asalkan tidak bertentangan dengan ketentuan undang-undang dan peraturan yang berlaku. Meskipun layanan *e-banking* memberikan banyak kemudahan dan efisiensi, penerapannya tidak lepas dari berbagai tantangan, terutama terkait aspek keamanan.[8]

Dalam dunia digital, risiko keamanan data nasabah menjadi salah satu perhatian utama, mengingat meningkatnya kasus kejahatan siber yang memanfaatkan celah dalam sistem perbankan. Kejahatan ini tidak hanya berdampak pada kerugian finansial, tetapi juga pada

[8] Arif Wicaksana and Tahar Rachman, "Perlindungan Hukum Terhadap Pengguna Internet Banking (Mobile Banking) Dari Upaya Kejahatan Cyber," *Angewandte Chemie International Edition, 6(11), 951–952.* 3, no. 1 (2018): 10–27, https://medium.com/@arifwicaksanaa/pengertian-use-case-a7e576e1b6bf.

integritas dan reputasi layanan perbankan itu sendiri Salah satu bentuk kejahatan elektronik yang sering terjadi dalam transaksi perbankan adalah pencurian data nasabah melalui teknik phishing. Phishing, atau singkatan dari password harvesting fishing, merupakan tindakan penipuan yang menggunakan email atau situs web palsu dengan tujuan mengelabui pengguna sehingga pelaku dapat memperoleh data pribadi korban. Modus operandi ini biasanya dilakukan melalui pengiriman email yang tampak seolah-olah berasal dari perusahaan resmi, seperti bank. Email tersebut bertujuan untuk mencuri data sensitif seperti PIN, nomor rekening, nomor kartu kredit, dan informasi pribadi lainnya, yang nantinya dapat digunakan oleh pelaku untuk tindakan kejahatan lebih lanjut. Kejahatan *phishing* tidak hanya menyebabkan kerugian finansial bagi nasabah, tetapi juga mengancam kepercayaan publik terhadap keamanan layanan perbankan digital di Indonesia. Oleh karena itu, perlindungan hukum bagi nasabah menjadi sangat penting untuk memastikan keamanan dan kenyamanan penggunaan layanan perbankan digital.[9]

Kasus phishing dalam layanan mobile banking di Indonesia semakin beragam dan merugikan nasabah secara signifikan. Salah satu kasus yang viral pada Mei 2022 melibatkan seorang nasabah yang kehilangan Rp16,4 juta akibat tautan palsu yang menyerupai situs resmi bank. Korban diminta memasukkan data seperti username, PIN, dan OTP, yang digunakan pelaku untuk menguras rekeningnya. Selain itu, modus lain yang sering terjadi adalah penyebaran file PDF melalui WhatsApp. File ini mengandung malware yang mencuri data akun korban secara otomatis setelah dibuka, bahkan memungkinkan pelaku mengakses aplikasi m-banking korban tanpa sepengetahuannya.

Contoh lain dari kasus *phishing* yang marak terjadi adalah modus yang melibatkan file PDF palsu yang dikirim melalui WhatsApp. Korban menerima pesan berisi file PDF yang tampak resmi, tetapi sebenarnya berisi malware. Ketika file ini diakses, malware tersebut mulai menginfeksi perangkat korban, mencuri informasi pribadi seperti username, password, PIN, dan kode OTP mobile banking. Dalam beberapa kasus, malware juga mengaktifkan fitur akses jarak jauh sehingga pelaku bisa langsung melakukan transaksi melalui aplikasi m-banking korban tanpa diketahui.

Modus-modus ini menunjukkan betapa beragamnya ancaman phishing yang dapat menargetkan nasabah. Oleh karena itu, perlindungan hukum dan langkah mitigasi menjadi sangat penting. Bank harus memastikan sistem mereka kebal terhadap serangan siber dan aktif

[9] Maisah et al., "Analisis Hukum Terhadap Perlindungan Data Pribadi Nasabah Dalam Layanan Perbankan Digital Di Indonesia," *Aufklarung: Jurnal Pendidikan* 3, no. 3 (2023): 285–90.

memberikan edukasi kepada nasabah tentang modus-modus terbaru. Di sisi lain, nasabah juga perlu meningkatkan kewaspadaan, seperti menghindari klik tautan yang mencurigakan, tidak membagikan data sensitif, dan memeriksa keaslian aplikasi sebelum mengunduh. Kombinasi upaya dari kedua belah pihak sangat diperlukan untuk menghadapi ancaman ini secara efektif.

Secara prinsip, perlindungan yang diberikan oleh bank digital terhadap nasabahnya sejatinya memiliki dasar hukum yang sama dengan perlindungan konsumen sebagaimana diatur dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Dalam undang-undang tersebut dinyatakan bahwa "segala upaya yang menjamin adanya kepastian hukum untuk memberikan perlindungan kepada konsumen" adalah suatu kewajiban. Oleh karena itu, bank digital diwajibkan secara hukum untuk memastikan bahwa hak-hak nasabah dilindungi tanpa terkecuali. Pada tahun 2021, Otoritas Jasa Keuangan (OJK) mengambil langkah untuk mendukung pengembangan bank digital yang aman bagi nasabah dengan menerbitkan sejumlah kebijakan penting. Salah satunya adalah Peraturan OJK Nomor 12 Tahun 2018 tentang Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum. Selain itu, ada juga POJK Nomor 38 Tahun 2016 yang mengatur Penerapan Manajemen Risiko dalam penggunaan Teknologi Informasi oleh Bank Umum. Kebijakan-kebijakan ini bertujuan untuk memastikan bahwa layanan perbankan digital yang diselenggarakan oleh bank umum mampu memberikan perlindungan maksimal kepada nasabahnya, baik dalam aspek keamanan transaksi maupun perlindungan hukum.

Dalam konteks perlindungan data pribadi nasabah dalam penggunaan layanan perbankan digital di Indonesia, terdapat beberapa hak yang dijamin kepada nasabah. Hak-hak tersebut meliputi:[10]

1. Hak atas Keamanan Data Pribadi

   Nasabah berhak atas jaminan bahwa data pribadi yang dikumpulkan oleh bank dalam layanan perbankan digital akan dijaga keamanannya dari akses tidak sah atau penyalahgunaan. Bank diwajibkan menerapkan langkah-langkah keamanan yang memadai, seperti teknologi enkripsi dan otentikasi ganda, guna melindungi data nasabah. Ketentuan ini tertuang dalam Pasal 6 dan Pasal 21 Ayat (1) Peraturan OJK No. 12/POJK.03/2018.

[10] Ramadhanti Achlina Tri Putri Putri and Heru Sugiyono, "Tanggung Jawab Bank Terhadap Tindakan Phising Dalam Sistem Penggunaan E-Banking (Studi : Kasus Phising Pada Pt . Bank Rakyat Indonesia (PERSERO) TBK)," *Jurnal Interpretasi Hukum* 4, no. 3 (2023): 682–90.

2. Hak atas Informasi dan Transparansi

   Nasabah berhak memperoleh informasi yang lengkap dan transparan mengenai proses pengumpulan, penggunaan, penyimpanan, serta pengolahan data pribadi mereka oleh bank. Bank harus memberikan penjelasan yang memadai tentang kebijakan privasi, termasuk hak nasabah untuk memberikan atau menolak persetujuan atas penggunaan data mereka. Ketentuan ini dijelaskan dalam Pasal 26 Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016.

3. Hak untuk Mengajukan Pengaduan

   Jika nasabah merasa hak-haknya dilanggar atau terjadi pelanggaran kebijakan privasi oleh bank, mereka berhak mengajukan pengaduan. Bank dan Otoritas Jasa Keuangan (OJK) menyediakan mekanisme untuk menangani keluhan tersebut secara adil dan transparan. Hak ini dijamin dalam Pasal 29 Ayat (1) dan (2) Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016.

4. Hak atas Penghapusan Data

   Nasabah dapat meminta penghapusan data pribadi yang tidak lagi diperlukan oleh bank atau jika penggunaannya melanggar hukum atau kebijakan privasi. Bank wajib menindaklanjuti permintaan ini dalam jangka waktu yang ditentukan oleh regulasi. Hak ini tercantum dalam Pasal 25 Ayat (1) Huruf b Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016.

5. Hak untuk Menarik Persetujuan

   Nasabah berhak mencabut persetujuan terkait penggunaan data pribadi mereka. Setelah persetujuan dicabut, bank harus menghentikan penggunaan data tersebut kecuali ada kewajiban hukum yang mengharuskan data tetap digunakan.

Hak-hak tersebut dirancang untuk memastikan bahwa nasabah mendapatkan perlindungan yang memadai atas data pribadi mereka. Dengan demikian, layanan perbankan digital dapat berjalan dengan aman, transparan, dan memberikan kendali yang lebih baik kepada nasabah terkait data pribadi mereka.

Dalam konteks layanan perbankan digital, tanggung jawab bank terhadap tindakan phishing mencakup langkah preventif dan represif untuk melindungi nasabah dari potensi kerugian. Secara preventif, bank berkewajiban meningkatkan kesadaran nasabah melalui edukasi mengenai ancaman *phishing* dan cara pencegahannya. Bank juga menggunakan berbagai saluran komunikasi, seperti media sosial dan email, untuk memberikan informasi terkait keamanan transaksi elektronik. Selain itu, implementasi teknologi keamanan yang

canggih dan manajemen risiko yang komprehensif menjadi langkah penting dalam mengurangi risiko terkait teknologi informasi. Di sisi represif, bank memiliki tanggung jawab untuk menangani keluhan nasabah yang menjadi korban phishing. Penanganan ini dilakukan dengan memastikan proses penyelesaian yang efisien, termasuk melalui mekanisme pengaduan kepada otoritas terkait, seperti OJK, jika solusi internal tidak memadai. Namun, bank tidak bertanggung jawab atas kerugian yang disebabkan oleh kelalaian nasabah, seperti membagikan informasi pribadi kepada pihak tidak bertanggung jawab. Dalam kasus ini, tanggung jawab beralih kepada nasabah sendiri.

Bank memprioritaskan penyelesaian sengketa secara damai melalui negosiasi atau mediasi untuk menjaga hubungan baik dengan nasabah dan melindungi reputasi perusahaan. Mekanisme hukum tetap menjadi opsi jika penyelesaian damai tidak tercapai, memungkinkan nasabah menggugat bank di pengadilan atau melalui bantuan lembaga pengawas keuangan. Pendekatan ini menunjukkan upaya bank untuk menyeimbangkan perlindungan nasabah dengan penegakan tanggung jawab masing-masing pihak dalam menghadapi ancaman phishing. Berikut mekanisme penyelesaian hukum bagi nasabah yang menjadi korban phishing dalam layanan perbankan digital:[11]

1. Melaporkan ke Bank

   Langkah pertama yang harus dilakukan nasabah adalah segera melapor ke bank setelah menyadari adanya aktivitas mencurigakan atau kehilangan dana. Bank akan melakukan langkah-langkah berikut:

   a. Memblokir akses ke rekening nasabah untuk mencegah kerugian lebih lanjut.
   b. Melakukan investigasi internal untuk menentukan sumber masalah, apakah dari sistem bank atau akibat kelalaian nasabah.

2. Membawa Bukti Kerugian

   Nasabah harus menyediakan bukti-bukti seperti riwayat transaksi mencurigakan, tangkapan layar pesan phishing, atau bukti bahwa nasabah tidak memberikan data secara langsung kepada pihak ketiga. Bukti ini penting untuk menentukan apakah bank memiliki tanggung jawab atas kerugian tersebut.

[11] Lis Julianti, "Tanggung Jawab Hukum Pihak Perbankan Dalam Pencurian Data Pribadi Nasabah Dengan Tekhnik 'Phising'Pada Transaksi Perbankan," *Prosiding Seminar Nasional FH Universitas Mahasaraswati Denpasar*, 2021, 144–59.

3. Mediasi melalui OJK atau BI

   Apabila nasabah tidak puas dengan respons bank, mereka dapat mengajukan pengaduan ke Otoritas Jasa Keuangan (OJK) melalui Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan (LAPS SJK). OJK akan memediasi antara nasabah dan bank untuk mencapai penyelesaian yang adil. Alternatif lain, nasabah dapat melapor ke Bank Indonesia (BI) jika permasalahan terkait dengan sistem pembayaran.

4. Tuntutan Hukum

   Jika mediasi tidak membuahkan hasil, nasabah dapat menempuh jalur hukum, baik melalui gugatan perdata atas dasar wanprestasi (Pasal 1239 KUHPerdata) maupun gugatan berdasarkan UU Perlindungan Konsumen atau UU PDP.

5. Laporan ke Aparat Penegak Hukum

   Dalam kasus dimana pelaku *phishing* berhasil diidentifikasi, nasabah dapat melaporkan kasus ini kepada polisi berdasarkan Pasal 30 dan Pasal 32 UU ITE untuk menuntut pelaku secara pidana.

Meski berbagai regulasi telah hadir, tantangan utama dalam penanganan kasus phishing adalah pelaksanaan dan penegakan hukum yang masih memiliki celah. Banyak kasus phishing sulit diungkap karena pelaku seringkali berada di luar negeri atau menggunakan teknologi canggih yang sulit dilacak. Selain itu, tidak semua nasabah memiliki kesadaran penuh tentang pentingnya menjaga keamanan data pribadi mereka. Misalnya, banyak nasabah yang masih terjebak oleh email atau pesan palsu yang terlihat sangat meyakinkan. Oleh karena itu, upaya preventif harus menjadi prioritas. Bank perlu secara aktif mengedukasi nasabah melalui kampanye publik tentang bahaya *phishing* dan cara mengenali serta menghindari modus-modus yang umum digunakan pelaku.

Dalam menghadapi kejahatan phishing, peran aktif masyarakat juga tidak kalah penting. Nasabah perlu meningkatkan literasi digital mereka agar lebih waspada terhadap ancaman phishing. Pemerintah dan bank dapat bekerja sama dalam mengembangkan program edukasi literasi digital yang ditujukan untuk masyarakat umum, termasuk memberikan simulasi dan pelatihan tentang cara mengidentifikasi upaya *phishing*. Dengan begitu, nasabah tidak hanya menjadi objek perlindungan hukum, tetapi juga subjek yang aktif dalam melindungi diri mereka sendiri dari kejahatan *phishing*.

4. KESIMPULAN

Dari uraian pembahasan diatas dapat disimpulkan bahwa artikel ini mengulas perlindungan hukum bagi nasabah terhadap kejahatan phishing dalam layanan perbankan digital di Indonesia. Digitalisasi sektor perbankan yang dipicu oleh Revolusi Industri 4.0 membawa kemudahan dan efisiensi dalam transaksi keuangan, terutama melalui layanan seperti *internet banking* dan *mobile banking*. Namun, perubahan ini juga meningkatkan risiko kejahatan siber, salah satunya *phishing*, yaitu modus penipuan dengan cara mencuri data sensitif nasabah seperti PIN, password, atau nomor rekening melalui situs palsu, email, atau pesan elektronik yang menyerupai pihak resmi. Beberapa kasus di Indonesia menunjukkan modus yang beragam, seperti penggunaan tautan palsu yang menyerupai situs bank hingga penyebaran *malware* melalui file PDF, yang dapat mencuri data nasabah secara otomatis.

Dalam kerangka hukum, kejahatan *phishing* diatur dalam UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE), yang merupakan revisi dari UU No. 11 Tahun 2008. Pasal-pasal penting seperti Pasal 28 ayat (1) mengatur tentang larangan penyebaran informasi elektronik yang menyesatkan, sementara Pasal 30 ayat (3) dan Pasal 35 jo. Pasal 51 ayat (1) memberikan sanksi terhadap akses ilegal dan pemalsuan data elektronik dengan ancaman hukuman hingga 12 tahun penjara atau denda maksimal Rp12 miliar. Selain itu, ketentuan dalam KUHP, seperti Pasal 362 dan 378 tentang pencurian dan penipuan, serta Pasal 263 tentang pemalsuan dokumen, juga dapat diterapkan untuk menjerat pelaku *phishing*.

Perlindungan hukum bagi nasabah juga didukung oleh regulasi perbankan, seperti UU No. 10 Tahun 1998 tentang Perbankan, yang mewajibkan bank menjaga kerahasiaan data nasabah (Pasal 40 ayat (1) dan (2)) dan memberikan edukasi mengenai risiko transaksi digital (Pasal 29 ayat (4)). Selain itu, POJK No. 12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital dan POJK No. 11 Tahun 2022 tentang Tata Kelola Teknologi Informasi mewajibkan bank untuk menerapkan sistem keamanan berbasis teknologi, melaksanakan literasi keuangan, dan menyediakan layanan pengaduan yang responsif. Edukasi kepada nasabah juga menjadi fokus dalam POJK No. 3 Tahun 2023 tentang Literasi dan Inklusi Keuangan, di mana bank diwajibkan melibatkan masyarakat dalam program literasi guna meningkatkan pemahaman terhadap risiko phishing dan keamanan transaksi digital.

Dengan dasar hukum yang kuat, seperti UU ITE, KUHP, dan berbagai regulasi OJK, upaya melindungi nasabah dari kejahatan *phishing* terus diperkuat. Namun, tanggung jawab tidak hanya berada pada pihak bank yang harus memastikan keamanan sistem dan memberikan edukasi, tetapi juga pada nasabah yang perlu meningkatkan literasi digital dan kewaspadaan. Kombinasi langkah preventif, penegakan hukum yang tegas, dan kolaborasi antara pemerintah,

bank, serta masyarakat diharapkan mampu menciptakan layanan perbankan digital yang aman dan terpercaya di Indonesia.

SARAN

Berdasarkan pembahasan dalam artikel, diperlukan langkah-langkah strategis untuk memperkuat perlindungan hukum bagi nasabah terhadap kejahatan phishing dalam layanan perbankan digital. Pertama, bank perlu meningkatkan keamanan sistem informasi mereka dengan teknologi canggih, seperti enkripsi data, otentikasi multi-faktor, dan deteksi aktivitas mencurigakan secara otomatis. Selain itu, literasi digital nasabah harus menjadi prioritas melalui program edukasi yang berkesinambungan. Bank dapat menggunakan media sosial, email, dan aplikasi *mobile banking* sebagai platform untuk memberikan informasi tentang modus *phishing* dan cara pencegahannya. Selanjutnya, pemerintah perlu memastikan implementasi hukum yang efektif dengan memperkuat koordinasi antara lembaga penegak hukum dan regulator keuangan untuk menangani kasus *phishing* secara cepat dan menyeluruh.

Di sisi lain, nasabah juga harus dilibatkan secara aktif dalam melindungi data pribadi mereka. Pemerintah dan lembaga perbankan dapat berkolaborasi untuk mengadakan pelatihan atau simulasi tentang cara mengenali dan menghindari upaya *phishing*. Selain itu, pengawasan terhadap aktivitas perbankan digital perlu ditingkatkan, terutama dalam mengidentifikasi celah keamanan yang dapat dimanfaatkan oleh pelaku kejahatan. Regulasi yang ada, seperti UU ITE dan POJK terkait, perlu ditinjau secara berkala untuk menyesuaikan dengan perkembangan teknologi dan modus kejahatan yang semakin kompleks. Dengan sinergi antara bank, pemerintah, dan masyarakat, diharapkan risiko kejahatan *phishing* dapat diminimalkan, sehingga kepercayaan terhadap layanan perbankan digital dapat terus meningkat.

5. DAFTAR PUSTAKA

Akhmad Fery Hasanudin, & A Basuki Babussalam. (2024). Perlindungan Hukum Bagi Korban Kejahatan Phising Yang Menguras Saldo M-Banking. Jurnal Gagasan Hukum, 6(01), 16-29. https://doi.org/10.31849/jgh.v6i01.18827

Chairunnisa, S., Murwadji, T., & Harrieti, N. (2024). Perlindungan Hukum Terhadap Nasabah atas Kejahatan Phising dan Hacking pada Layanan Bank Digital Ditinjau Berdasarkan Hukum Positif Indonesia. Hakim: Jurnal Ilmu Hukum dan Sosial, 2(1), 01-16.

Julianti, Lis. "Tanggung Jawab Hukum Pihak Perbankan Dalam Pencurian Data Pribadi Nasabah Dengan Tekhnik 'Phising' Pada Transaksi Perbankan." *Prosiding Seminar Nasional FH Universitas Mahasaraswati Denpasar*, 2021, 144–59.

Maisah, Sinta Pala Sari, Sudiarni, and Himsar Pariaman Ompusunggu. "Analisis Hukum Terhadap Perlindungan Data Pribadi Nasabah Dalam Layanan Perbankan Digital Di Indonesia." *Aufklarung: Jurnal Pendidikan* 3, no. 3 (2023): 285–90.

Maulana, R. A., & Apriani, R. (2021). Perlindungan Yuridis Terhadap Data Pribadi Nasabah Dalam Penggunaan Elektronik Banking (E-Banking). Jurnal Hukum De'rechtsstaat, 7(2), 163–172.

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

Putri, Ramadhanti Achlina Tri Putri, and Heru Sugiyono. "Tanggung Jawab Bank Terhadap Tindakan Phising Dalam Sistem Penggunaan E-Banking (Studi : Kasus Phising Pada Pt . Bank Rakyat Indonesia (PERSERO) TBK)." *Jurnal Interpretasi Hukum* 4, no. 3 (2023): 682–90.

Ramadhanti, A. N., Tias, T. A., Lestari, E. D., & Hosnah, A. U. (2024). Cara Operasi Kejahatan Phising di Ranah Siber yang Diatur Oleh Hukum Positif Indonesia. Jurnal Pendidikan Tambusai, 8(1), 1299-1305.

Tanonggi, J. T., Pusparini, I., Limbong, C. P., Thiffani, G., & Siagan, S. N. (2024). Tinjauan Hukum Terhadap Pertanggungjawaban Bank Kepada Data Nasabah Dalam Serangan Phishing. Indonesian Journal of Law, 1(6), 186-194.

Wicaksana, Arif, and Tahar Rachman. "Perlindungan Hukum Terhadap Pengguna Internet Banking (Mobile Banking) Dari Upaya Kejahatan Cyber." *Angewandte Chemie International Edition, 6(11), 951–952.* 3, no. 1 (2018): 10–27. https://medium.com/@arifwicaksanaa/pengertian-use-case-a7e576e1b6bf.

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.