Cerdika: Jurnal Ilmiah Indonesia, April 2025, 5 (4), 1641-1654
p-ISSN: 2774-6291 e-ISSN: 2774-6534

Available online at http://cerdika.publikasiindonesia.id/index.php/cerdika/index

ANALISIS TANGGUNG JAWAB HUKUM TERHADAP KEAMANAN PERBANKAN DAN NASABAH DALAM KASUS PHISHING

Putu Davis Justin Thenata[1], Ryan Jovan Susanto[2], Jeanette Olivia Kurniawati[3], Jessica Carol Lee[4]
Universitas Pelita Harapan, Indonesia
Email: Davistheata@gmail.com, nicholas.rjs15@gmail.com, jeanetteolivia07@gmail.com, jccleee@gmail.com

Abstrak
Phishing merupakan bentuk kejahatan siber yang kian berkembang seiring dengan kemajuan teknologi, khususnya dalam sektor perbankan. Kejahatan ini dilakukan dengan cara menyamar sebagai entitas terpercaya, seperti pihak bank, guna menipu korban agar memberikan informasi pribadi yang bersifat rahasia, seperti nomor rekening, PIN, atau kata sandi. Serangan phishing sangat merugikan nasabah karena dapat menyebabkan kebocoran data dan kerugian finansial. Oleh karena itu, upaya pencegahan phishing harus melibatkan kebijakan perlindungan hukum yang tegas serta peningkatan literasi digital di kalangan nasabah. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan. Sumber data diperoleh dari bahan hukum primer dan sekunder seperti undang-undang, jurnal hukum, dan dokumen resmi terkait perlindungan konsumen dan keamanan siber. Hasil penelitian menunjukkan bahwa perlindungan hukum terhadap nasabah korban phishing belum optimal. Pengaturan yang lebih spesifik dan sanksi terhadap pelaku phishing perlu diperkuat, serta mekanisme penyelesaian sengketa bagi nasabah harus disosialisasikan secara lebih luas. Nasabah harus diberikan hak untuk menyelesaikan masalah melalui mekanisme penyelesaian langsung dengan bank, jalur hukum formal, maupun lembaga penyelesaian sengketa konsumen. Implikasi dari penelitian ini menunjukkan bahwa perlindungan hukum terhadap phishing di sektor perbankan harus ditingkatkan melalui regulasi yang komprehensif dan pendidikan berkelanjutan kepada masyarakat untuk menciptakan sistem perbankan yang aman dan terpercaya.

Kata kunci: Phising, Keamanan Perbankan, UU ITE

Abstract
Phishing is a form of cybercrime that continues to evolve alongside advancements in technology, particularly within the banking sector. This crime involves perpetrators disguising themselves as trusted entities, such as banks, to deceive victims into providing confidential personal information, including account numbers, PINs, or passwords. Phishing attacks are highly detrimental to customers, often resulting in data breaches and financial losses. Therefore, preventive measures must include the enforcement of legal protections and the enhancement of digital literacy among customers. This research employs a normative legal research method using a statutory approach. Data sources are drawn from primary and secondary legal materials, including legislation, legal journals, and official documents related to consumer protection and cybersecurity. The findings indicate that legal protection for bank customers who fall victim to phishing remains suboptimal. There is a need for more specific regulatory frameworks and stricter sanctions against phishing perpetrators. Additionally, accessible and well-publicized dispute resolution mechanisms should be available for victims—whether through direct resolution with the bank, formal legal action, or alternative dispute resolution bodies. The implications of this study highlight the urgent necessity of strengthening legal safeguards against phishing in the banking sector through comprehensive regulations and ongoing public education efforts, thereby fostering a secure and trustworthy financial environment.
***Keywords**: Phishing, Banking Security, ITE Law*

**Correspondence Author: Putu Davis Justin Thenata*
Email: Davistheata@gmail.com

PENDAHULUAN

Beralihnya masa kemajuan digital membuat perkembangan industri juga memberikan dampak yang signifikan terhadap bidang yang berlaku untuk kehidupan sehari-hari salah satunya adalah sektor perbankan dan keuangan (Aris, 2019; Handayani et al., 2023; SE & Sugiyono, 2021). Perubahan yang terjadi akan memberikan dampak yang positif terhadap masyarakat dan perekonomian secara keseluruhan namun di sisi lain harus dikelola secara hati-hati karena urusan perbankan ini mencakup seluruh Sisi kelembagaan diantaranya yang Aktivitas bisnis dan metode yang ditetapkan dalam pelaksanaan kegiatan bank seperti yang dijelaskan di dalam Pasal 1 Ayat 1 Undang-Undang Nomor 10 Tahun 1998 Tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan (Rohaedi, 2021). Transaksi elektronik perbankan atau biasa disebut dengan elektronik banking merupakan gambaran dari pelaksanaan perkembangan teknologi informasi pada sisi perbankan di Indonesia (Aqil et al., 2022; Dwicky Cahyadi, 2019; Gulo et al., 2021; Mamesah, 2022; Rahmanto, 2019; Sumadi, 2016). Layanan e-banking dapat memberikan akses yang sangat memudahkan bagi nasabah karena mereka melakukan transaksi tersebut tanpa harus mengunjungi kantor bank (Firdaus & Sjahruddin, 2021; Hafizhah & Rosa, 2022; Ristiana & Widyastuti, 2022; P. R. Saputra & Wahyuningtyas, 2020; Winduwiratsoko, 2018).

Di dalam ketentuan Undang-Undang Nomor 10 Tahun 1998 Tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan dijadikan sebagai dasar hukum untuk memberlakukan elektronik banking. Tempat pada Pasal 5 Ayat 2 Di Undang-Undang ini dinyatakan bahwa bank umum memiliki kemampuan untuk mengkhususkan diri dalam pelaksanaan kegiatan tertentu atau memberikan perhatian yang lebih besar kepada sektor kegiatan tertentu. Selain itu juga pada Pasal 6 huruf a menjelaskan bahwa bank umum berhak untuk melakukan sejumlah kegiatan yang biasa dilakukan oleh pihak bank selama itu tidak bertentangan dengan ketentuan undang-undang yang diberlakukan di Indonesia. Bank juga diharuskan untuk membuat kebijakan dan melakukan serta menjalankan operasionalnya dengan ditingkat baik sesuai dengan peraturan perundang-undangan dan bank juga memiliki kemampuan untuk memberikan perlindungan hukum atau tanggung jawab kepada nasabah sebagai konsumen mereka sebelum ataupun sesudah terjadinya kejahatan selama transaksi yang berkaitan dengan bank.

Adanya pengaruh teknologi terhadap produk perbankan menjadi tanda bukti bahwa dunia perbankan telah mengalami perubahan ke dalam era digital yang biasa disebut financial teknologi (A, 2022; Rosita, 2020; M. A. D. Saputra et al., 2023). Hal ini memberikan dampak yang baik dan bermanfaat bagi transaksi yang dilakukan oleh masyarakat Misalnya saja akan memberikan kemudahan pada transaksi pembukaan rekening atau penyimpanan dana tabungan juga transaksi e-*commerce* yang dapat dilakukan dengan media digital. Untuk penyimpanan dana tabungan secara digital maka pihak bank harus menyiapkan layanan berupa m-banking yang Dalam penggunaannya nasabah harus menyetujui dahulu beberapa persyaratan dan ketentuan yang muncul pada aplikasi yang menjadi perjanjian baku dan mengikat para pihak antara nasabah dan pihak bank. Setiap perubahan dan perkembangan teknologi perbankan pasti akan menimbulkan beberapa permasalahan baru karena harus menyesuaikan kebijakan-kebijakan perusahaan. Pesatnya teknologi juga harus disesuaikan dan dimanfaatkan oleh bank dengan terus melakukan perbaikan dan perlindungan karena kemungkinan untuk terjadinya serangan dari pihak luar

untuk mencari resiko dan kelemahan bank karena kejahatan pada bidang perbankan semakin kompleks dan berinovasi dan yang banyak terjadi di masa sekarang adalah kejahatan *phishing*.

Phishing merupakan sebuah kejahatan peretasan yang berkembang seiring berjalannya waktu pada sektor perbankan. Phishing melibatkan kegiatan kriminal yang mana pelaku menyamar sebagai pihak yang terpercaya dan mengirimkan pesan elektronik dengan tujuan untuk mencari data pribadi yang sifatnya rahasia. Di dalam ketentuan Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dijelaskan bahwa setiap orang dilarang untuk dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer atau sistem elektronik dengan cara apapun yang melibatkan pelanggaran, penetrasi, atau membobol sistem keamanan. Maka kejahatan phishing ini yang dianggap sebagai sebuah tindakan kriminal telah melanggar hukum akan dijerat hukuman 8 tahun penjara atau denda sebesar Rp.800.000 000; (delapan ratus juta rupiah).

Kejahatan phishing ini selalu memanipulasi masyarakat dengan menyamar sebagai pihak bank kepada nasabah untuk mendapatkan informasi berupa nama lengkap nomor handphone, email ataupun rincian kartu kredit dengan tujuan memancing korban untuk menekan link yang dikirimkan. Kejahatan seperti ini jelas melanggar ketentuan Pasal 30 Ayat 3 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Nasabah yang menjadi korban dari tindakan phishing ini hampir tidak memiliki kekuatan untuk menggugat ganti rugi kepada pihak bank jika dana mereka hilang karena kesalahan pada mereka telah secara sukarela memberikan data pribadi yang sensitif kepada pelaku phising sehingga bank tidak memiliki tanggung jawab untuk mengganti kerugian karena kelalaian dilakukan oleh pihak nasabah. Para pelaku phising biasanya akan menyamar sebagai karyawan bank dan terus mencari kelemahan dan ketidaktahuan korban atas suatu informasi supaya korban tidak memiliki pilihan lain selain mengikuti instruksi yang diberikan oleh pelaku *phishing*.

Proses dari manajemen risiko yang dilakukan oleh bank dituntut harus sesuai dengan kebijakan yang telah ditentukan di dalam Peraturan Otoritas Jasa Keuangan nomor 18 Tahun 2016 tentang Penerapan Manajemen Risiko Bank Umum yang diatur di dalam Pasal 15 Ayat 1 huruf (a) POJK yang menjelaskan bahwa bank memiliki kewajiban dan tanggung jawab untuk melaksanakan sistem pengendalian terhadap seluruh jenjang organisasi bank dengan tingkat resiko yang melekat pada usahanya supaya bank mudah mendeteksi kelemahan atau kemungkinan penyimpangan-penyimpangan yang bisa saja terjadi. Maka untuk melaksanakan sistem elektronik pihak bank harus menjalankan sebuah sistem elektronik dengan tanggung jawab dan kewajiban untuk mengoperasikan sistem elektronik sesuai dengan persyaratan yaitu melindungi otentifikasi dan kerahasiaan informasi elektronik dari nasabah yang diatur di dalam Pasal 15 dan 16 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang bertujuan untuk memastikan bahwa pihak bank tidak lalai dalam menjaga sistem elektronik yang mereka miliki.

Jika melihat dan menilai dari segala aspek maka kejahatan phishing ini bukan masalah yang dapat disepelekan karena melihat dari dampaknya yang sangat merugikan secara finansial ataupun mengurangi kepercayaan masyarakat terhadap lembaga keuangan di Indonesia. Nasabah yang menjadi korban phishing ini akan kehilangan dana mereka dan bank selaku lembaga keuangan akan kehilangan reputasi mereka. Melihat ini semua maka

tanggung jawab pihak bank sebagai lembaga keuangan yang dipercaya oleh masyarakat dan banyak digunakan biasanya harus melakukan tindakan yang serius terhadap kejahatan phishing ini serta memberikan perlindungan nasabah dari segala kemungkinan serangan phishing. Penelitian ini dilakukan untuk dapat menjadi kontribusi di dalam pengembangan teori hukum dan implikasi dalam membantu lembaga keuangan seperti bank ataupun otoritas pengawas dalam memberikan upaya perlindungan terhadap nasabah dari ancaman phishing yang dapat mempengaruhi dan mengurangi kepercayaan nasabah kepada pelayanan bank. Selain itu penelitian ini juga menganalisa perlindungan hukum terhadap nasabah yang berfokus untuk memahami kerangka hukum yang diberikan oleh pemerintah Indonesia dalam menjamin perlindungan kepada nasabah dalam hal transaksi perbankan digital dan juga perlindungan hukum yang diberikan oleh pihak bank terhadap tindakan phishing.

Penelitian mengenai kejahatan phishing dalam sektor perbankan telah banyak dilakukan, salah satunya oleh Prabowo dan Purwanto (2020) yang menekankan pentingnya literasi digital sebagai bentuk preventif terhadap ancaman phishing di Indonesia. Selain itu, studi oleh Rachman dan Sari (2021) mengkaji efektivitas regulasi perlindungan data pribadi dalam mencegah kejahatan siber di sektor finansial, khususnya dalam konteks perbankan digital. Namun, penelitian ini menghadirkan kebaruan dengan secara khusus menyoroti keterkaitan langsung antara regulasi yang ada, seperti POJK No. 18/2016 dan UU ITE, serta tanggung jawab hukum lembaga keuangan terhadap nasabah yang menjadi korban phishing, tidak hanya dari perspektif literasi, tetapi juga dari aspek akuntabilitas lembaga dan perlindungan hukum yang operasional. Fokus ini memperluas cakupan dari pendekatan preventif menuju pendekatan yuridis-responsif yang konkret terhadap kasus phishing.

Penelitian ini bertujuan untuk mengkaji tanggung jawab hukum bank terhadap kejahatan phishing dalam layanan digital banking serta mengevaluasi efektivitas perlindungan hukum yang diberikan kepada nasabah berdasarkan regulasi yang berlaku di Indonesia. Manfaat penelitian ini secara teoritis adalah memperkaya literatur hukum di bidang perlindungan konsumen perbankan digital dan mendorong pembentukan kerangka hukum yang lebih adaptif terhadap ancaman siber. Secara praktis, hasil penelitian ini diharapkan dapat menjadi masukan bagi perbankan, OJK, dan pemerintah dalam merumuskan kebijakan penguatan keamanan digital dan perlindungan hukum yang lebih komprehensif terhadap nasabah, guna membangun kepercayaan publik terhadap sistem perbankan nasional.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis normatif dengan metode analisis kualitatif. Pendekatan normatif dipilih karena fokus penelitian adalah menganalisis aturan hukum, asas hukum, dan doktrin hukum yang relevan terhadap perlindungan hukum nasabah dalam kasus kejahatan phishing di sektor perbankan. Metode ini bertujuan untuk mengkaji norma-norma hukum positif yang tertuang dalam peraturan perundang-undangan serta menginterpretasikan ketentuan tersebut dalam konteks praktik keuangan digital saat ini.

Proses analisis dilakukan melalui tahapan telaah literatur hukum yang mendalam, yang meliputi identifikasi isu hukum, pengumpulan bahan hukum primer dan sekunder, interpretasi hukum menggunakan pendekatan gramatikal, sistematis, dan teleologis, serta penarikan kesimpulan yang argumentatif dan logis. Bahan hukum primer dalam penelitian ini mencakup Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, dan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Selain itu,

digunakan pula Peraturan OJK Nomor 18 Tahun 2016 tentang Penerapan Manajemen Risiko Bank Umum sebagai dasar penilaian tanggung jawab perbankan.

Sementara itu, bahan hukum sekunder terdiri atas literatur akademik, jurnal hukum, hasil penelitian sebelumnya, serta artikel ilmiah yang relevan dari database seperti Google Scholar. Teknik pengumpulan data dilakukan secara studi kepustakaan (library research), dengan seleksi sumber berdasarkan relevansi, otoritas, dan aktualitas. Analisis data dilakukan secara deskriptif-analitis dengan menekankan argumentasi hukum untuk mengungkapkan kejelasan posisi hukum serta tanggung jawab lembaga perbankan dalam menangani dan mencegah kejahatan phishing secara efektif.

HASIL DAN PEMBAHASAN

Cyber Crime Phising

Cybercrime merupakan sebuah tindakan yang dilakukan oleh seorang pelaku kejahatan menggunakan kecanggihan teknologi komputer dan jaringan internet dengan tujuan untuk melakukan sebuah penyerangan sistem informasi kepada korbannya. Contoh dari tindakan ini misalnya adalah membobol perangkat teknologi dan data-data pribadi dari seorang korban dan mengambil isi saldo pada m-banking atau kartu kredit korban. Pengaturan tentang hal ini ditegaskan di dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang telah diubah menjadi Undang-Undang Nomor 19 Tahun 2016 yang menjelaskan bahwa cybercrime merupakan:

1) Setiap orang yang dengan maksud sengaja meski tanpa hak telah melakukan melawan hukum dengan mengakses komputer atau sistem elektronik kepunyaan orang lain dengan cara apapun
2) Setiap orang yang sengaja dan tanpa adanya hak melakukan melawan hukum mengakses komputer atau sistem elektronik dengan cara apapun dengan tujuan memperoleh informasi elektronik atau dokumen elektronik milik orang lain
3) Setiap orang yang dengan sengaja dan tanpa adanya ha telah melakukan melawan hukum dengan mengakses komputer atau sistem elektronik dengan cara yang melanggar menerobos melampaui atau menjebol sistem pengamanan milik seseorang

Salah satu bentuk kejahatan cybercrime adalah phishing yang telah banyak merugikan masyarakat secara keseluruhan karena memiliki dampak kerugian secara materi karena terjadinya pencurian data atau informasi perbankan yang dapat menyebabkan masalah jangka panjang seperti rusaknya reputasi ataupun kesulitan untuk mengakses layanan keuangan serta juga dapat mengurangi kepercayaan masyarakat terhadap transaksi digital sehingga memperlambat teknologi baru. Phising adalah kejahatan yang menggunakan pemalsuan data pada sebuah situs web palsu yang sangat mirip sekali dengan situs aslinya dengan tujuan untuk memperoleh identitas atau data orang lain dan menggunakannya secara ilegal tanpa sepengetahuan pemiliknya. Kejahatan ini dilakukan dengan cara menipu yang dilakukan oleh penjahat untuk mendapatkan data pribadi seperti kata sandi atau kode nomor atau informasi sensitif lainnya melalui penyamaran menjadi seseorang dari pihak lembaga keuangan dengan cara mengirim pesan palsu yang sama persis dengan email atau teks resmi yang biasanya berisi sebuah tautan untuk mengarahkan korban kepada sebuah situs web palsu yang meniru situs resmi.

Di Indonesia sendiri kejahatan phishing ini telah diatur secara tegas di dalam undang-undang informasi dan transaksi elektronik tepatnya pada Pasal 30 dijelaskan bahwa untuk mencegah penggunaan informasi atau dokumen elektronik palsu yang dapat

menyesatkan dan merugikan pihak lain maka pemerintah memberikan landasan hukum untuk dapat menindaklanjuti pelaku yang dengan sengaja melakukan sebuah tindakan tersebut sehingga pengaksesan ilegal dapat dilarang terhadap sebuah sistem komputer yang mengakibatkan kerugian kehilangan kerusakan atau perubahan data elektronik milik seseorang. Pelaku kejahatan phishing dapat dikenai sanksi pidana kurungan atau denda sebagaimana yang diatur di dalam Pasal 28 dan Pasal 30 yang melarang akses ilegal terhadap sistem komputer milik orang lain ataupun perbuatan lainnya yang mengakibatkan penghilangan perusakan perubahan data elektronik akan dihukum pidana kurungan atau denda yang akan disesuaikan dengan tingkat kerusakan setiap kasus. Maka harus dipahami bahwa pemberlakuan hukum ini disesuaikan dengan penilaian Hakim terlebih dahulu dan kebijakan penegakan hukum yang diberlakukan di wilayah Indonesia.

Kejahatan phishing di internet banking adalah suatu ancaman yang menggunakan metode rekayasa sosial untuk menipu penggunanya agar tertarik dengan penawaran melalui pesan singkat ataupun email dari seorang pelaku yang menyamar sebagai karyawan bank dan bertujuan untuk mengajak nasabah untuk memberikan rahasia data pribadi dalam penggunaan bank. Beberapa penyebab yang mungkin menjadi dasar adanya ancaman fisik yaitu pengguna menggunakan layanan perbankan online masih minim kesadaran sehingga pengguna terus menjadi target incaran para penjahat phising yang mungkin bisa disebabkan beberapa faktor diantaranya yaitu masih kurangnya edukasi dan literasi digital kepada masyarakat yang membuat mereka tidak mengetahui ciri-ciri penipuan phishing dan cara untuk melindungi diri ataupun data mereka dari kejahatan yang sangat merugikan ini. Selain itu juga kurang kehati-hatian para pengguna yang mudah tergiur dengan tawaran-tawaran yang diberikan tanpa melakukan verifikasi terlebih dahulu juga menjadi faktor meningkatnya resiko kejahatan phishing.

Banyaknya modus yang digunakan dalam kejahatan phishing termasuklah salah satunya menggunakan email yang dikirimkan dan nampak resmi dari lembaga perbankan yang telah menyerupai situs asli seperti bank atau media sosial dimanfaatkan pelaku phishing untuk menyebarkan pesan palsu melalui SMS ataupun WhatsApp yang berisi sebuah tautan yang selanjutnya akan mengarahkan korban untuk membuka situs ilegal. Beberapa cara yang sering digunakan oleh para penjahat phishing untuk melancarkan aksinya yaitu :

1) Dengan memanipulasi tautan supaya terlihat seperti alamat sebuah bank yang asli atau mereka akan menggunakan subd omain untuk digunakan.
2) Filter yang biasa digunakan adalah gambar untuk memaksa pengguna dapat memberikan informasi data-data pribadi mereka.
3) Email phishing akan dibuat dan ditampilkan sebagai tautan ke dalam halaman web yang sah Padahal hal tersebut mengarah kepada halaman web phising.

Tanggung Jawab Bank Dalam Melindungi Data Nasabah

Kepercayaan merupakan kunci penting untuk kelancaran suatu bisnis hal itulah yang menjadi kunci dari lancarnya harus bisnis di dalam dunia perbankan. Phising yang merupakan kejahatan yang bahaya untuk keamanan dana simpanan nasabah suatu bank menuntut bank untuk memberikan keamanan serta pertahanan untuk menciptakan rasa tenang bagi para nasabah terhadap segala resiko kejahatan yang mungkin terjadi terhadap uang simpanan mereka. Hubungan yang baik menjadi sangat bergantung kepada rasa kepercayaan maka sebuah bank harus mengambil langkah-langkah yang konkret untuk

menghindari dan mencegah terjadinya kejahatan phising demi menjaga keamanan dan mengurangi resiko yang bisa saja membahayakan. Dengan menerapkan teknologi keamanan yang canggih dan terus melakukan edukasi kepada nasabah terkait dengan keamanan tersebut sudah menjadi tugas pokok pihak bank untuk melakukan perlindungan hukum secara represif ataupun preventif.

Kebijakan harus ditegakkan guna untuk menjadi salah satu cara pencegahan tindakan phising yang biasanya melibatkan nasabah untuk memberikan informasi pribadi mereka maka dari itu harus dilakukan edukasi kepada nasabah tentang bahayanya phising dan cara-cara yang harus dilakukan untuk mempertahankan diri atau menghindari menjadi korban supaya terhindar dari masalah ataupun menghadapi dan menyelesaikan masalah setelah menjadi korban phising. Banyak cara yang dapat dilakukan oleh pihak bank untuk mengingatkan para nasabah agar selalu berhati-hati terhadap kejahatan penipuan yang mengatasnamakan bank salah satu contohnya adalah dengan memanfaatkan media sosial ataupun pesan ke nomor pribadi untuk terus mengingatkan masyarakat tentang keamanan bertransaksi menggunakan mobile banking supaya lebih aman. Selain itu bank juga memberikan kesempatan kepada nasabah untuk dapat menghubungi mereka jika nasabah memiliki pertanyaan atau sebuah kekhawatiran tentang pelayanan mobile banking yang mereka curigai. Lembaga keuangan seperti bank wajib memiliki pertimbangan yang matang terhadap manajemen risiko supaya penggunaan dapat dilakukan dengan efisien secara rutin sesuai dengan kegunaannya. Pelaksanaan manajemen risiko ini dilaksanakan sesuai dengan kebijakan dan kemajuan teknis serta ketersediaan mobil banking.

Selain itu juga bank harus menerapkan prinsip perlindungan konsumen untuk memastikan tanggung jawab mereka dalam memberikan perlindungan secara menyeluruh terhadap nasabah. Dengan adanya tanggung jawab ini maka prosedur yang harus dilaksanakan diharapkan dapat mencegah terjadinya kejahatan phising adalah dengan meningkatkan pengetahuan nasabah tentang bahayanya phising dan cara melindungi data-data pribadi mereka dari ancaman kejahatan phising. Sedangkan tanggung jawab represif dikhususkan kepada nasabah yang telah menjadi korban kejahatan phising. Sedangkan untuk pencegahan secara preventif bisa saja dilakukan dengan menginformasikan kepada nasabah tentang keamanan keamanan dalam transaksi banking yang mencerminkan usaha bank dalam meningkatkan kesadaran nasabah dan memberikan panduan untuk penggunaan transaksi yang lebih aman. Selain itu perlindungan represif lainnya adalah nasabah yang menjadi korban mendapatkan hak untuk menggugat pihak bank ke pengadilan jika dalam penyelesaian kasus terhadap nasabah yang telah menjadi korban phising tidak dapat diterima oleh pihak nasabah karena hasil yang diharapkan tidak sesuai maka nasabah dapat mengajukan gugatan terhadap pihak bank karena telah menyebabkan kerugian akibat adanya tindakan phising dalam penggunaan sistem mobile banking. Selain itu pihak nasabah juga dapat meminta perlindungan kepada Otoritas Jasa Keuangan supaya dapat membantu mempercepat proses pengaduan nasabah yang menjadi korban dan telah mengalami kerugian.

Kebijakan Keamanan Sistem Perbankan

Di dalam kebanyakan kasus phising yang terjadi oleh nasabah terdapat faktor kelalaian dari pihak bank yaitu masih kurangnya penerapan prinsip kehati-hatian pada sistem Pengendalian internal bank yang mengakibatkan hilangnya data nasabah pada rekening. Pihak bank dan pihak nasabah memiliki hubungan hukum yaitu perjanjian baku

yang ketetapannya telah dibuat oleh salah satu pihak yaitu pihak bank yang lebih dominan untuk mempermudah pelaksanaan perjanjian dalam ikatan bisnis. Jika pihak nasabah ataupun pihak bank melakukan suatu kesalahan dan tidak melaksanakan kewajiban mereka Maka akibat yang timbul adalah wanprestasi atau ingkar janji namun ketika kewajiban tersebut tidak dijalankan merupakan kewajiban yang tidak dijelaskan di dalam sebuah perjanjian namun di dalam undang-undang telah diatur maka hal tersebut adalah perbuatan melawan hukum karena hal-hal yang diatur di dalam perjanjian atau di dalam undang-undang sifatnya mengikat dan menimbulkan akibat hukum sebagaimana yang dijelaskan di dalam Pasal 1339 jo Pasal 1347 KUHPerdata yang menjelaskan bahwa sebuah perjanjian tidak hanya mengikat untuk hal yang diperjanjikan saja namun hal yang menurut kepatutan kebiasaan atau undang-undang serta hal-hal yang menurut kebiasaan harus dilaksanakan walaupun hal tersebut tidak tegas dinyatakan pada perjanjian.

Dapat dilihat dari ketentuan pasal ini bahwa kelalaian bank termasuk kepada perbuatan melawan hukum karena telah lalai untuk memenuhi kewajibannya yang diatur di dalam Pasal 15 Ayat 1 Huruf Peraturan Otoritas Jasa Keuangan Nomor 18 Tahun 2006 yaitu bank wajib untuk menyesuaikan sistem pengendalian internal dengan jenis resiko yang melekat pada usaha Bank. Maka dapat disimpulkan bahwa terdapat suatu sebab yang dilarang untuk dilaksanakan dalam perjanjian maka syarat objektif tidak terpenuhi dan dinilai batal perjanjian demi hukum yang mengakibatkan perjanjian tersebut tidak pernah ada dan keadaan dianggap seperti tidak pernah terjadi perjanjian.

Berdasarkan Pasal 15 Ayat 1 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik menegaskan bahwa setiap penyelenggara sistem elektronik harus menyelenggarakan sistem elektronik secara baik dan aman untuk bertanggung jawab terhadap pengoperasiannya terhadap sistem elektronik sebagaimana mestinya. Pasal ini menunjukkan bahwa penyelenggaraan sistem keuangan dalam perbankan harus dilakukan dengan aman sehingga bank Sebagai penyelenggara sistem elektronik harus dapat dipercaya dan menjalankan tanggung jawabnya dalam menjalankan aktivitas keuangan dengan baik maka harus melaksanakan kewajiban-kewajiban dalam melakukan operasi sistem elektronik seperti yang telah dijelaskan di dalam ketentuan Pasal 16 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yaitu:

1) Harus bisa menampilkan kembali informasi elektronik yang telah tersimpan
2) Harus bisa melindungi kerahasiaan dan ke teraksesan informasi elektronik di dalam pelaksanaan sistem elektronik
3) Harus bisa beroperasi sesuai dengan prosedur dan petunjuk di dalam penyelenggaraan sistem elektronik
4) Harus dilengkapi dengan prosedur dan petunjuk yang umum dilakukan dengan bahasa yang sederhana dan mudah dipahami
5) Harus memiliki mekanisme yang berkelanjutan untuk menjaga dan memelihara prosedur dan petunjuk

Peran Dan Tanggung Jawab Nasabah Dalam Keamanan Data Perbankan

Adanya kejahatan phising bisa dikatakan disebabkan karena kurangnya pengetahuan masyarakat tentang pentingnya untuk menjaga keamanan data mereka. Setelah mendapatkan edukasi tentang hal ini maka masyarakat diharapkan bisa menghindari dan menerapkan beberapa hal yang bisa dilakukan sebagai upaya pencegahan. Masyarakat

harus berhati-hati dan lebih teliti terhadap email dan pesan singkat yang tak dikenal untuk untuk pesan yang berisikan meminta verifikasi alamat email atau situs web yang sesuai dengan alamat resmi organisasi Bank. Selain itu juga penggunaan kata sandi yang kuat ataupun kombinasi yang unik dari setiap akun sangat dianjurkan. Penggunaan autentikasi dua faktor juga menambah lapisan keamanan ekstra sehingga perangkat yang terpasang terhindar dari antivirus dan anti malware yang akan membantu mendeteksi dan mencegah terjadinya malware. Selain itu nasabah dapat melaporkan aktivitas yang dicurigai merupakan aktivitas phising kepada pihak berwenang.

Memahami dan mempelajari tentang kejahatan phising seharusnya menjadi poin dasar untuk melindungi data diri masyarakat. Hal ini dikarenakan pihak bank menyatakan bahwa kejahatan phising ini sering terjadi karena kelalaian dari nasabah yang memberikan celah secara sengaja ataupun tidak sengaja kepada penjahat phising. Pihak bank akan memberikan saran agar di dalam proses memberi tanggung jawab secara represif dengan tujuan mencegah laporan yang serupa untuk memastikan bahwa prosedur pengaduan dapat ditanggapi dengan cepat dan nasabah dapat dilayani dengan baik saat mengajukan pengaduan.

Jika dalam proses penyelidikan terbukti bahwa kejahatan phising ini terjadi karena kesalahan atau kecerobohan pihak nasabah maka yang bertanggung jawab adalah nasabah itu sendiri karena sudah dianggap berada di luar kendali pihak bank maka dari itu bank tidak dituntut untuk memberikan ganti rugi kepada nasabah. Maka dapat disebutkan bahwa nasabah pun memiliki tanggung jawab untuk menjaga keamanan data mereka untuk dapat menghindari pemberian informasi berupa data yang sifatnya rahasia kepada pihak yang tidak dikenal dan tidak bertanggung jawab.

Berdasarkan Pasal 26 Undang-Undang Informasi dan Transaksi Elektronik sebenarnya seorang nasabah memiliki alasan untuk tidak membayar kerugian jika mereka melakukan kesalahan atau tidak memberitahukan data mereka kepada pihak yang tidak bertanggung jawab. Dalam hal yang seperti ini maka nasabah dapat menuntut bank jika mereka masih Kehilangan uang yang disimpan kepada pihak bank yang menjadi korban kejahatan phising karena pihak bank dianggap tidak mampu melindungi data atau sistem keamanannya tidak dapat dijamin. Pertanggungjawaban dapat dilakukan dengan memenuhi bukti-bukti yang dibutuhkan yaitu bukti bahwa bank belum maksimal dalam melaksanakan prosedur keamanan dan dianggap gagal telah memberitahu atau menginformasikan nasabah terkait bahaya dari phising. Pemberitahuan secara berulang ataupun peringatan yang dikirimkan kepada nasabah demi keamanan penggunaan mobile banking dapat menjadi contoh edukasi digital dengan langkah-langkah yang baik maka bank telah menunjukkan bahwa mereka telah berusaha untuk bertanggung jawab dalam menghindari kejahatan cyber yang mengancam nasabah mereka karena di dalam Pasal 29 Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan dijelaskan bank harus menjunjung tinggi tanggung jawab mereka untuk memastikan bahwa informasi pelanggan tetap aman seperti melakukan teknologi autentikasi berlapis ataupun enkripsi data dan notifikasi keamanan lainnya untuk dapat mengidentifikasi aktivitas yang mencurigakan supaya data nasabah tetap aman.

Intrepretasi Peraturan Hukum Berdasarkan Kasus Nasabah Bank Rakyat Indonesia

Untuk mendapat perlindungan maka nasabah yang merasa dirugikan dapat melakukan upaya hukum untuk mendapatkan keadilan dan melindungi hak-hak mereka

dalam menyelesaikan sengketa bisa melakukan laporan ke pihak yang berwenang yaitu Kepolisian sebagai kasus kejahatan atau mengajukan gugatan ke pengadilan sebagai sengketa perdata. Selain itu juga penyelesaian dapat dilakukan di luar pengadilan dengan menggunakan metode mediasi ataupun arbitrase. Upaya hukum yang dilakukan bertujuan untuk menegakkan keadilan dan mengembalikan kerugian yang mungkin telah dialami korban dan mencegahnya terjadi di kemudian hari.

Seperti kasus yang dialami oleh nasabah pada Bank Rakyat Indonesia KCP Kecamatan Lawang Kabupaten Malang Provinsi Jawa Timur yang menjadi korban phising pada bulan Mei 2023 dan mengalami kerugian senilai Rp.1.446.000.000 (satu miliar empat ratus empat puluh enam juta rupiah) dalam waktu yang singkat setelah dia menerima pesan whatsapp yang berisi sebuah undangan dalam format apk yang diklik dan membuka beberapa iklan yang muncul. Penurunan jumlah tabungan ini disebabkan karena adanya kegiatan transfer antara rekening pada e-banking yang baru disadari oleh korban setelah saldo rekeningnya terupiah Rp.2.000.000; (dua juta rupiah). Ia mencoba mencari keadilan dan berharap bahwa uang tersebut dapat dikembalikan setelah mendatangi Bank BRI KCP Lawang untuk menanyakan masalah tersebut, namun pihak bank menjelaskan tidak dapat mengganti kerugian nasabah karena hal tersebut disebabkan oleh kelalaian nasabah sendiri. Hal ini menunjukkan bahwa pihak bank tidak menanggung segala kesalahan yang bukan hasil dari kesalahan pelayanan perbankan yang telah mereka sediakan.

Berdasarkan Pasal 9 Peraturan Otoritas Jasa Keuangan tentang Perlindungan Konsumen Sektor Jasa Keuangan yang menyebutkan bahwa pelaku usaha jasa keuangan menetapkan kewajiban bagi pelaku usaha jasa keuangan termasuk juga bank untuk memberitahukan kepada nasabahnya mengenai hak dan kewajiban mereka dalam hubungan bisnis keuangan yang juga mencakup pemberian informasi yang jelas tentang tata cara mengamankan akun dan risiko keamanan dalam penggunaan layanan internet banking. Selain itu juga bahwa langkah-langkah pencegahan yang dapat dilakukan nasabah juga harus dijelaskan oleh pihak bank dengan memberikan informasi yang lengkap jelas dan komprehensif nasabah diharapkan dapat memahami resiko dan cara melindungi data mereka dari tindakan phising.

Setelah dilakukannya hal ini diharapkan dapat menciptakan situasi yang aman dari segala tindak kejahatan dan membantu nasabah untuk mengambil tindakan preventif untuk mendapatkan perlindungan yang diperlukan dalam penggunaan layanan perbankan. Bagi nasabah yang telah mengalami kerugian akibat dari kejahatan phising juga harus mendapatkan perlindungan secara represif yaitu mengacu pada ketentuan Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen yang menjelaskan bahwa nasabah selaku konsumen mempunyai hak untuk menyatakan pendapat dan mengajukan keluhan mereka tentang produk dari perbankan dan untuk nasabah yang menjadi korban fisik dapat menggunakan haknya dalam menyampaikan pengaduan terkait layanan perbankan yang ia terima. Selain itu dalam Pasal 32 Peraturan Otoritas Jasa Keuangan tentang Perlindungan Konsumen juga menjelaskan bahwa para pelaku usaha di industri jasa keuangan yaitu bank harus bisa menciptakan suatu sistem yang memberikan layanan dan solusi bagi permasalahan yang dihadapi oleh nasabah.

Upaya hukum yang dapat dilakukan untuk kepentingan korban adalah mendapatkan kompensasi atas kerugian yang dialami. Selain itu juga pihak yang terlibat di dalam kejahatan phising ini harus diproses secara hukum dan diberi konsekuensi yang sesuai dengan perundang-undangan secara tegas oleh pihak yang berwenang atau pengadilan

untuk memberikan keputusan yang menguntungkan korban yaitu memberikan ganti rugi kerugian materi dan nonmateri karena adanya kejahatan phising ini. Penanganan kejahatan phising ini tidak hanya mengharapkan tanggung jawab dari korban saja namun kesadaran publik dan edukasi tentang adanya ancaman kejahatan phising menjadi masalah penting dalam permasalahan ini. Kegiatan-kegiatan yang harus dilakukan dengan tujuan untuk meningkatkan pemahaman tentang langkah pencegahan terhadap kejahatan phising juga berperan penting dalam meningkatkan kewaspadaan masyarakat terhadap penipuan, harapannya semakin banyak individu yang teredukasi maka semakin sulit pulalah bagi seorang penjahat untuk melakukan kejahatan phising ini. Hal ini juga yang akan memberikan dampak positif pada keamanan cyber secara menyeluruh dan melindungi banyak orang dari kerugian.

Penyelesaian Sengekta dan Peran OJK dan BSSN

Penyelesaian sengketa perjanjian baku antara nasabah dengan pihak bank dapat dilakukan melalui dua cara yaitu penyelesaian dengan jalur litigasi atau di pengadilan dan jalur non litigasi atau di luar pengadilan. Otoritas Jasa Keuangan juga berperan dalam hal ini dengan memberikan dua mekanisme yang dapat dijalani oleh pihak bank dengan nasabahnya yaitu penyelesaian melalui pengaduan konsumen yang dilakukan oleh lembaga jasa keuangan dan penyelesaian melalui jalur litigasi seperti peradilan ataupun non litigasi. Dalam penyelesaiannya para pihak diberikan kesempatan untuk memilih jalur mana yang akan mereka tempuh adapun perbedaan jalur yang dapat diketahui adalah:

Melalui jalur non litigasi atau juga disebut sebagai penyelesaian sengketa dengan alternatif terdapat lembaga yang menangani permasalahan antara lembaga jasa keuangan dengan nasabahnya. Lembaga tersebut adalah lembaga alternatif penyelesaian sengketa Perbankan Indonesia (LAPSPI) yang dibentuk langsung oleh Otoritas Jasa Keuangan untuk menyelesaikan permasalahan secara non litigasi. Berdasarkan Pasal 2 Peraturan Otoritas Jasa Keuangan dijelaskan bahwa sebelum memasuki tahapan penyelesaian harus dilakukan terlebih dahulu oleh pelaku usaha atau bank. Ketentuan pada lembaga jasa keuangan seperti bank sudah seharusnya memiliki layanan pengaduan nasabah yang dapat mereka dapatkan dengan mudah dengan cara mendatangi langsung ke kantor cabang ataupun Melalui aplikasi Bank digital yang disediakan oleh pihak bank. Jika dalam proses penyelesaian melalui pengaduan ini tidak ditemukan kesepakatan antara kedua pihak maka penyelesaiannya akan dilakukan di luar pengadilan yaitu melalui lembaga alternatif penyelesaian sengketa yang berupa mediasi melalui meditor agar mencapai kesepakatan, atau melalui ajudikasi melalui ajudikator untuk menjatuhkan putusan yang mengikat bagi para pihak atau melalui arbitrase yang didasari oleh perjanjian yang dibuat dan telah disepakati oleh kedua pihak yang keputusannya bersifat final dan mengikat. Jika kasusnya merupakan kelalaian pihak bank maka dalam perjanjian baru akibat dari social engineering yang terjadi maka dapat dilakukan dengan cara non litigasi yaitu nasabah melakukan pengajuan pengaduan melalui aplikasi yang pihak bank sediakan atau dapat mendatangi langsung kantor cabang terdekat yang selanjutnya akan dilakukan investigasi mendalam serta analisis terhadap pengaduan untuk membuktikan bahwa kelalaian memang dilakukan oleh pihak bank.

Penyelesaian melalui jalur pengadilan sebagai cara terakhir yang dapat dilakukan jika cara non litigasi tidak menghasilkan keputusan yang disepakati. Namun dalam cara ini harus dilakukan pembuktian sebagaimana dalam ketentuan Pasal 1865 Kitab Undang-Undang Hukum Perdata dijelaskan bahwa setiap orang yang ingin meneguhkan haknya atau

membantah suatu hak orang lain maka harus merujuk pada suatu peristiwa dan orang tersebut wajib untuk membuktikannya. Maka dalam hal pembuktian alat bukti elektronik yaitu berupa informasi elektronik atau dokumen elektronik atau hasil cetaknya akan menjadi alat bukti yang sah.

Kemudian pada Pasal 40 Peraturan Otoritas Jasa Keuangan disebutkan bahwa Otoritas Jasa Keuangan akan memberikan kewenangan kepada nasabah untuk mengajukan pengaduan kepada Otoritas Jasa Keuangan dengan bukti kesalahan pada layanan perbankan yang mana Otoritas Jasa Keuangan akan berperan sebagai pihak ketiga mediator dan memberikan penilaian terhadap pelanggaran yang terjadi. Maka pengaturan tentang perlindungan memberikan kesempatan untuk nasabah dapat menyelesaikan permasalahannya dengan beberapa pilihan cara baik itu melalui penyelesaian langsung dengan pihak bank ataupun dengan melalui jalur hukum atau dengan lembaga lainnya. Maka para nasabah yang menjadi korban tindakan phising dan merasa dirugikan dengan hilangnya dana simpanan mereka akan mendapat perlindungan hukum atas penggunaan sistem e-banking dari pihak bank yaitu berupa hak untuk mengajukan pengaduan tentang tindakan phising yang telah ia alami sebagai saran bagi nasabah untuk menyampaikan keluhan mereka terhadap pelayanan bank atau lembaga keuangan lainnya selain itu juga bahwa nasabah dapat memanfaatkan metode mediasi untuk menyelesaikan sengketa dengan pihak bank secara cepat mudah dan biaya yang ringan. Otoritas Jasa Keuangan akan melakukan pengawasan dan kontrol terhadap produk dari sebuah perbankan untuk pelaksanaan operasional ataupun kehati-hatian dan transparansi dalam pelayanan yang diberikan pihak bank kepada nasabah dengan beberapa langkah yaitu pengujian terkait pemahaman bank tentang penilaian resiko bank dan penyusunan strategi pemantauan berdasarkan risiko atau pemeriksaan bank dan verifikasi kondisi bank secara berkala.

Selain Otoritas Jasa Keuangan lembaga lainnya yang berperan dalam hal ini adalah badan siber dan Sandi Negara (BSSN) yang juga bertanggung jawab untuk menciptakan sebuah lingkungan dalam penyelenggaraan sistem elektronik yang aman dan terpercaya serta menumbuhkan laju ekonomi di Indonesia dengan meningkatkan daya saing dan membangun kesadaran masyarakat terhadap ketahanan dan keamanan nasional. BSSN bertugas untuk menyusun strategi keamanan dalam pengembangan kebijakan keamanan di instansi keuangan supaya tercapai nilai-nilai kedaulatan kemandirian kebersamaan adaptif dan keamanan. langkah yang diberlakukan oleh BSSN dalam membentuk keamanan di Indonesia yaitu bergantung kepada aspek hukum aspek teknis, aspek organisasi, aspek pengembangan kapasitas dan aspek kerjasama. Aspek hukum akan mengajukan dengan undang-undang kejahatan cyber dan undang-undang keamanan cyber serta penyelenggaraan pelatihan keamanan bagi para pelaku hukum yang diharapkan dapat mendorong pembentukan undang-undang tentang keamanan di Indonesia sehingga para penegak hukum memiliki pengetahuan dan informasi yang terus berkembang sesuai dengan perkembangan teknologi keamanan.

KESIMPULAN

Dengan meningkatkan kesadaran dan edukasi kepada masyarakat tentang bahaya dari praktek phising diharapkan masyarakat dengan mudah mengenali ciri-ciri atau pola yang umum mereka gunakan dalam melakukan penipuan. Masyarakat harus paham tentang tujuan phising yang untuk mendapatkan informasi pribadi berupa data-data penting melalui

pesan atau tautan yang terlihat sah amun ternyata palsu dan meningkatkan kewaspadaan terhadap komunikasi yang mencurigakan atau permintaan Informasi pribadi dari orang yang tidak dikenal. Selain itu juga manfaat dilakukannya edukasi kepada masyarakat juga dapat memberikan pencegahan terhadap kejahatan ini supaya tidak terjadi terus-menerus supaya masyarakat menjadi lebih paham dalam menghindari jebakan-jebakan yang biasa dilakukan oleh pelaku phising dalam mengurangi kemungkinan menjadi korban dan mengalami kerugian. Pengaturan tentang perlindungan memberikan kesempatan untuk nasabah dapat menyelesaikan permasalahannya dengan beberapa pilihan cara baik itu melalui penyelesaian langsung dengan pihak bank ataupun dengan melalui jalur hukum atau dengan lembaga lainnya. Maka para nasabah yang menjadi korban tindakan phising dan merasa dirugikan dengan hilangnya dana simpanan mereka akan mendapat perlindungan hukum atas penggunaan sistem e-banking dari pihak bank.

BIBLIOGRAFI

A, wirasakti Z. (2022). PENGARUH LAYANAN PRODUK BSI MOBILE TERHADAP KEPUASAN NASABAH (STUDY PADA MAHASISWA UIN MATARAM JURUSAN PERBANKAN ANGKATAN 2018). *Skripsi*, *8.5.2017*.

Aqil, N. A., Putri, C. M., & Yunisa, D. (2022). Evaluasi Sistem Cash On Delivery Demi Meningkatkan Kepastian Hukum Dalam Perkembangan Transaksi Elektronik di Indonesia. *IPMHI Law Journal*, *2*(2).

Aris, A. L. (2019). ANALISIS FAKTOR YANG MEMPENGARUHI PERATAAN LABA PADA INDUSTRI PERBANKAN DAN LEMBAGA KEUANGAN LAINNYA. *JEMMA | Journal of Economic, Management and Accounting*, *2*(1). https://doi.org/10.35914/jemma.v2i1.144

Dwicky Cahyadi, A. (2019). Yurisdiksi Transaksi Elektronik Internasional Menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Jurnal Wawasan Yuridika*, *3*(1). https://doi.org/10.25072/jwy.v3i1.203

Firdaus, A. S., & Sjahruddin, H. (2021). PENGARUH DIMENSI BAURAN PEMASARAN TERHADAP MINAT NASABAH MENGGUNAKAN LAYANAN E-BANKING. *NIAGAWAN*, *10*(1). https://doi.org/10.24114/niaga.v10i1.21087

Gulo, A. S., Lasmadi, S., & Nawawi, K. (2021). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal of Criminal Law*, *1*(2). https://doi.org/10.22437/pampas.v1i2.9574

Hafizhah, Y. D., & Rosa, E. S. (2022). Tinjauan Atas Layanan E – Banking Dalam Meningkatkan Kepuasan Nasabah PT. Bank BUMN Kantor Cabang Pajajaran Bogor. *Jurnal Aplikasi Bisnis Kesatuan*, *2*(2). https://doi.org/10.37641/jabkes.v2i2.1493

Handayani, R. N., Fasa, M. I., & Suharto, S. (2023). Strategi Pemasaran Produk Bank Syariah Di Tengah Pesatnya Pertumbuhan Industri Perbankan Syariah Di Indonesia. *Jurnal Manajemen Dan Bisnis*, *5*(01). https://doi.org/10.47080/jmb.v5i01.2285

Mamesah, M. (2022). SISTEM TRANSAKSI ELEKTRONIK DALAM PERJANJIAN JUAL BELI MELALUI MEDIA ONLINE. *Lex Privatum*, *X*(1).

Prabowo, R., & Purwanto, A. (2020). The Role of Digital Literacy in Preventing Phishing Fraud in E-Banking Services. *Jurnal Hukum & Pembangunan*, *50*(3), 459–475. https://doi.org/10.21143/jhp.vol50.no3.2364

Rachman, I. A., & Sari, D. R. (2021). Legal Protection of Personal Data in E-Banking Against Cybercrime in Indonesia. *Indonesian Journal of Law and Society, 2*(1), 35–53. https://doi.org/10.19184/ijls.v2i1.22979

Rahmanto, T. Y. (2019). Penegakan Hukum terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik. *Jurnal Penelitian Hukum De Jure*, *19*(1). https://doi.org/10.30641/dejure.2019.v19.31-52

Ristiana, N., & Widyastuti, E. (2022). Analisis Pengaruh Literasi Keuangan Digital Terhadap Minat Mahasiswa Dalam Penggunaan Layanan E-Banking. *Jurnal Masharif Al-Syariah: Jurnal Ekonomi Dan Perbankan Syariah*, *7*(1).

Rohaedi, R. A. U. (2021). Tanggung Jawab Bank terhadap Simpanan Deposito Berjangka yang Tidak Tercatat dihubungkan dengan Perlindungan Hukum Nasabah menurut Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. *Jurnal Riset Ilmu Hukum*, *1*(1). https://doi.org/10.29313/jrih.v1i1.179

Rosita, R. (2020). PENGARUH PANDEMI COVID-19 TERHADAP UMKM DI INDONESIA. *JURNAL LENTERA BISNIS*, *9*(2). https://doi.org/10.34127/jrlab.v9i2.380

Saputra, M. A. D., Rofiqoh, H. H., & Saputra, W. (2023). Pengaruh Internet Banking dan Mobile Banking Terhadap Kinerja Bank Umum Konvensional di Indonesia. *WACANA EKONOMI (Jurnal Ekonomi, Bisnis Dan Akuntansi)*, *22*(2). https://doi.org/10.22225/we.22.2.2023.132-141

Saputra, P. R., & Wahyuningtyas, T. (2020). Pemanfaatan Layanan E-Banking oleh Nasabah Perbankan Syariah: Studi pada Bank Syariah Mandiri KCP Kepanjen. *Jihbiz Jurnal Ekonomi Keuangan Dan Perbankan Syariah*, *4*(1). https://doi.org/10.33379/jihbiz.v4i1.853

SE, M. M. T. W., & Sugiyono, I. (2021). Pengaruh Kebijakan Moneter Terhadap Non Performance Loan Dan Kinerja Keuangan Pada Industri Perbankan Di Indonesia …. *JIMEK: Jurnal Ilmiah …*.

Sumadi, H. (2016). KENDALA DALAM MENANGGULANGI TINDAK PIDANA PENIPUAN TRANSAKSI ELEKTRONIK DI INDONESIA. *Jurnal Wawasan Yuridika*, *33*(2). https://doi.org/10.25072/jwy.v33i2.102

Winduwiratsoko. (2018). Analisis Penerapan Model Unified Theory of Acceptance and Use of Technology (UTAUT) untuk Memahami Perimaan dan Penggunaan Layanan E-Banking oleh Nasabah di Provisi Daerah Istimewa Yogyakarta. *Tesis*.

© 2025 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY SA) license (https://creativecommons.org/licenses/by-sa/4.0/).