Jurnal Masharif al-Syariah: Jurnal Ekonomi dan Perbankan Syariah
ISSN: 2527 - 6344 (Printed), ISSN: 2580 - 5800 (Online)
Accredited No. 204/E/KPT/2022
DOI: https://doi.org/10.30651/jms.v10i5.30415
Volume 10, No. 5, 2025 (4173-4186)

PERLINDUNGAN HUKUM DALAM MENGANTISIPASI DAN MENANGANI KERUGIAN NASABAH AKIBAT SCAM MELALUI *LINK PHISING* PADA *MOBILE BANKING*

Indah Tri Sari Harahap[1], Alya Arianti Nasution[2], Keisya Putri Balqis[3], Wahyudin[4], Nikmah Dalimunthe[5]
Universitas Islam Negeri Sumatera Utara
Indahhr2003@gmail.com[1], alyaarianti16@gmail.com[2],
keisyaputribalqis17@gmail.com[3] wahyudinfebiuinsu@gmail.com[4],
nikmahdalimunthe@uinsu.ac.id[5]

Abstrak

Dengan hadirnya transformasi digital pada sektor keuangan membuat kemudahan signifikan bagi masyarakat, tetapi menambah kejahatan siber. Salah satu ancaman yang sering terjadi ialah penipuan digital yang menggunakan kelengahan pengguna lewat tautan palsu yang menyerupai layanan resmi perbankan. Penelitian ini ditujukan agar mengkaji bagaimana perlindungan hukum untuk melindungi nasabah serta bagaimana mekanisme mencegah serta menangani kerugian dilakukan. Metode penelitian yang dimanfaatkan ialah deskriptif kualitatif memakai pendekatan kepustakaan lewat pengkajian jurnal ilmiah, buku, serta aturan hukum yang ada. Hasil penelitian memperlihatkan yakni regulasi sudah mengatur kewajiban perbankan ketika memelihara keamanan sistem juga menyediakan mekanisme pengaduan bagi nasabah. Dengan begitu, masih ada hambatan pada penerapan perlindungan hukum, utamanya tentang rendahnya literasi digital serta sulitnya pembuktian. Kesimpulan penelitian mengutamakanperlunya penguatan regulasi, peningkatan edukasi masyarakat, serta tanggung jawab perbankan yang dimaksimalkan. Kolaborasi antara regulator, lembaga perbankan, serta masyarakat sebagai fondasi utama dalam membentukkeamanan, keadilan, dan kelanjutan pada sistem perbankan digital.

Kata Kunci: Perlindungan Hukum, Perbankan Digital, Phishing, Nasabah

Abstract

With the presence of digital transformation in the financial sector, it makes significant convenience for the community, but adds to cybercrime. One of the threats that often occurs is digital fraud that uses user negligence through fake links that resemble official banking services. This research is intended to examine how legal protection to protect customers and how mechanisms to prevent and handle losses are carried out. The research method used is descriptive qualitative using a literature approach through the study of scientific journals, books, and existing laws. The results of the research show that regulations have regulated the obligations of banks when maintaining system

security as well as providing a complaint mechanism for customers. That way, there are still obstacles to the application of legal protection, especially regarding low digital literacy and difficulty of proof. The research conclusion prioritizes the need to strengthen regulations, increase public education, and maximize banking responsibilities. Collaboration between regulators, banking institutions, and the community as the main foundation in shaping security, justice, and continuity in the digital banking system.

Keywords: *Legal Protection, Digital Banking, Phishing, Customers*

1. Pendahuluan

Kemajuan teknologi informasi sudah memberi perubahan besar pada pola aktivitas masyarakat, termasuk pada pemanfaatan layanan keuangan yang makin berbasis sistem digital. Dari menggunakan teknologi ini membuat kemudahan, kecepatan, serta efisiensi ketika bertransaksi keuangan sehari-hari. Akan tetapi, kemajuan teknologi juga memberipeluang adanya sejumlah bentuk kejahatan siber yang memanfaatkan celah keamanan sistem serta minimnyasikap waspada seorang pengguna. Kejahatan di dunia digital berkembang seiring bertambahnya ketergantungan masyarakat terhadap layanan berbasis teknologi. Hal inipun memunculkan tantangan baru untuk mengupayakan perlindungan kepentingan masyarakat menjadi pengguna layanan keuangan digital(Lubis & Nasution, 2023).

Layanan digital yang makin bertambahtaksenantiasa diiringi dengan pemahaman yang terpenuhi menyesuaikan risiko keamanan yang mungkin terjadi. Banyak pengguna masih punya tingkatan kesadaran yang rendah pada ancaman kejahatan siber sehingga mudah terpengaruh oleh informasi yang tampak meyakinkan. Pelaku kejahatan yang seringkali modus dalam menipumakinbanyak jenisnyaserta sulit dibedakan dari layanan resmi. Yang muncul bukan hanya berbentuk kerugian finansial, tetapi juga berdampak pada kepercayaan masyarakat bagi sistem keuangan. Maka dari itu, aspek keamanan dan perlindungan hukum sebagai hal yang sangat diperlukanketika menyelenggarakan layanan digital(Amane *et al*., 2025).

Penelitian terdahulu dariNervia dkk. (2025)berkaitan dengan fenomena kejahatan siber pada layanan perbankan digital lewat tindakan phishing dengan memanfaatkan tautan palsu. Penelitian inipun memperlihatkan yakni kemajuan teknologi perbankan digital tak saja memberikan kemudahan, namun memberi kesempatanadanya penipuan yang menargetkan kelengahan nasabah. Modus phishing dilakukan dengan cara menyerupai tampilan layanan resmi perbankan makanya korban dengan tak sadar memberi data pribadinya dan informasi keuangan. Penelitian ini memakai pendekatan hukum normatif yang menelaah aturanterkait

perundang-undangan tentang kejahatan siber serta perlindungan nasabah. Hasil kajian memperlihatkan yakni pengaturan hukum di Indonesia tak membentuk dasar sanksi pada seseorang yang bertindak phishing. Namun demikian, masih saja ditemui persoalanketika mengimplementasikan perlindungan hukum dengan efektif bagi nasabah. Oleh sebab itu, penelitian ini mengedepankan perlunya penguatan sistem keamanan digital, penambahan tingkat kesadaran masyarakat, serta penegakan hukum yang maksimal.

Link phishing merupakan salah satu bentuk penipuan yang dilakukan dengan cara mengirimkan tautan palsu yang menyerupai situs resmi bank, sehingga dapat menipu pengguna untuk memasukkan data pribadi maupun data rekening mereka. Akibatnya, nasabah dapat mengalami kerugian finansial yang signifikan dan kehilangan aset mereka secara tidak langsung. Oleh karena itu, perlindungan hukum sangat penting bagi pihak bank maupun nasabah dalam menghadapi dan menanggulangi risiko tersebut. Oleh sebab itu, penelitian ini mengedepankan perlunya penguatan sistem keamanan digital, penambahan tingkat kesadaran masyarakat, serta penegakan hukum yang maksimal.

2. Kajian Pustaka

2.1 Pengertian Perlindungan

Perlindungan ialah upaya yang dilaksanakan agar menjamin keamanan serta kepastian bagi setiap individu ketika melaksanakan hak dan kewajibannya. Pada aspek hukum, perlindungan diartikan menjadi langkah dengan sifatnya yang mencegah maupun penindakan bagi potensi dan akibat pelanggaran. Perlindungan ini tak saja berlaku pada kerugian, namun juga terwujud lewataturan yang ditujukan agar mencegah terjadinya pelanggaran. Kehadiran perlindungan memperlihatkan peranan negara dalam membentuk perasaanaman pada masyarakatnya. Perlindungan juga mengharuskan bisa menanggungkewajiban dari pihak yang lebih berkewenangan. Dari perlindungan hukum inimembentuk keseimbangan hak dan kewajiban dapat terjaga. Konsep perlindungan jadi makin diperlukan seiring berkembangnya pemanfaatan teknologi digital(Atmoko & Saputri, 2022).

2.2 Pengertian Nasabah

Nasabah diartikan sebagaiseorang pemakai jasa perbankan dengan mengamanahkan dananyaserta informasi dirinyapada lembaga keuangan. Dalam hubungan hukum, nasabah terletak di kedudukan yang memerlukan jaminan keamanan karena keterbatasan penguasaan pada sistem perbankan. Nasabah berhak agarmeraih layanan yang aman, transparan, dan dapat

dipertanggungjawabkan. Pada lain sisi, nasabah juga diwajibkan menaatiaturan pemakaian layanan yang sudah disetujui sebelumnya. Keterkaitan pada nasabah dengan bank menyesuaikan asas kepercayaan yang tinggi. Kepercayaan ini sebagai dasar utama ketika menyelenggarakan layanan perbankan. Dengan begitu, bentuk perlindungan inisangat diperlukan pada sistem hukum perbankan(Natalia, 2022).

2.3 Pengertian *Phishing*

Phishing diartikan sebagai bentuk kejahatan siber yang diadakan memakai cara menipu korban supaya meyerahkan data pribadi atau informasi keuangan secara tidak sadar. Kejahatan ini senantiasa dilaksanakan lewat media digital yang menyerupai komunikasi resmi suatu lembaga. Dengan menggunakan rekayasa sosial agarmemberikan kesan urgensi serta kepercayaan palsu. Bahasa yang dimunculkan biasanya sulit dibedakan dari layanan resmi. Akibat dari phishing bisa berbentuk penyalahgunaan data sertakerugian finansial pada korban. Tindakan ini terus bertambah seiring berkembanganya teknologi informasi. Maka dari itu, phishing dikatakan sebagai ancaman serius ketika memanfaatkan layanan perbankan digital(Rahmawati *et al.,* 2024).

3. Metode Penelitian

Penelitian ini memanfaatkan pendekatan deskriptif kualitatif yang ditujukan agar memperlihatkan dengan komprehensif persoalan hukum dalam layanan perbankan digital. Dengan memilih pendekatan ini, makabisa dijelaskan fenomena hukum secara mendalam lewat kajian normatif serta konseptualnya. Fokus penelitian diarahkan pada pemahaman pada ketentuan hukum dan konsep perlindungan nasabah. Sumber data yang didapatkan dari bahan hukum sekunder termasuk buku, jurnal ilmiah, juga aturan perundang-undangan yang ada. Dengan begitu penelitian diinginkan bisa memberikan gambaran yang sistematis serta utuh(Citriadin, 2020).

Tahap mengumpulkan data lewat studi kepustakaan dengan menelaah sejumlah literatur terkait pada hukum perbankan dan kejahatan siber. Literatur yang

dimanfaatkan dipilih menyesuaikan topik penelitian serta tingkatan kredibilitas sumbernya. Proses pengumpulan diadakan dengan terstruktur guna membentukpengetahuan yang dalampada persoalan. Penelitian ini mengedepankan penguraian isi serta pemaknaan dari setiap bahan pustaka. Maka dari itu, data yang didapatkan bisamemperlihatkan kondisi hukum yang ada. Hal ini memberi kemungkinan analisis yang sifatnya deskriptif dan konseptual.

Metode deskriptif kualitatif pada penelitian ini tak menitikberatkan pada pengolahan data numerik atau statistik. Dengan terfokus pada pemaparan serta penjelasan fenomena hukum menyesuaikan norma yang diberlakukan. Di tiap temuan tersusun dengan runtut supaya mudah diketahui. Hasil kajian kemudian diuraikan dalam bentuk narasi yang sistematis. Pendekatan ini menghadirkan ruang guna menjelaskan dengan baik serta keseluruhan. Dengan begitu, metode penelitian ini relevan agar meresponpersoalan yang dirumuskan.

4. Hasil dan Pembahasan

A. Bentuk Perlindungan Hukum terhadap Nasabah

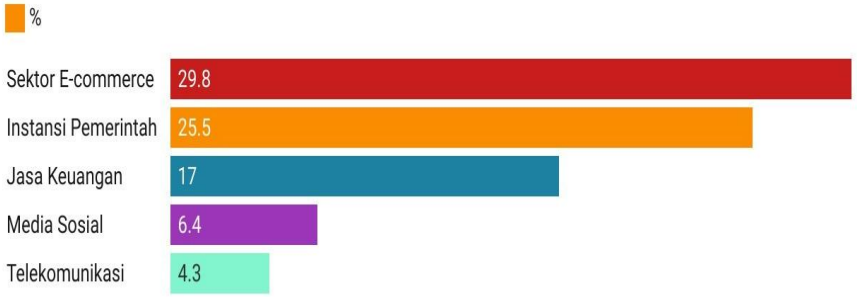
Perlindungan hukum bagi nasabah ialah unsur fundamental ketika memberi jaminan keamanan pemanfaatan layanan perbankan digital. Nasabah menjadi pengguna layanan memiliki hak agar merasa aman pada setiap aktivitas bertransaksi yang dilakukan. Perlindungan ini fungsinya menjadi sarana agar menghindari adanya kerugian akibat perbuatan yang merugikan pihak lain. Pada aspek digital, hal ini meliputi pengamanan sistem serta perlindungan data pribadi. Kehadiran perlindungan hukum memperlihatkan komitmen negara dan lembaga keuangan pada keperluan penting masyarakat. Dari perlindungan ini membuat nasabah mempunyai kepastian atas hak(Sihombing, 2021).

Pada perbankan digital, perlindungan hukum fungsinya menjadi langkah preventif yang ditujukan agar menghindari kerugian sebelum terjadi. Salah satu bentuknya ialah implementasi standar keamanan yang wajib dilaksanakan dari penyedia layanan, mulai dari sistem autentikasi sampai memantau aktifitas bertransaksi secara rutin. Regulasi ini membantu bank agar meminimalkan risiko kebocoran data dan penipuan digitalnya. Selain teknologi, kesediaan internal bank, sepertilangkah operasional serta pelatihan staf, sebagai elemen dari perlindungan preventif. Pada sistem yang bisa diandalkan, memberi peluang kesalahan atau serangan bisa dikurangi. Perlindungan preventif memperlihatkan yakni keamanan harus diperhatikan dengan keseluruhan, baik dari sisi teknologi serta manajemen.

Sementara itu, edukasi nasabah juga jadi hal yang dibutuhkan pada perlindungan preventif. Dengan pemahaman yang mendalam dari pengguna terhadap risiko digital membuat mereka lebih waspada pada potensi penipuan atau kesalahan transaksi. Edukasi dapat disampaikan melalui aplikasi, email, maupun media komunikasi lain yang mudah diakses. Nasabah yang sadar akan risiko cenderung mengambil langkah pencegahan sendiri, seperti memeriksa tautan dan memastikan keamanan perangkat. Kesadaran ini mendorong perilaku penggunaan layanan yang lebih hati-hati dan bertanggung jawab. Dengan demikian, perlindungan preventif tidak hanya fokus pada sistem, tetapi juga pada kesiapan dan perilaku pengguna(Sinta *et al*., 2025).

Selain pencegahan, perlindungan hukum juga diberikan dalam bentuk represif setelah kerugian terjadi. Perlindungan represif diwujudkan melalui mekanisme pengaduan dan penyelesaian sengketa. Nasabah diberikan hak untuk menyampaikan keluhan atas kerugian yang dialaminya. Mekanisme ini bertujuan untuk memulihkan hak dan kepentingan nasabah. Perlindungan represif juga mencakup penindakan terhadap pelaku kejahatan. Dengan demikian, hukum berfungsi sebagai sarana penegakan keadilan.

Pengaturan perlindungan nasabah tercermin dalam kewajiban penyelenggara layanan untuk menjaga keamanan sistem elektronik. Bank dituntut untuk menerapkan prinsip kehati-hatian dalam setiap operasional layanan digital. Prinsip ini bertujuan untuk mengurangi risiko yang dapat merugikan nasabah. Apabila prinsip tersebut tidak dijalankan dengan baik, potensi kerugian akan meningkat. Oleh karena itu, pengawasan terhadap penyelenggaraan layanan menjadi sangat penting. Perlindungan nasabah merupakan tanggung jawab yang tidak dapat diabaikan(Tanumulia *et al.*, 2024).



Gambar 1. Deretan Kebocoran Data
Sumber: https://www.idxchannel.com/economics/deretan-kebocoran-data-e-commerce-dan-sektor-perbankan-seberapa-bahaya

Perlindungan hukum di perbankan juga mencakup pengamanan data pribadi nasabah. Informasi pribadi nasabah dianggap sangat penting karena dapat memengaruhi keamanan finansial mereka. Oleh sebab itu, bank wajib menjaga kerahasiaan data agar tidak disalahgunakan oleh pihak yang tidak berhak. Setiap kebocoran data bisa menimbulkan risiko serius bagi nasabah, termasuk kerugian finansial dan pelanggaran privasi. Pengelolaan data harus dilakukan secara hati-hati, aman, dan sesuai dengan prosedur yang berlaku. Bank sebagai pengelola sistem menanggung tanggung jawab penuh atas perlindungan data tersebut.

Seluruh aktivitas pengolahan data harus mempertimbangkan kemungkinan ancaman dan cara mitigasinya. Kegagalan dalam menjaga data dapat merugikan nasabah sekaligus menurunkan reputasi bank. Perlindungan data pribadi bukan sekadar kewajiban formal, tetapi merupakan bagian penting dari tanggung jawab hukum bank. Penerapan kebijakan keamanan yang efektif dapat meningkatkan kepercayaan nasabah terhadap layanan. Dengan begitu, perlindungan data menjadi unsur krusial dalam keseluruhan sistem perlindungan hukum nasabah.

Keberadaan perlindungan hukum memberikan rasa aman dan kepercayaan bagi nasabah dalam menggunakan layanan digital. Rasa aman tersebut mendorong masyarakat untuk memanfaatkan teknologi secara berkelanjutan. Tanpa perlindungan yang memadai, tingkat kepercayaan masyarakat dapat menurun. Perlindungan hukum menjamin bahwa kerugian yang dialami nasabah mendapatkan perhatian serius. Dengan demikian, hukum berperan sebagai penyeimbang dalam hubungan antara bank dan nasabah. Hubungan yang adil tercipta apabila hak dan kewajiban dihormati(Romli *et al*., 2024).

Perlindungan hukum yang efektif membutuhkan keterlibatan semua pihak yang terkait. Tidak hanya bank dan regulator, tetapi juga nasabah sebagai pengguna layanan. Nasabah diharapkan memiliki kesadaran dalam menjaga keamanan informasi pribadinya. Literasi hukum dan literasi digital menjadi faktor penting dalam efektivitas perlindungan. Dengan kerja sama yang baik, risiko kerugian dapat diminimalkan. Perlindungan hukum yang optimal akan menciptakan sistem perbankan digital yang lebih aman.

B. Tanggung Jawab Pihak Perbankan dalam Menangani Kerugian Nasabah

Pihak perbankan memegang peranan penting dalam memastikan keamanan layanan perbankan berbasis digital. Sebagai penyedia layanan, bank bertanggung jawab terhadap pengelolaan sistem yang digunakan oleh nasabah. Tanggung jawab ini timbul karena bank memiliki kendali atas infrastruktur teknologi yang dijalankan. Kepercayaan nasabah terhadap layanan digital sangat bergantung pada kemampuan bank menjaga keamanan tersebut. Oleh karena itu, bank harus mampu

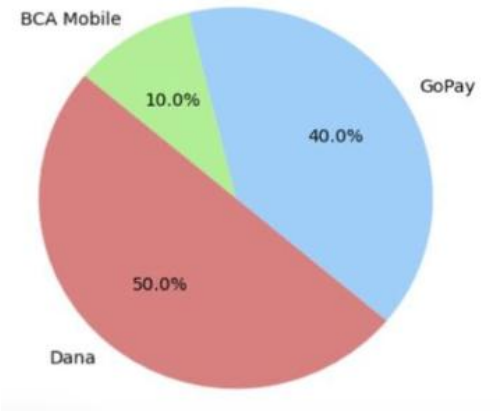
mengantisipasi berbagai risiko yang dapat merugikan nasabah. Tanggung jawab ini merupakan konsekuensi dari hubungan hukum antara bank dan pengguna layanan(Yetno, 2024).

Tabel 1. Contoh Kasus Kerugian Nasabah dan Tanggung Jawab Bank

Kasus	Tanggung Jawab Bank
Data nasabah dicuri oleh pihak luar	Bank harus membuktikan sistem keamanan memadai. Kelalaian dapat menimbulkan tuntutan hukum.
Identitas palsu digunakan untuk aktivasi mobile banking	Bank wajib memperketat verifikasi identitas. Sistem lemah menunjukkan kelalaian operasional.
Akun nasabah tidak segera diblokir setelah laporan	Bank bisa memperbesar kerugian nasabah. Tindakan cepat mencerminkan tanggung jawab institusi.
Prosedur penyelesaian sengketa transaksi tidak sesuai standar	Bank wajib mengikuti standar penyelesaian sengketa. Kesalahan prosedur bisa merugikan posisi hukum bank.
Ganti rugi ditolak tanpa penjelasan jelas	Bank harus memberikan alasan secara transparan. Penolakan sepihak melanggar hak nasabah.

Tanggung jawab perbankan terlihat pada implementasi prinsip kehati-hatian pada setiap aktivitas operasional. Prinsip inipunmengharuskan bank agar senantiasa mengidentifikasi serta mengendalikan potensi risiko keamanan. Impelementasi teknologi pengamanan beragam jadisuatu bentuk penerapan tanggung jawab tersebut. Dengan memperbarui sistem yang berkala butuh diadakanagar bisa menghadapi perkembangan kejahatan siber. Lalai dalam mengimplementasikan prinsip kehati-hatian bisa menambah risiko kerugian. Pada keadaan tertentu, hal inipun bisa memunculkan pertanggungjawaban hukum pada pihak bank.

Selain itu, tanggung jawab perbankan juga meliputi penanganan kerugian yang dirasakan bagi seorang nasabah. Penyediaan saluran pengaduandari bankserta kemudahan mengaksesserta transparan. Lewatlangkah ini, nasabah bisa mengeluarkan keluhan atas kerugian yang terjadi. Tahap menangani pengaduan harus diadakan dengan profesional dan objektif. Bank juga berkewajiban membentukkejelasanterkait persoalanyang dirasakan nasabah. Hal ini ditujukan agar memenuhi hak nasabah atas kejelasan informasinya itu(Setiono *et al.*, 2022).



Gambar 2. Layanan Digital
Sumber: https://lensametro.com/mengungkap-pola-kejahatan-phising-di-sektor-perbankan-dan-dompet-digital/

Tanggung jawab bank tidak hanya terbatas pada aspek teknis, tetapi juga mencakup aspek administratif dan komunikasi. Bank harus menyampaikan informasi yang benar dan mudah dipahami mengenai penggunaan layanan digital. Informasi yang jelas membantu nasabah memahami risiko dan cara penggunaan layanan dengan aman. Kurangnya informasi dapat meningkatkan potensi kesalahan pengguna. Oleh karena itu, transparansi menjadi bagian penting dari tanggung jawab perbankan. Komunikasi yang efektif berperan dalam mencegah terjadinya kerugian(Annafa, 2024).

Dalam menghadapi kerugian nasabah, bank dituntut untuk bersikap adil dan proporsional. Setiap kasus perlu ditangani berdasarkan fakta dan ketentuan yang berlaku. Bank tidak dapat secara sepihak membebankan seluruh tanggung jawab kepada nasabah. Evaluasi terhadap penyebab kerugian harus dilakukan secara menyeluruh. Pendekatan yang adil akan membantu menjaga kepercayaan nasabah. Sikap profesional menjadi cerminan tanggung jawab bank dalam penyelesaian masalah(Husniyyah, 2024).

Peran perbankan juga terlihat dalam kerja sama dengan pihak berwenang dalam menangani kejahatan siber. Kerja sama ini penting untuk mengungkap pelaku dan mencegah kejadian serupa di masa mendatang. Bank memiliki informasi yang dapat mendukung proses penegakan hukum. Partisipasi aktif bank menunjukkan komitmen terhadap perlindungan nasabah. Dengan adanya kerja sama tersebut, upaya penanggulangan kejahatan dapat berjalan lebih efektif. Tanggung jawab bank tidak hanya bersifat internal, tetapi juga eksternal.

Tanggung jawab perbankan pada akhirnya bertujuan untuk menjaga

kepercayaan masyarakat terhadap sistem keuangan. Kepercayaan merupakan elemen utama dalam hubungan antara bank dan nasabah. Apabila tanggung jawab dijalankan dengan baik, risiko kerugian dapat ditekan. Nasabah akan merasa lebih aman dalam menggunakan layanan digital. Pelaksanaan tanggung jawab secara konsisten akan menciptakan hubungan yang harmonis. Dengan demikian, perbankan berkontribusi dalam menciptakan sistem perbankan digital yang aman dan stabil(Endrawati *et al*., 2024).

C. Upaya Pencegahan untuk Meminimalkan Kerugian Nasabah

Upaya pencegahan ialah strategi yang diperlukan dalam mengurangi tingkat kerugian yang mungkin saja dirasakan nasabah pada layanan perbankan digital. Fokus pencegahan ialah meminimalkan peluang adanya tindakan kejahatan sebelum memunculkan dampak yang lebih luas. Pencegahan tak saja berkaitan pada teknologi, tetapi juga mengikutsertakantindakan pengguna ketika memakai layanan digital.

Seluruhkalangan, termasuk bank juga pihak nasabah, memiliki peran aktif dalam mengimplementasikan beberapa preventif. Persiapan dari bank terkait sistem keamanan yang bisa mengetahui aktivitas mencurigakan sejak awal. Memperbarui serta menjaga teknologi dengan berkala sebagai hal yang diperlukan agar sistem tetap tangguh menghadapi ancaman baru. Dibutuhkan edukasi yang baik untuk pihak nasabah agar lebih sadar terhadap risiko digital dan bisa melakukan tindakan yang preventif.

Perencanaan pencegahan sebaiknya dilaksanakan dengan keseluruhan dan terstruktur supaya seluruh tahapan saling mendukung. Pada pencegahan ini yang berkelanjutan supaya efektivitasnya tetap terpelihara. Kolaborasi dari regulator bersama aparat penegak hukum bisa menguatkan upaya pencegahan dengan berkolektif. Pada implementasi strategi dengan tepat, risiko kerugian nasabah bisa ditekan dengan bersignifikan. Maka dari itu, pencegahan sebagaikeharusan bersama yang menyatukan sistem, manajemen, juga kesadaran penggunanya(Arsyadona *et al.,* 2025).

Tabel 2. Strategi Pencegahan Kerugian Nasabah pada Perbankan Digital

Strategi Pencegahan	Penjelasan Singkat
Peningkatan keamanan sistem	Bank menggunakan lapisan proteksi tambahan dan memonitor transaksi secara kontinu. Sistem diperbarui agar sesuai dengan ancaman terbaru.
Edukasi digital untuk nasabah	Nasabah dibekali pengetahuan agar dapat mengenali modus penipuan. Informasi disampaikan melalui berbagai

	media komunikasi.
Komunikasi aktif dengan nasabah	Bank menyampaikan peringatan dan panduan keamanan secara rutin. Cara ini memudahkan nasabah untuk mengambil tindakan preventif.
Kepatuhan terhadap aturan dan pengawasan	Semua prosedur bank mengikuti regulasi yang berlaku. Pengawasan internal membantu mengurangi kesalahan atau kelalaian.
Kolaborasi dengan pihak eksternal	Bank bekerja sama dengan regulator dan aparat hukum. Pertukaran informasi membuat upaya pencegahan lebih efektif.
Membangun rasa aman nasabah	Strategi pencegahan meningkatkan kepercayaan nasabah. Pengguna terdorong memakai layanan digital dengan lebih hati-hati.

Penguatan sistem keamanan teknologi menjadi salah satu bentuk utama dari upaya pencegahan. Bank dituntut untuk menggunakan teknologi pengamanan yang mampu melindungi transaksi dan data nasabah. Penerapan sistem verifikasi berlapis dapat mengurangi kemungkinan akses yang tidak sah. Selain itu, pemantauan aktivitas transaksi secara berkelanjutan membantu mendeteksi potensi ancaman lebih awal. Sistem keamanan harus terus diperbarui sesuai perkembangan modus kejahatan. Dengan teknologi yang andal, potensi kerugian dapat diminimalkan.

Pencegahan juga berkaitan erat dengan peningkatan pemahaman nasabah terhadap keamanan digital. Nasabah perlu dibekali pengetahuan mengenai risiko penggunaan layanan digital dan cara menghindarinya. Edukasi ini dapat dilakukan melalui berbagai sarana komunikasi yang mudah dijangkau. Dengan pengetahuan yang cukup, nasabah mampu mengenali indikasi penipuan. Kesadaran yang tinggi mendorong nasabah untuk lebih berhati-hati. Literasi digital menjadi elemen penting dalam strategi pencegahan(Lestari *et al*., 2025).

Selain edukasi, komunikasi yang berkelanjutan antara bank dan nasabah juga berperan dalam upaya pencegahan. Bank perlu secara rutin memberikan informasi dan peringatan mengenai potensi ancaman keamanan. Informasi tersebut harus disampaikan secara jelas dan mudah dipahami. Komunikasi yang baik membantu nasabah mengambil langkah pencegahan secara mandiri. Keterbukaan informasi juga meningkatkan rasa percaya terhadap layanan perbankan. Dengan demikian, komunikasi menjadi bagian penting dari pencegahan.

Upaya pencegahan juga didukung oleh penguatan regulasi dan mekanisme pengawasan. Regulasi memberikan pedoman bagi penyelenggara layanan dalam mengelola risiko keamanan. Pengawasan yang efektif memastikan bahwa ketentuan

yang ada dijalankan dengan konsisten. Dengan adanya pengawasan, potensi kelalaian dapat diminimalkan. Regulasi dan pengawasan berfungsi sebagai kontrol terhadap pelaksanaan layanan digital. Hal ini memperkuat sistem pencegahan secara keseluruhan(Hasanah & Sayuti, 2024).

Kolaborasi antara bank, regulator, dan aparat penegak hukum merupakan komponen penting dalam upaya mencegah kerugian nasabah. Kerja sama ini memungkinkan pihak-pihak terkait untuk berbagi informasi mengenai pola dan metode kejahatan siber yang berkembang. Informasi yang diperoleh dapat digunakan untuk merancang langkah-langkah pencegahan yang lebih tepat dan efektif.

Dari koordinasi yang baik, bank bisa memenuhi protokol keamanan internalnya untuk menghadapi ancaman terbaru. Sinergi ini menyegerakan identifikasi risiko yang bisa dilewatkanketika bank bertindak sendiri. Pengalaman dan praktik terbaik dari tiap pihaknya serta bisa diimplementasikan dengan bersama-sama agar menambah tingkat perlindungan. Ketika mengadakan pencegahan yang berkolektif memberi kemungkinan pada pemantauan yang lebih keseluruhanpada kegiatanyang dicurigai.

Seluruh kalangan bisa mengenali pola ancaman yang sulit terlihat secara individual. Kolaborasi nipun memudahkan penentuan langkah tanggap darurat jika terjadi insiden keamanan. Hal ini bisa menambah tingkat kesadaran setiap pihak terhadap tiap tanggung jawab mereka. Dengan bersama sama menerapkan sistem pencegahanmemperoleh lebih efektif daripada denganperlakuan seorang diri. Pendekatan kolektif juga memudahkan pengadaan sistem perbankan digital yang lebih aman dan andal. Dengan demikian, koordinasi dan kerja sama menjadi fondasi utama dalam menjaga keamanan dan integritas layanan perbankan digital.

Upaya pencegahan bertujuan menciptakan rasa aman bagi nasabah dalam menggunakan layanan perbankan digital. Rasa aman tersebut mendorong penggunaan teknologi secara bertanggung jawab. Pencegahan yang dilakukan secara konsisten membantu menjaga stabilitas sistem perbankan. Dengan risiko yang terkendali, kepercayaan masyarakat dapat dipertahankan. Pencegahan bukan hanya kebutuhan, tetapi juga kewajiban dalam era digital. Oleh karena itu, pencegahan harus menjadi prioritas utama dalam layanan perbankan digital(Pasaribu & Ningtias, 2025)

5. Simpulan

A. Kesimpulan

Penggunaan layanan perbankan digital bisa memudahkan masyarakat, namun juga memunculkan risiko kejahatan siber yang buth diantisipasi dengan serius. Kerugian dari pihak nasabah memperlihatkan adanya perlindungan hukum punya peranan yang diperlukanketika menjamin keamanan dan kepastian penggunaan

layanan digital. Perlindungan hukum tak saja fungsinya menjadi sarana penanganan sesudah kerugian terjadi, namun bisa menjadi upaya pencegahan lewat pengaturan dan pengawasan. Tanggung jawab pihak perbankan sebagai faktor utama ketika memelihara keamanan sistem juga menangani dengan penuh keadilan. Mengupayakan hal ini bisa mendukung penguatan teknologi serta menambah tingkat kesadaran pengguna sebagai tahapan strategis ketika meminimalkan risiko kerugian. Sinergi antara perbankan, regulator, dan nasabah dibutuhkan agar membentuk sistem perbankan digital yang aman sertadipercaya.

B. Saran

Lembaga perbankan diinginkan bisa terus menambah tingkat sistem keamanan digital guna menyesuaikan diri pada kemajuan kejahatan siber makin kompleks. Bentuk edukasi bagi nasabah butuh dilaksanakan dengan berkelanjutan supaya pengetahuan yang mendalam terkait keamanan digital makin bertambah. Regulator diinginkan bisa menguatkan pengawasan juga menjamin implementsi perlindungan nasabah terlaksana dengan konsisten. Nasabah juga butuh kehati hatian dalam memelihara kerahasiaan data pribadi dan informasi akses layanan perbankan. Lewat kolaborasi dengan sinergis antara seluruh pihak, risiko kerugian nasabah bisa dikurangiserta bentuk kepercayaan pada layanan perbankan digital bisa selalu dijaga.

6. DaftarPustaka

Amane, A. P. O., Lestari, A., & Badruddin, S. (2025). Inovasi Dan Kebijakan Publik Di Era Digital. Cv. Eureka Media Aksara.

Annafa, S. W. (2024). Tanggung Jawab Hukum Bank Dalam Kasus Kebocoran Data Nasabah. 1(6), 129–135.

Arsyadona, Manik, D. T. S., & Mahyu, F. R. O. (2025). Analisis Risiko: Langkah Strategis Untuk Mencegah Kerugian Dan Meningkatkan Profitabilitas Suatu Perusahaan. (Studi Kasus: Perkembangan Pariwisata Di Kota Medan).

Atmoko, D., & Saputri, A. S. (2022). Hukum Perlindungan Konsumen. Cv. Literasi Nusantara Abadi.

Citriadin, Y. (2020). Metode Penelitian Kualitatif: Suatu Pendekatan Dasar. Sanabil.

Endrawati, E. A., Kaemirawati, D. T., & Herawati, S. (2024). Perlindungan Hukum Sebagai Upaya Meningkatkan Kepercayaan Masyarakat Terhadap Perbankan : Studi Kasus Kejahatan Perbankan Di Indonesia. 13, 589–602. Https://Doi.Org/10.37893/Jbh.V13i2.945

Hasanah, N., & Sayuti, M. N. (2024). Optimalisasi Regulasi Perbankan Syariah Oleh Bank Indonesia Dan Otoritas Jasa Keuangan Dalam Akselerasi Transformasi Digital. 13(03), 709–723.

Husniyyah, N. B. (2024). Pertanggung Jawaban Perbankan Terhadap Nasabah Yang Dirugikan Dalam Pembobolan Rekening Dana Nasabah.

Lestari, P. A., Fasa, M. I., Islam, U., Raden, N., Lampung, I., & Lampung, B. (2025).

Transformasi Digital Banking : Manfaat Dan Risiko Transaksi Online Modern (Internet Banking Dan Mobile Banking) Transformasi Digital Banking : Manfaat Dan Risiko Transaksi Online Modern (Internet Banking Dan Mobile Banking). 3(4).

Lubis, N. S., & Nasution, M. I. P. (2023). Perkembangan Teknologi Informasi Dan Dampaknya Pada Masyarakat.

Natalia, T. S. (2022). Tanggung Jawab Bank Terhadap Penyalahgunaan Data Informasi Nasabah.

Nervia, C., Wardhana, K. A., Sie, P. A., & Talim, T. L. (2025). Analisis Yuridis Terhadap Kejahatan Phising Dalam Sistem Perbankan Digital Melalui Scam Link Berbahaya.

Pasaribu, M. R., & Ningtias, S. R. A. (2025). Perlindungan Nasabah Dalam Penggunaan Layanan Mobile Banking Di Bank Syariah Kota Medan.

Rahmawati, D., Viendyasari, M., Lumakto, G., Kholifatur, R., Anindhita, W., Ameliah, R., Bachna, S., Adienda, A., Pembina, D., Trihandini, I., & Saleh, R. (2024). Waspada Kejahatan Phishing Attack! Pt. Literasi Nusantara Abadi Grup.

Romli, Is, M. S., & Rani, F. H. (2024). Perlindungan Hukum. Cv. Doki Course And Training.

Setiono, G. C., Rahman, I., Ananfa, E. D., Hukum, F., & Kadiri, U. (2022). Tanggung Jawab Bank Sebagai Wujud Perlindungan Hukum Bagi Nasabah Kontrak Perbankan. 5(1), 66–79.

Sihombing, S. M. (2021). Perlindungan Hukum Bagi Debitur Bank Menurut Peraturan Perundang-Undangan Di Indonesia.

Sinta, D., Zakia, S. P., & Safitri, U. (2025). Analisis Perlindungan Hukum Bagi Nasabah Bank Dalam Digitalisasi Layanan Perbankan Di Indonesia.

Tanumulia, R., Astutik, S., Widodo, E., & Unitomo, U. (2024). Perlindungan Hukum Terhadap Kerahasian Data Pribadi Nasabah Di Era Digitalisasi Perbankan.

Yetno, A. (2024). Tanggung Jawab Bank Dalam Menjaga Keamanan Dan Kerahasiaan Data Nasabah Perbankan Di Indonesia.