Journal Terekam Jejak (JTJ), Copyright © 2025
Vol. 3, Num. 1, 2025
https://journal.terekamjejak.com/index.php/jtj/index
Author: **Miftahul Risko, Handaru Lumintang Bagus Krisnadi**

Penegakan Hukum Pidana dan Penanggulangan Perkara Tindak Pidana Penipuan Melalui Transfer Mobile Banking

ABSTRACT

In line with the progress of time, technological innovation has experienced very rapid growth. The development of this technology covers all aspects of human life, from information and communication to the financial sector. In the financial sector, especially banking, utilizing the latest technology to make it easier for customers to make financial transactions by accelerating, facilitating, and simplifying the transaction process. With this technological advancepment, interpersonal social interaction has become easier, but people still need to be vigilant to maintain the security of their important data to avoid unwanted things, including banking data which is often the target of criminals in cyberspace, mostly due to the carelessness and ignorance of bank account owners. Cybercrime or cybercrime is a type of crime related to technology and has been regulated in laws and regulations related to national technology and information, which includes elements of criminal acts committed in cyberspace and are considered to be detrimental to individuals, organizations, or other parties who feel disadvantaged by cybercrime.

Keyword: Countermeasures, Criminal Act, Transfer, Mobile Banking

ABSTRAK

Sejalan dengan kemajuan waktu, inovasi teknologi mengalami pertumbuhan yang sangat cepat. Perkembangan teknologi ini meliputi semua aspek kehidupan manusia, dari informasi dan komunikasi hingga sektor keuangan. Dalam sektor keuangan, terutama perbankan, memanfaatkan teknologi terkini untuk memudahkan nasabah melakukan transaksi keuangan dengan cara mempercepat, mempermudah, dan menyederhanakan proses transaksi. Dengan kemajuan teknologi ini, interaksi sosial antarpersonal menjadi lebih mudah, namun masyarakat tetap perlu waspada untuk menjaga keamanan data penting mereka agar terhindar dari hal-hal yang tidak diinginkan, termasuk data perbankan yang sering menjadi target para penjahat di dunia maya, sebagian besar akibat kecerobohan dan ketidaktahuan pemilik akun perbankan. Kejahatan siber atau kejahatan di dunia maya adalah jenis kejahatan yang berhubungan dengan teknologi dan telah diatur dalam peraturan perundang-undangan yang terkait dengan teknologi dan informasi nasional, yang mencakup unsur-unsur tindak pidana yang dilakukan di dunia maya dan dianggap dapat merugikan individu, organisasi, atau pihak lain yang merasa dirugikan akibat kejahatan siber.

Kata Kunci: Penanggulangan, Tindak Pidana, Transfer, Mobile Banking

PENDAHULUAN

Bank adalah institusi yang memiliki peran yang sangat penting dalam ekonomi. Peran bank menuntun adanya pembinaan dan pengawasan secara efektif untuk seluruh aktivitasnya. Hal ini perlu dilakukan untuk membuat indonesia dapat bersaing secara global. Bank dibutuhkan guna melindungi serta menyalurkan dana masyarakat dengan baik dan aman (Adiwijaya; 2018).

Bank berperan penting dalam perdagangan internasional dan pembangunan nasional. Menurut Pasal 1 Ayat 2 UU Perbankan, bank adalah badan usaha yang menghimpun dana dalam bentuk simpanan masyarakat, kemudian menyalurkannya kepada masyarakat dalam bentuk pinjaman dan bentuk lain untuk pembangunan.

Dalam era di mana teknologi menjadi tulang punggung transaksi keuangan, mobile banking telah menjadi sarana yang sangat populer bagi masyarakat untuk mengelola dan melakukan transaksi keuangannya secara efisien dan mudah. Namun, sejalan dengan meningkatnya penggunaan mobile banking, juga muncul tantangan baru dalam bentuk kejahatan digital, terutama dalam hal penipuan transfer. Kejahatan dalam penipuan transfer mobile banking merupakan ancaman yang serius bagi keamanan finansial individu dan institusi keuangan.

Tindakan penipuan merupakan tindakan merugikan pihak lain sehingga dapat dipidana. Melalui penipuan transfer mobile banking, para pelaku kejahatan dapat dengan mudah memanfaatkan celah-celah dalam sistem keamanan untuk merugikan nasabah dan lembaga keuangan. Dengan modus yang semakin canggih dan kompleks, penjahat mampu menyusup dan mengambil keuntungan secara tidak sah dari transaksi keuangan melalui perangkat mobile.

Oleh karena itu, pentingnya upaya antisipasi dan pencegahan terhadap kejahatan dalam penipuan transfer mobile banking menjadi semakin mendesak. Langkah-langkah perlindungan yang efektif perlu diambil untuk melindungi data dan dana nasabah dari ancaman penipuan yang mengintai.

Dalam konteks ini, pendekatan yang holistik dan berbasis teknologi menjadi kunci dalam memperkuat sistem keamanan mobile banking. Selain itu, kesadaran akan risiko dan tindakan pencegahan yang diperlukan juga perlu ditingkatkan baik dari pihak pengguna maupun penyedia layanan mobile banking.

Dalam tulisan ini, akan dibahas beberapa strategi penanggulangan tindak pidana penipuan yang dapat diterapkan untuk mengurangi risiko kejahatan dalam penipuan transfer mobile banking. Dari upaya teknis hingga sosial, langkah-langkah tersebut bertujuan untuk menjaga integritas dan keamanan dalam transaksi keuangan digital, sehingga masyarakat dapat menggunakan layanan mobile banking dengan lebih aman dan percaya (Haryadi; 2019). Penanggulangan tindak pidana penipuan melalui transfer mobile banking sangatlah penting untuk menyadari kompleksitas dan kerentanan yang terlibat dalam penggunaan teknologi keuangan modern. Dengan kemajuan teknologi, mobile banking telah menjadi sarana yang populer dan nyaman bagi individu untuk melakukan transaksi keuangan. Namun, seiring dengan kepopulerannya, muncul pula ancaman penipuan yang semakin canggih dan kompleks. Tindak pidana penipuan melalui mobile banking sering kali melibatkan skema penipuan yang rumit, seperti phishing, malware, dan social engineering, yang dapat merugikan pengguna secara finansial.

Maka dari itu, penting untuk mengidentifikasi risiko-risiko yang terkait dengan penggunaan mobile banking dan mengembangkan strategi penanggulangan yang efektif. pentingnya kolaborasi antara pemerintah, lembaga keuangan, penyedia layanan, dan masyarakat dalam melawan tindak pidana penipuan melalui transfer mobile banking. Melalui pendekatan yang terintegrasi dan upaya bersama, diharapkan dapat menciptakan lingkungan keuangan yang lebih aman dan terpercaya bagi semua pihak yang terlibat.

METODE PENELITIAN

Penelitian ini merupakan sebuah upaya yang dilakukan dengan pendekatan normatif, yang merujuk pada metode studi kepustakaan (library research) yang digunakan untuk mengeksplorasi dan menganalisis teori, konsep, serta peraturan perundang-undangan yang relevan dengan bidang penelitian ini. Pendekatan normatif ini mendasarkan analisisnya pada pemahaman yang mendalam terhadap berbagai bahan data sekunder, termasuk literatur, kamus hukum, beragam buku referensi, jurnal ilmiah, dan artikel- artikel yang terkait.

HASIL DAN PEMBAHASAN

Identifikasi Risiko

Penipuan melalui mobile banking adalah tindakan memanipulasi atau menipu pengguna layanan perbankan elektronik, seperti transfer dana, pembayaran tagihan, atau penggunaan kartu kredit, dengan cara yang merugikan korban secara finansial. Ini bisa meliputi pencurian informasi login, transaksi yang tidak sah, atau praktik penipuan lainnya yang dilakukan melalui aplikasi atau platform perbankan yang diakses melalui perangkat mobile seperti ponsel atau tablet. Di era digitalisasi dan teknologi saat ini, banyak layanan perbankan, termasuk layanan produk mobile banking yang berbasis digital, memberikan banyak keunggulan dalam kenyamanan nasabah. Namun penggunaan dan risiko tidak dapat dipisahkan (Hasan; 2024).

Perbankan melalui mobile banking menawarkan banyak keuntungan bagi nasabah yang memanfaatkan fasilitas tersebut, namun di sisi lain juga terdapat beberapa kekurangan dari layanan mobile banking ini. Misalnya saja kesalahan manusia, penipuan, kejahatan dunia maya, atau kesalahan lainnya yang mungkin terjadi saat menggunakan layanan mobile banking kami. Meskipun penggunaan TI mengandung berbagai risiko, namun tidak dapat dipungkiri bahwa

penggunaan layanan yang memanfaatkan teknologi semakin meningkat (Rokhman, 2020).

Risiko penipuan transfer uang mobile banking dapat timbul dari berbagai faktor, antara lain: Kelemahan keamanan sistem, kemungkinan kesalahan entri data, dan kemungkinan pengguna memfasilitasi penipuan (Atmaja, 2018). Untuk mengendalikan risiko penipuan kawat di mobile banking, bank harus mengembangkan dan menerapkan strategi pencegahan penipuan yang efektif, termasuk menganalisis data transaksi untuk mencari pola yang menunjukkan risiko tinggi. Bank juga harus menjamin keamanan data nasabah, menggunakan sistem yang aman, dan memverifikasi transaksi yang dilakukan. Pelanggan juga harus mengambil langkah-langkah keamanan seperti menggunakan rekening giro dan platform tepercaya.

Aplikasi perbankan seluler menggunakan aplikasi perangkat lunak yang dikembangkan khusus dan dipasang di ponsel cerdas atau tablet, memberikan antarmuka yang lebih mudah digunakan daripada SMS atau perbankan melalui browser seluler (Hasan, 2024). Ini membuatnya menjadi saluran pengiriman mobile banking yang berkembang paling pesat. Namun, saluran ini memiliki risiko yang mungkin timbul jika pihak ketiga menulis kode untuk aplikasi ini dan jika pelanggan menginstal perangkat lunak yang berbahaya, rusak, atau berbahaya (Wahid, 2018).

Penyimpanan data pelanggan di ponsel atau tablet dapat dimanfaatkan jika perangkat tersebut hilang atau dicuri. Selain itu, serangan potensial terhadap mobile banking meliputi permintaan penipuan, seperti email phishing atau pesan SMS, yang meminta instalasi aplikasi baru atau fitur keamanan bank, atau pencurian kredensial pengguna yang dapat digunakan untuk mencuri nomor rekening dan meminta Anda memasukkan akun dan kata sandi (Hamzah, 2019).

Sumber informasi yang sangat berguna tentang risiko keamanan seluler adalah *Open Web Application Security Project* (OWASP), sebuah organisasi nirlaba global yang berfokus pada peningkatan keamanan perangkat lunak aplikasi web. Mereka telah menyusun daftar 10 risiko teratas yang muncul dari

penggunaan aplikasi seluler. Di bawah ini adalah ringkasan risiko yang kami anggap paling relevan bagi bank komunitas (Amin, 2020):

1. Penyimpanan data yang tidak aman, termasuk kehilangan atau pencurian ponsel atau tablet, serta kemungkinan malware mengakses perangkat.
2. Kontrol yang lemah di sisi server, termasuk keamanan, autentikasi, dan kontrol yang harus kuat pada komputer backend yang digunakan dalam proses mobile banking.
3. Perlindungan lapisan transportasi yang tidak memadai, yang mengakibatkan data tidak dienkripsi saat dikirim melalui jaringan publik.
4. Otorisasi dan autentikasi yang tidak memadai, di mana beberapa aplikasi seluler hanya mengandalkan nilai autentikasi yang dapat disusupi, dan beberapa informasi pengidentifikasian mungkin tetap ada bahkan setelah dihapus atau disetel ulang.

Meskipun mobile banking membawa risiko, ancaman, dan tantangan keamanan baru bagi lembaga keuangan, tidak ada rencana mitigasi risiko yang dapat sepenuhnya menghilangkan risiko. Namun, bank harus mengembangkan prosedur yang dapat memastikan bahwa proses mobile banking tetap efektif. Dengan mewaspadai risiko keamanan dan mengembangkan praktik perbankan seluler yang efektif, bank dapat mengurangi dan mengelola risiko hukum, operasional, dan reputasi dengan lebih baik (Oktaviani, 2022).

Strategi Pengamanan

Penting untuk meningkatkan kesadaran masyarakat tentang risiko penipuan melalui mobile banking. Program edukasi dapat mencakup pengenalan taktik penipuan yang umum, langkah-langkah pencegahan, dan cara melaporkan aktivitas mencurigakan (Farra, 2024). Antisipasi kejahatan dalam penipuan

transfer mobile banking merupakan hal penting untuk menjaga keamanan finansial. Beberapa langkah atau strategi yang bisa diambil meliputi:

1. Pendidikan dan Kesadaran: Edukasi pengguna mengenai risiko penipuan dan praktik keamanan yang baik sangat penting. Ini bisa dilakukan melalui kampanye kesadaran dan panduan pengguna.
2. Verifikasi Identitas: Pastikan bahwa pengguna yang melakukan transfer 8adalah pemilik sah akun tersebut dengan memverifikasi melalui metode autentikasi ganda, seperti kode OTP atau biometrik.
3. Pemantauan Transaksi: Sistem pemantauan transaksi yang canggih dapat mendeteksi pola transaksi yang mencurigakan dan menghentikan transaksi yang tidak sah.
4. Enkripsi Data: Pastikan bahwa semua data yang ditransfer melalui aplikasi mobile banking dienkripsi dengan aman untuk melindungi informasi sensitif pengguna.
5. Pembaruan Perangkat Lunak: Pastikan aplikasi mobile banking selalu diperbarui dengan versi terbaru untuk memperbaiki kerentanan keamanan dan melindungi pengguna dari serangan yang sudah diketahui.
6. Validasi Penerima: Sebelum melakukan transfer, pastikan untuk memverifikasi informasi penerima dengan cermat, terutama jika itu melibatkan penerima baru atau tidak dikenal.
7. Pemeriksaan Reguler: Lakukan pemeriksaan reguler terhadap aktivitas akun, termasuk saldo dan transaksi terakhir, untuk mendeteksi aktivitas yang mencurigakan dengan cepat.
8. Laporkan Kecurangan: Jika ada kecurigaan aktivitas penipuan, segera laporkan ke pihak bank atau penyedia layanan mobile banking agar langkah- langkah pencegahan dapat diambil secepat mungkin.

Peran Teknologi

Teknologi memiliki peran krusial dalam perkembangan mobile banking. Melalui aplikasi perbankan di ponsel, teknologi memungkinkan akses ke layanan perbankan kapanpun dan di manapun. Ini memberikan kemudahan bagi pengguna untuk melakukan berbagai transaksi seperti pembayaran tagihan, transfer dana, cek saldo, dan bahkan investasi, tanpa harus mengunjungi kantor cabang fisik (Ilyas, 2019).

Selain itu, teknologi juga meningkatkan keamanan dengan fitur keamanan seperti autentikasi dua faktor dan enkripsi data, serta memberikan kemudahan aksesibilitas bagi mereka yang memiliki keterbatasan fisik, atau mobilitas pengaruh kemampuan sistem teknologi yang semakin canggih; meningkatnya minat transaksi mobile banking. Sejalan dengan pernyataan Kotler dan Keller (2012), bahwa kapabilitas sistem teknologi mewakili aspek kunci dari karakteristik bersama fitur mobile banking (Bachtiar, 2020). Kemampuan ini mencakup keseluruhan fitur dan atribut suatu produk atau layanan. Pemberian kualitas dicapai melalui layanan yang ditawarkan kepada nasabah, dan akses e-banking lebih sederhana dan cepat dibandingkan perusahaan pesaing.

Kemudahan penggunaan mengurangi upaya yang dibutuhkan individu untuk mempelajari TI. Perbandingan kemudahan ini memberikan indikasi bahwa individu yang menggunakan teknologi informasi mengalami alur kerja yang lebih lancar dibandingkan dengan mereka yang tidak menggunakan teknologi informasi. Keberhasilan e-banking dapat dikaitkan dengan kemampuannya dalam memenuhi kebutuhan nasabah melalui pemanfaatan fitur. Inovasi produk tidak lepas dari ketersediaan teknologi yang sesuai, pengenalan produk yang sesuai, dan pengembangan layanan relevan yang memfasilitasi layanan e- banking yang lebih mudah bagi nasabah.

Menurut Kotler (2014), layanan mencakup tindakan atau aktivitas yang dapat ditawarkan oleh satu pihak kepada pihak lain. Mendorong inovasi teknologi dalam pengembangan solusi keamanan yang lebih baik, seperti kecerdasan buatan dan analisis data, penting untuk mendeteksi pola penipuan

yang kompleks. Perusahaan teknologi keuangan harus terus meningkatkan keamanan platform mobile banking mereka dengan menerapkan enkripsi data yang kuat, autentikasi multi-faktor, dan deteksi anomali untuk melindungi pengguna dari serangan cyber (Hasan, 2023).

Menghindari Tindak Pidana Penipuan

Beberapa cara menghindari tindak pidana penipuan bank digital menurut Otoritas Jasa Keuangan (OJK) antara lain (Bachtiar, 2018):

1. Jaga kerahasiaan PIN Anda dari siapapun.
2. Jangan catat atau simpan PIN SMS banking di tempat umum.
3. Verifikasi detail transaksi sebelum konfirmasi.
4. Tunggu respons transaksi setiap kali bertransaksi.
5. Cek notifikasi transaksi (SMS/email) di inbox dan laporkan ke bank jika ada kejanggalan.
6. Segera ganti PIN jika dicurigai diketahui pihak lain.
7. Laporkan kehilangan/pencurian/pergantian kepemilikan SIM Card GSM ke bank atau call center secepatnya.
8. Waspadai aplikasi internet berbahaya (spam/malware) yang berpotensi mencuri dan menyalahgunakan data pribadi.
9. Hindari transaksi internet di jaringan publik (warnet, Wi-Fi gratis) karena risiko pencurian data.
10. Selalu *log out* setelah selesai menggunakan internet banking.
11. Pastikan seluruh data terhapus saat mengganti ponsel untuk mencegah penyalahgunaan.

KESIMPULAN

Kesimpulan dari materi ini adalah bahwa meskipun layanan mobile banking memberikan banyak keunggulan dalam hal kenyamanan bagi nasabah, penggunaan teknologi ini juga membawa risiko yang tidak dapat diabaikan, seperti penipuan, kesalahan manusia, dan ancaman keamanan dunia maya lainnya. Namun, dengan pengembangan strategi pencegahan penipuan yang efektif dan penerapan langkah-langkah keamanan yang tepat, bank dapat mengurangi dan mengelola risiko yang terkait dengan penggunaan mobile banking, seperti pendidikan dan kesadaran pengguna, verifikasi identitas, pemantauan transaksi, enkripsi data, pembaruan perangkat lunak, validasi penerima, pemeriksaan reguler, dan pelaporan kecurangan.

Selain itu, penting juga untuk mengakui peran teknologi dalam meningkatkan efisiensi layanan perbankan dan memenuhi kebutuhan nasabah melalui inovasi produk yang sesuai dengan perkembangan teknologi, sehingga keberhasilan e-banking dapat dicapai melalui pemanfaatan fitur yang sesuai dengan kebutuhan nasabah dan pengembangan layanan yang relevan, dengan memastikan keamanan dan kenyamanan bagi para pengguna. Perkembangan teknologi perbankan ini sangat memudahkan dan mempercepat proses transaksi keuangan, dengan demikian para pengguna transaksi internet m-banking harus tetap menjaga dan tetap waspada terhadap adanya kejahatan dalam dunia elektronik termasuk elektronik perbankan, atas keamanan akun, identitas dan keamanan tentang internet m-banking.

DAFTAR PUSTAKA

Adiwijaya, I Gusti Bagus Putra. 2018. Kemudahan Penggunaan, Tingkat Keberhasilan Transaksi, Kemampuan Sistem Teknologi, Kepercayaan dan Minat Bertransaksi Menggunakan Mobile Banking. Jurnal Manajemen Bisnis. Vol 15.No. 3.

Amin, Rahman. 2020. Hukum Pembuktian Dalam Perkara Pidana dan Perdata. Yogyakarta: Deepublish.

Atmaja, Gede Marhaendra Wija. 2018. Hukum Perundang-undangan. Sidoarjo: Uwais Inspirasi Indonesia.

Bachtiar. 2018. Metode Pnenelitian Hukum. Tanggerang: Unpam Press. Barkatullah, Abdul Halim. 2020.. Hukum Transaksi Elektronik Di Indonesia. Bandung: Penerbit Nusa Media Efritadewi. 2020. Modul Hukum Siber. Tanjung Pinang: Umrah Press.

Farra, Maysa Al. 2024. Penegakan Hukum Pidana Terhadap Pelaku Pencurian Data (Phising) Pada Bri Mobile Banking (Brimo).

Hamzah, Andi. 2019. Surat Dakwaan Dalam Hukum Acara Pidana Indonesia. Bandung: Alumni.

Haryadi, Dwi. 2018. Kebijakan Integral Penanggulangan Cyberporn Diindonesia. Semarang: Lima.

Hasan, Z. (2019). Sosiologi: hukum, masyarakat, dan kebudayaan integrasi nilai sosial untuk pembangunan (Cet. 1). Bandar Lampung:

Hasan, Z. (2025). Mewujudkan keadilan substantif dalam penegakan hukum pidana di Indonesia: Studi empirik terhadap praktik keadilan koordinatif. UBL Press.

Hasan, Z. 2023. Faktor Penyebab Tindak Pidana Perampokan Bank Arta Kedaton di Bandar Lampung. Jurnal Pendidikan Dan Ilmu Sosial. Vol 1 No 3.

Hasan, Z. 2023. Penegakan Hukum Terhadap Pelaku Tindak Pidana Perjudian Online. Jurnal Multi Disiplin Dehasen (MUDE) Vol 2 No 3.

Hasan, Z. 2024. Kejahatan Mayantara Berupa Tindak Pidana Perjudian Melalui Media Elektronik. Journal Of Social Science Research. Vol 4 No 1.

Ilyas, Amir. 2019. Asas-Asas Hukum Pidana. Yogyakarta: Mahakarya Rangkang Offset Yogyakarta.

Lubis, Fauziah. 2020. Bunga Rampai Hukum Acara Pidana. Medan: Manhaji. Margono. 2019. Asas Keadilan, Kemanfaatan, dan Kepastian Hukum dalam Putusan Hakim. Jakarta Timur: Sinar Grafika.

Oktaviani, Sukma. 2022. Analisi Manajemen Risiko Layanan Mobile Banking Pada Bank Syariah.jurnal Manjemen dan Penellitian Akuntansi. Vol 15. No 1.

Rokhman, Miftakhur. Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangan Dalam Sistem Hukum Indonesia, Vol 23, No 2, Desember, 2020.

Wahid, Abdul. 2018, Kejahatan Mayantara (cyber Crime), PT Refika, Jakarta.