HUMANITIS: Jurnal Humaniora, Sosial dan Bisnis
Vol. 1 No. 9 2024, hal. 475-482 e-ISSN: 2988-6287

PENAGGULANGAN TINDAK PIDANA PENIPUAN MELALUI TRANSFER MOBILE MBANKING

Zainudin Hasan *[1]
Fakultas Hukum Universitas Bandar Lampung
zainudinhasan@ubl.ac.id

Anisa Merti Ayu
Fakultas Hukum Universitas Bandar Lampung
annisamertiayu123@gmail.com

Chinthia Dita M
Fakultas Hukum Universitas Bandar Lampung
chinthia7@gmail.com

Mayse Trisnawati
Fakultas Hukum Universitas Bandar Lampung
Miseeiskandarrm@gmail.com

M. Ardan Aldika R.A
Fakultas Hukum Universitas Bandar Lampung
ardanaldika@gmail.com

ABSTRACT

As time goes by, technological developments have increased very rapidly. The development of this technology has penetrated all aspects of human life, from information and communication to the financial sector. In the financial world, especially banking, utilizes advances in technology to make it easier for customers to carry out financial transactions by shortening, simplifying and speeding up transactions. Through the development of this technology, it makes it easier for social interaction between one another, but behind that, all people must continue to anticipate to maintain the security of their important data in order to avoid unwanted things and one of them is their banking data which is often targeted. Criminals in the internet world are rampant because of the carelessness and ignorance of banking account holders. Crime in cyberspace or cyber (cyber crime) is a form of crime related to the world of technology and has been regulated in laws and regulations relating *to technology and national information which contain elements of criminal acts committed in cyberspace which are considered to be detrimental to people. others, organizations or other parties who feel they have been harmed by crime in cyberspace.*

Keywords*: Countermeasures, Criminal Act, Transfer, Mobile Banking*

ABSTRAK

Seiring berkembangnya jaman, perkembangan teknologi mengalami peningkatan yang begitu pesat. Perkembangan teknologi ini masuk kesemua tataan kehidupan manusia mulai dari untuk informasi dan komunikasi hingga dalam bidang keuangan. Dalam dunia keuangan khususnya perbankan memanfaatkan kemajuan teknologi untuk mempermudah nasabah dalam melalukan transaksi keungan dengan mempersingkat, mempermudah dan mempercepat dalam melakukan transaksi. Melalui perkembangan teknologi ini mempermudah adanya interaksi

[1] Korespondensi Penulis.

sosial antara yang satu dengan yang lainnya, namum dibalik itu semua masyarakat harus tetap berantisipasi untuk menjaga keamanan data-data penting miliknya agar terhindar dari hal-hal yang tidak diinginkan dan salah satunya adalah data perbankannya yang sering menjadi sasaran para penjahat di dunia internet yang marak terjadi karena kecerobohan dan ketidaktahuan dari pemilik akun perbankan. Kejahatan di dunia maya atau siber (cyber crime) merupakan bentuk kejahatan yang berkaitan dengan dunia teknologi dan sudah diatur dalam peraturan Perundang-Undangan yang berkaitan dengan teknologi dan informasi nasional yang memuat unsur-unsur tindak pidana yang dilakukan dalam dunia maya yang dianggap dapat merugikan orang lain, organisasi ataupun pihak lain yang merasa telah dirugikan oleh adanya kejahatan dalam dunia maya.
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 pada semua aktivitas perbankan.hal ini perlu dilakukan untuk pembinaa dan pengawasan yang efektif yang didasari oleh gerak kokoh dari lembaga perbankan yang akan membuat indonesa mampu bersaing di era global secara efisien,wajar, mampu melindungi serta menyalurkan dana masyarakat secara baik dan aman (Sukma Oktaviani, 2022).

Kemajuan informasi dan teknologi telah memberikan dampak yang luas terhadap Indonesia, termasuk industri keuangan sebagai lembaga keuangan, bank berperan penting dalam perdagangan internasional dan upaya pembangunan nasional. Berdasarkan Undang-Undang Nomor 7 Tahun 1992 dan Tambahan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan (Sukma Oktaviani, 2022). Menurut Pasal 1 Ayat 2 UU Perbankan, bank adalah badan usaha yang menghimpun dana dalam bentuk simpanan dari masyarakat dan menyalurkannya kepada masyarakat dalam bentuk pinjaman dan bentuk lain untuk pembangunan masyarakat yang sehat standar hidup masyarakat (Ilyas, Amir. 2019).

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, (Gusti Bagus Putra Adiwijaya, 2018) 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 suatu tindakan yang merugikan orang lain sehingga dapat dikenakan hukum pidana. Pada pasal 378 KUHP bahwa siapa dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hak,menggunakan nama palsu atau sifat palsu aataupun menggunakan tipu muslihat atau susunan kata-kata bohong, menggerakan orang lain untuk menyerahkan suatu benda atau mengadakan suatu perjanjian hutang atau meniadakan suatu piutang, karena salah telah melakukan penipuan, dihukum dengan hukuman penjara selama-lamanya empat tahun.

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 yang dilakukan 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 (Haryadi, Dwi. 2019) 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. 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 dan menyebabkan kerugian yang signifikan. Oleh karena 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 (Zainudin Hasan, 2024) normatif, yang merujuk pada metode studi kepustakaan (library research) yang digunakan untuk mengeksplorasi dan menganalisis teori-teori, konsep-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.

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.

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.

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.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. 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.

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.

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:

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, otentikasi, 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 otentikasi yang tidak memadai, di mana beberapa aplikasi seluler hanya mengandalkan nilai autentikasi yang dapat disusupi, dan beberapa informasi pengidentifikasi mungkin tetap ada bahkan setelah dihapus atau disetel ulang (Zainudin Hasan, 2024).

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.

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. 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 (Amin, Rahman, 2023) adalah pemilik sah akun tersebut dengan memverifikasi melalui metode otentikasi 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.

Kombinasi dari langkah-langkah ini dapat membantu mengurangi risiko penipuan transfer mobile banking.

Peran Teknologi

Teknologi memiliki peran krusial dalam perkembangan mobile banking. Melalui aplikasi perbankan di ponsel, teknologi memungkinkan akses ke layanan perbankan kapan saja dan di mana saja. Ini memberikan kemudahan bagi pengguna untuk melakukan berbagai transaksi seperti transfer dana, pembayaran tagihan, cek saldo, dan bahkan investasi, tanpa harus mengunjungi kantor cabang fisik. Selain itu, teknologi juga meningkatkan keamanan dengan fitur keamanan seperti otentikasi dua

faktor dan enkripsi data, serta memberikan kemudahan aksesibilitas bagi (Batchtiar, Bandung, 2020) mereka yang memiliki keterbatasan fisik atau mobilitas

Pengaruh kemampuan sistem teknologi yang semakin tinggi meningkatnya minat terhadap transaksi mobile banking sejalan dengan pernyataan Kotler dan Keller (2012) bahwa kapabilitas sistem teknologi mewakili aspek kunci dari karakteristik bersama fitur mobile banking. Kemampuan ini mencakup keseluruhan fitur dan atribut suatu produk atau layanan yang memengaruhi kemampuannya untuk memenuhi kebutuhan yang dinyatakan atau tersirat. Pemberian kualitas dicapai melalui layanan yang ditawarkan kepada nasabah, dan akses e-banking lebih sederhana dan cepat dibandingkan perusahaan pesaing. Kemudahan penggunaan mengurangi upaya, baik dari segi waktu dan tenaga, 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 apa pun yang dapat ditawarkan oleh satu pihak kepada pihak lain, yang pada dasarnya tidak berwujud dan tidak menimbulkan kepemilikan apa pun. Lalu terus mendorong inovasi teknologi dalam pengembangan solusi keamanan yang lebih baik, seperti kecerdasan buatan dan analisis data, untuk mendeteksi pola penipuan yang kompleks. Perusahaan teknologi keuangan harus terus meningkatkan keamanan platform mobile banking mereka dengan menerapkan enkripsi data yang kuat, otentikasi multi-faktor, dan deteksi anomali untuk melindungi pengguna dari serangan cyber.

Cara Agar Terhindar Dari Tindak Pidana Penipuan

Dengan maraknya modus penipuan dan kejahatan digital menjaga kerahasiaan informasi login, menggunakan koneksi internet yang aman, menghindari tautan atau aplikasi yang mencurigakan, memeriksa transaksi secara berkala, dan menggunakan fitur keamanan tambahan yang disediakan oleh penyedia layanan mobile banking.lainnya, Otoritas Jasa Keuangan (OJK) membagikan tips untuk masyarakat agar dapat menghindari kejahatan *digital banking* atau bank digital. Berikut adalah tips menghindari kejatahan digital banking dari OJK:

1. Tidak memberitahukan data rahasia yaitu kode akses/nomor pribadi Personal Identification Number (PIN) kepada pihak lain.
2. Tidak mencatat dan menyimpan kode akses/nomor pribadi SMS banking di tempat yang mudah diketahui orang lain.
3. Memeriksa transaksi secara teliti sebelum melakukan konfirmasi atas transaksi tersebut untuk dijalankan.
4. Setiap kali melakukan transaksi, baiknya menunggu selama beberapa saat hingga menerima respon balik atas transaksi tersebut.
5. Untuk setiap transaksi, nasabah akan menerima pesan notifikasi atas transaksi berupa SMS atau email yang akan tersimpan di dalam inbox. Periksa secara teliti isi notifikasi tersebut dan segera kontak ke bank apabila ada transaksi yang mencurigakan.

6. Jika merasa PIN Anda diketahui oleh orang lain, segera lakukan penggantian PIN.
7. Bila kehilangan SIM Card GSM atau dicuri/dipindahtangankan kepada pihak lain, segera beritahukan ke cabang bank terdekat atau segera melaporkan ke call center bank tersebut.
8. Hati-hati dengan aplikasi di internet yang merupakan spam atau *malware* yang mungkin dapat mencuri data-data pribadi dan menyalahgunakannya di kemudian hari.
9. Tidak melakukan transaksi internet di tempat umum seperti warnet, WIFI gratis, karena datadata kita berpotensi dicuri oleh pihak lain dalam jaringan yang sama.
10. Tidak lupa melakukan proses log out setelah selesai melakukan transaksi di internet banking; serta
11. Jika berganti ponsel, pastikan bahwa semua data-data sudah terhapus untuk menghindari penyalahgunaan oleh pihak lain yang menggunakan ponsel tersebut.

KESIMPULAN

Kesimpulan dari materi ini adalah bahwa meskipun layanan mobile (Zainudin Hasan, 2023) 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 mbanking harus tetap menjaga dan tetap waspada terhadap adanya kejahatan dalam dunia elektronik termasuk elektronik perbankan, atas keamanan akun, identitas dan keamanan tentang internet mbanking.

DAFTAR PUSTAKA

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

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.

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

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

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

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.

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

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

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

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

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

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