JURNAL GAGASAN HUKUM
e-ISSN : 2714-8688
p-ISSN : 2828-9196

Article History:
Received: 15-01-2024 | Revised:27-06 | Accepted: 29-06-2024 | Published: 30-06-2024

Upaya Hukum Bagi Korban Kejahatan *Phising* Yang Menguras Saldo *M-Banking*

Akhmad Fery Hasanudin, A Basuki Babussalam
Fakultas Hukum Universitas Muhammadyah Surabaya
e-mail: feryhasundin99@gmail.com

Abstract

Kejahatan *cyber* atau kerap dikenal dengan *cybercrime* merupakan tindakan perilaku kejahatan berbasis komputer serta jaringan internet biasanya si pelaku kejahatan *cyber* biasanya akan meretas sistem untuk memperoleh data korban yang bersifat privasi adapun kejahatan *cyber* yang akan dibahas disini yakni terkait kejahatan *phising*. Maka dari itu penelitian ini bertujuan untuk mengidentifikasi kejahatan *phising* berdasarkan peraturan hukum di indonesia serta mengetahui upaya hukum yang dapat dilakukan oleh korban. Penelitian ini menggunakan metode penelitian hukum normatif yang bersumber dari bahan hukum primer dan skunder dengan menggunakan pendekatan perundang-undangan serta jurnal hukum dan dokument-dokument resmi. Hasil penelitian ini terdapat hasil bahwa upaya hukum bagi korban kejahatan *phising* melalui *chat whatsapp* yang menguras isi saldo m-bankking telah diatur pada Undang-Undang Nomor 11 Tahun 2008 yang diubah menjadi Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE)
Kata Kunci : Upaya hukum, *cybercrime,* kejahatan *phising*.

Abstract

Cyber crime or often known as cybercrime is an act of Computer-Based Crime behavior and internet networks usually the perpetrators of cyber crimes will usually hack the system to obtain victim data that is privacy as for cyber crimes that will be discussed here are related to hacking crimes. An attempt to infiltrate a computer system without permission. Done by sending links and documents that are not clear to the victim to break into the system, steal personal data, and Financial data(m-Banking balance). Therefore, this study aims to identify cyber crimes WhatsApp chat link based on legal regulations in indonesia and know the legal remedies that can be done by the victim. This study uses normative legal research methods sourced from primary and secondary legal materials by using a statutory approach as well as legal journals and official documents, so that from this study there are

results that legal protection for victims of cyber crime through whatsapp chats that drain the contents of m-banking balances has been regulated in Law Number 11 of 2008 which was changed to Law Number 19 of 2016 on information and Electronic Transactions (UU ITE).
Keywords: *legal protection, cyber crime, phishing crime.*

1. PENDAHULUAN

Media sosial merupakan medium di internet yang berkemungkinan untuk mempersentasikan si pengguna untuk berinteraksi, bekerjasama, berbagi, berkomunikasi dengan pengguna yang lain untuk membentuk hubungan sosial secara virtual. Android merupakan sistem operasi untuk telepon seluler yang berbasis Linux. Android menyediakan platform yang terbuka untuk para pengembang atau Developer dalam membuat aplikasi mereka sendiri agar dapat digunakan bermacam peranti bergerak. Android yang biasa digunakan pada Smartphone dan juga di tablet PC. Fungsinya sama seperti sistem operasi Symbian di Nokia, iOS di Apple dan BlackBerry iOS. [1] Salah satu media sosial yang sering digunakan oleh masyarakat yakni Whatsapp dan terdekat ini ditemukan kejahatan *cyber* melalui media sosial tersebut dengan cara mengirimkan *link* ataupun dokumen yang tidak jelas terhadap korban sehingga dapat meretas aplikasi yang ada di handphone ataupun gawai seperti hal nya dompet digital salah satunya M-Banking. [2] Ketika para korban berharap uang mereka kembali namun dalam praktik hukum tidak berseragam pemahaman antara penipuan dalam hukum pidana dan penipuan dalam hukum perdata sehingga hak korban pun terabaikan. [3] Korban dari tindak pidana penipuan ini untuk mendapatkan perlindungan hukum mereka kesulitan [4]. Kekaburan norma dalam perlindungan hukum tersebut terlihat dalam Kitab Undang-Undang Hukum Pidana, dengan Kitab Undang-Undang Hukum Pidana dan Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Penggantian kerugianhanya diatur dalam Undang-Undang Informasi dan Transaksi Elektronik sedangkan dalam KUHP hanya menjerat pelaku dan unsur-unsur pidana.[5]

Kejahatan *cyber* banyak sekali jenisnya namun yang akan dibahas oleh penulis disini terkait kejahatan *phising*. *Phishing* adalah kejahatan peretasan yang

berkembang seiring berjalannya waktu di sektor perbankan. Pada dasarnya, *phishing* melibatkan kegiatan kriminal di mana pelaku menyamar sebagai individu atau entitas tepercaya dalam pesan elektronik dengan tujuan memperoleh data pribadi yang bersifat rahasia. Metode ini sering kali terkait dengan taktik rekayasa sosial(S et al., 2016). UU No.19 Tahun 2016 tentang Perubahan Atas UU No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur bahwa setiap orang dilarang dengan sengaja dan tanpa hak, atau melawan hukum, mengakses komputer dan/atau sistem elektronik dengancara apa pun yang melibatkan pelanggaran, penetrasi, melewati, atau membobol sistem keamanan. Oleh karena itu, *phishing* dianggap sebagai tindakan kriminal yang melanggar hukum, dan menurut pasal ini, dapat dikenai hukuman penjara hingga 8 tahun dan/atau denda sebesar Rp800.000.000,00 (delapan ratus juta rupiah). Dengan demikian,menunjukkan adanya keseriusan sanksi yang dapat diterapkan untuk melindungi keamanan dan integritas sistem elektronik terhadap kejahatan seperti *phishing*.

Jika melihat dari berbagai aspek, *phishing* bukanlah masalah yang ringan. Hal ini dikarenakan, dampak dari *phising* bisa sangat merugikan, baik secara finansial maupun dari segi kepercayaan nasabah terhadaplembaga keuangan. Nasabah yang menjadi korban *phishing* dapat kehilangan dana mereka, dan bank sebagai lembaga keuangan dapat menghadapi risiko reputasi yang serius. Oleh karena itu, tanggung jawab bank selaku lembaga keuangan terhadap tindakan *phising* serta perlindungan nasabah dari serangan phishing adalah suatu prioritas. Sehingga, urgensi penelitian ini bukan hanya menjadi kontribusi penting dalam pengembangan teori hukum, tetapi juga memiliki implikasi praktis yang signifikan. Hal ini akan membantu lembaga keuangan seperti halnya bank, otoritas pengawas, dan praktisi hukum dalam memberikan upaya melindungi nasabah dari ancaman *phishing* yang terus berkembang dan memperkuat kepercayaan nasabah dalam penggunaan layanan *e-banking* Berdasarkan uraian tersebut penulis tertarik untuk meneliti sebagai upaya bentuk karya ilmiah dengan judul "Upaya Hukum Bagi Korban Kejahatan *Phising* Yang Menguras Saldo *M-Banking*".

2. METODE PENELITIAN

Penelitian ini merupakan tipe penelitian Normatif yang dimana mengkaji studi dokumen dengan menggunakan berbagai data sekunder seperti peraturan perundang-undangan, keputusan pengadilan, teori hukum, dan dapat berupa pendapat para sarjana. Penelitian normatif ini mengunakan analisis kualitatif yakni dengan menjelaskan data-data yang ada dengan kata – kata atau pernyataan bukan dengan angka- angka. Menurut Peter Mahmud Marzuki penelitian hukum normatif adalah suatu proses untuk menemukan suatu aturan hukum, prinsip-prinsip hukum, maupun doktrin-doktrin hukum guna menjawab isu hukum yang dihadapi. Dalam pendekatan pada isu hukum ini menggunakan pendekatan perundang-undangan yang dimana dilakukan penulis dengan cara menganalisis aturan dan regulasi yang berkaitan dengan isu hukum tersebut [6]. Suatu penelitian normatif tentu harus menggunakan pendekatan perundang – undangan karena yang akan diteliti adalah berbagai aturan hukum yang menjadi fokus sekaligus tema sentral suatu penelitian [7]. Bahan hukum yng dipergunakan dalam penelitian ini yakni Undang-Undang Nomor 11 Tahun 2008 yang dirubah menjadi Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), serta Undang-Undang nomor 8 tahun 1999 tentang perlindungan konsumen seperti halnya hubungan nasabah/korban dengan bank yakni antara konsumen dan pelaku usaha Serta Undang-Undang nomor 10 tahun 1998 tentang perbankan. .

3. PEMBAHASAN

3.1. Identifikasi kejahatan *phissing* (*link whatsapp*).

Cybercrime ialah suatu tindakan ilegal yang dilakukan oleh oknum pelaku kejahatan dengan menggunakan teknologi komputer dan jaringan internet untuk melakukan penyerangan sistem informasi terhadap suatu korban. Seperti halnya terjadi *hack* akun sosial media, membobol perangkat teknologi serta data korban, kemudian menyikat habis isi saldo di M-Banking atau kartu kartu kredit korban. Di Indonesia diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik(UU ITE) sebagaimana telah diubah menjadi UU Nomor 19 tahun 2016. *Cybercrim*e termasuk dalam kategori perbuatan yang dilarang dalam UU ITE [8].

1. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun.
2. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh Informasi elektronik dan/atau dokumen Elektronik.
3. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Di Indonesia, praktik kejahatan seperti *phising* diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Pasal-pasal yang relevan antara lain Pasal 30 UU ITE yang sebagai mana isi dan maksud dari Pasal 30 UU ITE yakni untuk mencegah penggunaan informasi atau dokumen elektronik palsu yang dapat menyesatkan dan merugikan pihak lain, memberikan landasan hukum untuk menindak pelaku yang sengaja melakukan tindakan tersebut. Sehingga melarang akses ilegal terhadap sistem komputer serta perbuatan yang mengakibatkan kehilangan, perusakan, atau perubahan data elektronik [15]. Pelaku tindak pidana *phishing* di Indonesia dapat dikenai sanksi pidana yang berlaku seperti kurungan dan denda yang telah diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Pasal-pasal terkait, seperti Pasal 28 dan Pasal 30, melarang akses ilegal terhadap sistem komputer dan perbuatan yang mengakibatkan kehilangan, perusakan, atau perubahan data elektronik. Sanksi pidana yang dapat dikenakan mencakup kurungan dan denda, bergantung pada tingkat kerusakan dan keadaan khusus dari setiap kasus. Penting untuk memahami bahwa penerapan hukum dapat bervariasi sesuai dengan penilaian hakim dan kebijakan penegakan hukum yang berlaku. Penting untuk selalu berhati-hati dalam beraktivitas *online* dan melindungi informasi pribadi untuk mencegah menjadi korban praktik phishing.

Kejahatan *phising* melalui *chat link whatsapp* melibatkan upaya penipuan yang dimana pelaku mencoba menyamar sebagai entitas terpercaya untuk mendapatkan informasi pribadi ataupun keuangan dari korban serta dapat melibatkan pemahaman terhadap tanda-tanda khas dalam serangan kejahatan *phising* ini. Adapun uraian identifikasi masalah kejahatan phising melalui *link chat whatsapp* yakni:

- Tautan yang mencurigakan, sebelum mengeklik tautan yang terkirim seharusnya pastikan dulu bahwasanya link yang terkirim pada chat whatsapp itu aman yakni dengan memeriksa tautan yang diberikan, karena kejahatan phissing sendiri sering menggunakan URL palsu atau modifikasi kecil pada URL resmi sehingga tautan yang sekirannya mencurigakan dapat dihindari.
- Pesan menekan atau darurat, sebuah pesan yang dimana seolah-olah meyakinkan terus-terusan terhadap penerima pesan agar dapan menekan apa yang dikirim oleh pelaku phissing sehingga dapat diwaspadai pesan yang menciptakan urgensi atau tekanan. Seperti ancaman yang mengancam penonaktifan akun ataupun ada masalah keamanan yang mendesak, pelaku *phising* sering kali menggunakan taktik seperti ini agar korban tampak panik dan dapat melakukan apa yang diperintah oleh pelaku.
- Permintaan informasi pribadi, *phising* sering kali mengirimkan pesan ataupun tautan yang meminta agar penerima pesan dapat mengirimkan identitasnya sebagai data pelaku untuk melakukan tindakan kejahatan phissing, jika penerima pesan chat terdapat pesan seperti ini setidaknya penerima pesan tidak mengirimkan identitas pribadinya terlebih yang telah meminta informasi pribadi yang sensitif melalui tautan yang dikirim kechat whatsapp.
- Pemalsuan identitas, periksa terlebih dahulu pengirim pesan dan pastikan dengan baik bahwa pengirim pesan tersebut benar-benar dari orang ataupun entitas yang diwakilinya, phisher atau pelaku kejahatan *phisin*g

dapat melakukan pemalsuan identitas ataupun melakukan peretasan akun untuk mengirim pesan palsu terhadap korban [16].

- Bahasa dan tata bahasa yang mencurigakan, waspadai dan telitih bahasa yang digunakan dalam menerima pesan jika terdapat bahasa yang tidak biasa atau kesalahan tata bahasa dalam pesan yang dikirimkan. *Phising* sering kali memanfaatkan ketidak jelasan ataupun kesalahan dalam pengiriman pesannya dan itu bertujuan untuk mengecoh korban agar korban melakukan apa yang diperintah dari pesan chat yang disampaikan.
- Verifikasi logo dan grafis, jika pengirim pesan terdapat mencantumkan logo atau grafis perusahaan pada profilnya pastikan dulu bahwa chat yang masuk itu benar dan dijamin keasliannya dan tidak dimanipulasi [17]. *Phisher* sering juga menggunakan taktik ini untuk mencoba meniru elemen desain untuk menipu korban phissing.
- Penyamaran URL dengan *Hyperlink*, jika tautan disematkan dalam kata-kata tertentu dapat diperhatikan terlebih dahulu bahwa URL yang sebenarnya mungkin akan terlihat berbeda dari apa yang ditampilkan. *Hover mouse* diatas tautan untuk melihat URL yang sebenarnya dan dapat terdeteksi mana yang asli dan mana yang palsu.
- Pesan yang tidak biasa dari kontak yang dikenal, jika pesan yang dikirim tidak biasa atau dapat dicurigai dari isi pesannya dari kontak yang sudah dikenal perlu adanya verifikasi keasliannya dengan cara menghubungi perngirim pesan secara terpisah sebelum mengambil tindakan yang diinginkan.
- Penggunaan teknologi rekayasa sosial, *phisher* sering kali menggunakan teknik rekayasa sosial seperti hal nya memanipulasi emosi atau menciptakan suatu alasan yang mendesak untuk meningkatkan peluang korban memberikan informasi kepada pelaku kejahatan phissing melalui chat whatsapp tersebut sehingga secara tidak langsung korban telah mengirimkan informasi kepada pelaku.

Langkah awal yang dapat dilakukan jika indikasi terjadi *phising adalah* melaporkan kejadian jika terdapat kecurigaan terhadap chat ataupun tautan chat whatsapp yang diterima laporkan kejadian tersebut ke whatsapp dan beritahukan kontak yang telah terdampak dari chat yang dikirimkan tersebut. Identifikasi masalah kejahatan *phising* ini memang membutuhkan kewaspadaan serta kecermatan yang mendalam dalam berinteraksi dengan pesan maupun tautan serta pemahaman yang bagus tentang cara melindungi diri dari upaya kejahatan *phising* ataupun penipuan *online* yang telah marak terjadi terdekat ini.

3.2 Upaya hukum yang dapat dilakukan oleh korban kejahatan *phising.*

Upaya hukum adalah langkah-langkah yang diambil oleh individu atau pihak terlibat dalam situasi hukum tertentu untuk mencari keadilan, melindungi hak, atau menyelesaikan sengketa [18]. Ini bisa berupa pelaporan ke pihak berwenang seperti kepolisian dalam kasus kejahatan, pengajuan gugatan atau tuntutan ke pengadilan dalam sengketa perdata, atau konsultasi dengan ahli hukum atau pengacara untuk mendapatkan panduan legal. Terkadang, penyelesaian dilakukan melalui mediasi atau arbitrase di luar pengadilan, atau melalui langkah-langkah perlindungan hukum seperti perintah pengadilan atau pembelaan hukum. Upaya hukum merupakan cara bagi individu atau pihak terlibat untuk menggunakan sistem hukum untuk melindungi diri, menyelesaikan masalah hukum, atau memastikan hak-hak mereka diakui dan dijaga.

Upaya hukum menjadi penting bagi korban kejahatan *phishing* melalui tautan *WhatsApp* karena membantu dalam melindungi hak-hak mereka yang telah dilanggar [19]. *Phishing* merupakan bentuk penipuan yang dapat mengakibatkan pencurian informasi pribadi atau keuangan korban. Dalam kasus ini, upaya hukum menjadi sarana untuk menegakkan keadilan, memulihkan kerugian yang mungkin dialami korban, dan mencegah kerugian lebih lanjut. Melalui langkah-langkah hukum, seperti pelaporan kepada pihak berwenang atau konsultasi dengan ahli hukum, korban dapat memperoleh bantuan dalam menangani kejahatan yang mereka alami. Selain itu, langkah-langkah hukum juga membantu dalam memastikan bahwa pihak-pihak yang terlibat dalam aktivitas *phishing* bertanggung

jawab atas tindakan mereka, serta mendorong penegakan hukum yang lebih baik untuk mencegah terjadinya kejahatan serupa di masa depan.

Ketika seseorang menjadi korban kejahatan *phishing* melalui tautan WhatsApp, langkah-langkah hukum menjadi penting untuk melindungi diri dan memulihkan kerugian. Phishing, yang melibatkan praktik penipuan dengan menyamar sebagai entitas tepercaya untuk mendapatkan informasi sensitif, seringkali menimbulkan konsekuensi serius bagi korban [20]. Melaporkan kejadian ini kepada pihak berwenang, seperti kepolisian atau otoritas hukum, adalah langkah awal yang penting untuk memulai penyelidikan dan pengumpulan bukti. Selain itu, menghubungi langsung layanan *WhatsApp* untuk memberi tahu tentang tautan atau pesan *phishing* bisa menjadi langkah proaktif dalam memerangi kejahatan tersebut. Adanya bantuan dari ahli hukum atau pengacara juga dapat memberikan panduan dalam menavigasi opsi hukum yang tersedia, termasuk upaya untuk mendapatkan kompensasi atas kerugian yang mungkin timbul [21]. Perlindungan terhadap data pribadi juga menjadi kunci, dengan mengganti kata sandi, memperkuat keamanan akun, dan mengambil langkah-langkah lain untuk mencegah serangan lebih lanjut. Dengan tindakan yang tepat dalam ranah hukum dan keamanan, korban bisa mendapatkan bantuan serta meminimalkan dampak yang diakibatkan oleh kejahatan *phishing* melalui tautan *WhatsApp*. Kejahatan *phishing* melalui tautan *WhatsApp* merupakan ancaman serius bagi privasi dan keamanan data seseorang. Ketika seseorang menjadi korban praktik penipuan semacam itu, aspek hukum menjadi krusial untuk melindungi diri, mengatasi kerugian, dan menegakkan keadilan. *Phishing*, yang sering kali meniru entitas yang terpercaya [22], memanfaatkan pesan atau tautan palsu untuk memperoleh informasi sensitif seperti kata sandi, informasi keuangan, atau data pribadi lainnya. Langkah pertama yang perlu diambil oleh korban adalah melaporkan kejahatan ini kepada pihak berwenang, seperti kepolisian atau lembaga penegak hukum setempat. Laporan ini memicu penyelidikan lebih lanjut untuk mengidentifikasi pelaku serta mencegah terjadinya serangan serupa di masa depan.

Selanjutnya, penting bagi korban untuk segera menghubungi layanan WhatsApp untuk memberitahukan tentang pesan atau tautan phishing yang

diterima. Langkah ini memungkinkan WhatsApp untuk mengambil tindakan yang tepat terhadap akun atau pesan yang terlibat dalam kejahatan tersebut. Selain itu, mengambil langkah preventif dengan mengonsultasikan masalah ini dengan ahli hukum atau pengacara dapat memberikan gambaran yang lebih jelas tentang opsi hukum yang tersedia bagi korban. Ahli hukum dapat memberikan bantuan dalam menyusun strategi hukum, mengumpulkan bukti yang diperlukan, dan memahami hak-hak yang dimiliki korban dalam situasi tersebut. Pengalaman phishing sering kali meninggalkan dampak psikologis dan finansial yang signifikan bagi korban. Oleh karena itu, mendapatkan bantuan psikologis atau dukungan emosional juga menjadi penting bagi mereka yang terkena dampaknya [23]. Sementara itu, dalam upaya untuk melindungi data pribadi dan mengamankan akun-akun yang terkait, perlu dilakukan langkah-langkah seperti mengganti kata sandi, mengaktifkan fitur keamanan tambahan, atau melakukan verifikasi dua langkah untuk mencegah akses yang tidak sah ke akun.

Pihak terkait dengan tautan atau pesan palsu yang digunakan dalam praktik phishing juga perlu menjadi fokus. Korban dapat mengajukan pengaduan langsung kepada platform atau layanan yang terlibat dalam serangan tersebut. Tindakan ini mungkin membantu dalam meminimalisir penyebaran informasi palsu atau mencurigakan yang terkait dengan kejahatan phishing. Di sisi lain, memperoleh informasi mengenai langkah-langkah perlindungan yang disediakan oleh layanan *WhatsApp* atau *platform* serupa juga akan sangat membantu korban untuk menghindari situasi serupa di masa depan [13]. Bagi korban, upaya untuk mendapatkan kompensasi atas kerugian yang dialami juga merupakan bagian dari upaya hukum. Pihak yang terlibat dalam kejahatan *phishing* dapat diproses secara hukum dan dihadapkan pada konsekuensi yang sesuai dengan perundang-undangan yang berlaku. Pihak berwenang atau pengadilan mungkin dapat memberikan keputusan yang mendukung korban untuk mendapatkan ganti rugi atas kerugian finansial atau non-finansial yang diakibatkan oleh praktik *phishing* tersebut [24].

Dalam konteks yang lebih luas, penanganan kejahatan phishing tidak hanya mengandalkan tanggung jawab individu atau korban semata. Pendidikan dan kesadaran publik mengenai ancaman siber seperti phishing menjadi kunci dalam

memerangi praktik ini. Program-program edukasi yang bertujuan untuk meningkatkan pemahaman mengenai tanda-tanda dan langkah-langkah pencegahan terhadap phishing memiliki peran yang penting dalam meningkatkan tingkat kewaspadaan masyarakat terhadap upaya penipuan semacam itu.

Dengan meningkatnya kesadaran mengenai metode phishing, masyarakat dapat lebih mudah mengenali ciri-ciri atau pola umum dari serangan ini. Melalui edukasi, mereka bisa memahami bahwa phishing sering kali melibatkan upaya mendapatkan informasi pribadi melalui pesan atau tautan yang terlihat sah namun sebenarnya tidak. Dengan pengetahuan ini, mereka dapat lebih waspada dan skeptis terhadap komunikasi yang mencurigakan atau permintaan informasi pribadi yang tidak biasa [25]. Program edukasi juga memainkan peran dalam mengajarkan tindakan pencegahan kepada masyarakat, seperti memeriksa alamat email atau URL yang mencurigakan, tidak mengklik tautan dari sumber yang tidak dikenal, atau memverifikasi keaslian komunikasi sebelum memberikan informasi sensitif. Dengan begitu, masyarakat menjadi lebih terlatih dalam menghindari jebakan phishing, sehingga mengurangi kemungkinan menjadi korban dari serangan ini. Selain itu, pemahaman yang ditingkatkan melalui edukasi dapat membantu dalam mengurangi dampak dari kejahatan phishing secara keseluruhan. Semakin banyak individu yang teredukasi tentang ancaman siber ini, semakin sulit bagi para penjahat untuk berhasil melakukan serangan phishing dengan sukses. Hal ini akan berdampak positif pada tingkat keamanan siber secara keseluruhan, melindungi lebih banyak orang dari kerugian dan memperkecil kesempatan penjahat siber untuk merugikan masyarakat secara luas. Dengan demikian, upaya edukasi menjadi salah satu aspek yang sangat penting dalam melawan kejahatan siber seperti phishing [26].

4. KESIMPULAN

Dari uraian tersebut penulis dapat memberikan kesimpulan terhadap hasil dari pada penelitian tersebut, yakni : penegakan hukum terhadap pelaku tindak pidana kejahatan cyber (*cyber crime*) terhadap nasabah pemilik akun M-bankking *(Mobile Bankking*) yang terkuras melalui chat whatsapp orang tak dikenal sehingga

menghilangkan isi saldo yang terdapat di M-Banking korban dengan menerapkan pasal 30 ayat (1) tentang penggunaan informasi atau dokumentasi, serta pasal 32 ayat (1) tentang mengakses sistem komputer dengan tanpa hak atau melawan hukum dapat disanksi dengan sanksi pidana penjara paling lama 12 tahun dan/atau denda paling banyak senilai 12 miliar rupiah.

DAFTAR PUSTAKA

[1] A. N. Balqis, L. Ramadhana, R. Wirawan, and I. N. Isnainiyah, "Bid-Fish: An android application for online fish auction based on case study from Muara Angke, Indonesia," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 508, no. 1, 2019, doi: 10.1088/1757-899X/508/1/012128.

[2] A. Supriyo, L. Latifah, and M. Isnawati, "Pendampingan Legalitas Usaha Perlindungan Hukum Bagi UMKM di Mitra PCM Gunung Anyar Surabaya Hingga Penerbitan Nomor Induk Berusaha (NIB)," *Borobudur J. Leg. Serv.*, vol. 4, no. 1, pp. 44–52, 2023, doi: 10.31603/bjls.v4i1.8558.

[3] I. Ramadhan, A. Kurniawan, and A. S. Putra, "Penentuan Pola Penindakan Pelanggaran Lalu Lintas di DKI Jakarta Menggunakan Metode Analytic Network Process (ANP)," *IKRA-ITH Inform. J. Komput. dan Inform.*, vol. 5, no. 1, pp. 51–57, 2021, [Online]. Available: https://journals.upi-yai.ac.id/index.php/ikraith-informatika/article/view/913

[4] M. N. Purwanti and A. Hariri, "Perlindungan Hukum bagi Konsumen atas Kelangkaan Minyak Goreng Ditinjau dari Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen," *Sultan Jurisprud. J. Ris. Ilmu Huk.*, vol. 2, no. 1, p. 1, 2022, doi: 10.51825/sjp.v2i1.15055.

[5] N. K. Dewi, B. H. Irawan, E. Fitry, and A. S. Putra, "Konsep Aplikasi E-Dakwah Untuk Generasi Milenial Jakarta," *J. IKRA-ITH Inform.*, vol. 5, no. 2, pp. 26–33, 2021.

[6] S. U. Wp, "Perlindungan Hukum Korban Kerusakan Lingkungan Sebagai Dampak Korupsi di Sektor Sumber Daya Alam," no. July, 2021.

[7] S. Saxby, "Cyber law," *Comput. Law Secur. Rev.*, vol. 23, no. 1, p. 86, 2007, doi: 10.1016/j.clsr.2006.10.006.

[8] R. J. Puspitasari and A. Q. P. Sulistyo, "Perlindungan Hukum bagi Korban Penipuan Online Shop Dengan Merujuk pada Undang-Undang Nomor 19 Tahun 2016," *Eksaminasi J. Huk.*, vol. 2, no. 1, pp. 1–8, 2022, [Online]. Available: http://jurnal.umpwr.ac.id/index.php/eksaminasi/article/view/2088%0Ahttp:

//jurnal.umpwr.ac.id/index.php/eksaminasi/article/download/2088/1213

[9] D. Rahmawati, G. Lumakto, R. Ameliah, M. Viendyasari, R. A. Negara, and S. Bachna, "Modul Pinjaman Online," p. 45, 2023.

[10] N. Qomariyah and A. D. Irawan, "Perlindungan Hukum Terhadap Debitur Dalam Pinjaman Dana Tanpa Agunan Dimasa Pandemi Covid-19," *Ius Civ. Refleks. Penegakan Huk. dan Keadilan*, vol. 5, no. 2, pp. 156–169, 2021, doi: 10.35308/jic.v5i2.3700.

[11] S. U. W. Prakasa and P. E. Noviandi Nur, "Analysist of cyber espionage in international law and indonesian law," *Humanit. Soc. Sci. Rev.*, vol. 7, no. 3, pp. 38–44, 2019, doi: 10.18510/hssr.2019.736.

[12] Barita Sidabutar, "Legal Security Of Land Ownership By The System Law In Indonesia And Judicia Practice," *J. Gagasan Huk.*, vol. 5, no. 01, pp. 41–50, 2023, doi: 10.31849/jgh.v5i01.13232.

[13] R. P. Erdiyanto, "PENIPUAN MENGATASNAMAKAN BANK BERBENTUK PHISING," vol. 1, no. 2, pp. 71–79, 2023.

[14] S. Arifin and K. Rahman, "DINAMIKA KEJAHATAN DUNIA MAYA MENGENAI ONLINE CHILD SEXUAL EXPLOITATION DI TENGAH PANDEMI COVID-19," vol. 10, no. 2, pp. 89–99, 2019.

[15] Irawan & Irsyad, "Perlindungan Hukum Bagi Konsumen Jual Beli Online Atas Barang Tidak Sesuai," *J. Educ. Dev.*, vol. 10, no. 3, p. 264, 2022.

[16] Meiliana Nurcahyani and Anang Dony Irawan, "Protection of Children Involved in Online Prostitution Cases in Terms of Law of Children Protection," *Indones. Law Reform J.*, vol. 2, no. 2, pp. 153–165, 2022, doi: 10.22219/ilrej.v2i2.21587.

[17] S. Amelia, E. Permatadani, I. A. Rosida, R. A. Akmaliya, and A. D. Irawan, "Legal Protection for Workers who Have Harmed Employers: Case Study of Supreme Court Verdict Number 702K/Pdt.Sus-Phi/2021," *Indones. Law Reform J.*, vol. 3, no. 1, pp. 56–68, 2023, [Online]. Available: https://ejournal.umm.ac.id/index.php/ilrej/article/view/24464

[18] I. M. W. W. Kusuma, I. M. Sepud, and N. M. S. Karma, "Upaya Hukum Praperadilan dalam Sistem Peradilan Pidana di Indonesia," *J. Interpret. Huk.*, vol. 1, no. 2, pp. 73–77, 2020, doi: 10.22225/juinhum.1.2.2438.73-77.

[19] E. V. Febriani, "Upaya Perlindungan Hukum Oleh Komnas Perempuan Terhadap Korban Kejahatan Sekstorsi Di Dunia Maya," *J. Huk. Adigama*, vol. 5, no. 1, pp. 279–303, 2022.

[20] E. Soesanto, "KESADARAN KORBAN CYBER CRIME DALAM KASUS PHISING," vol. 1, no. 7, pp. 1093–1098, 2023.

[21] D. Saputra and Z. A. Marpaung, "Analisis Yuridis Penanggulangan Penyalahgunaan Data Pribadi Dalam Bentuk Phising Yang Dilakukan Oleh

Paid Verified Account Di Media Sosial Menurut Undang- Undang Perlindungan Data Pribadi," *Uneslaw Rev.*, vol. 5, no. 4, pp. 4764–4775, 2023.

[22] M. Nizar, P. Ma, A. N. Zahra, and M. Z. Darmawan, "Analisis Modus Penipuan Digital Teknik Phising melalui Aplikasi WhatsApp Menggunakan Metode BPMN (Studi Kasus Pada Peretasan Kata Kunci :," no. September, pp. 3800–3806, 2023.

[23] S. K. Ananta Fadli Sutarli, "Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia," *J. Soc. Sci. Res.*, vol. 3, no. 2, pp. 4208–4221, 2023.

[24] L. Ekayani and H. Djanggih, "Perlindungan Hukum Nasabah Terhadap Kejahatan Pencurian Data Pribadi (Phising) Di Lingkungan Perbankan," *J. Philos.*, vol. 4, pp. 22–40, 2023.

[25] Devy Putri Kussanti, "PENYULUHAN INTERNET SEHAT SEBAGAI EDUKASI DAN INFORMASI BAGI ANGGOTA FATAYAT NU KECAMATAN CILEDUG TANGERANG," *J. Japan Weld. Soc.*, vol. 91, no. 5, pp. 328–341, 2022, doi: 10.2207/jjws.91.328.

[26] M. R. Ramadhani and A. R. Pratama, "Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Indonesia," *Journal.Uii.Ac.Id*, vol. 1, no. 2, pp. 1–8, 2020.