PENIPUAN DIGITAL MELALUI TAUTAN PHISHING

Afifah Sahfitri[1], Rosmalinda[2]
[12]Magister Ilmu Hukum Universitas Sumatera Utara
E-mail: [1]afifahsahfitri@students.usu.ac.id , [2]rosmalinda@usu.ac.id

Abstract
Digital fraud is one of the cybercrimes that has been widely discussed in various studies, especially related to digital security and digital literacy. Along with the high level of access and people's dependence on all forms of digital services, the number of digital fraud crimes is getting higher. One of the digital scams circulating in the community is digital fraud through phishing links via email or social media such as WhatsApp, Telegram, Facebook, and other digital media. The study aims to find out the legal regulation of digital fraud through Phishing links as well as the factors and remediation efforts. The research method used is normative. The result of this research is that digital fraud through phishing links is a criminal act as regulated in Article 378 of the Criminal Code. The punishment for digital fraud through phishing links is regulated in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions and Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) depending on what results are obtained from digital fraud through phishing links and efforts that must be taken to prevent it so that people can improve digital literacy, and education about the dangers of digital crime, as well as strengthening cooperation between related parties in law enforcement as well as improving and perfecting aspects of legal regulations governing phishing crimes in order to provide more effective and efficient legal protection for victims.
Keywords: *legal regulation, digital fraud, phishing*

Abstrak
Penipuan digital adalah salah satu kejahatan siber yang banyak dibahas dalam berbagai Kajian, terutama yang berkaitan dengan keamanan digital dan literasi digital. Seiring dengan Tingkat akses yang tinggi dan ketergantungan masyarakat terhadap segala bentuk layanan digital, maka angka kejahatan penipuan digital semakin tinggi. Salah satu penipuan digital yang beredar di masyarakat adalah penipuan digital melalui tautan *Phishing* melalui email atau media sosial seperti WhatsApp, Telegram, Facebook, dan media digital lainnya. Penelitian bertujuan untuk mengetahui pengaturan hukum terhadap penipuan digital melalui tautan *Phishing* serta faktor dan Upaya penanggulangannya. Metode penelitian yang digunakan normatif. Hasil dari penilitian ini adalah Penipuan digital melalui tautan *phishing* merupakan perilaku perbuatan tindak pidana sebagaimana diatur dalam Pasal 378 KUHP. Hukuman penipuan digital melalui tautan *phishing* diatur didalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik dan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UU ITE) tergantung hasil apa yang di peroleh dari penipuan digital melalui tautan *phishing* tersebut dan Upaya yang penanggulangan harus terus dilalukan agar masyarakat dapat meningkatkan literasi digital, dan edukasi tentang bahaya kejahatan digital, serta memperkuat kerjasama antara pihak-pihak terkait dalam penegakan hukum serta perbaikan dan penyempurnaan dari aspek regulasi hukum yang mengatur tentang kejahatan phishing agar dapat memberikan perlindungan hukum yang lebih efektif dan efisien bagi korban.
Kata kunci: Pengaturan hukum, penipuan digital, phishing

1. PENDAHULUAN

Secara umum, literasi digital sering kita anggap sebagai kecakapan menggunakan internet dan media digital. Namun begitu, acap kali ada pandangan bahwa kecakapan penguasaan teknologi adalah kecakapan

yang paling utama. Padahal literasi digital adalah sebuah konsep dan praktik yang bukan sekadar menitikberatkan pada kecakapan untuk menguasai teknologi. Seorang pengguna yang memiliki kecakapan literasi digital yang bagus tidak hanya mampu mengoperasikan alat, melainkan juga mampu bermedia digital dengan penuh tanggung jawab.

Perubahan zaman menjadi serba digital menawarkan kemudahan dan kepraktisan dalam melakukan berbagai aktivitas. Namun masyarakat perlu tanggap dalam menghadapi berbagai ancaman di ruang digital. Bahkan saat ini, masyarakat semakin nyaman dan percaya dalam melakukan aktivitas keuangan digital yang selama ini dianggap berisiko tinggi. Hal itu tentunya akan sangat berbahaya jika tidak dibarengi dengan kemampuan menjaga keamanan digital. Penipuan digital adalah jenis kejahatan siber yang paling umum dan menjadi masalah global.

Penipuan digital adalah salah satu kejahatan siber yang banyak dibahas dalam berbagai kajian, terutama yang berkaitan dengan keamanan digital dan literasi digital. Penipuan digital mencakup berbagai istilah, seperti penipuan online dan siber. Pada dasarnya, istilah-istilah tersebut mengacu pada penipuan yang menggunakan media dan perangkat komunikasi digital.[1] Seiring dengan Tingkat akses yang tinggi dan ketergantungan masyarakat terhadap segala bentuk layanan digital, maka angka kejahatan penipuan digital semakin tinggi. Salah satu penipuan digital yang beredar di masyarakat adalah penipuan digital *Phishing*. Sebagian besar tautan phishing dikirim melalui email atau media sosial seperti WhatsApp, Telegram, Facebook, dan media digital lainnya.

Phishing berasal dari kata *fishing* berarti memancing. *Phishing* adalah ketika seorang peretas menipu pengguna Internet agar secara sukarela mengungkapkan informasi pribadi tanpa menyadari bahwa mereka adalah korban serangan peretas. Trik yang dilakukan hacker adalah dengan membujuk atau mengelabui korbannya agar mengklik link atau lampiran dan memasukkan informasi pribadi sensitif seperti

[1] Ahmad; noval, sayid muhammad rifqi; soecipto; jamaludin, *Perlindungan Hak Digital Ancaman PrivasiDitenga-Serangan Social* (Depok: PT Rajawali Grafindo, 2022).

username dan password. Dengan menggunakan pesan persuasif, *phisher* biasanya menyamar sebagai pihak atau lembaga resmi, seperti bank, lembaga pemerintah, lembaga pendidikan, dan penyedia telekomunikasi. Pesan ini meminta korban untuk mengunduh atau mengklik dokumen dan tautan palsu sebanyak mungkin. Tindakan mengunduh atau mengklik di sini merupakan pintu bagi peretas untuk secara potensial dan otomatis mengakses perangkat dan akun pribadi korban.[2] Di bawah pengaruh seorang hacker yang menyamar sebagai figur otoritas, korban tanpa sadar membagikan informasi pribadi (nama, umur, alamat, NIK, nomor paspor), informasi rekening (*Username, user* ID, *Password*), dan informasi finasial (Nomor rekening bank, nomor identifikasi pribadi ATM, nomor kartu *kredit/debit* dan masa berlakunya, CCV/CVC atau tiga angka di belakang kartu, *password* untuk satu kali transaksi). Informasi sensitif ini digunakan oleh peretas untuk mengambil alih rekening pribadi dan keuangan korban. Peretas kemudian menarik dana dari rekening atau menghabiskkan *limit* transaksi pada kartu *kredit* korban. Peretas juga bebas menjual data sensitif kepada pihak lain di pasar gelap digital (dark web). Sebagian besar tautan phishing dikirim melalui email atau media sosial seperti WhatsApp, Telegram, Facebook, dan sebagainya.

Berdasarkan laporan IDADX, total Pengaduan serangan *Phishing* di Indonesia mengalami peningkatan signifikan. Tercatat, IDADX menerima sebanyak 26.675 laporan seerangan *Phishing* pada priode kuartal *pertama* pada tahun 2023. Sedangkan, pada priode kuartal *keempat* pada tahun 2022 hanya terdapat 6.106 laporan *phishing*. Hal tersebut mengalami kenaikan sebanyak 20.569 laporan *phishing*.[3] platform *cyber security training* dan *security testing* yang dirancang khusus untuk membantu melindungi bisnis dari serangan *ransomware* dan ancaman siber lainnya yaitu knowbe4 menemukan bahwa Lebih dari 90%

[2] Agus Sudibyo, *Bernalar Sebelum Klik: Panduan Literasi Digital*, ed. galang aji gautama, candra; putro, cetakan pe (jakarta: KPG (Kepustakaan Populer Gramedia), 2023).
[3] Bank Jombang. "Serangan Phishing di Indonesia Terus Meningkat, Berikut Data Lengkapnya",https://bankjombang.co.id/serangan-phishing-di-indonesia-terus meningkat-berikut-data-lengkapnya/diakses pada 30 September 2024.

peretasan dan pelanggaran data yang berhasil diawali dengan penipuan *phishing*.

Penanganan penipuan *Phishing* sangat penting karena dampaknya yang merugikan terhadap ekonomi, keamanan, dan privasi individu. Penipuan *Phishing* tidak hanya mengakibatkan kerugian moneter yang signifikan, tetapi juga dapat merusak reputasi, menimbulkan ketidakamanan, dan menimbulkan ketakutan di masyarakat. Menyesuaikan peraturan saat ini dengan dinamika kejahatan siber yang terus berkembang merupakan tantangan terbesar dalam hal hukum. Hukum harus mampu melindungi hak-hak korban, mengejar pelaku kejahatan, dan mencegah kejahatan serupa di masa depan. Perubahan teknologi memerlukan regulasi yang tepat dan adaptasi cepat. Untuk menciptakan lingkungan digital yang aman dan terpercaya, masyarakat harus lebih menyadari ancaman kejahatan siber dan cara mencegahnya. Masyarakat harus dididik tentang pentingnya praktik keamanan digital dan bagaimana melindungi diri dari ancaman siber.

2. METODE PENELITIAN

Dalam penulisan ini, pendekatan yang digunakan merupakan pendekatan sosiologi hukum, yaitu perubahan sosial terjadi sebagai hasil dari konflik daripada penyesuaian nilai yang membawa perubahan. Sifat dari penulisan ini adalah Penelitian normatif, yang berlandaskan pada dokumen peraturan perundang-undangan dan kepustakaan, dengan penekanan pada norma dan asas hukum. Sumber data yang digunakan dalam penelitian ini adalah bahan hukum primer dan sekunder. Sumber bahan hukum yang digunakan KUHP, Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik dan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

3. Pembahasan

3.1. Pengaturan Hukum Penipuan Digital Melalui Tautan Phishing

Penipuan digital melalui tautan *phishing* bertujuan agar target korban untuk mengunduh tautan virus, sehingga memberikan nomor kartu kredit, data pribadi, atau memberikan informasi login atau akun untuk situs web tertentu. Efek yang dialami oleh korban yang mengklik tautan phishing berbeda-beda. Setelah mengklik tautan phishing, hal-hal berikut dapat terjadi: *pertama,* Peretas dapat mendapatkan informasi dari atau tentang korban. Jika seseorang mengklik tautan phishing, penyerang akan secara otomatis mendapatkan statistik perangkat, perkiraan lokasi, dan informasi lain yang mungkin diberikan secara sukarela. *Kedua,* Kemungkinan virus *malware* terpasang pada perangkat korban. Perangkat lunak berbahaya seperti virus atau spyware dapat diinstal tanpa pengguna tahu dan dapat menginfeksi perangkat korban dan memberi peretas data rahasia. *Ketiga,* Peretas dapat mengekspoitasi jaringan dan kontak korban. Jika korban mengklik tautan phishing dan peretas mulai mengirim pesan *phishing* kepada orang-orang di daftar kontak korban dan hal paling buruk, dapat mengakses laptop korban dari jarak jauh. [4]

Menurut teori konflik, perubahan sosial terjadi sebagai hasil dari konflik daripada penyesuaian nilai yang membawa perubahan.[5] Perubahan sosial yang cepat, seperti globalisasi dan urbanisasi, dan penetrasi internet yang tinggi, menciptakan ekosistem di mana penipuan digital dapat berkembang. Kebocoran data dan penipuan digital meningkat karena teknologi yang semakin terhubung. Masyarakat yang semakin bergantung pada teknologi informasi dan komunikasi menghadapi masalah keamanan yang lebih besar, terutama karena banyaknya data

[4] noval, sayid muhammad rifqi; soecipto; jamaludin, *Perlindungan Hak Digital Ancaman PrivasiDitenga-Serangan Social*.
[5] M. Wahid Nur Tualeka, "Teori Konflik Sosiologi Klasik Dan Modern," *Al-Hikmah : Jurnal Studi Agama-Agama* 3, no. 1 (2017): 32–48, https://journal.um-surabaya.ac.id/Ah/article/view/409.

pribadi yang tersimpan secara digital. Kebijakan yang ada di Indonesia tentang penanganan penipuan digital harus mempertimbangkan konteks teknologi dan sosial ini. Regulasi yang ada juga harus mampu mengakomodasi perubahan cepat dalam perilaku sosial dan teknologi. Selain itu, pemerintah harus mendorong program literasi digital untuk meningkatkan kesadaran masyarakat tentang risiko penipuan digital dan cara menghadapinya.[6]

Berdasarkan hal ini, maka pengaturan hukum terhadap penipuan digital melalui tautan *phishing* sebagai perilaku perbuatan tindak kejahatan pidana penipuan sebagaimana diatur dalam Pasal 378 KUHP, yang berbunyi "Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama 4 (empat) tahun." [7] Pengaturan selanjutnya terdapat Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik dan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UU ITE) sebagai peraturan yang secara khusus membahas terkait kejahatan-kejatan digital seperti penipuan digital. Meskipun UU ITE tidak menjelaskan secara jelas pengaturan penipuan *phishing*, tetapi terdapat beberapa pasal yang dirasa dapat melnjadi payung hukum atas

[6] Afifah Rizqy Widianingrum, "Analisis Implementasi Kebijakan Hukum Terhadap Penanganan Kejahatan Siber Di Era Digital," *Journal Iuris Scientia* 2, no. 2 (2024): 90–102, https://doi.org/10.62263/jis.v2i2.40.

[7] Ardi Saputra Gulo, Sahuri Lasmadi, and Khabib Nawawi, "Cyber Crime Dalam Bentuk Phising Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik," *PAMPAS: Journal of Criminal Law* 1, no. 2 (2021): 68–81, https://doi.org/10.22437/pampas.v1i2.9574.

kasus penipuan *phishing,* yaitu Pasal 30 Ayat (1), Pasal 32, dan Pasal 35 UU ITE. Belrikut pelnjellasan dari pasal-pasal tersebut:

a. Pasal 30 Ayat (1) UU ITE

Pasal 30 Ayat (1) UU ITE berbunyi "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun". Isi pasal tersebut dapat dikaitkan dengan penipuan digital melalui tautan *phishing* "setiap orang" dalam hal ini adalah *phisher* yang dengan sengaja dan tanpa haknya mengakses system elektronik korban dengan mengirim tautan yang jika diklik maka dapat mengases seluruh system perangkat korban, bahkan aplikasi m-banking milik korban. Penjatuhan hukuman dari Pasal 30 Ayat (1) ada pada ketentuan Pasal 46 yaitu dengan dipidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).

b. Pasal 32 Ayat (1) UU ITE

Pasal 32 Ayat (1) UU ITE berbunyi "setiap orang yang dengan sengaja dan tanpa hak memindahkan atau mentransfer data pribadi orang lain tanpa izin,. Keltelntuan pada pasal tersebut dapat dikaitkan dengan kasus *phishing* mellalui file apk. Unsur "setiap orang" dalam hal ini adalah *phisher* yang dengan sengaja dan tanpa haknya merusak system perangkat milik korban dan memindahkan informasi atau dokumen milik korban misalnya uang di rekening *m-banking* korban. Penjatuhan hukuman dari Pasal 32 Ayat (1) ada pada ketentuan Pasal 48 yaitu dengan dipidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).

c. Pasal 35 UU ITE

Pasal 32 Ayat (1) UU ITE berbunyi "Setiap orang yang dengan sengaja dan tanpa hak atau melanggar hukum membuat, mengubah, menambah, mengurangi, melakukan

transmisi, merusak, menghilangkan, atau memindahkan Informasi Elektronik dan/atau Dokumen Elektronik" Unsur "setiap orang" dalam hal ini adalah *phisher* yang dengan sengaja dan tanpa haknya melmanipulasi tautan dengan memberikan tautan seakan-akan itu tautan resmi seperti, tautan pendaftaran CPNS. Penjatuhan hukuman dari Pasal 51 yaitu dengan di pidana penjara yang akan dilakukan paling lama 12 (dua belas) tahun dan dikenakan denda paling banyak Rp12.000.000.000,00 (dua bellas miliar rupiah).[8]

Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik dan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (yang selanjutnya disingkat dengan UU ITE) terhadap penipuan digital melalui tautan *phishing* memberikan hukuman dalam bentuk hukuman pidana pokok dalam bentuk baik itu pidana penjara maupun pidana denda sepelrti apa yang tercantum dalam KUHP. Namun, pada kenyataannya, pasal-pasal tersebut masih belum cukup untuk memenuhi elemen-elemen yang diperlukan dalam kasus penipuan digital melalui tautan *phishing*. Kemudian, bagi bagi *phisher* yang menyebarluaskan data pribadi korban. Hal ini terjadi jika pelaku *phishing* juga mengambil uang di rekening m-banking korban serta informasi terkait kesehatan korban dan data *biometric* lainnya. maka *phisher* tersebut dapat dikenakan hukuman berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (selanjutnya disingkat melnjadi UU PDP). Namun, UU PDP hanya sebatas memberikan pengaturan terkait pencurian data pribadi saja seperti yang telrcantum dalam Pasal 67 Ayat (1) UU PDP berbunyi "Setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan

[8] Artanti Zahra Adisa and Andriyanto Adhi Nugroho, "Perlindungan Hukum Terhadap Korban Phising Terkait Pengiriman File Apk," *Justisi* 10, no. 1 (2024): 242–56, https://doi.org/10.33506/js.v10i1.2980.

data pribadi yang bukan miliknya, dipidana dengan pidana penjara paling lama 5 tahun dan/atau pidana denda paling banyak Rp. 5.000.000.000 (lima miliar rupiah).[9]

Pengaturan hukum terhadap penipuan digital melalui tautan phishing terhadap kejahatan digital hanya sebatas itu saja belum ada pengaturan yang baru dan rinci terhadap pembaruan Pengaturan hukum tentang kejahatan penipuan digital melalui tautan *phishing.* hal ini masih menimbulkan perdebatan terutama berkaitan dengan efektivitas hukuman dan sanksi terhadap pelaku tindak pidana yang selama ini diterapkan.[10] Pengaturan hukum terhadap penipuan digital harus di perbaharui dan disempurnakan agar memebrikan efek jera dan perubahan sosial.

3.2. Faktor Dan Upaya Penanggulangan Yang Di Perlukan Dalam Penipuan Digital Melalui Tautan *Phishing* Bagi Masyarakat

Penipuan digital sebagai penggunaan layanan internet atau software dengan akses internet untuk menipu atau mengambil keuntungan dari korban, misalnya uang dan mencuri informasi atau identitas pribadi.[11] Ketika melakukan kejahatan pasti memliki faktor. Adapun Faktor-faktor mempengaruhi terjadinya penipuan digital melalui tautan phishing antara lain *Pertama,* Kurang pengetahuan pengguna internet. Orang yang menggunakan internet masih kurang memahami tentang keamanan data, seperti membedakan nama domain dari akun resmi dan palsu. *Kedua,* Individu yang menggunakan perangkat digital yang tidak memiliki pengetahuan tentang startegi penipuan digital melalui tautan *phishing* dan kejahatan digital lainya, seperti tidak melakukan klarifikasi pada email atau tautan yang meminta identitas dan password pribadi mereka. *ketiga,* Psikologi juga berperan dalam

[9] Pasal 67 Ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi
[10] Yazid Haikal Lokapala, Fuad Januar Nurfauzi, and Yeni Widowaty, "Aspek Yuridis Kejahatan Phishing Dalam Ketentuan Hukum Di Indonesia," *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 5, no. 1 (2024): 22.
[11] Novi Kurnia et al., *Penipuan Digital Di Indonesia (Modus, Medium, Dan Rekomendasi)*, vol. 1, 2022.

penipuan digital karena masyarakat dianggap mudah terpengaruh oleh penawaran menarik seperti promosi dan total hadiah. *Ketika*, masyarakat menerima penawaran seperti itu, masyarakat langsung menyerahkan apa yang diminta oleh pelaku kejahatan dan hanya mengikuti instruksi yang diberikan oleh pelaku. *Keempat,* Pelaku penipuan digital melalui *phishing* adalah orang yang cerdas dan dapat menggunakan teknologi digital dengan lebih baik daripada operator komputer.[12] Dari faktor-faktor tersebut dapat menetukan penanggulangan terhadap penipuan. Adapun, Upaya yang di perlukan dalam penanggulangan penipuan digital melalui tautan *phishing* didalam masyarakat yang harus diperhatikan dalam dua keadaan:

1) korban penipuan digital melalui tautan phishing beberapa hal yang dapat mereka lakukan untuk mengurangi risiko tersebut, seperti berikut.
   a. Putuskan sambungan perangkat yang digunakan.

      Hal pertama yang harus dilakukan adalah menghentikan perangkat yang terhubung ke internet segera. Untuk perangkat yang menggunakan koneksi kabel, langkah termudah untuk melakukan ini adalah dengan menghapus kabel ethernet dari komputer. Apabila Anda terhubung ke jaringan Wi-Fi, cari pengaturan jaringan pada perangkat dan putuskan sambungan dari jaringan tersebut. Jika Anda tidak dapat menemukan pengaturan jaringan pada perangkat, Anda dapat membuka router Wi-Fi secara langsung dan mematikannya. Langkah ini akan mengurangi risiko penyebaran malware ke perangkat lain pada jaringan, serta mencegah malware mengirimkan informasi sensitif dari perangkat dan mencegah seseorang mengakses perangkat dari jarak jauh.

   b. Back up Data.

[12] La Ode and Muhammad Ichsan, "Kajian Sosiologi Kriminal Terhadap Penanggulangan Cybercrime Melalui Phising" 33, no. 2 (2018).

Langkah selanjutnya adalah menyimpan kembali file, atau back up, setelah perangkat terputus dari internet. Dalam proses pemulihan setelah serangan phishing, data dapat dihapus atau dihancurkan.Jika Anda sering mencadangkan file menggunakan metode seperti penyimpanan cloud, hard drive eksternal, atau USB, maka Anda hanya harus mencadangkan file yang telah dibuat atau diperbarui sejak pencadangan terakhir. Melindungi dokumen dan informasi yang sangat sensitif, serta file yang tak tergantikan seperti foto dan video keluarga, adalah prioritas utama. Namun, sangat disarankan untuk memilih salah satu metode penyimpanan yang disebutkan di atas jika Anda belum pernah melakukannya sebelumnya untuk menyalin file ke perangkat atau program cadangan.

c. Pindai Sistem Anda Dari *Malware*

Sangat disarankan untuk berkonsultasi atau meminta bantuan ahli di bidang Anda jika Anda tidak memahami secara mendalam tentang masalah pindai sistem. Namun, lakukan pemindaian sistem secara menyeluruh jika Anda ingin menangani masalah tersebut sendiri. gunakan program antivirus untuk melakukan pemindaian. Apabila terdapat peringatan yang menunjukkan hasil pemindaian, pastikan untuk menghapus file atau mengarantinanya. Perlu diketahui bahwa beberapa malware dapat menyamar sebagai file operasi yang sah, membuatnya sulit bagi program antivirus untuk mendeteksinya. Bawa perangkat ke ahlinya secara proaktif jika Anda ingin memastikan sistem Anda bersih atau jika masih mengalami masalah dengan perangkat.

d. Ubah Kredensial

Malware dapat mengumpulkan data pribadi seperti nama pengguna dan kata sandi, nomor kartu kredit, nomor rekening bank, dan informasi lainnya. Jika seseorang

merasa telah ditipu untuk bertindak berdasarkan pesan phishing, mereka harus segera mengubah kredensial mereka. Ini berlaku untuk semua akun email, bank online, media sosial, dll. Hindari menggunakan nama pengguna dan kata sandi yang sama untuk semua akun Anda di internet karena hal ini memungkinkan penjahat untuk mencuri kredensial, mendapatkan informasi pribadi, dan bahkan mencuri dana.

e. Hapus pesan

Di era teknologi modern, phishing melalui tautan dari pesan email dan media sosial telah berkembang menjadi ancaman berbahaya, tetapi tidak terhindarkan. Perlindungan terbaik adalah dengan memperhatikan dan segera menghapus pesan email dan teks yang tampak meragukan. Organisasi atau perusahaan yang sah tidak akan pernah meminta orang untuk memberikan data pribadi sensitif melalui saluran yang tidak aman seperti email, teks, atau pesan pop-up.Pengirim pesan akan mencoba berkomunikasi melalui metode terverifikasi, seperti telepon, jika pesan tersebut benar-benar penting.[13]

2) Upaya penanggulangan yang dilakukan sebelum masyarakat terkena penipuan digital melalui tautan, upaya yang dilakukan adalah Penegakan hukum melalui aspek kultural agar terdapat kesadaran dan partisipasi masyarakat dalam mencegah dan menangani penipuan digital melalui tautan *phishing*. Berikut ini adalah aspek kultural yang dapat dilakukan melalui beberapa program yang bertujuan untuk meningkatkan literasi dan edukasi siber bagi masyarakat, seperti:

a. Gerakan Nasional Siber Bersih (Gernas Cinta Siber) merupakan gerakan bersama antara pemerintah, swasta,

[13] Kurnia et al., *Penipuan Digital Di Indonesia (Modus, Medium, Dan Rekomendasi).*

akademisi, dan masyarakat sipil untuk menciptakan lingkungan siber yang bersih, sehat, dan aman di Indonesia.

b. *Indonesia Cyber Security Forum* (ICSF) merupakan forum yang menghimpun berbagai pemangku kepentingan di bidang keamanan siber untuk berbagi informasi, pengetahuan, dan pengalaman dalam menghadapi tantangan siber di Indonesia.
c. *Indonesia Security Incident Response Team on Internet Infrastructure* (ID-SIRTII) merupakan tim tanggap insiden keamanan siber yang berfokus pada infrastruktur internet di Indonesia, termasuk memberikan layanan pemberitahuan, peringatan, dan rekomendasi terkait dengan ancaman siber.
d. Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), yang merupakan asosiasi yang mewadahi para penyelenggara jasa internet di Indonesia, termasuk memberikan edukasi dan sosialisasi mengenai etika dan tata cara berinternet yang baik dan benar.[14]

Upaya yang penanggulangan harus terus dilalukan agar masyarakat dapat meningkatkan literasi digital, dan edukasi tentang bahaya kejahatan digital, serta memperkuat kerjasama antara pihak-pihak terkait dalam penegakan hukum serta perbaikan dan penyempurnaan dari aspek regulasi hukum yang mengatur tentang kejahatan phishing agar dapat memberikan perlindungan hukum yang lebih efektif dan efisien bagi korban.

4. KESIMPULAN

Penipuan digital melalui tautan *phishing* merupakan perilaku perbuatan tindak pidana sebagaimana diatur dalam Pasal 378 KUHP. Hukuman penipuan digital melalui tautan *phishing* diatur didalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas

[14] Lokapala, Nurfauzi, and Widowaty, "Aspek Yuridis Kejahatan Phishing Dalam Ketentuan Hukum Di Indonesia."

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik dan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UU ITE) tergantung hasil apa yang di peroleh dari penipuan digital melalui tautan *phishing* tersebut. Namun, pengaturan hukum terhadap regulasi penipuan digital ini ada pengaturan yang tidak dibahas secara rinci, maupun tidak ada regulasi nya maka di perlukannya perbaikan dan penyempurnaan dari aspek regulasi hukum yang mengatur tentang kejahatan phishing agar dapat memberikan perlindungan hukum yang lebih efektif dan efisien bagi korban.

DAFTAR PUSTAKA

A. Buku

Noval, sayid muhammad rifqi; soecipto; jamaludin, Ahmad; *Perlindungan Hak Digital Ancaman privasiditenga-Serangan Social*. Depok: PT Rajawali Grafindo, 2022.

Kurnia, Novi, Rahayu, Engelbertus Wendratama, Zainuddin Muda Z Monggilo, Acniah Damayanti, Dewa Ayu Diah Angendari, Firya Qurratu'ain Abisono Irnasya Shafira, and Desmalinda. *Penipuan Digital Di Indonesia (Modus, Medium, Dan Rekomendasi)*. Vol. 1, 2022.

Sudibyo, Agus. *Bernalar Sebelum Klik: Panduan Literasi Digital*. Edited by galang aji gautama, candra; putro. Cetakan pe. Jakarta: KPG (Kepustakaan Populer Gramedia), 2023.

B. Karya Ilmiah

Artanti Zahra Adisa, and Andriyanto Adhi Nugroho. "Perlindungan Hukum Terhadap Korban Phising Terkait Pengiriman File Apk." *Justisi* 10, no. 1 (2024): 242–56. https://doi.org/10.33506/js.v10i1.2980.

Gulo, Ardi Saputra, Sahuri Lasmadi, and Khabib Nawawi. "Cyber Crime Dalam Bentuk Phising Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik." *PAMPAS: Journal of Criminal Law* 1,

no. 2 (2021): 68–81. https://doi.org/10.22437/pampas.v1i2.9574.

Kurnia, Novi, Rahayu, Engelbertus Wendratama, Zainuddin Muda Z Monggilo, Acniah Damayanti, Dewa Ayu Diah Angendari, Firya Qurratu'ain Abisono Irnasya Shafira, and Desmalinda. *Penipuan Digital Di Indonesia (Modus, Medium, Dan Rekomendasi)*. Vol. 1, 2022.

Lokapala, Yazid Haikal, Fuad Januar Nurfauzi, and Yeni Widowaty. "Aspek Yuridis Kejahatan Phishing Dalam Ketentuan Hukum Di Indonesia." *Indonesian Journal of Criminal Law and Criminology (IJCLC)* 5, no. 1 (2024): 22.

noval, sayid muhammad rifqi; soecipto; jamaludin, Ahmad; *Perlindungan Hak Digital Ancaman PrivasiDitenga-Serangan Social*. Depok: PT Rajawali Grafindo, 2022.

Ode, La, and Muhammad Ichsan. "Kajian Sosiologi Kriminal Terhadap Penanggulangan Cybercrime Melalui Phising" 33, no. 2 (2018).

Sudibyo, Agus. *Bernalar Sebelum Klik: Panduan Literasi Digital*. Edited by galang aji gautama, candra; putro. Cetakan pe. jakarta: KPG (Kepustakaan Populer Gramedia), 2023.

Tualeka, M. Wahid Nur. "Teori Konflik Sosiologi Klasik Dan Modern." *Al-Hikmah : Jurnal Studi Agama-Agama* 3, no. 1 (2017): 32–48. https://journal.um-surabaya.ac.id/Ah/article/view/409.

Widianingrum, Afifah Rizqy. "Analisis Implementasi Kebijakan Hukum Terhadap Penanganan Kejahatan Siber Di Era Digital." *Journal Iuris Scientia* 2, no. 2 (2024): 90–102. https://doi.org/10.62263/jis.v2i2.40.

C. Perundang-Undangan

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

D. Website

Https://bankjombang.co.id/serangan-phishing-di-indonesia-terus meningkat-berikut-data-lengkapnya/