**PENGARUH KEMAJUAN TEKNOLOGI TERHADAP PERKEMBANGAN TINDAK
PIDANA *CYBERCRIME*
(Studi Kasus Phising Sebagai Ancaman Keamanan Digital)**

¹Irma Yurita, ²M. Kevin Ramadhan, ³M. Candra
[¹irmayurita06@gmail.com](mailto:irmayurita06@gmail.com) [²kepinram@gmail.com](mailto:kepinram@gmail.com) [³muh.chandra72@gmail.com](mailto:muh.chandra72@gmail.com)

^{1,2,3}Universitas Muhammadiyah Kotabumi

***Abstract:** Technological progress embodies an era of change that brings increasingly modern human progress. Technological advancements have also influenced cybercrime in many ways. First, the speed and availability of Internet access makes it easier for cybercriminals to gain access to global networks. This also leads to frequent and damaging phishing attacks. Additionally, continued software development has allowed the creation of more sophisticated phishing applications. This article aims to learn more deeply about cybercrime in the form of phishing. Technological advances provide many opportunities for cybercriminals to carry out phishing attacks. They can use various online methods, email, social media, malware to try to deceive their victims. Phishing is an attempt to falsify personal or financial information from an unsuspecting person or group. This research discusses the influence of technological advances on the development of phishing as a cybercrime crime. This article also covers prevention and law enforcement efforts taken to deal with the development of phishing. The results of this research are to provide a better understanding of the relationship between technology and the development of cybercrime, phishing, and can contribute to effective prevention and law enforcement efforts.*

***Keywords:** technological advances, cybercrime, phishing*

Abstrak: Kemajuan teknologi mewujudkan suatu perubahan zaman yang membawa kemajuan manusia semakin modern. Kemajuan teknologi juga telah mempengaruhi kejahatan dunia maya dalam banyak hal. Pertama, kecepatan dan ketersediaan akses Internet memudahkan penjahat dunia maya mendapatkan akses ke jaringan global. Hal ini juga menyebabkan serangan phishing yang sering terjadi dan merusak. Selain itu, pengembangan perangkat lunak yang berkelanjutan telah memungkinkan terciptanya aplikasi phishing yang lebih canggih. Artikel ini bertujuan untuk mempelajari lebih dalam lagi mengenai kejahatan *cybercrime* dalam bentuk phising. Kemajuan teknologi memberikan banyak peluang bagi kejahatan *cybercrime* untuk melancarkan kejahatan serangan phising. Mereka dapat menggunakan berbagai metode online, email, media social, malware untuk mencoba menipu korbannya. Phising adalah upaya pemalsuan informasi pribadi atau keuangan dari orang atau kelompok yang tidak menaruh curiga. Penelitian ini membahas pengaruh kemajuan teknologi terhadap perkembangan phishing sebagai tindak pidana *cybercrime*. artikel ini juga mencakup upaya pencegahan dan penegakan hukum yang dilakukan untuk menghadapi perkembangan phishing. Hasil penelitian ini untuk memberikan pemahan yang lebih baik tentang hubungan antara

teknologi dan perkembangan kejahatan *cybercrime*, phishing, dan dapat berkontribusi pada upaya pencegahan dan penegakan hukum yang efektif.

Kata Kunci: Kemajuan Teknologi, Kejahatan Dunia Maya, Phising

A. PENDAHULUAN

Munculnya teknologi internet menyebabkan munculnya golongan tindakan ilegal yang biasa disebut dengan *cybercrime* atau pelanggaran yang dilakukan melalui jaringan internet. Phishing merupakan contoh penting dari kejahatan dunia maya. Phishing dikategorikan sebagai jenis serangan cyber di mana penyerang berusaha memperoleh informasi pribadi atau rahasia secara tidak sah dari individu atau entitas dengan menyamar sebagai bisnis yang dapat dipercaya. Pelaku biasanya menggunakan strategi yang menipu, seperti membuat komunikasi elektronik, pesan teks, atau situs web palsu yang sangat mirip dengan platform sah, untuk menyesatkan individu yang tidak menaruh curiga agar mengungkapkan informasi sensitif, seperti kata sandi, rincian kartu kredit, atau data keuangan penting lainnya. Phishing adalah praktik umum yang bertujuan melakukan pencurian identitas, melakukan tindakan penipuan terkait informasi keuangan, atau secara tidak sah memperoleh akses tidak sah ke akun dan data korban.

Frekuensi aktivitas phishing semakin meningkat, terbukti dari data global yang dipublikasikan di situs resmi kelompok kerja anti-phishing (APWG). Studi bulanan mengungkapkan bahwa skema phishing mencakup 42% dari seluruh tindakan penipuan yang dilaporkan. Catatan komprehensif telah dikumpulkan, mendokumentasikan total 12,845 email phishing unik, yang diamati bersamaan dengan penyebaran 2,560 situs web palsu sebagai metode untuk melakukan serangan phishing. Sesuai dengan temuan (Gulo, A. S., Lasmadi, S., & Nawawi 2021), salah satu faktor yang berkontribusi terhadap maraknya phishing adalah kurangnya pemahaman pengguna terhadap teknologi yang digunakan. Oleh karena itu, sangat penting bagi mereka yang memiliki keahlian teknis untuk memperoleh pemahaman menyeluruh tentang mekanisme operasional teknologi. Seperti yang telah dijelaskan sebelumnya, kurangnya kesadaran pengguna memainkan peran penting dalam menjamurnya kejahatan dunia maya, khususnya dalam bidang kegiatan ilmiah, seperti phishing. Salah satu sudut pandang berpendapat bahwa kejahatan dapat

dipahami sebagai cerminan keadaan masyarakat, yang menyatakan bahwa kejahatan adalah hasil dari pengorganisasian dan berfungsinya masyarakat.

Pentingnya terobosan teknologi dan munculnya kejahatan phishing menjadi semakin relevan dalam lanskap digital modern. Fenomena phishing, yang melibatkan penggunaan penipuan online untuk mendapatkan informasi pribadi dan sumber daya keuangan dari individu atau kelompok, telah mengalami perubahan signifikan sebagai reaksi terhadap kemajuan teknologi. Tujuan dari esai ini adalah untuk memberikan analisis komprehensif tentang pengaruh teknologi terhadap perkembangan phishing sebagai praktik kriminal. Apa saja tindakan pencegahannya? Apa saja peraturan dan kebijakan hukum mengenai kejahatan dunia maya, dengan fokus khusus pada tindakan phishing?

B. METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif. Pendekatan yang digunakan dalam penelitian yaitu pendekatan perundang-undangan dan pendekatan konseptual. Pendekatan perundang-undangan berfokus pada analisis terhadap norma-norma hukum

yang berlaku, sementara pendekatan konseptual lebih menitikberatkan pada konsep-konsep hukum yang mendasari perundang-undangan tersebut. Kombinasi kedua pendekatan ini memungkinkan penelitian untuk menggali pemahaman mendalam terkait aspek normatif dan konseptual dalam ranah hukum.

Karena penelitian hukum normatif menggunakan data sekunder (bahasa sastra), maka penyusunan sistem kegiatan sementara (strategi) dapat dihilangkan, namun penyusunan sistem konseptual sangat penting. Dalam mengembangkan kerangka teori, harus digunakan kerangka teori yang menjadi landasan penelitian. (Amiruddin and Asikin 2016)

C. PEMBAHASAN

1. Pengaruh Kemajuan Teknologi Terhadap Perkembangan Phising Sebagai Tindak Pidana

Di era teknologi digital saat ini, sebagian besar masyarakat di seluruh dunia menunjukkan tingkat keakraban dan ketergantungan pada telepon pintar atau ponsel, sehingga membuat mereka rentan terhadap partisipasi dalam aktivitas dunia maya. Dalam ranah kejahatan dunia maya (*cybercrime*), kemunculan fenomena ini bukanlah suatu perkembangan baru, namun

merupakan perpindahan perilaku kriminal konvensional dari ruang fisik ke lingkungan digital. Ini dikenal sebagai kejahatan dunia maya. Di era saat ini, terdapat berbagai macam kejahatan dunia maya, salah satunya adalah kejadian penting yang disebut dengan phishing. Phishing adalah aktivitas penipuan yang ditandai dengan upaya sengaja untuk menyesatkan individu agar membocorkan informasi rahasia. Dalam bahasa Indonesia, frasa “penipuan” atau “pengelabuan” digunakan ketika melakukan penerjemahan. Adapun pengertian yang diberikan dalam Kamus Besar Bahasa Indonesia, penipuan adalah suatu pendekatan atau teknik sistematis yang meliputi kegiatan yang disengaja dengan tujuan untuk menyesatkan atau mengelabui orang lain. Istilah “trik” dapat diartikan sebagai tindakan yang disengaja yang dilakukan dengan tujuan mengalihkan fokus individu dari suatu aktivitas atau peristiwa tertentu yang ditujukan padanya.

Kemajuan teknologi memberikan dampak yang luar biasa terhadap menjamurnya phishing sebagai kegiatan kriminal, sehingga menimbulkan banyak akibat:

1. Peningkatan keterampilan

Kemajuan teknologi telah memfasilitasi peningkatan kemampuan kriminal di kalangan phisher, yang kini dapat memanfaatkan alat rekayasa canggih untuk membuat konten palsu dan situs

web palsu. Perkembangan ini memberikan kesulitan yang cukup besar dalam hal identifikasi.

2. *Social engineering* yang lebih canggih
Dengan meningkatnya aksesibilitas data pribadi melalui media sosial dan internet, individu dengan niat jahat kini memiliki kapasitas untuk terlibat dalam kegiatan teknis yang lebih canggih. Individu memiliki kapasitas untuk menciptakan bentuk komunikasi yang menarik berdasarkan kepemilikan mereka atas informasi pribadi yang relevan dengan penerima yang dituju.

3. Kecerdasan buatan (AI)

Insiden kecerdasan buatan (AI) dalam upaya phishing semakin meningkat, karena digunakan untuk mengoordinasikan serangan, mengidentifikasi calon korban, dan mendistribusikan pesan-pesan yang menarik.

Konsekuensi dari fenomena ini adalah perbaikan terus-menerus pada sistem anti-phishing dan deteksi, semakin pentingnya keamanan siber, dan perlunya meningkatkan edukasi mengenai bahaya phishing untuk menjaga keamanan digital.

Hukum pidana Indonesia mencakup pencurian sebagai tindak pidana komprehensif yang diatur dalam Kitab Undang-undang Hukum Pidana (KUHP). Meski demikian, tindakan penyebaran informasi melalui teknik phishing

dikategorikan sebagai kejahatan siber. Penggolongan tersebut di atas sesuai dengan gagasan *lex specialis derogate lex generalis* yang menyatakan bahwa undang-undang yang bersifat khusus mempunyai kewenangan yang lebih besar dibandingkan dengan undang-undang yang bersifat umum. Ketika pokok bahasannya mencakup topik yang luas, kerangka hukum terkait beralih dari KUHP ke peraturan yang ditentukan dalam Undang-Undang Informasi dan Transaksi Elektronik (ITE) nomor 19 Tahun 2016 (Arya Budi Mahesa 2023).

Sesuai dengan peraturan perundang-undangan di atas, Pasal 35 mengatur bahwa setiap orang yang dengan sengaja dan melawan hukum melakukan manipulasi, pembuatan, modifikasi, penghapusan, atau pemusnahan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan untuk menunjukkan keasliannya secara tidak benar, dapat dikenakan sanksi pidana. ketentuan Pasal 35 juncto Pasal 51 ayat (1) UUD ITE. Berdasarkan ketentuan ini, siapa pun yang melakukan pembuatan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan untuk mengelabui orang lain agar yakin bahwa data tersebut asli, dapat dipidana dengan pidana penjara paling lama 12 tahun dan/atau denda uang paling banyak. sebesar dua belas miliar rupiah. Konsep yang dijelaskan berkaitan dengan prosedur phishing, yang mencakup suatu

bentuk aktivitas kriminal dunia maya yang ditandai dengan pembuatan situs web palsu yang sangat mirip dengan situs resmi.

Disiplin hukum dapat dipahami sebagai kerangka konseptual yang mengakui pentingnya perolehan pengetahuan, penyelesaian masalah masyarakat, dan pembentukan representasi yang adil secara konseptual. Sifat dasar hukum pada hakikatnya bersifat abadi dan komprehensif, terus beradaptasi untuk mengakomodasi perubahan masyarakat sesuai dengan hukum yang berkaitan dengan pertimbangan kemanusiaan, sejalan dengan kemajuan hubungan antarmanusia. Selain itu, penting untuk menyadari bahwa terdapat interkoneksi intrinsik antara hukum dan masyarakat. Konsep ini didukung oleh pepatah hukum “ubi societas, ibi ius”, yang menyatakan bahwa hukum harus hidup berdampingan dimanapun ada masyarakat. Dalam konteks Indonesia, hubungan antara perlindungan data pribadi dan layanan keamanan siber ditunjukkan melalui hadirnya peraturan yang mengatur kedua bidang tersebut. Topik yang dibicarakan berkaitan dengan prinsip inti atau keyakinan. (Saputra and Marpaung 2023).

2. Upaya Pencegahan Phising

Analisis Kaspersky Security Network 2021 mengungkapkan bahwa serangan

phishing memberikan masalah keamanan siber yang menonjol dalam konteks Indonesia. Pada kuartal keempat tahun 2020, sejumlah besar 1,6 juta kasus serangan phishing terdeteksi. Serangan phishing merupakan masalah yang sangat memprihatinkan di seluruh Asia Tenggara, dan Indonesia menjadi negara terdepan dalam hal frekuensi serangan ini. Meningkatnya serangan phishing di Indonesia dapat disebabkan oleh beberapa faktor, termasuk meningkatnya populasi pengguna internet di negara ini, kurangnya kesadaran mengenai keamanan siber, dan kerentanan yang sudah ada dalam infrastruktur Internet. Selain itu, sebagian besar orang yang menggunakan internet kurang memahami metodologi dan persiapan yang diterapkan oleh mereka yang terlibat dalam aktivitas phishing, sehingga menambah situasi yang disebutkan di atas.

Berdasarkan statistik di atas, terlihat jelas bahwa terjadinya serangan siber terus meningkat. Hal ini dibarengi dengan tumbuh dan berkembangnya berbagai jenis serangan phishing secara simultan, sejalan dengan kemajuan teknologi digital. Tujuan serangan phishing bervariasi tergantung pada targetnya, mencakup berbagai motivasi seperti terlibat dalam serangan phishing untuk tujuan rekreasi, mencari keuntungan finansial melalui trial and error, mengejar tujuan politik, meningkatkan

langkah-langkah keselamatan dan keamanan, dan niat lain sebagaimana ditentukan oleh pelaku. Banyaknya maksud dan tujuan serangan phishing mempunyai dampak yang signifikan terhadap individu yang menjadi sasaran aktivitas berbahaya ini. Pilihan target serangan phishing menunjukkan variasi yang cukup besar berdasarkan pentingnya atau tujuan serangan *cyber* (Widyanto & Pudyo, 2022).

Upaya yang diarahkan untuk memitigasi dan memberantas serangan phishing juga mengalami tren yang meningkat di Indonesia. Ada beberapa strategi yang dapat digunakan untuk mengurangi kejadian serangan phishing. Metode-metode yang disebutkan di atas mencakup peningkatan pengetahuan dan pendidikan terkait keamanan siber, penerapan teknologi keamanan seperti perlindungan virus, keamanan jaringan, dan sertifikat SSL di situs web, serta penerapan tindakan tegas terhadap penjahat dunia maya yang terlibat dalam serangan phishing. Partisipasi aktif lembaga pemerintah dan penegak hukum sangat penting dalam memitigasi upaya phishing secara efektif dalam konteks spesifik Indonesia.

Beberapa lembaga pemerintah, seperti Kementerian Komunikasi dan Informatika (Kemenkominfo) dan Badan Siber dan Sandi Negara (BSSN), telah melakukan berbagai upaya yang bertujuan

untuk meningkatkan kesadaran dan edukasi masyarakat mengenai keamanan siber. Selain itu, lembaga-lembaga ini terlihat berhasil membangun protokol pemantauan dan secara efektif menangani insiden upaya phishing (Ramadhan, R. P., & Desyani 2023).

Sehubungan dengan hal tersebut di atas, pemerintah menerapkan Undang-Undang Nomor 11 Tahun 2008 yang biasa disebut dengan “Informasi dan Bisnis Elektronik” atau ITE. Penekanan utama undang-undang ini terutama berkaitan dengan aktivitas ekonomi elektronik, meskipun undang-undang ini juga memiliki peraturan yang bertujuan untuk melindungi data pribadi. Pengaturan perlindungan data pribadi secara khusus diatur dalam Pasal 26 undang-undang tersebut:

1. Dengan tidak adanya mandat legislatif, penggunaan data pribadi yang diperoleh melalui sarana elektronik memerlukan persetujuan eksplisit dari individu terkait.
2. Mereka yang mengalami pelanggaran terhadap hak-haknya sebagaimana dimaksud pada bagian tersebut di atas, mempunyai hak untuk mencari upaya hukum atas segala kerugian yang diakibatkannya sesuai dengan peraturan perundang-undangan ini (Saputra and Marpaung 2023).

Ketika terlibat dalam proses pengembangan undang-undang, sangatlah

penting untuk menciptakan tujuan yang jelas. UU ITE mempunyai maksud dan tujuan yang luas. Pasal 4 UU Informasi dan Transaksi Elektronik (ITE) menguraikan penerapan teknologi informasi dalam menyederhanakan transaksi elektronik dengan tujuan meningkatkan taraf hidup masyarakat informasi di seluruh dunia. Hal ini mencakup fasilitasi perluasan perdagangan dan kemajuan perekonomian nasional, peningkatan kesejahteraan masyarakat, serta peningkatan penyediaan pelayanan publik yang efektif dan efisien. Lebih jauh lagi, ketentuan di atas menggarisbawahi pentingnya memastikan akses yang adil bagi individu untuk memanfaatkan ide dan keterampilan mereka di bidang teknologi informasi, sekaligus menekankan pentingnya penggunaan yang bertanggung jawab. Tujuan utama dari undang-undang ini adalah untuk menciptakan struktur yang mendorong peningkatan tingkat keamanan, keadilan, dan kepatuhan terhadap hukum, khususnya di antara individu yang bekerja di bidang teknologi informasi dan mereka yang bertanggung jawab atas administrasinya.

Tujuan UU ITE adalah untuk memberikan tingkat kepastian dan perlindungan yang lebih tinggi bagi mereka yang berinteraksi dengan teknologi. Dalam beberapa situasi genting, individu yang menjadi korban pelanggaran terkait

teknologi berhak mendapatkan perlindungan. Informasi yang diuraikan di atas dituangkan dalam Undang-Undang Nomor 31 Tahun 2014, sebuah dokumen peraturan perundang-undangan yang secara khusus mengatur perlindungan saksi dan korban (Pongoh, J. K., & Popal 2023).

Kerangka hukum yang ada di Indonesia tetap relevan dalam mengatasi berbagai permasalahan kontemporer, karena peraturan perundang-undangan yang mencakup Informasi dan Transaksi Elektronik (ITE) tidak sepenuhnya melindungi individu dan menghalangi aktivitas penipuan terkait data. Ada peningkatan yang signifikan dalam tingkat transparansi mengenai penegakan hukum dan isu-isu terkait pertanahan. Tingkat koordinasi antar lembaga di Indonesia saat ini masih kurang. Meskipun demikian, terdapat prospek untuk meningkatkan pencegahan penipuan siber di dalam negeri melalui penerapan langkah-langkah yang patut dicontoh di negara lain, yaitu Inggris dan Australia. Singkatnya, metodologi yang disarankan mencakup tiga elemen mendasar: perluasan dan modernisasi kerangka peraturan, pembentukan lembaga-lembaga baru dan pelaksanaan reformasi organisasi, serta peningkatan kerja sama dan kolaborasi. Dalam proses revisi undang-undang, penting untuk membangun kerangka peraturan yang memuat istilah-istilah yang berkaitan

dengan aktivitas penipuan dan menjaga keamanan data pribadi. Selama era reformasi kelembagaan, tujuan utamanya adalah meningkatkan efektivitas lembaga-lembaga negara dengan memastikan bahwa lembaga-lembaga tersebut selaras dengan tanggung jawabnya. Selain itu, terdapat harapan untuk terciptanya pusat pemberitaan baru yang memiliki fokus khusus. Kebutuhan akan pencegahan yang efektif memerlukan pembentukan upaya kooperatif dan kolaboratif di antara badan-badan pemerintah, organisasi perusahaan, dan lembaga sukarela (Caroline, Kuntadi, and Pramukty 2023)

3. Kebijakan Hukum Terhadap *Cyber* Dalam Bentuk Phising

Undang-undang legislatif memainkan fungsi penting dalam bidang penegakan hukum dan kewenangan pihak berwenang untuk mengatasi tindakan terlarang dan menerapkan tindakan yang sesuai terhadap pelakunya. Dalam ranah kejahatan dunia maya, sangat penting untuk mempertimbangkan bahwa kategorisasi pelanggaran dan pendekatan yang digunakan untuk membangun kasus bergantung pada yurisdiksi hukum spesifik yang bersangkutan. Pemerintah Republik Indonesia telah menunjukkan dedikasi yang tegas dalam menanggulangi permasalahan kejahatan dunia maya. Upaya pemerintah Indonesia untuk mengatasi kejahatan yang

berkaitan dengan teknologi komunikasi dan informasi mencapai tonggak penting dengan penerapan dan dukungan Undang-Undang Informasi dan Transaksi Elektronik tahun 2008. Dengan mematuhi proses yang ditentukan ini, lembaga penegak hukum akan memperoleh sumber daya yang diperlukan untuk mengambil tindakan dan memulai prosedur hukum terhadap orang-orang yang terlibat dalam aktivitas kejahatan dunia maya.

Pemberantasan kejahatan dunia maya pada dasarnya saling berhubungan dengan domain kebijakan pencegahan kejahatan, yang biasa dikenal dengan “strategi kejahatan”. Menurut Sudarto, kebijakan kejahatan adalah upaya masyarakat yang terarah dan sistematis untuk menghadapi dan meringankan perilaku kriminal. Saling ketergantungan antara perumusan UU ITE dengan agenda politik kriminal terlihat jelas jika mempertimbangkan tujuan yang dimaksudkan, antara lain peningkatan kesejahteraan sosial dan pemeliharaan keamanan masyarakat (Hardianto Djanggih 2013).

Beberapa langkah pemerintah dalam menangani phising:

1. Penegakan protokol dan pedoman mengenai keamanan siber dan phishing merupakan elemen penting dalam perlindungan sistem digital dan mitigasi bahaya online. Contoh nyatanya bisa kita lihat pada penerapan Undang-

Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

2. Lembaga penegak hukum memainkan peran penting dalam mengidentifikasi dan mengadili mereka yang terlibat dalam aktivitas phishing, sehingga berfungsi sebagai pencegahan terhadap penjahat dunia maya. Hal ini sejalan dengan peraturan yang tercantum dalam pasal 46 ayat (3) Undang-undang Informasi dan Teknologi Elektronik (undang-undang ITE).

Lebih lanjut, strategi Indonesia dalam memerangi penipuan siber didasarkan pada kerangka peraturan perundang-undangan yang ditetapkan dalam Undang-Undang Informasi dan Transaksi Elektronik (ITE) Nomor 16 Tahun 2016. Ayat kedua Pasal 28 mengesampingkan ayat 2 Pasal 28 Undang-undang Informasi dan Transaksi Elektronik (ITE).) Undang-undang tahun 2008. Kewajiban yang dimaksudkan untuk mencegah dan menjaga keseimbangan biasa disebut dengan kewajiban hukum. Pengakuan perlunya kerangka utuh dalam melakukan penyidikan dan penegakan hukum diakui Polri. Pengakuan ini mengharuskan Kementerian Komunikasi dan Teknologi (MCT) untuk mengembangkan undang-undang yang sesuai. Meskipun teknik sering disorot sebagai faktor utama yang berkontribusi terhadap permasalahan, khususnya dalam hal implementasi, penting bagi polisi

penipuan siber di Indonesia untuk memperkuat kemampuan mereka dalam memecahkan masalah. (Syah 2023) telah mengidentifikasi hambatan-hambatan yang terkait dengan pelaksanaan standar kepolisian.

Kejahatan dunia maya memiliki kapasitas untuk menyerang banyak entitas, antara lain mencakup komunitas, badan pemerintah, dan kelompok lain. Dalam konteks berinteraksi dengan lanskap digital, sangatlah penting bagi setiap individu untuk bersikap hati-hati dan menahan diri saat menghadapi materi dalam lingkup ini. Selain itu, sangat penting bagi pengguna untuk memperoleh pemahaman komprehensif tentang beragam komponen unik di dalam domain dunia maya agar dapat memitigasi risiko aktivitas dunia maya, seperti phishing dengan baik (Odie et al. 2022).

D. PENUTUP

1. Pengaruh kemajuan teknologi terhadap perkembangan phishing sebagai tindak pidana dunia maya (cybercrime) mencakup tindakan pelanggaran yang secara eksplisit melibatkan komputer atau perangkat komunikasi sebagai target dan alat untuk melakukan tindakan, atau dalam beberapa hal terkait dengan pelanggaran yang dikategorikan

sebagai kejahatan komputer. Ada berbagai bentuk tindakan kriminal yang dapat diamati, dimana individu memiliki kapasitas untuk memilih metode operasi yang diinginkan untuk berpartisipasi dalam kejahatan dunia maya. Salah satu strategi tersebut dikenal sebagai phishing.

2. Upaya pencegahan phishing melibatkan kesadaran pengguna, teknologi keamanan, dan tindakan proaktif. Pengguna perlu waspada terhadap email atau pesan mencurigakan, menghindari klik tautan yang mencurigakan, dan selalu memverifikasi sumber informasi. Penerapan teknologi keamanan seperti filter email, firewalls, dan antivirus juga krusial. Organisasi dapat menyediakan pelatihan keamanan siber, melakukan uji phishing internal, dan memastikan kepatuhan terhadap praktik keamanan yang ketat. Kombinasi strategi ini dapat membantu mengurangi risiko serangan phishing.
3. Kebijakan hukum terhadap cyber, khususnya dalam konteks phishing, menunjukkan pentingnya perlindungan terhadap keamanan digital. Upaya pencegahan dan penegakan hukum yang kuat menjadi kunci dalam melindungi individu dan organisasi dari ancaman phishing. Perluasan regulasi dan kerjasama lintas negara juga diperlukan untuk mengatasi sifat lintas batas dari

serangan cyber, menciptakan lingkungan online yang lebih aman bagi semua pihak.

Selain kesimpulan, ada beberapa saran yang perlu disampaikan:

1. Pengaruh kemajuan teknologi terhadap perkembangan phising sebagai tindak pidana, dukungan pemerintah terhadap pengembangan teknologi informasi sangatlah penting dan harus dibarengi dengan pembentukan kerangka hukum dan peraturan yang komprehensif. Hal ini akan meningkatkan penerapan pemanfaatan teknologi informasi secara aman, dengan fokus khusus pada menghindari konsekuensi negatif yang terkait dengan kejahatan dunia maya.
2. Upaya pencegahan terhadap phising, pengguna harus selalu menjaga

dan jangan membagikan informasi pribadi atau rahasia kata sandi melewati email atau pesan tanpa verifikasi keaslian situs dan/atau aplikasi. Jika pengguna menemukan tautan yang mencurigakan terhadap suatu email atau pesan, jangan ragu menghubungi penyedia layanan email atau situs web terkait untuk memverifikasi keaslian tautan.

3. Kebijakan hukum terhadap kejahatan cyber, pendidikan dan kesadaran masyarakat terhadap bahaya dunia maya atau *cybercrime* perlu ditingkatkan dan harus diberi edukasi tentang masalah tersebut, sehingga masyarakat dapat lebih berhati-hati dan melindungi diri sendiri dari kejahatan *cybercrime* atau dunia maya.

DAFTAR PUSTAKA

Buku

Amiruddin, and Zainal Asikin. 2016. *Pengantar Metode Penelitian Hukum*. Depok: PT RajaGrafindo Persada.

Jurnal Artikel

Arya Budi Mahesa, S. 2023. "Optimalisasi Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dalam Penanganan Perkara Tindak Pidana Phising." *COMSERVA Indonesian Journal of Community Services and Development* 2 (11): 2686–2696. <https://doi.org/10.59141/comserva.v2i11.670>.

Bodhi, S., & Tan, D. 2022. "Keamanan Data Pribadi Dalam Sistem Pembayaran E-Wallet Terhadap Ancaman Penipuan Dan Pengelabuan (Cybercrime)." *UNES Law Review* 4 (3):

297–308.

- Caroline, Evline, Cris Kuntadi, and Rachmat Pramukty. 2023. “Pengaruh Pengalaman Auditor , Dukungan Manajemen Dan Efektivitas Pengendalian Internal Terhadap Efektivitas Fungsi Audit Internal” 2: 1487–97.
- Dewantoro, N. M., & Dian Alan Setiawan SH, M. H. 2023. “Penegakan Hukum Kejahatan Siber Berbasis Phising Dalam Bentuk Application Package Kit (APK) Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik.” *In Bandung Conference Series: Law Studies* 3 (2): 892–900.
- Ferrary, A. A. I., Hartini, S., & Purwaningsih, P. 2023. “Kajian Hukum Terhadap Tindak Pidana Cyber Phising Yang Digunakan Untuk Mengambil Data Pribadi Pada Situs Digital Trading Dihadirkan Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Transaksi El.” *Univeritas Ibn Khaldun Bogor* 10 (2): 1–12.
- Fikri, A. W. N., Fauzi, A., Rachman, A. A., Khaerunisa, A., Sari, D. P., Vernanda, P., ... & Fadyanti, T. P. 2023. “Analisis Keamanan Sistem Operasi Dalam Menghadapi Ancaman Phishing Dalam Layanan Online Banking.” *Jurnal Ilmu Multidisplin* 2 (1): 84–91.
- Gulo, A. S., Lasmadi, S., & Nawawi, K. 2021. “Cybercrime Dalam Bentuk Phishing Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik.” *PAMPAS: Journal of Criminal Law* 1 (2): 68–81. <https://doi.org/10.22437/pampas.v1i2.9574>.
- Hardianto Djanggih. 2013. “No Title.” *Jurnal Media Hukum* 1, No2 (Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Cyber Crime Di Bidang Kesusilaan): halaman 12.
- Ketaren, E. 2016. “Cybercrime, Cyber Space, Dan Cyber Law.” *Jurnal Times* 5 (2): 35–42.
- Luthfi, R. 2022. “Perlindungan Data Pribadi Sebagai Perwujudan Perlindungan Hak Asasi Manusia.” *Jurnal Sosial Dan Teknologi* 2 (5): 431–36.
- Muftiadi, A., Agustina, T. P. M., & Evi, M. 2022. “Studi Kasus Keamanan Jaringan Komputer: Analisis Ancaman Phising Terhadap Layanan Online Banking.” *Hexatech: Jurnal Ilmiah Teknik* 1 (2): 60–65.
- Odie, I Kadek, Kharisma Putra, I Made Adi Darmawan, and I Putu Gede Juliana. 2022. “Crime Actions In The Digital World In The Form Of Phising” 5 (2): 77–82.
- P, W. P. 2022. “Analisis Intejan Atas Potensi Ancaman Serangan Siber Pada Presiden KTT G20 Tahun 2022 Di Indonesia” 1 (03): 81–94.
- Pongoh, J. K., & Popal, D. F. T. 2023. *Upaya Penanggulangan Tindak Pidana Mayantara (Cyber Crime)*.
- Putusan, D., Agung, M., Indonesia, R., Sumbul, B. Y., Ds, K., & Sumbul, Y. 2021. *Hukum Dan Mahkamah Agung Republik Indonesia*.
- Ramadhan, R. P., & Desyani, T. 2023. “Implementasi Algoritma J48 Untuk Identifikasi Website Phising” 1 (2): 46–54.

- Saputra, Dewana, and Zaid Alfauza Marpaung. 2023. "Analisis Yuridis Penanggulangan Penyalahgunaan Data Pribadi Dalam Bentuk Phising Yang Dilakukan Oleh Paid Verified Account Di Media Sosial Menurut Undang- Undang Perlindungan Data Pribadi" 5 (4): 4764–75.
- Setiawan, R., & Arista, M. O. 2013. "Efektivitas Undang-Undang Informasi Dan Transaksi Elektronik Di Indonesia Dalam Aspek Hukum Pidana." *Jurnal Hukum Pidana Dan Penanggulangan Kejahatan* 2 (2).