E-ISSN: 2622-7045 I P-ISSN: 2654-3605
UNES LAW REVIEW
https://review-unes.com uneslawreview@gmail.com +62 856-5804-3983
DOI: https://doi.org/10.31933/unesrev.v6i1
Received: 15 Oktober 2023, **Revised:** 24 Oktober 2023, **Publish:** 26 Oktober 2023

Tinjauan Kasus Cyber Phishing 16 Shop Berdasarkan UU ITE Nomor 19 Tahun 2016

Azzahra Ayu Nur Permata[1], Elfrida Ratnawati[2].
[1] Universitas Trisakti, Jakarta, Indonesia
Email: Azzahraa.ayuu@gmail.com
[2] Universitas Trisakti, Jakarta, Indonesia
Email: Elfrida.r@trisakti.ac.id

Corresponding Author: Azzahraa.ayuu@gmail.com

Abstract: *This study discusses the case of cyber phishing carried out by the phishing Group 16 Shop, namely fraud by creating and selling fake website and software platforms resembling genuine electronic transaction sites for the purpose of deceiving targets. has the ITE Law Number 19 of 2016 been effectively implemented by the government to protect victims and enforce laws related to Cyber Phishing crimes? Is the principal problem of writing this study. The research method used in this study is normative legal research that connects various sources of legal material and is analyzed descriptively. This study aims to analyze the case of "Cyber Phishing 16 Shop" associated with ITE Law Number 19 of 2016 in the role of regulating and protecting cybercriminals related to electronic transactions.*

Keyword: *Cyber Phishing, electronic transactions, ITE Law Number 19 of 2016*

Abstrak: Penelitian ini membahas mengenai kasus cyber phishing yang dilakukan oleh kelompok phishing 16 Shop, yaitu dilakukannya penipuan dengan cara membuat dan menjual platform website dan software palsu menyerupai situs transaksi elektronik asli untuk tujuan mengelabui target. apakah UU ITE Nomor 19 Tahun 2016 telah diimplementasikan secara efektif oleh pemerintah untuk melindungi korban dan menegakkan hukum terkait dengan tindak pidana Cyber Phishing? Merupakan pokok masalah dari penulisan penelitian ini. Metode penelitian yang digunakan dalam penelitian ini adalah penelitian hukum normatif yaitu menghubungkan berbagai sumber bahan hukum dan dianalisis secara deskriptif. Penelitian ini bertujuan untuk menganalisis kasus "Cyber Phishing 16 Shop" mengaitkan dengan UU ITE Nomor 19 Tahun 2016 dalam berperan mengatur dan melindungi tindak pidana siber terkait transaksi eletronik.
Kata Kunci: Cyber Phishing, transaksi elektronik, UU ITE Nomor 19 Tahun 2016

PENDAHULUAN

Perkembangan teknologi dalam era globalisasi telah membawa kemajuan dalam berbagai aspek kehidupan manusia. Namun, tidak semua dampak yang dihasilkan selalu bersifat positif. Salah satu dampak negatif yang muncul seiring dengan pesatnya perkembangan teknologi informasi yakni kejahatan siber atau sering disebut sebagai Cyber Crime. kejahatan siber atau cyber crime telah menjadi semakin umum dan kompleks dalam beberapa tahun terakhir.

Pelaku kejahatan dalam dunia siber ini sering disebut dengan istilah cracking maupun cracker dimana mereka melakukan kejahatan dengan berbagai tujuan. Salah satu kejahatan cracking maupun cracker yakni Phishing. Phishing merupakan kejahatan yang tujuan utamanya adalah untuk menguntungkan diri sendiri, dan tentunya kejahatan ini juga sangat merugikan pihak lain. Di sisi lain Phishing juga dapat dikatakan sebagai salah satu tindak kriminal elektronik yang mengambil bentuk penipuan. Menurut laporan organisasi internasional Anti-Phishing Working Group (APWG) sepanjang tahun 2022 tercatat ada lebih dari 4,7 juta serangan Phishing, dan jumlah tersebut sudah meningkat sejak awal tahun 2019 sekitar sebanyak 150% per tahun.

Banyak korban dari serangan ancaman Phishing ini sangat dirugikan dalam hal privasi yaitu pencurian data, penyalahgunaan dan tidak jarang juga dirugikan dalam hal kerugian finansial yang sangat besar. Proses ancaman serangan Phishing yang dilakukan para cracking maupun cracker adalah bertujuan untuk memperoleh informasi yang sangat sensitif, seperti nama pengguna, sandi, dan rincian kartu kredit, dengan menyamar sebagai entitas yang terpercaya seperti pihak yang berwenang, administrator sistem, pegawai pemerintahan serta organisasi sah dan umumnya berkomunikasi secara elektronik dalam bentuk berupa ajakan untuk melakukan pembaharuan informasi akun yang ditargetkan.

Dalam kasus Cyber Phishing Internasional dikenal dengan kelompok Phishing “16 Shop” yang terjadi pada tahun 2021, melibatkan WNI asal Kalimantan Selatan sebagai pembuat dan pengembang versi awal dari Phishing “16 shop”. “16 shop” sendiri merupakan alat peretas yang dibuat dan diperuntukkan untuk mencuri kredensial (username dan password) para pengguna layanan transaksi internasional. Diketahui dalam hasil penyelidikan, kelompok Phishing Internasional ini mempunyai perusahaan yang berbasis lokasi di Amerika Serikat (AS) namun informasi pendaftarannya berbasis di Indonesia. Kelompok Phishing Internasional ini berperan dalam menyediakan tools seperti (perangkat lunak layaknya software dan sebagainya) yang diperlukan oleh cracker atau cracking untuk melancarkan kegiatan Phishing.

Dalam kelompok Cyber Phishing “16 shop” ada WNI asal Kalimatan Selatan yang berperan sebagai pembuat alat peretas yang digunakan untuk melakukan Phishing ke beberapa transaksi internasional yakni kepada para pengguna Paypal, Cash App, Apple, Amazon, hingga American Express. Salah satu trik yang digunakan pelaku Phishing ini adalah dengan menggunakan dokumen PDF palsu yang memancing para korban untuk mengisi data-data sensitif, di samping itu Pelaku Phishing “16 shop” ini juga menyediakan konten penipuan dengan bahasa sesuai dengan lokasi target dimana korban berasal. Menurut data dari sumber cyberthreat.id, bahwa WNI asal Kalimatan Selatan tersebut merupakan pembuat dan penjual kode/script yang dapat digunakan untuk meretas akun pembayaran elektronik internasional, hingga kartu kredit yang beroperasi di seluruh dunia. Berdasarkan informasi dari interpol mengungkapkan bahwa kode peretasan yang dibuat Kelompok Phishing 16 Shop telah menyasar sekitar lebih dari 70.000 akun pengguna dari beberapa perusahaan unicorn internasional yang tersebar dari 43 negara dan menjadi korban serangan Phishing yang dilakukan melalui halaman yang diciptakan oleh “16 shop”.

Bahkan, kerugian diperkirakan telah mencapai angka sekitar Rp. 127 milyar. informasi yang dicuri selama serangan ancaman yaitu termasuk rincian pribadi, akun e-mail, kata sandi,

kartu identitas, nomor kartu kredit, dan nomor telepon. Informasi tersebut dikumpulkan para pelaku Phishing untuk mencuri uang korban, melakukan pemerasan, dan bahkan menjualnya kepada pelaku penjahat lainnya. Di Indonesia saat ini belum ada Undang-Undang ataupun Peraturan yang secara khusus mengatur mengenai Cyber dalam bentuk Phishing, akan tetapi pelaku Phishing di Indonesia dimungkinkan dijerat dengan ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP) Pasal 378 dan juga dapat dikenakan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

Dalam UU ITE pada umunya pelaku phishing dimungkinkan dapat dikenakan dengan Pasal 35 jo. Pasal 51 UU ITE karena pelaku Phishing memanipulasi korban dengan membuat situs penipuan yang menyerupai seolah-olah situs tersebut adalah situs asli yang resmi. Berdasarkan pendahuluan tersebut diatas, maka permasalahan yang akan dibahas dalam penelitian ini adalah:

1. Bagaimana sistem pembuktian dalam kejahatan siber, dan apakah UU ITE Nomor 19 Tahun 2016 telah diimplementasikan secara efektif oleh pemerintah untuk melindungi korban dan menegakkan hukum terkait dengan tindak pidana Cyber Phishing?

METODE

Jenis Penelitian

Jenis penelitian ini menggunakan metode penelitian normatif (normative law research) yaitu dengan menggunakan studi kasus normatif berupa produk perilaku hukum yang kemudian dianalisis dengan peraturan perundang-undangan serta dikaji dengan fokus objek kajian terhadap segi-segi hukum yang berkaitan dengan tindak pidana Cyber Phishing kemudian dihubungkan dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Pendekatan Penlitian

Pendekatan dalam Penelitian ini menggunakan 2 pendekatan yaitu :

a. Penelitian ini mengadopsi pendekatan perundang-undangan (statue approach), di mana penelitian ini fokus pada penggunaan bahan hukum dalam bentuk peraturan perundang-undangan sebagai landasan utama dalam penyelidikan. Pendekatan ini melibatkan analisis seluruh peraturan perundang-undangan yang relevan dengan isu hukum yang sedang dihadapi.

b. Penelitian ini mengadopsi Pendekatan konseptual (conceptual approach) dalam penelitian hukum adalah jenis pendekatan yang memfokuskan analisis penyelesaian permasalahan dalam penelitian hukum pada aspek-aspek konseptual hukum yang mendasarinya, atau bahkan mengidentifikasi nilai-nilai yang terkandung dalam pengaturan suatu peraturan dalam hubungannya dengan konsep-konsep yang digunakan.

Sumber bahan Hukum

Sumber Hukum terbagi 3, yaitu :

a. Bahan hukum primer, yaitu bahan yang bersifat seperti Undang-Undang atau Peraturan lainnya. Dalam penelitian ini menggunakan bahan hukum primer sebagai berikut :

   1) Undang-Undang Republik Indonesia Nomor 19 tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

b. Bahan hukum Sekunder, yaitu bahan hukum yang memiliki karakteristik sebagai penjelasan terhadap bahan hukum primer, yang meliputi berbagai sumber seperti literatur, jurnal, dan penelitian yang telah dilakukan sebelumnya;

c. Bahan hukum tersier, yaitu merujuk kepada bahan hukum yang memberikan penjelasan terhadap bahan hukum primer dan sekunder, termasuk tetapi tidak terbatas pada surat kabar dan sumber-sumber dari internet.

Teknik Pengumpulan Bahan Hukum

Metode pengumpulan materi hukum yang diterapkan dalam penelitian ini adalah melalui penerapan studi dokumen. Dalam proses ini, penulis melakukan analisis terhadap berbagai dokumen, baik dalam bentuk tulisan maupun elektronik, dengan tujuan untuk menghasilkan tinjauan yang sistematis dan terintegrasi.

Analisis Bahan Hukum

Dalam penelitian ini, analisis dilakukan dengan menggabungkan data dari berbagai sumber hukum yang tersedia, kemudian dianalisis menggunakan pendekatan kualitatif dengan dukungan logika berpikir deduktif. Hal ini bertujuan untuk memberikan jawaban terhadap isu-isu hukum yang muncul dalam penulisan.

HASIL DAN PEMBAHASAN

Landasan Teori The "Cyber Routine Activities Theory" oleh Lawrence E Cohen

Prinsip utama dari teori ini menjelaskan mengenai pemahaman bahwa kejahatan dapat terjadi ketika keadaan dapat mendukung kejahatan tersebut dan menghasilkan peluang kriminal. Teori ini juga termasuk ke dalam teori kriminologi yang menjelaskan bagaimana kejahatan terjadi sebagai akibat dari tiga elemen utama: pelaku yang termotivasi, target yang sesuai, dan kurangnya pengawasan yang mampu. Berdasarkan dari Kasus Cyber Phishing 16 Shop diatas, Teori Aktivitas Rutin Cyber erat kaitannya antara dengan kejahatan elektronik yang dilakukan dengan penerapan prinsip-prinsip ini ke dunia digital, di mana aktivitas rutin melibatkan perilaku dan interaksi online.

Teori ini didukung oleh beberapa faktor, antara lain yaitu Pelaku yang Termotivasi; Dalam kasus Phishing, para pelaku merupakan kelompok yang memiliki motivasi untuk melakukan kejahatan siber. Motivasi yang dimaksud disini merupakan motivasi finansial untuk memperoleh informasi pribadi yang bersifat sensitif dari korban, seperti nomor kartu kredit dan kata sandi, motivasi ini yang merupakan pendorong utama di balik ancaman serangan yang dilakukan dengan didukung keahlian dan pengetahuan di dunia digital. Motivasi ini didukung oleh intelektual dan keahlian para pelaku di bidang digital. Target yang Sesuai; indikator pendukung yang lain dalam kasus phishing sama seperti dalam praktiknya, di dunia maya, mereka juga memanfaatkan target yang lebih sesuai bagi pelaku kejahatan dunia maya. Target-target ini dapat mencakup individu maupun kelompok yang memiliki informasi berharga, sumber daya keuangan, atau kerentanannya yang dapat dimanfaatkan.

Kurangnya Pengawasan yang Mampu; faktor lainnya juga didukung oleh rendahnya pemahaman keamanan. Para korban dalam kasus Cyber Phishing 16 Shop mungkin tidak memiliki pemahaman yang memadai tentang cara mengenali serangan phishing atau mungkin tidak dilengkapi dengan langkah-langkah keamanan yang efektif dalam melindungi informasi pribadi mereka. Tidak ada langkah-langkah keamanan siber yang efektif seperti kata sandi yang lemah, pembaruan perangkat lunak yang tidak memadai, atau kurangnya edukasi pengguna, ini dapat menciptakan peluang bagi pelaku kejahatan dunia maya.

Pengaturan perundang-undangan Cyber Crime dalam bentuk Phishing

Cyber crime adalah istilah yang secara umum digunakan untuk menggambarkan tindakan kejahatan yang melibatkan penggunaan komputer dan internet.

Menurut Hius, dkk. (2014), faktor-faktor berikut memainkan peran penting dalam penyebab terjadinya Cyber Crime:

a. Ketersediaan akses internet yang tak terbatas;
b. Ketidakhati-hatian pengguna komputer;

c. Kemudahan pelaksanaannya dan sulitnya pelacakan;
d. Pelaku umumnya individu dengan tingkat kecerdasan yang tinggi dan tingkat rasa ingin tahu yang besar.

Berbagai jenis kategori kejahatan siber melibatkan berbagai aspek dalam kejahatan di dunia maya, termasuk:

Tabel 1.1

	Kategori siber mengandung kekerasan (*cybercrime with violence*)	Identifikasi
a	*Cyberstalking*	Penguntitan di Internet
b.	*Child Pornography*	Pornografi anak
c.	*Cyberterrorism, Assault by Threat*	Serangan dengan ancaman

Tabel 1.2

	Kategori siber tanpa kekerasan (*cyber without violence*)	Identifikasi
a.	*Cyber Phishing*	Pencurian data pribadi antara lain berawal dari penipuan berupa link/situs website
b.	*Cyber Laundering*	Pencucian uang
c.	*Cyber Drugs Sales*	Penjualan obat & narkotika di internet
d.	*Cybergamblin*	Perjudian di Internet
e.	*Destructive Cybercrimes*	Merusak jaringan
f.	*Cyber Prostitute Ads*	Iklan internet prostitusi
g.	*Cyberfraud*	Penipuan di internet
h.	*Cybertheft*	Mencuri informasi
i.	*Cybertrespass*	Memasuki jaringan tanpa izin

Kejahatan siber dalam bentuk phishing dikategorikan sebagai kejahatan dalam tindak pidana penipuan. Dalam melakukan modus operasinya, kelompok cyber phishing 16 Shop menjual perangkat kit phishing. Kit phishing yang dijual oleh platform 16 Shop digunakan untuk meretas salah satu layanan elektronik, yaitu CashApp, dan termasuk template situs yang meniru dengan sangat mirip dengan template situs resmi milik Cash App. Selain itu, mereka menciptakan alur kerja yang sangat menyerupai dengan situs aslinya untuk proses

login atau masuk. Ketika tautan phishing yang meniru situs Cash App di-klik, serangkaian pemeriksaan akan dijalankan sebelum halaman phishing dimuat.

Berbagai informasi seperti alamat IP pengunjung, agen pengguna yang mereka gunakan, dan rincian penyedia layanan internet (ISP) dikumpulkan dan diproses guna mencegah akses teknologi keamanan dan alat pengindeks konten internet (web crawler). Jika pemeriksaan ini melewati tahap tersebut, pengunjung akan diarahkan ke halaman phishing 16 Shop dan diminta untuk mengisi alamat email mereka yang terkait dengan akun Cash App. Setelah pengisian alamat email akun Cash App, situs phishing tersebut kemudian memberi tahu pengguna tentang status akun mereka, di mana tombol yang disediakan digunakan untuk membuka kunci akun. Secara singkat, 16 Shop menciptakan kesan palsu bagi pengguna Cash App bahwa akun mereka telah terkunci karena masalah keamanan sebagai upaya untuk menipu calon korban.

Korban yang cemas dan mengira bahwa tindakan tersebut akan membantu mereka menyelamatkan akun mereka dari dikunci, tentu akan mengklik tombol untuk membuka kunci akun. Jika mereka melakukannya, dari sinilah masalah dimulai. Sebab, korban akan diminta untuk memasukkan data yang bersifat sensitif, termasuk:

a. Dokumen identifikasi (KTP atau SIM);
b. Identitas seperti nama lengkap dan alamat;
c. Alamat email;
d. Password;
e. Nomor jaminan sosial (SSN);
f. Rincian kartu debit (nomor kartu, tanggal dan tahun kedaluwarsa, CVV);
g. PIN Cash App.

Data-data itu kemudian akan digunakan oleh peretas untuk mengambil alih akun Cash App asli milik korban yang terperdaya. Tindakan yang dilakukan oleh pelaku Phishing tersebut dapat digolongkan sebagai tindak penipuan. Secara umum, penipuan diatur dalam ketentuan yang terdapat dalam Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP) dan juga dapat diterapkan pada tindakan phishing karena pada dasarnya phishing merupakan bentuk tindak pidana penipuan. Unsur-unsur yang terkandung di dalam Pasal 378 KUHP diantaranya :

1. “Dengan maksud untuk menguntungkan diri secara melawan hukum”;
2. “Menggerakkan orang untuk menyerahkan barang sesuatu”;
3. “Dengan menggunakan salah satu upaya penipuan (dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan)”.

Penipuan dalam Pasal 378 KUHP dirumuskan sebagai berikut : “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 empat tahun.”

Akan tetapi unsur-unsur yang terkandung di dalam Pasal 378 KUHP dirasa kurang relevan dan kurang tepat untuk di aplikasikan dalam kejahatan siber dalam bentuk phishing, oleh karena itu melalui kewenangannya pemerintah memberlakukan dan mengesahkan Undang-Undang nomor 11 tahun 2008 yang dikenal dengan UU ITE atau UU Informasi dan Transaksi Elektronik. Walaupun di Indonesia sendiri saat ini belum ada undang-undang atau peraturan khusus yang secara eksplisit mengatur dan melindungi dari ancaman terhadap cyber phishing, namun ancaman Phishing masuk dalam cakupan yang diatur di dalam Undang-Undang nomor 11 tahun 2008.

Undang-Undang Nomor 11 tahun 2008 mengatur mengenai aspek yang berkaitan dengan kejahatan siber dalam bentuk penipuan diatur dan dirumuskan dalam :

Bunyi dalam Pasal 34 ayat (1) dan ayat (2) :

1. “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki” :
    a. “perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33”;
    b. “sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33”.
2. “Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.”

Bunyi dalam Pasal 50 : “Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 34 ayat (1) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).”

Selanjutnya dalam Pasal 35 jo Pasal 51 ayat (1) yang dirumuskan sebagai berikut : “Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.”

Pasal 51 : “Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp 12.000.000.000,00 (dua belas miliar rupiah).” Unsur-unsur yang terdapat di dalam Pasal 35, yaitu:

1. “Setiap orang”;
2. “Dengan sengaja dan tanpa hak atau melawan hukum”;
3. “Melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik”;
4. “Dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik t ersebut dianggap seolah-olah data yang otentik”.

Perbuatan phishing tidak hanya dapat dikategorikan sebagai sebuah perilaku penipuan biasa; dalam phishing, salah satu ciri khas yang menonjol adalah penipuan yang menggunakan pemanfaatan teknologi yaitu pembuatan situs yang sangat menyerupai situs asli, yang kemudian digunakan untuk menipu korban. Praktik ini seringkali mengakibatkan kerugian finansial yang sangat besar bagi korban, seperti yang terjadi pada kasus serangan cyber phishing "16 Shop." Pada kasus tersebut, para pelaku melalui platform yang mereka buat melakukan phishing untuk mendapatkan akses ke beberapa transaksi internasional. Pada umumnya perbuatan Cyber Phishing merupakan bentuk kriminal yang serius, dan berdampak pada keamanan dan privasi individu serta perusahaan. Kejahatan ini tidak hanya mencakup penipuan tradisional tetapi juga memanfaatkan teknologi modern untuk menciptakan situs web tiruan yang sangat meyakinkan. Situs web palsu tersebut digunakan sebagai alat utama untuk mengecoh dan merayu korbannya dengan tujuan meraih keuntungan finansial secara ilegal.

Seperti yang terjadi pada kasus phishing "16 Shop" menggambarkan betapa berbahayanya praktik ini. Para pelaku yang cerdik dan berpengetahuan teknologi menggunakan situs web tiruan dan platform palsu untuk mencuri informasi pribadi korban,

seperti kata sandi, nomor kartu kredit, dan informasi keuangan lainnya. Mereka bahkan menyasar layanan internasional terkemuka seperti Paypal, Cash App, Apple, Amazon, dan American Express, menambahkan dimensi internasional pada ancaman ini.

Akibat serangan phishing, korban mengalami kerugian finansial yang signifikan, kehilangan akses ke akun mereka, serta risiko pencurian identitas dan penyalahgunaan data pribadi. Oleh karena itu, perlindungan terhadap keamanan siber dan pemahaman yang lebih dalam tentang ancaman seperti phishing sangat penting dalam upaya menjaga keamanan data pribadi secara online. Organisasi dan individu harus terus meningkatkan kesadaran mereka terhadap serangan ini dan menerapkan tindakan pencegahan serta kebijakan keamanan yang kuat untuk melindungi diri dari ancaman phishing.

Dalam rumusan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik dapat disimpulkan bahwa pengaturan cyber crime dalam bentuk phishing relevan dan sesuai dengan asas "Lex Specialis Derogat Legi Generali" yang mana bahwa aturan-aturan hukum yang bersifat khusus dianggap berlaku meskipun bertentangan dengan aturan-aturan hukum yang umum. Oleh karena itu Undang-undang ini berlaku untuk digunakan karena undang-undang ini bersifat khusus.

Dalam tindakannya, terdapat sistem pembuktian pada kejahatan siber di dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Pada Pasal 5 Bab II merumuskan sebagai berikut :

1. "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah";
2. "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia";
3. "Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini";
4. "Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk:
    a. "surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis"; dan
    b. "surat beserta dokumennya yang menurut Undang- Undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta".

Melalui peraturan dan pasal-pasal yang terkandung dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik pemerintah terbukti telah menjalankan dan menegakkan hukum terkait dengan kejahatan siber dan transaksi elektronik, dimana dalam kasus "Cyber Phishing 16 Shop" terdakwa yang merupakan pembuat dan pengembang versi awal platform website dan software palsu yang merupakan WNI asal Kalimantan Selatan dijerat dengan Pasal 50 jo Pasal 34 Ayat 1 Undang - Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang - Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) karena terbukti sebagai entitas yang menjual software palsu tersebut kepada pihak ketiga.

Dalam memaksimalkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008, di Indonesia terdapat Undang-Undang Nomor 27 Tahun 2002 tentang Perlindungan Data Pribadi yang memiliki tujuan untuk melindungi privasi data pribadi individu dan mengatur bagaimana data pribadi harus dikelola dan diproses. UU ini memiliki potensi untuk memaksimalkan perlindungan korban serangan phishing yang diatur dalam Pasal 36, 37, 38 dan 39 ayat (1) dan (2) Undang-Undang Nomor 27 Tahun 2002 tentang Perlindungan Data Pribadi. Pasal-pasal dalam UU tentang

Perlindungan Data Pribadi merinci mengenai tanggung jawab dan kewajiban pengendali Data Pribadi dalam menjaga kerahasiaan, melindungi, dan mencegah akses tidak sah terhadap Data Pribadi yang mereka proses. Hal ini merupakan bagian penting dalam peraturan perlindungan data untuk memastikan bahwa informasi pribadi individu tetap aman dan dilindungi.

Pasal Pasal yang disebutkan dalam Undang-Undang Nomor 27 Tahun 2002 tentang Perlindungan Data Pribadi diatas menetapkan standar dan kewajiban bagi pengendali data pribadi untuk menjaga privasi dan keamanan data pribadi. Meskipun serangan phishing adalah ancaman terhadap keamanan terhadap data pribadi, penerapan prinsip-prinsip dalam Undang-Undang Perlindungan Data Pribadi dapat membantu meminimalkan risiko dan kerugian yang mungkin dialami oleh korban serangan phishing. Melalui pengawasan, pemrosesan yang sah, dan sistem keamanan yang andal, undang-undang tersebut menciptakan kerangka kerja yang dapat mendukung perlindungan data pribadi dan pengurangan risiko yang terkait dengan serangan phishing

KESIMPULAN

Berdasarkan hasil dan pembahasan dalam penelitian, UU ITE dapat diterapkan terhadap tindakan tertentu berdasarkan kategori perbuatan yang dilakukan, dengan mempertimbangkan konteks dan karakteristik dari setiap tindakan tersebut. Hal ini memungkinkan penegakan hukum secara tepat menangani perbuatan yang melibatkan penggunaan teknologi informasi, dan menyesuaikan respon hukum dengan serangkaian tindakan yang berbeda sesuai dengan kategorinya. UU ITE dalam perkara tindak pidana “16 Shop” dimana pengaturan hukum terhadap cyber crime dalam bentuk phishing yakni dapat dijerat dengan Pasal 50 jo Pasal 34 Ayat 1 Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) karena di dalamnya memuat unsur memproduksi serta menjual perangkat keras atau perangkat lunak Komputer kepada suatu entitas dengan maksud semata-mata untuk mengambil keuntungan secara pribadi dan merugikan target korbannya dalam hal finansial. Dalam memaksimalkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008, terdapat Undang-Undang Nomor 27 Tahun 2002 tentang Perlindungan Data Pribadi yang perlu dioptimalkan karena dianggap sangat penting dalam menangani masalah yang seringkali muncul seiring dengan peningkatan penggunaan data pribadi dalam transaksi berbasis teknologi informasi di berbagai aspek kehidupan.

REFERENSI

Andi Hamzah, Aspek-aspek Pidana di Bidang Komputer, penerbit Sinar Grafika, Jakarta, 2005. Hlm 30

Kitab Undang-Undang Hukum Pidana

Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 27 Tahun 2002 Tentang Perlindungan Data Pribadi

https://tekno.kompas.com/read/2023/08/10/08000097/interpol-tangkap-warga-indonesia-penyedia-layanan-phising-16shop-?page=all

https://cyberthreat.id/insightdetil/10707/Jejak-Phishing-Kit-16Shop

https://cyberthreat.id/read/13600/Polisi-FBI-dan-Interpol-Tangkap-Riswanda-Hacker-Indonesia-yang-Bikin-Alat-Peretas-16Shop

https://www.saplaw.top/pendekatan-perundang-undangan-statute-approach-dalam-penelitian-hukum/