PENGATURAN SANKSI PIDANA BAGI PELAKU PENIPUAN PHISING BERBASIS WEB

"Diajukan Sebagai Salah Satu Syarat Akhir Guna Memperoleh Gelar Sarjana Hukum"

Oleh :

Nama	**: Tiara Dea Reza**
Nim	**: 21150036**
Program Studi	**: Ilmu Hukum**
Program Kekhususan	**: Hukum Pidana**

FAKULTAS HUKUM

UNIVERSITAS MUHAMMADIYAH SUMATERA BARAT

BUKITTINGGI

2025

LEMBAR PENGESAHAN JURNAL

Pengaturan Sanksi Pidana Bagi Pelaku Penipuan Phising Berbasis Web

Oleh

Nama	**: Tiara Dea Reza**
NIM	**: 21150036**
Program Studi	**: Ilmu Hukum**
Program Kekhususan	**: Hukum Pidana**

Jurnal ini telah dipertahankan dihadapan Tim Penguji *Ujian Komprehensif* Fakultas Hukum Universitas Muhammadiyah Sumatera Barat Pada Tanggal 15 Februari 2025 dan dinyatakan **LULUS**

Tim Penguji

Ketua

Mahlil Adriaman, SH., MH
NIDN. 1021018404

Sekretaris

Nessa Fajriyana Farda, SH., MH
NIDN. 1006018801

Pembimbing I

Yenny Fitri Z, SH MH
NIDN. 1008068601

Penguji I

Dr. Wendra Yunaldi SH., MH
NIDN. 1017077801

Penguji II

Yon Efri SH., MH
NIDN.1003066801

Diketahui Oleh
Dekan Fakultas Hukum
Universitas Muammadiyah Sumatera Barat

Dr. Wendra Yunaldi, SH., MH
NIDN. 1017077801

LEMBAR PERSETUJUAN JURNAL

Pengaturan Sanksi Pidana Bagi Pelaku Penipuan Phising Berbasis Web

Oleh

Nama	**: Tiara Dea Reza**
NIM	**: 21150036**
Program Studi	**: Ilmu Hukum**
Program Kekhususan	**: Hukum Pidana**

Telah disetujui Dosen Pembimbing

Di Bukittinggi

18 Februari 2025

Pembimbing I

Yenny Fitri.Z, SH.,MH

NIDN. 1008068601

HALAMAN PERNYATAAN KEASLIAN JURNAL

Yang bertandatangan di bawah ini :

Nama	: Tiara Dea Reza
NIM	: 21150036
Judul Jurnal	: Pengaturan Sanksi Pidana Bagi Pelaku Penipuan Phising Berbasis Web

Menyatakan bahwa Jurnal ini merupakan hasil karya penulis sendiri, dan bukan merupakan duplikasi ataupun *plagiasi* (jiplakan) dari hasil penelitian orang lain, sepengetahuan penulis, topik atau judul skripsi ini belum pernah ditulis orang lain.

Apabila Jurnal ini terbukti merupakan hasil duplikasi atau *plagiasi* (jiplakan) dari hasil penelitian orang lain, maka saya bersedia menerima sanksi yang diberikan sesuai aturan yang berlaku.

Demikian Surat Pernyataan ini Penulis buat dengan sebenar-benarnya.

Bukittinggi, 09 Syawal 1446 H
08 April 2025 M

Yang Menyatakan

TIARA DEA REZA

NIM. 21150036

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
Vol. x, No. x, hlm xx-xx
http://ejournal.ulka-bogor.ac.id/index.php/YUSTISI

PENGATURAN SANKSI PIDANA BAGI PELAKU PENIPUAN *PHISING* BERBASIS WEB

Tiara Dea Reza[1], Yenny Fitri Z[2]
[1,2,]Universitas Muhammadiyah Sumatera Barat, Indonesia
Email: tiaradearezaa@gmail.com
Email: yennyfitri54@gmail.com

Abstrak

Penipuan p*hishing* adalah tindakan menipu seseorang untuk melakukan kejahatan dunia maya (*cybercrime*) di mana seseorang menyamar sebagai lembaga yang sah menghubungi korban atau target melalui email, telepon, atau pesan teks, agar ia memberikan data sensitif seperti informasi identitas pribadi, detail perbankan dan kartu kredit, serta kata sandi. Penipuan phishing merupakan tindakan berbahaya yang tidak hanya merugikan individu tetapi juga mengancam keamanan data secara luas. Dalam konteks hukum pidana, phishing dikategorikan sebagai kejahatan penipuan dan pelanggaran terhadap undang-undang perlindungan data pribadi. Rumusan masalah pada penelitian ini adalah: apakah kualifikasi tindak pidana penipuan phising berbasis web dan bagaimana pengaturan hukum terhadap pelaku tindak pidana penipuan phising di Indonesia. Metode penulisan ini menggunakan metode yuridis normatif. Hasil Penelitian ini adalah tindak pidana penipuan phishing berbasis web merupakan kejahatan siber yang dilakukan dengan menciptakan situs web palsu yang menyerupai situs resmi untuk mencuri data sensitif pengguna. Karakteristik utama dari serangan phishing meliputi penggunaan alamat email atau URL mencurigakan, permintaan informasi sensitif secara mendesak, penggunaan bahasa yang buruk, serta tautan mencurigakan. Untuk membuktikan kasus phishing, diperlukan bukti digital berupa situs web palsu, rekaman transaksi elektronik, data korban yang dicuri, dan bukti kerugian materiil. Pengaturan hukum terhadap tindak pidana phishing di Indonesia diatur dalam beberapa instrumen hukum. Meskipun tidak secara khusus diatur dalam KUHP, tindakan ini dapat dijerat dengan Pasal 378 KUHP tentang penipuan. Selain itu, UU ITE No. 19 Tahun 2016 perubahan atas Undang-undang Nomor 11 tahun 2008 maupun perubahannya dalam UU Nomor 1 Tahun 2024 mengatur secara lebih spesifik tentang kejahatan tindak pidana penipuan phising ini.
Kata kunci: Tindak Pidana; Pelaku Penipuan Phising; Cyber Crime.

Abstract

Phishing fraud is the act of tricking someone into committing cybercrime in which someone posing as a legitimate institution contacts a victim or target via email, telephone or text message, to get him to provide sensitive data such as personal identity information, banking and credit card details, as well as password. Phishing fraud is a dangerous act that not only harms individuals but also threatens data security at large. In the context of criminal law, phishing is categorized as a crime of fraud and a violation of personal data protection laws. The formulation of the problem in this research is: what are the qualifications for criminal acts of web-based phishing fraud and what are the legal regulations for perpetrators of criminal acts of phishing fraud in Indonesia. This writing method uses a normative juridical method. The crime of web-based phishing fraud is a cyber crime committed by creating a

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
http://ojournal.ulka-bogor.ac.id/Index.php/YUSTISI

fake website that resembles an official site to steal sensitive user data. The main characteristics of phishing attacks include the use of suspicious email addresses or URLs, urgent requests for sensitive information, use of poor language, and suspicious links. To prove a phishing case, digital evidence is needed in the form of a fake website, electronic transaction records, stolen victim data, and proof of material loss. Legal regulations for phishing crimes in Indonesia are regulated in several legal instruments. Even though it is not specifically regulated in the Criminal Code, this action can be charged under Article 378 of the Criminal Code concerning fraud. Apart from that, ITE Law no. 19 of 2016, amendments to Law Number 11 of 2008 and amendments to Law Number 1 of 2024 regulate more specifically the crime of phishing fraud.
***Keywords**: Criminal Act; Phishing Scam Perpetrators; Cyber Crime.*

PENDAHULUAN

Teknologi adalah sesuatu yang diciptakan untuk memudahkan hidup manusia dengan bekal pengetahuan melalui akal manusia. Teknologi informasi mencakup perangkat keras dan perangkat lunak untuk satu atau sejumlah tugas pemrosesan data.[1] Pemanfaatan dan perkembangan teknologi informasi menghasilkan ciptaan baru berupa komputer, kecerdasan buatan, rekayasa perangkat lunak dan internet.[2] Perkembangan teknologi informasi juga membentuk masyarakat dunia baru yang tidak lagi dihalangi oleh batas-batas teritorial dan telah membalikkan segalanya yang jauh jadi dekat dan yang khayal jadi nyata.[3] Namun perkembangan teknologi informasi ini juga membawa berbagai tantangan dan dampak yang perlu diwaspadai. Di satu sisi, kemudahan akses informasi dan komunikasi global telah menciptakan peluang baru dalam bidang pendidikan, bisnis, dan hubungan sosial. Tetapi di sisi lain, fenomena ini juga memunculkan masalah-masalah baru yaitu *cyber crime*.

Cyber crime adalah mereka yang memiliki ahli tinggi dalam ilmu komputer, pelaku *cyber crime* umumnya menguasai algoritma dan pemograman computer untuk membuat *script*/kode *malware*.[4] Cyber crime muncul bersamaan dengan lahirnya kemajuan teknologi informasi.[5] Pelaku *Cyber Crime* adalah individu dengan beragam latar belakang dan keahlian**,** meskipun keahlian teknis dalam komputer merupakan faktor yang penting, namun motivasi, akses ke alat dan teknologi, serta kemampuan untuk beradaptasi juga memainkan peran penting dalam dunia kejahatan *cyber*. Para pelaku kejahatan siber ini dapat dikelompokkan menjadi beberapa kategori, mulai dari pemula yang hanya memanfaatkan alat-alat yang sudah tersedia, hingga peretas profesional yang mampu menciptakan malware canggih. Mereka bisa bekerja secara individual atau tergabung

[1] I Made Wartana, "*Mengenal Teknologi Informasi*", Cet.1 (Malang:Media Nusa Kreatif,2017), hlm.6.
[2] Muhammad Sadi, "*Aspek Hukum Informasi Di Indonesia*", Cet.1 (Jakarta:Kencana,2021), hlm.37.
[3] Andri Winjaya Laksana, "*Pemidanaan Cybercrime Dalam Perspektif Hukum Pidana Positif*", Jurnal Hukum Unissula 35, No.1,2019.
[4] Sahat Maruli T.Situmeanf, "*Cyber Law*", Cet.1 (Bandung:Penerbit Cakra,2020), hlm.24.
[5] Muh.Akbar Fhad Syahril, "*Hukum Informasi dan Transaksi Elektronik*", (Jawa Tengah:CV.Eureka Media Aksara,2023), hlm.63.

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
http://ojournal.ulka-bogor.ac.id/Index.php/YUSTISI

dalam kelompok kejahatan terorganisir yang memiliki jaringan luas. Salah satu bentuk kejahatannya adalah penipuan phising berbasis web.

Phising berasal dari istilah dalam bahasa inggris yaitu *fishing* yang artinya memancing, istilah memancing disini digunakan untuk menjebak korban dengan maksud tertentu.[6] *Phishing* merupakan bentuk penipuan online di mana pelaku mencoba untuk mendapatkan informasi rahasia atau sensitif dari korban dengan menyamar sebagai entitas tepercaya. Modus operandi ini dapat terjadi melalui email, situs web palsu, atau pesan palsu yang dikirimkan melalui berbagai platform untuk mengecoh orang agar memberikan informasi rahasia seperti *username*, *password*, atau bahkan nomor kartu kredit.[7] Web Phising, biasanya menggunakan media website palsu untuk menjerat calon korban. Di mana, pelaku akan membuat email dengan nama domain yang seolah-olah resmi atau juga disebut dengan domain spoofing.[8] Dengan web datang revolusi jejaring sosial, interaksi tinggi dan partisipasi pengguna dalam produksi konten[9]. Namun, di sisi lain, meningkatnya keterlibatan pengguna juga membuka celah bagi berbagai ancaman siber, seperti penyebaran informasi palsu, pencurian data pribadi, serta serangan phishing yang semakin canggih.

Contoh kasus mengenai penipuan phising berbasis web adalah pada tahun 2022 penipuan yang mengatasnamakan Bank BRI beredar di media sosial, korban dihubungi melalui chat WA mengenai pemberitahuan perubahan biaya transfer dari Bank BRI kepada Bank lain. Jika korban tidak membalas berarti korban menyetujui perubahan tersebut, korban membalas chat WA tersebut dengan kalimat tidak setuju. Lalu pelaku mengirimkan berupa formulir dan link kepada korban. link tersebut dikirimkan berupa http://perubahantarifbri6500.zyrosite.com. Selanjutnya korban mengklik link tersebut dan masuk ke dalam link yang diberikan pelaku. Kemudian korban mengisi username, password dan pin. Selanjutnya korban mendapatkan sms dari pihak BRI berupa kode OTP dan korban menyalin kode OTP tersebut kedalam link yang diberikan melalui WA tadi. Setelah itu korban mendapatkan notifikasi aplikasi brimo adanya pembayaran BRIVA atas nama korban sebesar 300 ribu dan adanya transfer dari aplikasi brimo sebesar 250 juta. Tanpa disadari korban telah terpedaya dalam chat WA tersebut. Persoalan phising merupakan kelalaian nasabah yang memberikan data pribadi, akun dan finansial. Akibatnya penipu bisa mengakses data tersebut untuk mengambil uang korban di rekening melalui phising, korban pun mengalami kerugian berupa kehilangan uang di rekening tabungannya di Bank BRI.[10]

---

[6] Vikran Fasyadhiyaksa Putra Y, "*Modus Operandi Tindak Pidana Phising Menurut UU ITE*", Jurnal Jurist-Diction, Vol.4, No.6,2021.

[7] Sabrina Tabrani, "*Kejahatan Phising Ditinjau Dari Perspektif Hukum dan Kejahatan Siber*", Jurnal Kajian Hukum dan Pendidikan Kewarganegaraan, Vol.3, No.1, Januari 2024

[8] Purnamasari, "*Analisis Kejahatan Online Phising Pada Institusi Pemerintah/Pendidik Sehari-hari*", Jurnal Digital Teknologi Informasi, Vol.06, No.01, Maret 2023.

[9] Andi Asari, "*Pengembangan Website*", (Malang:Media Nusa Creative,2023), hlm.3

[10] https://regional.Kompas.com

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
http://ojournal.ulka-bogor.ac.id/Index.php/YUSTISI

Berdasarkan uraian di atas maka di temukan beberapa rumusan masalah yang terjadi. Pertama apakah kualifikasi dari tindak pidana penipuan phising berbasis web? Kedua bagaimana pengaturan hukum terhadap pelaku tindak pidana penipuan phising di Indonesia?

METODE PENELITIAN

1. **METODE PENDEKATAN**
   Adapun pendekatan yang dipakai dalam penelitian ini adalah pendekatan yuridis normatif, suatu metode penelitian hukum yang hanya ditunjukkan pada peraturan-peraturan tertulis sehingga penelitian ini sangat erat hubungannya pada perpustakaan karena akan membahas tentang penipuan phising berbasis web

2. **Sifat dan Tujuan Penelitian**
   Penelitian ini merupakan penelitian hukum deskriptif, yaitu penelitian suatu metode yang menggambarkan keadaan yang sebenarnya terjadi dan menguraikan suatu kejadian dan permasalahan yang diteliti dengan melakukan pengkajian secara deskriptif tentang ketentuan peraturan perundang-undangan dan landasan teori yang berkaitan dengan tindak pidana yang berkaitan dengan penipuan phising berbasis web

3. **Analisis Data**
   Analisis data yang digunakan dalam penelitian ini adalah analisis *kualitatif* yaitu mengamati gejala hukum tanpa menggunakan alat ukur yang menghasilkan angka berupa informasi yang hanya dapat dinilai dengan menggunakan peraturan perundang-undangan, pandangan teori dan konsepsi, para ahli serta logika, tindak pidana yang berkaitan dengan penipuan phising berbasiHasil dan Pembahasan

HASIL DAN PEMBAHASAN

Kualifikasi Dari Tindak Pidana Penipuan Phising Berbasis Web

Tindak pidana penipuan phishing berbasis web merupakan salah satu bentuk kejahatan siber yang semakin berkembang di era digital. Menurut Victoria (2013) Phishing (*Password Harvesting Fishing*) adalah aktivitas penipuan yang menggunakan email atau situs web palsu untuk mengelabui pengguna agar memungkinkan perlaku memperoleh informasi pengguna.[11] Pelaku kejahatan ini biasanya menciptakan situs web palsu yang tampak identik dengan situs web resmi dari institusi terpercaya seperti bank, e-commerce, atau layanan email. Tujuan utama dari tindakan ini adalah untuk mencuri data sensitif pengguna seperti username, password, nomor kartu kredit, dan informasi pribadi lainnya.[12] Metode yang digunakan umumnya melibatkan pengiriman email atau pesan yang mengandung tautan ke situs web palsu tersebut, di mana korban kemudian diminta untuk memasukkan informasi pribadi mereka dengan berbagai dalih yang meyakinkan.

[11] Devi Puspitasari, "*Analisis Kejahatan Phising Pada Sektor E-Commerce*", Jurnal Digital Teknologi Informasi, Vol. 06, No. 02, September 2023.

[12] Muhammad Rizal Supriadi, "*Deteksi Halaman Website Phising*", (Bandung:Buku Pedia,2023), hlm.1

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
http://ojournal.ulka-bogor.ac.id/Index.php/YUSTISI

Tindakan ini jelas melanggar beberapa pasal dalam UU ITE (Informasi dan Transaksi Elektronik), khususnya yang berkaitan dengan manipulasi, penciptaan, perubahan, penghilangan, dan perusakan Informasi Elektronik. Taktik phising paling umum adalah menargetkan sisi emosional korban, contohnya dengan mengirimkan hal-hal yang berkaitan atau disukai si korban sehingga tertarik untuk mengarahkan si korban kepada tautan peretail online palsu.[13] Sisi emosional korban yang dimaksud seperti rasa penasaran atau rasa ingin tau yang dimiliki pelaku untuk dapat menjebak korban kedalam situs palsu.

Ciri-ciri umum dari serangan phishing yang diidentifikasi dalam berbagai penelitian, termasuk studi yang dilakukan di Indonesia:[14]

a) Alamat Email atau URL yang Mencurigakan Phishing sering menggunakan alamat email atau URL yang terlihat mirip dengan yang asli namun memiliki perbedaan kecil yang sering kali tidak disadari oleh pengguna. Perbedaan ini sengaja dibuat untuk membingungkan dan mengecoh korban agar menganggap email atau situs tersebut sah. Pengguna sering kali tidak memperhatikan perbedaan kecil tersebut. Misalnya, URL yang menggunakan karakter mirip seperti "rn" sebagai pengganti "m" atau menambahkan kata tambahan dalam alamat email.
   Contoh : URL asli: www.mandiri.co.id
   URL phishing: www.rnandiri.co.id
b) Permintaan informasi sensitif secara mendesak pesan phishing sering kali meminta korban untuk memberikan informasi pribadi atau finansial secara mendesak, misalnya kata sandi, nomor kartu kredit, atau informasi rekening bank, dengan alasan seperti keamanan akun atau hadiah yang akan segera kedaluwarsa. Taktik ini digunakan untuk memanipulasi korban agar bertindak cepat tanpa berpikir panjang, sering kali dengan dalih bahwa akun mereka dalam bahaya atau ada tawaran menarik yang harus segera diklaim.
   Contoh: "PENTING: Akun anda akan diblokir dalam 24 jam! Segera verifikasi dengan mengisi data kartu kredit dan PIN anda di link berikut untuk menghindari pemblokiran permanen."
c) Penggunaan bahasa yang buruk atau tidak biasa banyak email phishing yang mengandung kesalahan tata bahasa, ejaan, atau kalimat yang terdengar tidak alami. Hal ini bisa menjadi tanda bahwa email tersebut tidak berasal dari sumber yang sah.
   Contoh: "Kami dari Tim Keamanan Bank telah mendeteksi aktivitas mencurigakan pada akun anda. Mohon segera klik link dibawah ini untuk memverifikasi identitas anda supaya tidak terjadi hal yang tidak diinginkan pada akun anda yang berharga."
d) Lampiran atau tautan yang mencurigakan, phishing sering kali menyertakan lampiran atau tautan yang jika diklik atau diundu dapat menginstal malware pada perangkat korban atau mengarahkan mereka ke situs web palsu yang dirancang untuk mencuri informasi mereka. Lampiran ini sering kali memiliki nama yang mengesankan, tetapi sebenarnya merupakan file berbahaya.

[13] Ismail, "*Bahaya Phising*", (Tempo Publishing,2024), hlm.12.
[14] Ananda Dias Sulistyo, "*Strategi Penanggulangan Serangan Phising Di Media Sosial*", Seminar Nasional Teknologi Informasi dan bisnis (SENATIB) 2024.

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
http://ojournal.ulka-bogor.ac.id/Index.php/YUSTISI

Contoh: "Faktur_Pembayaran_BCA.exe"

e) Tidak ada informasi kontak yang Jelas: ini tidak menyediakan informasi kontak yang dapat diverifikasi, seperti nomor telepon resmi, alamat kantor, atau email resmi. Hal ini membuatnya sulit bagi korban untuk menghubungi pihak yang sah dan memverifikasi kebenaran pesan tersebut.
Contoh: "untuk informasi lebih lanjut hubungi tim support kami" (tanpa mencantumkan nomor telepon resmi, alamat kantor, atau email yang bisa diverifikasi)

f) Perasaan terlalu bagus untuk menjadi kenyataan, seperti tawaran yang terlalu menggiurkan untuk menarik perhatian Anda.
Contoh: "Selamat! Anda terpilih sebagai pemenang undian Bank BNI dengan hadiah Rp 1 Miliar. Untuk mengklaim, segera transfer biaya administrasi sebesar Rp 1 juta ke rekening berikut..."

g) Identitas pengirim yang disamarkan: phishing sering menyamarkan identitas pengirim dengan menggunakan nama yang mirip dengan lembaga resmi atau dengan menampilkan alamat email yang mencurigakan. Hal ini dimaksudkan untuk membuat korban percaya bahwa pesan tersebut berasal dari pihak yang sah.
Contoh: Nama pengirim: "BCA Security Team"
Alamat email: security.team123@gmail.com

Penulis berpendapat bahwa, ciri-ciri serangan phishing yang dipaparkan dalam penelitian ini menunjukkan pola yang sangat sistematis dan terencana dalam upaya menipu pengguna internet. Pemahaman ini sangat penting bagi semua pengguna internet, karena ini menjadi langkah pertama untuk mencegah agar tidak menjadi korban dalam penipuan phising. Dalam hal ini, semua pengguna internet harus berhati hati dan teliti agar tidak sembarangan mengklik tautan atau mengunduh lampiran yang mencurigakan. Jika ragu, pengguna dapat menghubungi langsung institusi terkait melalui saluran resmi. Dengan memahami dan menerapkan pengetahuan tentang ciri-ciri serangan phishing ini, pengguna internet dapat lebih efektif melindungi diri dari upaya penipuan yang dapat merugikan.

Cara kerja phising melalui web adalah pada situs web mereka akan diminta untuk memasukkan informasi rahasia pribadi, seperti password dan nomor rekening bank yang pada akhirnya akan digunakan untuk pencurian identitas phising juga menggunakan tool untuk mencuri kode sumber laman web yang sah dan menggantinya dengan web palsu. Selain itu phising menciptakan tautan palsu (*embedding link)* untuk mendapatkan informasi sensitif milik korban.[15] Untuk membuktikan kasus phishing, penegak hukum perlu mengumpulkan:

1. bukti digital berupa situs web palsu
2. rekaman transaksi elektronik
3. data korban yang dicuri, riwayat komunikasi pelaku
4. bukti kerugian materiil korban.

[15] Mia Haryati Wibowo, "*Ancaman Phising Terhadap Pengguna Social Media Dalam Dunia Cyber Crime*", JOEICT (Jurnal Of Education and Information Communication Technology), Vol.1, No.1, 2017.

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
http://ojournal.ulka-bogor.ac.id/Index.php/YUSTISI

Upaya pencegahan phising dapat dilakukan dengan cara:

1. Periksa URL: pastikan URL situs web yang anda kunjungi sesuai dan valid. Waspadai perubahan kecil dalam pengejaan atau karakter.
2. Jangan klik Tautan yang Mencurigakan: Anda harus menghindari mengklik tautan yang mencurigakan yang dikirim melalui email, pesan teks, atau media sosial Anda lebih baik menggunakan bookmark Anda atau secara manual.
3. Verifikasi Keaslian Situs Web: Jika Anda merasa bahwa situs web yang Anda kunjungi tampak mencurigakan, Anda harus menghubungi pihak berwenang secara langsung atau melalui saluran komunikasi yang terpercaya untuk memastikan bahwa itu benar.[16]
4. Peningkatan pengetahuan dan pendidikan terkait keamanan siber.
5. Penerapan teknologi keamanan seperti perlindungan virus, kemanan jaringan dan sertifikat SSL di situs web.
6. Penerapan tindakan tegas terhadap penjahat dunia maya yang terlibat dalam serangan phising.[17]

Penulis berpendapat bahwa keamanan siber menjadi aspek yang sangat penting di era digital ini, dalam menghindari ancaman phishing, penting bagi pengguna untuk selalu memeriksa keaslian URL situs web yang dikunjungi, jangan mengklik tautan mencurigakan yang dikirim melalui email, pesan teks, atau media sosial. Jika menemukan situs web yang mencurigakan, sebaiknya diabaikan saja agar tidak berisiko terkena serangan phishing. Peningkatan pengetahuan dan edukasi tentang keamanan siber sangat diperlukan agar pengguna lebih waspada. Dengan memahami cara kerja serangan siber serta langkah-langkah pencegahannya, pengguna dapat lebih berhati-hati dalam beraktivitas di dunia maya sehingga dapat mengurangi risiko menjadi korban kejahatan siber. Selain itu, peningkatan pengetahuan tentang keamanan siber menjadi fondasi penting dalam mencegah serangan phishing.

Pengaturan Hukum Terhadap Pelaku Tindak Pidana Penipuan Phising Di Indonesia

a) KUHP

Phising secara khusus tidak diatur dalam KUHP (Kitab Undang-undang Hukum Pidana) namun bentuk kejahatannya dapat dilihat dalam pasal 378 KUHP yang mengatur bahwa:

> *"Barangsiapa dengan maksud hendak menguntungkan diri sendiri atau orang lain dengan melawan hak, baik dengan memakai nama palsu atau keadaan palsu, baik dengan akal dan tipu muslihat, maupun dengan karangan perkataan-perkataan bohong, membujuk orang supaya memberikan sesuatu barang, membuat utang atau menghapuskan piutang, dihukum karena penipuan dengan hukuman penjara selama-lamanya 4 tahun."*[18]

---

[16] Devie Rahmawati, "*Waspada Kejahatan Phising Attack*", (Malang:PT. Literasi Nusantara abadi Grup,2024), hlm.67.

[17] Irma Yunita, "*Pengaruh Kemajuan Teknologi Terhadap Perkembangan Tindak Pidana Cyber Crime*", Jurnal Hukum Legalitas, Vol.5, No.2, Desember 2023.

[18] Pasal 378 KUHP

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
http://ojournal.uika-bogor.ac.id/index.php/YUSTISI

Adapun unsur-unsur dalam pasal 378 tersebut yaitu:
1) Unsur-unsur objektif yang terdiri dari:
   a. Menggerakkan: berarti melakukan tindakan yang mendorong atau memengaruhi orang lain untuk melakukan sesuatu. Tindakan ini bisa dilakukan secara langsung (misalnya dengan perintah atau permintaan) atau tidak langsung (misalnya dengan memanipulasi situasi atau informasi)
   b. Orang lain: unsur ini mengacu pada pihak yang menjadi sasaran dari tindakan tersebut. Orang lain adalah subjek yang dipengaruhi oleh pelaku untuk melakukan suatu tindakan sesuai kehendak pelaku.
   c. Untuk menyerahkan suatu barang/benda: unsur ini berarti pelaku berusaha memengaruhi orang lain agar menyerahkan barang atau benda tertentu
   d. Untuk memberi hutang: mengacu pada tindakan pelaku yang memengaruhi orang lain agar memberikan fasilitas pinjaman atau utang, baik dalam bentuk uang, barang, maupun jasa.
   e. Untuk menghapus piutang: mengacu pada tindakan pelaku yang memengaruhi orang lain agar melepaskan atau menghapuskan haknya untuk menagih piutang
   f. Dengan menggunakan daya dan upaya, seperti: memakai nama atau, martabat palsu, dengan tipu muslihat dan rangkaian kebohongan: seperti, menggunakan identitas palsu atau memalsukan martabat, menggunakan tipu muslihat (manipulasi, penipuan), menyusun rangkaian kebohongan yang terencana untuk menipu korban.
2) Unsur-unsur subjektif yang terdiri dari:
   a. Dengan maksud: menunjukkan adanya niat atau kehendak dari pelaku untuk mencapai tujuan tertentu.
   b. Untuk menguntungkan diri sendiri atau orang lain: tujuan pelaku, yaitu untuk memperoleh keuntungan, baik untuk dirinya sendiri maupun untuk orang lain.
   c. Secara melawan hukum[19] : tindakan pelaku bertentangan dengan hukum atau aturan yang berlaku

Penulis berpendapat bahwa, dari segi unsur objektif, "menggerakkan orang lain" dalam konteks phishing terjadi melalui pengiriman situs web palsu atau pembuatan situs web tiruan yang mendorong korban untuk melakukan tindakan tersebut. Unsur "menyerahkan barang" dalam kegiatan phishing sering terwujud dalam bentuk korban yang tertipu untuk memberikan data sensitif seperti informasi kartu kredit, password ke aset digital. Penggunaan "daya upaya" seperti nama palsu, tipu muslihat, dan rangkaian kebohongan sangat relevan dengan teknik phishing yang umumnya memanfaatkan pemalsuan identitas institusi tepercaya dan manipulasi korban. Sementara itu, unsur subjektif pasal ini juga sejalan dengan karakteristik kejahatan phishing. "Maksud untuk menguntungkan diri sendiri atau orang lain" terlihat jelas dalam motif para pelaku phishing yang berusaha mendapatkan keuntungan finansial. Unsur "melawan hukum" terpenuhi karena tindakan phishing jelas melanggar hak-hak korban dan ketentuan hukum yang berlaku.

[19] Tony Yuri Rahmanto, "*Penegakan Hukum Terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik*", Jurnal Penelitian Hukum:DE JURE, Vol.19, No.1, Maret 2019.

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
http://ejournal.uika-bogor.ac.id/index.php/YUSTISI

b) Undang-Undang Negara Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dalam beberapa pasal yang dapat dikenakan, antara lain:

1. Pasal 28 ayat (1) menyebutkan bahwa "Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik." jo. Pasal 45 A ayat (1) menyebutkan bahwa "Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000. 000.000,00 (satu miliar rupiah) ayat (2) sebagai ketentuan pidananya bahwa "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)."

   Adapun unsur-unsur yang terdapat dalam pasal 28 ayat (1) jo pasal 45 A ayat (1):
   Pasal 28 ayat (1)
   a. Unsur Objektif UU ITE Pasal 28 UU ITE
      a) Perbuatannya: Menyebarkan: Perbuatan menyebarkan yang dimaksud dalam Pasal 28 (1) UU ITE.
      b) Mengakibatkan Kerugian Konsumen dalam Transaksi Elektronik: unsur ini mensyaratkan berita bohong dan menyesatkan tersebut harus mengakibatkan suatu kerugian konsumen. Artinya tidak dapat dilakukan pemidanaan apabila tidak terjadi kerugian konsumen dalam transaksi elektronik[20]
   b. Unsur Subjektif UU ITE Pasal 28 UU ITE
      a) Dengan Sengaja: Unsur dengan sengaja pada Pasal 28 Ayat (1) ini dimaksud pada perbuatan yang menyebarkan berita bohong dengan menggunakan internet sebagai medianya.
      b) Tanpa Hak (Melawan Hukum): Terkait dengan penipuan melalui internet, yang menyebarkan informasi (iklan) yang palsu berarti telah melakukan perbuatan melawan hukum.[21]

   Pasal 45 A ayat (1)
   a. Unsur Subjektif:
      a) Dengan sengaja: menunjukkan adanya kesengajaan atau niat dalam melakukan perbuatan
      b) Tanpa hak: menunjukkan bahwa pelaku tidak memiliki kewenangan atau izin yang sah

[20] Aswan, "*Tindak Pidana Penipuan Berbasis Elektronik*" (Makasar:GuePedia,2019), hlm.40
[21] Dhaniar Eka Budiastanti, "*Perlindungan Hukum Terhadap Korban Tindak Pidana Penipuan Melalui Internet*", Jurnal Cakrawala Hukum, Vol.8, No.1 Juni 2017.

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
http://ojournal.ulka-bogor.ac.id/Index.php/YUSTISI

b. Unsur Objektif:
   a) Menyebarkan berita bohong dan menyesatkan perbuatan yang dilarang berupa: Menyebarkan informasi yang tidak benar, Informasi tersebut bersifat menyesatkan
   b) Mengakibatkan kerugian konsumen dalam Transaksi Elektronik. akibat yang ditimbulkan yaitu: ada kerugian yang dialami konsumen, kerugian terjadi dalam konteks transaksi elektronik
   c) Ancaman pidana: pidana penjara maksimal 6 tahun, denda maksimal Rp 1 miliar, dapat dijatuhkan secara kumulatif (dan/atau)

Penulis berpendapat bahwa unsur-unsur yang terdapat pada pasal 28 ayat (1) Jo pasal 45 ayat (1) UU ITE ini kejahatan tindak pidana dilakukan dalam bentuk kesengajaan, perbuatan tersebut dilakukan dengan kesadaran penuh dan bukan karena kelalaian dan perbuatannya termasuk kedalam perbuatan ilegal. unsur objektif memfokuskan pada perbuatan "menyebarkan" dan akibat yang ditimbulkan berupa "kerugian konsumen dalam transaksi elektronik". Hal ini menunjukkan bahwa pasal ini secara spesifik ditujukan untuk melindungi konsumen dalam konteks ekonomi digital. Ketentuan pidana yang diatur dalam Pasal 45A ayat (1) memberikan sanksi yang cukup berat, yaitu pidana penjara maksimal 6 tahun dan/atau denda maksimal Rp 1 miliar sudah sesuai atas kejahatan siber yang dilakukan pelaku untuk menjerumuskan korban.

2. Pasal 30 ayat (2) menyebutkan bahwa "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik." Jo. Pasal 46 ayat (2) sebagai ketentuan pidananya bahwa "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah)."

   Adapun unsur-unsur dalam pasal 30 ayat (2) jo pasal 46 ayat (2):
   Pasal 30 ayat (2)
   a. Unsur subjektif:
      a) Dengan sengaja: menunjukkan adanya kesengajan/niat (dolus) mengakses computer dan system elektronik
      b) Secara melawan hukum: menunjukkan adanya perbuatan dilakukan yang bertentangan dengan hukum
   b. Unsur objektif:
      a) Mengakses komputer dan/atau system elektronik dengan cara apapun
      b) Untuk tujuan memperoleh informasi elektronik dan/atau dokumen elektronik[22]

[22] Hetty Hassanah, "*Tindakan Hukum terhadap pelaku Penyebaran Virus Komputer Melalui E-mail Berdasarkan ketentuan Tentang Informasi dan Transaksi Elektronik*", Res Nullis:Law Jurnal, Vol.5, No.1, Januari 2023.

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
http://ojournal.ulka-bogor.ac.id/Index.php/YUSTISI

Pasal 46 ayat (2)

a. Unsur subjektif:
   a) Dengan sengaja: menunjukkan adanya kesengajaan/niat (dolus)
   b) Tanpa hak tau melawan hukum: menunjukkan perbuatan dilakukan secara melawan hukum
b. Unsur objektif:
   a) Yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (2), merujuk pada perbuatan: mengakses komputer dan/atau system elektronik, dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik
   b) Ancaman pidana, pidana penjara maksimal 7 tahun dan/atau denda maksimal Rp 700.000 (tujuh ratus juta rupiah)

Penulis berpendapat bahwa unsur-unsur yang terdapat pada pasal 30 ayat (2) Jo pasal 46 ayat (2) UU ITE ini kejahatan tindak pidana dilakukan dalam bentuk kesengajaan, perbuatan tersebut dilakukan dengan kesadaran penuh dan bukan karena kelalaian. Pasal ini dibentuk untuk menangani berbagai bentuk peretasan (*hacking*) atau akses tidak sah ke sistem elektronik. Dalam unsur objektif pada kalimat "untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik" menjelaskan bahwa pasal ini fokus pada tindakan pencurian data atau informasi digital, bukan sekedar akses tidak sah ke sistem. Sanksi yang diancamkan berupa pidana penjara maksimal 7 tahun dan denda maksimal Rp 700 juta ini sudah sesuai dengan kejahatan siber yang dilakukan.

3. Pasal 32 ayat (2) menyebutkan bahwa “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak” Jo. Pasal 48 ayat (2) sebagai ketentuan pidananya bahwa“Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah).”

   Adapun unsur-unsur dari pasal 32 ayat (2) jo pasal 48 ayat (2) Pasal 32 ayat (2) Pasal 32 ayat (2)

   a. Unsur Subjektif:
      a) Dengan sengaja: menunjukkan adanya kesengajaan/niat (dolus) memindahkan atau mentransfer Informasi Elektronik dan/atau dokumen elektronik kepada sistem elektronik orang lain
      b) Tanpa hak atau melawan hukum: menunjukkan sifat melawan hukum dari perbuatan tersebut
   b. Unsur Objektif:
      a) Memindahkan atau mentransfer perbuatan yang dilarang
      b) Informasi Elektronik dan/atau Dokumen Elektronik: objek yang dipindahkan/ditransfer
      c) Kepada Sistem Elektronik Orang lain yang tidak berhak: tujuan/sasaran perbuatan
      d) Dengan cara apapun: cara melakukan perbuatan tersebut

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
http://ojournal.ulka-bogor.ac.id/Index.php/YUSTISI

Pasal 48 ayat (2):

a. Unsur Subjektif:
    a) Dengan sengaja: menunjukkan adanya kesengajaan/niat (dolus)
    b) Tanpa hak atau melawan hukum: menunjukkan sifat melawan hukum dari perbuatan tersebut
b. Unsur Objektif:
    a) Melakukan pemindahan atau transfer informasi elektronik dan/atau dokumen elektronik
    b) Kepada sistem elektronik orang lain yang tidak berhak: tindakan tersebut dilakukan terhadap sistem elektronik yang dimiliki oleh pihak lain, di mana pelaku tidak memiliki hak atau otoritas untuk mentransfer data ke dalamnya.
    c) Ancaman pidana, pidana penjara maksimal 9 tahun dan/atau denda maksimal Rp 3.000.000.000 (tiga miliar rupiah).

Penulis berpendapat bahwa unsur-unsur yang terdapat pada pasal 32 ayat (2) Jo pasal 48 ayat (2) UU ITE ini kejahatan tindak pidana dilakukan dalam bentuk kesengajaan, perbuatan tersebut dilakukan dengan kesadaran penuh dan bukan karena kelalaian. unsur objektif kedua pasal ini secara spesifik mengatur tindakan pemindahan atau transfer informasi elektronik kepada sistem elektronik milik orang lain yang tidak berhak, seperti pembajakan data, penyalinan ilegal yang dilakukan dalam kejahatan siber. Sanksi yang diancamkan berupa pidana penjara maksimal 9 tahun dan denda maksimal Rp 3 miliar ini sudah sesuai atas kejahatan yang dilakukan.

4. Pasal 35 menyebutkan bahwa “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” jo. Pasal 51 ayat (1) sebagai ketentuan pidananya bahwa “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 Rp12.000.000.000,00 (dua belas miliar rupiah).”

   Adapun unsur- unsur pasal 35 jo pasal 51 ayat (1):
   Pasal 35
   a. Unsur Subjektif:
       a) Dengan sengaja: menunjukkan adanya niat/kesengajaan (dolus) dalam melakukan perbuatan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau dokumen Elektronik
       b) Tanpa hak atau melawan hukum: menunjukkan perbuatan tersebut dilakukan secara illegal atau tidak sah
   b. Unsur Objektif:
       a) Perbuatan yang dilarang meliputi, manipulasi, penciptaan, perubahan, penghilangan, pengrusakan

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
http://ojournal.uika-bogor.ac.id/index.php/YUSTISI

b) Informasi Elektronik dan/atau Dokumen Elektronik: objek yang dimanipulasi
c) Dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik: menunjukkan tujuan khusus yaitu agar data palsu dianggap otentik

Pasal 51 ayat (1)
a. Unsur Subjektif:
   a) Dengan sengaja: menunjukkan adanya kesengajaan/niat (dolus)
   b) Tanpa hak atau melawan hukum: menunjukkan sifat melawan hukum dari perbuatan tersebut
b. Unsur Objektif:
   a) Melakukan manipulasi, penciptaan, perubahan, penghilangan, atau penghancuran informasi elektronik dan/atau dokumen elektronik
   b) Dianggap sebagai data otentik: tindakan pelaku bertujuan agar data hasil manipulasi, penciptaan, atau perubahan tersebut dianggap asli, valid, atau otentik.
   c) Ancaman pidana. pidana penjara maksimal 12 tahun dan/atau denda maksimal Rp 12.000.000.000 (dua belas miliar rupiah)

Penulis berpendapat bahwa unsur-unsur yang terdapat pada pasal 35 Jo pasal 51 ayat (1) UU ITE ini kejahtan tindak pidana dilakukan dalam bentuk kesengajaan, perbuatan tersebut dilakukan dengan kesadaran penuh dan bukan karena kelalaian. Unsur objektif dari kedua pasal tersebut menggambarkan ruang lingkup perbuatan yang cukup luas mulai dari manipulasi hingga pengrusakan. Penekanan pada tujuan agar informasi atau dokumen elektronik "dianggap seolah-olah data yang otentik" menunjukkan bahwa pasal ini secara khusus ditujukan untuk mencegah dan menindak pemalsuan data digital. Sanksi pidana yang diancamkan yaitu pidana penjara maksimal 12 tahun dan denda maksimal Rp 12 miliar menunjukkan bahwa pembentuk undang-undang memandang kejahatan ini sebagai pelanggaran serius. Besaran sanksi ini mencerminkan upaya untuk memberikan efek jera sekaligus menanggulangi potensi kerugian material yang dapat ditimbulkan dari manipulasi data elektronik.

c) Undang-Undang Negara Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, namun ada perubahan dalam pasal 28 ayat 1 dan pasal 45 A ayat (1) yang menyebutkan bahwa:
   1. Pasal 28 ayat (1) menyebutkan bahwa “Setiap orang dengan sengaja mendistribusikan dan atau mentransmisikan informasi elektronik dan/atau dokumen elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan yang mengakibatkan kerugian material bagi konsumen dalam transaksi elektronik.”
      a. Unsur subjektif:
         Dengan sengaja: Pelaku melakukan tindakan tersebut dengan niat atau kesengajaan, bukan tanpa sengaja atau karena kelalaian. Ini menunjukkan

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
http://ejournal.ulka-bogor.ac.id/Index.php/YUSTISI

bahwa pelaku memiliki kesadaran penuh terhadap dampak dari informasi yang disebarkan atau ditransmisikan

b. Unsur objektif
   a) Mendistribusikan dan/atau mentransmisikan informasi elektronik dan/atau dokumen elektronik: Tindakan mendistribusikan atau mentransmisikan informasi atau dokumen secara elektronik, baik melalui email, media sosial, atau platform lainnya.
   b) Yang berisi pemberitahuan bohong atau informasi menyesatkan: Informasi atau pemberitahuan yang tidak benar (bohong) atau yang dapat membingungkan dan menyesatkan penerima informasi.
   c) Yang mengakibatkan kerugian material bagi konsumen dalam transaksi elektronik: Informasi yang salah atau menyesatkan tersebut menyebabkan kerugian nyata (material) bagi konsumen dalam transaksi elektronik, seperti kehilangan uang, data pribadi, atau aset lainnya.

2. Pasal 45 A ayat (1) menyebutkan bahwa "Setiap Orang yang dengan sengaja mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan yang mengakibatkan kerugian materiel bagi konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
   a. Unsur subjektif:
      a) Dengan sengaja: Pelaku melakukan tindakan tersebut dengan niat atau kesengajaan. Ini berarti bahwa pelaku memiliki tujuan tertentu dalam mendistribusikan informasi bohong atau menyesatkan, mengetahui dengan jelas bahwa tindakan tersebut dapat merugikan orang lain.
   b. Unsur objektif
      a) Mendistribusikan dan/atau mentransmisikan informasi elektronik dan/atau dokumen elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan: Sama seperti dalam Pasal 28 ayat (1), yang mencakup tindakan mendistribusikan atau mentransmisikan informasi palsu atau menyesatkan.
      b) Yang mengakibatkan kerugian materiil bagi konsumen dalam transaksi elektronik: Tindakan tersebut harus mengakibatkan kerugian nyata bagi konsumen, seperti kehilangan uang, barang, atau data pribadi yang dapat merugikan konsumen secara finansial.
      c) Ancaman pidana, pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1.000.000.000,00: Pasal ini menetapkan sanksi yang cukup berat, yakni penjara dengan durasi maksimal enam tahun atau denda yang dapat mencapai satu miliar rupiah sebagai bentuk hukuman bagi pelaku. Sanksi ini menunjukkan betapa seriusnya dampak dari tindakan penyebaran informasi bohong atau menyesatkan yang dapat merugikan konsumen.

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
http://ejournal.uika-bogor.ac.id/index.php/YUSTISI

Penulis berpendapat bahwa dalam pasal 28 ayat (1) Jo pasal 45 A ayat (1) Undang-undang Nomor 19 Tahun 2016 dengan Perubahan Undang-undang Nomor 1 Tahun 2024 tidak ditemukan perbedaan, masih memiliki makna atau tujuan yang sama yaitu mengatur larangan penyebaran berita bohong dan menyesatkan yang mengakibatkan kerugian bagi konsumen dalam transaksi elektronik. Hanya saja perubahan dalam Undang-undang Nomor 1 Tahun 2024 ini memperjelas kriteria kerugian konsumen dalam konteks transaksi elektronik. Dengan melakukan penambahan kalimat seperti halnya mendistribusikan dan atau mentransmisikan informasi elektronik dan/atau dokumen elektronik.

PENUTUP

Tindak pidana penipuan phishing berbasis web merupakan kejahatan siber yang dilakukan dengan menciptakan situs web palsu yang menyerupai situs resmi untuk mencuri data sensitif pengguna. Karakteristik utama dari serangan phishing meliputi penggunaan alamat email atau URL mencurigakan, permintaan informasi sensitif secara mendesak, penggunaan bahasa yang buruk, serta tautan mencurigakan. Untuk membuktikan kasus phishing, diperlukan bukti digital berupa situs web palsu, rekaman transaksi elektronik, data korban yang dicuri, dan bukti kerugian materiil. Pengaturan hukum terhadap tindak pidana phishing di Indonesia diatur dalam beberapa instrumen hukum. Meskipun tidak secara khusus diatur dalam KUHP, tindakan ini dapat dijerat dengan Pasal 378 KUHP tentang penipuan. Selain itu, UU ITE No. 19 Tahun 2016 perubahan atas Undang-undang Nomor 11 tahun 2008 maupun perubahannya dalam UU Nomor 1 Tahun 2024 mengatur secara lebih spesifik tentang kejahatan tindak pidana penipuan phising ini.

DAFTAR PUSTAKA

Buku

1. Andi Asari, "*Pengembangan Website*", (Malang:Media Nusa Creative,2023).
2. Aswan, "*Tindak Pidana Penipuan Berbasis Elektronik*" (Makasar:GuePedia,2019)
3. Devie Rahmawati, "*Waspada Kejahatan Phising Attack*" (Malang:PT. Literasi Nusantara Abadi Grup,2024)
4. I Made Wartana, "*Mengenal Teknologi Informasi*", Cet 1 (Malang:Media Nusa Kreatif,2017
5. Ismail, "*Bahaya Phising*", (Tempo publishing,2024)
6. Muh. Akbar Fhad Syahril, "*Hukum Informasi dan Transaksi Elektonik*" (Jawa Tengah:CV.Eureka Media Aksara, 2023)
7. Muhammad Aenur Rosyid, "*Hukum Pidana*", (Jember,2020)
8. Muhammad Rizal Supriadi, "Deteksi Halaman Website Phising" (Bandung:Buku Pedia,2023)
9. Muhammad Sadi, "*Aspek Hukum Informasi Di Indonesia*", Cet.1 (Jakarta:Kencana,2021)
10. Sahat Maruli T.Situmeang, "*Cyber Law*", Cet.1 (Bandung:Penerbit Cakra,2020)

Peraturan Perundang-Undangan

11. Kitab Undang-Undang Hukum Pidana (KUHP)
12. Undang undang No.19 Tahun 2016 Perubahan Atas Undang-undang No 11 Tahun 2008 Tentang ITE
13. Undang undang No.1 Tahun 2024 Perubahan kedua Atas Undang-undang No 11 Tahun 2008 Tentang ITE

Jurnal

14. Ananda Dias Sulistyo, "*Strategi Penanggulangan Serangan Phishing di Media Sosial*", Seminar Nasional Teknologi Informasi dan Bisnis (SENATIB) 2024.
15. Andri Winjaya Laksana, "*Pemidanaan Cybercrime Dalam Perspektif Hukum Pidana Positif,"* Jurnal Hukum Unissula 35, No. 1, 2019.
16. Devi Puspitasari, "*Analisis Kejahatan Phising Pada Sektor E-Commerce*", Jurnal Digital Teknologi Informasi, Vol. 06, No. 02, September 2023.
17. Hetty Hassanah, "*Tindakan Hukum Terhadap Pelaku Penyebaran Virus Komputer Melalui E-mail (Cyber Spamming) Berdasarkan Ketentuan Tentang Informasi dan Transaksi Elektronik*", Res Nullis:Law Jurnal, Vol. 5 No. 1 Januari 2023.
18. Irma Yunita, "*Pengaruh Kemajuan Teknologi Terhadap perkembangan Tindak Pidana Cyber Crime"*", Jurnal Hukum Legalitas, Vol.5, No.2, Desember 2023.
19. Mia Haryati Wibowo, "*Ancaman Phising Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime".* JOEICT(Jurnal Of Education and Information Communication Technology), Vol. 1, No.1, 2017.
20. Purnamasari, "*Analisis kejahatan online phising pada institusi pemerintah/pendidik sehari-hari*", Jurnal Digital Teknologi Informasi, Vol. 06, No. 01, Maret 2023.
21. Sabrina Tabrani, dkk, "*Kejahatan Phising Ditinjau Dari Perspektif Hukum dan Kejahatan Siber*" Jurnal Kajian Hukum dan Pendidikan Kewarganegaraan, Vol.3, No.1, Januari 2024.
22. Tony Yuri Rahmanto, "*Penegakan Hukum Terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik*", Jurnal Penelitian Hukum:DE JURE, Vol. 19 No. 1, Maret 2019.
23. Vikran Fasyadhiyaksa Putra Y, "*Modus Operandi Tindak Pidana Phising Menurut UU ITE*", Jurnal Jurist-Diction, Vol.4, No 6, 2021.

Website dan Lainnya

24. https://regional.Kompas.com

YUSTISI
JURNAL HUKUM & HUKUM ISLAM
P-ISSN: 1907-5251
E-ISSN: 2620-7915
http://ejournal.uika-bogor.ac.id/Index.php/YUSTISI

SURAT KETERANGAN
PENERIMAAN JURNAL YUSTISI FAKULTAS HUKUM
UNIVERSITAS IBN KHALDUN BOGOR

No. 183/YUSTISI-FH/2025

Pengelola Jurnal YUSTISI (Jurnal Hukum dan Hukum Islam) Fakultas Hukum Universitas Ibn Khaldun Bogor telah menerima dari :

Nama : **Tiara Dea Reza, Yenny Fitri Z**
Email : *tiaradearezaa@gmail.com*
Judul : **Pengaturan Sanksi Pidana Bagi Pelaku Penipuan Phising Berbasis Web**
Asal Instansi : **Universitas Muhammadiyah Sumatera Barat**

Menyatakan bahwa artikel tersebut akan diproses sesuai prosedur penulisan Jurnal YUSTISI (Jurnal Hukum dan Hukum Islam) Fakultas Hukum Universitas Ibn Khaldun Bogor Terakreditasi Sinta 5 yang diterbitkan pada bulan Oktober Tahun 2025 dengan Volume. 12 No. 3.

https://ejournal.uika-bogor.ac.id/index.php/YUSTISI/index

Demikian surat keterangan ini dibuat dan harap dipergunakan dengan sebaik-baiknya.

Bogor, 18 Februari 2025

YUSTISI FH UIKA

UNIVERSITAS MUHAMMADIYAH SUMATERA BARAT
FAKULTAS HUKUM
Kampus 3: Jln. By Pass Aur Kuning No.1 Bukittinggi

SURAT KEPUTUSAN

NOMOR:036/KEP/II.3.AU/F/2024

Tentang

PENUNJUKKAN DOSEN PEMBIMBING TUGAS AKHIR PENULISAN HUKUM (LEGAL MEMORANDUM, STUDI KASUS, DAN SKRIPSI) SEMESTER GENAP T.A. 2023/2024

Dekan Fakultas Hukum Universitas Muhammadiyah Sumatera Barat, setelah;

Membaca : Permohonan pengusulan penulisan Hukum Mahasiswa atas nama : **TIARA DEA REZA**
NIM : 21150036

Menimbang :
a. Bahwa Mahasiswa yang akan menyelesaikan studinya di Fakultas Hukum UM-Sumbar diharuskan untuk melakukan tugas akhir berupa penulisan hukum (Legal Memorandum, Studi Kasus, dan skripsi);
b. Bahwa mahasiswa yang tersebut diatas telah memenuhi syarat untuk melaksanakan penulisan Hukum sesuai dengan bidang yang diinginkan;
c. Bahwa untuk terarahnya penulisan hukum dimaksud, dirasa perlu untuk menunjuk dosen pembimbing dengan surat Keputusan Dekan;

Mengingat :
1. Undang-undang No.12 Tahun 2012 tentang Pendidikan Tinggi
2. Peraturan Pemerintah No. 4 Tahun 2014 tentang Penyelenggaraan Pendidikan Tinggi dan Pengelolaan Perguruan Tinggi.
3. Peraturan Presiden No. 8 Tahun 2012 tentang kerangka Kualifikasi Nasional Indonesia (KKNI).
4. Peraturan Mentri Riset, Teknologi, dan pendidikan Tinggi RI No.44 Tahun 2015 tentang standar Nasional Pendidikan Tinggi.
5. Peraturan Mentri Riset, Teknologi, dan pendidikan Tinggi RI No.32 Tahun 2016 tentang Akreditasi Program Studi dan Perguruan Tinggi.
6. Peraturan Mentri Riset, Teknologi, dan pendidikan Tinggi RI No.62 Tahun 2016 tentang sistem Penjamin Mutu Pendidikan Tinggi.
7. Peraturan Mentri Riset, Teknologi, dan pendidikan Tinggi RI No.100 Tahun 2016 tentang pendirian perubahan, pembubaran perguruan tinggi negeri, dan pendirian, perubahan, pencabutan, pencabutan izin perguruan tinggi swasta.
8. Peraturan Pimpinan Pusat Muhammadiyah No. 01/PRN/I.0/B/2012 tentang Majelis Pendidikan Tinggi.
9. Pedoman Pimpinan Pusat Muhammadiyah No. 02/PED/1.0/B/2012 tanggal 16 April 2012 tentang Perguruan Tinggi Muhammadiyah.
10 Ketentuan Majelis Pendidkan Tinggi Pimpinan Pusat Muhammadiyah No 178/KET/1.3/D/2012 tentang penjabaran pedoman Pimpinan Pusat Muhammadiyah No. 02.PED/1.0/B/ 2012 tentang Perguruan Tinggi Muhammadiyah.
11 Statuta Universitas Muhammadiyah Sumatera Barat Tahun 2020
12 SK Dekan No. 0059/KEP/II.3.AU/D/2015 tanggal 13 Februari 2015 tentang Kurikulum Fakultas Hukum UM-Sumbar .
13 SK Rektor No. 970/II.3.AU/2021 tanggal 20 April 2021 tentang penetapan berlakunya Kurikulum Program Studi Ilmu Hukum Fakultas Hukum UM Sumbar TA. 2020.
14 SK Rektor No. 1436/KEP/II/3.AU/F/2021 tanggal, 15 September 2021 tentang Penetapan berlakunya Kurikulum Program Studi Ilmu Hukum UM Sumbar Tahun 2021.
15 Kalender Akademik Universitas Muhammadiyah Sumatera Barat Tahun Akademik 2021/2022

MEMUTUSKAN

MENETAPKAN

Pertama : Menunjuk Saudara **"YENNY FITRI.Z,SH.MH"** sebagai Dosen Pembimbing I dalam Penulisan Hukum Mahasiswa :
Nama/NIM : **TIARA DEA REZA/ 21150036**
Judul Skripsi : **PENGATURAN TINDAK PIDANA BAGI PELAKU PENIPUAN PHISING BERBASIS WEB**

Kedua : Segala biaya yang ditimbulkan akibat daripelaksanaan bimbingan penulisan hukum ini dibebankan kepada anggaran Fakultas Hukum UM-Sumbar

Ketiga : Surat Keputusan ini berlaku sejak tanggal ditetapkan dan akan ditinjau kembali, apabila dikemudian hari terdapat kekeliruan dan kesalahan dalam penetapan ini.

DITETAPKAN DI : Bukittinggi
PADA TANGGAL : *15 Zulkaidah 1445 H*
18 Mei 2024 M

Ketua Prodi,

Mahlil Adriaman,SH. MH
NIDN. 1021018404

Tembusan:
1 *Dekan Fakultas Hukum sebagai laporan*
2.. *Kasubag Keuangan Fakultas Hukum*
3. *Mahasiswa/I Yang bersangkutan*
4. *PertinggL*

KARTU KENDALI DAN
BIMBINGAN SKRIPSI/ JURNAL MAHASISWA

NAMA : Tiara Dea Reza
NIM : 21150036
KOSENTRASI : *Hukum Pidana/Hukum Perdata/Hukum Tata Negara*
DOSEN PEMBIMBING : 1. Yenny Fitri. Z — Sebagai Pembimbing I
: 2. — Sebagai Pembimbing II

JUDUL SKRIPSI / JURNAL : Pengaturan Sanksi Pidana Bagi Pelaku Penipuan Phising Berbasis Web

Mulai Bimbingan : s/d

NO	Hari/Tanggal	Jam Bimbingan	Materi Bimbingan	Saran	Paraf Pmbb	Ket
1	Senin / 3 Juni	14.00				
2	Kamis/ 6 Juni	12.00		Perbaiki		
3	Senin / 10 Juni			Acc proposal.		
4	Jumat/ 17-01			Perbaikan.		
5	Minggu/25-01	10.00		Acc Draf		
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						

Bukittinggi, ...

Mahasiswa

.....

UNIVERSITAS DHARMA ANDALAS

JADWAL KEHADIRAN
SEMINAR PROPOSAL DAN UJIAN SKRIPSI / JURNAL

NO	Hari/ Tanggal	Nama Peserta/ NIM	Judul Skripsi / Jurnal	Paraf Ketua Penyelenggara
1	Rabu/ 24-4-2024	Zari (20150155)	Perbandingan hukum Islam dengan hukum positif terhadap pelaku main hakim sendiri yg menyebabkan kematian	
2	Rabu/ 24-4-2024	Olivia Novera (20150174)	Analisis Penegakan hukum terhadap penyalahgunaan teknologi artificial intelligence (AI) dalam penyebaran konten pornografi melalui akun media sosial	
3	Rabu/ 24-4-2024	Jemi Mardesa (20150218)	Aspek Kriminologis keterlibatan Perempuan dalam tindak pidana narkotika	
4	Rabu/ 24-4-2024	Dedi Afriadi (20150095)	Tindakan yg dapat dilakukan dalam rangka perlindungan konsumen terkait wanprestasi thd bagasi penumpang yang hilang oleh perusahaan penerbangan	
5	Rabu/ 24-4-2024	Rani dwi Putri (20150126)	Penciptaan thd sinematografi dalam film berdasarkan UU no 28 tahun 2014 tentang hak cipta	
6	Rabu/ 10/4/2024	Fitri Ramadhani Musnal (20150105)	Analisis Putusan Perkara pidana No 37/Pid.B/2022/PN PDP tentang kealpaan pemasangan arus listrik yg menyebabkan kematian	
7	Rabu/ 10/4/2024	Muhammad Fakhrul Hidayat (20150009)	perlindungan hukum thd pelaku penyadapan dilakukan oleh Provos pendidikan di rahim Reserse kepolisian resor kota bukittinggi	
8	Rabu/ 10/4/2024	Ulfa Mayanita (20150028)	Studi normatif kebijakan pidana narkotika : Tinjauan terhadap efektivitas dan keadilan sosial dalam peraturan hukum pidana narkotika di Indonesia	
9	Rabu/ 10/4/2024	Aldila Putri (20150051)	Penegakan hukum thd WNA yang melakukan pelanggaran keimigrasi an (Studi kasus Kantor Imigrasi kelas II non TPI Agam)	
10	Rabu/ 10/4/2024	Darmilis (1910002742 01221)	Kajian yuridis penyalahgunaan hukum tindak pidana pencurian data pribadi (phishing) di Indonesia	

Catatan : 5 menghadiri Seminar Proposal dan 5 menghadiri Ujian Komprehensif terbuka

Bukittinggi, ...
Mahasiswa

.....