PENINGKATAN DETEKSI TINDAK PIDANA PHISING MELALUI SERANGAN HOMOGRAP

Meirza Aulia Chairani*
Fakultas Hukum, Universitas Merdeka Madiun

Angga Pramodya Pradhan
Fakultas Hukum, Universitas Merdeka Madiun

Abstrak:

Urgensi penelitian ini untuk menanggulangi dan mendeteksi serangan homograp saat ini terjadi di Indonesia. Tujuan penelitian ini adalah untuk mengetahui dan mendeteksi pola tindak pidana serang an homograp. Untuk mengetahui pertanggungjawaban pidana bagi pelaku tindak pidana serangan ho mograp. Metode penelitian yang digunakan adalah penelitian yuridis normatif, yang menggunakan pen dekatan perundang-undangan dan pendekatan konseptual. Maka penelitian ini mencari pola deteksi pe nyerang serangan homograp mengelabui korban dengan menggunakan tulisan yang serupa dengan web aslinya untuk mengelabui korbanya dengan web palsu atau *Phising* untuk memasukan informasi atau data-data pribadi, bagi korban yang tidak teliti terhadap nama web dan link url web resmi dengan *Spoo fing* oleh pelaku tindak pidana homograph akan melakukan aksinya dengan membobol data pribadinya untuk masuk ke akses perbankan dan akses-akses yang bisa di bobol oleh pelaku tindak pidana homo grap. Sanksi pidana bagi pelaku homograp ini sementara di atur di dalam Pasal 35 UU ITE dan menda patkan sanksi paling lama 12 tahun denda 12 miliar rupiah terdapat dalam Pasal 51 UU ITE dan Pasal 378 KUHP lama dan Pasal 492 KUHP baru dengan tindak pidana penipuan. Pembuatan situs website dengan menyakan bentuk tulisan yang sama dengn website asli makan pelaku tindak pidana homograp ini dapat mengelabui korban dan dapat mudah di aksesnya data pribadi korban atau yang sering disebut dengan *web forgery* membuat web mirip dengan aslinya. Korban masukan user id dan paswordnya ma kan data akan tersimpan di data base di situs website tersebut dan pelaku dapat dengan muah meng gunakan data tersebut untuk kepentinganya. Bagi pelaku dengan mengakases data pribdai korban yang sudah masuk web palsu tersebut dapat dikenai Pasal 67 UU PDP karena secara melawan hukum menggunakan data pribadi orang lain tanpa izin.

Kata Kunci: Tindak Pidana Homograp; *Phishing*; *Spoofing*; *Web Forgery*; Sanksi Pidana.

Abstract

The urgency of this research is to overcome and detect homograph attacks that are currently rampant in Indonesia. The purpose of this research is to know and detect the pattern of homographed attack criminal offense. To determine the criminal liability for the perpetrators of homographed attack criminal offense. The research method used is normative juridical research, which uses a statutory ap proach and conceptual approach. So that this research looks for patterns of detection of homographed attack perpetrators to trick victims by using writing similar to the original web to trick victims with fa ke or phishing webs to enter information or personal data, for victims who are not careful about web names and official web url links that are spoofed by the perpetrators of homographed attack crimes, the perpetrators of homographed attack crimes will carry out their actions by breaking into the vic tim's personal data to enter banking access and accesses that can be broken into by the perpetrators of homographed attack crimes. Criminal sanctions for perpetrators of homograph crimes are temporarily

* Alamat korespondensi: meirza.aulia@unmer-madiun.ac.id

regulated in Article 35 of the ITE Law and get a maximum sanction of 12 years with a fine of 12 billion rupiah contained in Article 51 of the ITE Law and Article 378 of the old Criminal Code and Article 492 of the new Criminal Code with the crime of fraud. The creation of a website by requesting the same form of writing as the original website so that the perpetrator of this homograph crime can make the website look like the original website.

Keywords: Homographic Crime; Phishing; Spoofing; Web Forgery; Criminal Sanctions.

A. Latar Belakang Masalah

Dengan perkembangan teknologi yang semakin pesat, Revolusi Industri 4.0 sedang berlangsung, di mana robot mulai menggantikan manusia di tempat kerja. elain itu, karena semakin terhu bung secara digital, dunia semakin de kat. Namun, hal ini menimbulkan baha ya yang semakin meningkat. Hecker-he cker menggunakannya untuk melaku kan penipuan dan mencari pundi-pundi kekayaan. Dengan kemajuan teknologi, pelaku kriminal menggunakan media in ternet untuk mencari cara untuk menipu dengan antivirus yang tidak dapat died teksi. Ini adalah bentuk kejahatan untuk mengelabui pengguna.

Karena kejahatan digital semakin marak, masyarakat semakin bergantung pada teknologi untuk melakukan apa pu n dan berkomunikasi dengan siapa saja kapan saja. Semua tindakan yang meng gunakan sistem elektronik akan mengha silkan sejumlah besar data dan informa si yang disimpan di komputer, ponsel, dan berbagai jenis jaringan komputer la innya. Data pribadi kita rentan terhadap pencurian jika tidak memiliki perlindu ngan dan keamanan yang cukup.

Orang yang tidak bertanggung ja wab dapat menggunakan kebocoran da ta untuk memeras atau menyalahguna kan data pribadi korban. Mencari keun tungan semata membuat pelaku kejahat an lebih termotivasi untuk melakukan tindak pidana. Mulai dari kelas bawah hingga kelas kakap, banyak faktor yang dapat memengaruhi banyak serangan *cy ber* yang terjadi di seluruh dunia. Untuk mencegah kejahatan *cyber*, beberapa ne gara segera membuat undang - undang kejahatan digital. Ada beberapa kejaha tan digital yang perlu diketahui, seperti phising yang menggunakan kemiripann tulisan web, yang biasanya dikenal seba gai serangan homograph atau serangan homograp.

Pelaku kejahatan saat ini menggu nakan berbagai teknik untuk mengela bui korbannya, salah satunya adalah *Phi sing*, di mana mereka menggunakan ga mbar yang meyakinkan atau meraik kon ten dalam frame dari halaman aslinya. Jenis kejahatan dunia maya yang paling umum adalah *phising*, yang melibatkan pencurian informasi pribadi dan data sensitif orang lain dengan mengirim me reka pesan, email atau komukasi digital lainnya. Serangan ini menipu pengguna dengan menggunakan kemiripan karak ter alfabet yang berbeda untuk menga rahkan mereka ke situs web palsu.

Di Indonesia, penyalahgunaan tin dak pidana homograp masih belum ada. Konsep homograp mungkin relevan un tuk kejahatan siber di Indonesia, teruta ma dalam hal penipuan online seperti *phising* dan *spoofing*. Jenis penipuan ini dapat digunakan untuk menyamarkan identitas pelaku dengan membuat email atau domain yang sangat mirip dengan yang sebenarnya sehingga korban tidak

menyadari bahwa mereka sedang berin teraksi dengan penipu.

Seperti web forgery atau web phi sing, situs web yang dimaksudkan un tuk menipu penggunanya Tampilan a wal situs web dimodifikasi secara ber tahap. Korban kemudian diminta untuk mengisi formulir yang telah disiapkan pelaku untuk menunjukkan identitas nya. Data akan disimpan dalam databa se di situs web setelah korban memberi kan identitas pengguna dan password. Ini adalah data yang disimpan yang di incar pelaku untuk disalahgunakan un tuk kepentingannya sendiri.[1]

Pelaku phishing dapat mengguna kan homograp untuk membuat URL yang terlihat seperti situs resmi, tetapi memiliki arti yang berbeda. Misalnya, membuat alamat web yang terlihat sah dengan menggunakan karakter yang mi rip dengan alfabet yang berbeda, seperti huruf *Cyrillic*.

Homograph attack, juga dikenal sebagai serangan homograp, adalah mo dus kejahatan *cyber* yang harus diwaspa dai. Ini adalah metode penipuan di ma na penipu menggunakan kesamaan kara kter font untuk membuat dan mendaftar kan domain palsu yang sudah ada agar mampu menipu dan menarik pengguna untuk mengunjungi situs web mereka.[2] Sementara *Phising Homofraph*, juga di kenal sebagai *Homoglyph*, didasarkan pada penggunaan karakter yang mirip untuk menyamar sebagai situs lain. [3]

Istilah "homograp" sendiri berasal dari istilah inggris "*homograph*", yang mengacu pada bentuk ucapan yang sa ma tetapi makna dan ucapan yang ber beda.[4] *Homograph is a type of word play which has identical spelling but dif ferrent sounds. For example, the word close in English refers to change some thing from being open to not being open and refers to not far in position.* (Homo grap adalah contoh jenis kata yang me miliki ejaan yang sama tetapi bunyinya berbeda. Misalnya, kata *"close"* dalam bahasa Inggris mengacu pada posisi ya ng tidak jauh dan menggambarkan peru bahan dari terbuka menjadi tidak terbu ka). [5]

Pelaku melakukan kejahatan ho mograp dengan membuat dan menulis url web yang mirip dengan website as linya. Jika korban tidak memeriksa situs web dengan cermat, data pribadi korban akan digunakan pelaku untuk membuat akun perbankan dan akun lain yang da pat digunakan untuk kepentingan pela ku.[6]

---

[1] S.H. Erizka Permatasari, "Jerat Hukum Pelaku Phishing Dan Modusnya," Hukum onli ne.com, 2021, https://www.hukumonline.com /klinik/a/jerat-hukum-pelaku-iphishing-i-dan-modusnya-cl5050/.

[2] Justina Nur Landhiani, "Waspada! Ke tahui Apa Itu Modus Penipuan Homograph At tack Yang Semakin Merajalela," TrenAsia, 2023.

[3] admin, "Phishing Homograph Bisa Menyerang Saat Tidak Cukupnya Kesadaran Pe ngguna," bitdefenderindonesia, 2022, https:// bitdefenderindonesia.com/phishing-homograph/.

[4] Abdul Chaer, *Linguistik Umum* (Jakar ta: Rineka Cipta, 2012).

[5] Anindia Ayu Rahmawat, "Verbal Humor In The Rio Animated Film And Its Translation In The Indonesian Subtitling" (2013).

[6] DarkNews by AF Themes, "Mengulik Tipuan URL Trik Serangan Homograf," Pros Perita It News, 2024, https://news.pros perita.co.id/mengulik-tipuan-url-trik-serangan-homograf/.

Dalam Bahasa Indonesia, sera ngan homograp IDN adalah singkat an dari nama domain internasionalisasi a tau alamat domain internasional, yang digunakan oleh pihak yang tidak ber tanggung jawab untuk mengambil atau menerima data dari perangkat yang ber interaksi dengan sistem mereka. Tujuan utama phising homograph adalah untuk mendapatkan akses ilegal ke akun sese orang atau mencuri data identitas target atau korban. Pelaku dapat melakukan berbagai jenis penipuan, seperti pencuri an identitas, pencurian dan pencucian uang, atau serangan terhadap komputer dan sistem jaringan dengan informasi yang mereka peroleh. Korban dapat me ngalami kerugian yang sangat besar, se perti kehilangan uang, pencurian iden titas, atau kehilangan data pribadi. Kor ban yang tidak teliti tahu tentang phisi ng dan tahu apa yang mereka dapat laku kan untuk mencegahnya. Mereka dapat menghindari mengeklik tautan yang me ncurigakan, memastikan bahwa ema il dan pesan lain asli, dan menghindari me mberikan informasi sensitif melalui salu ran komunikasi yang tidak aman. Ru musan masalah berikut dapat dibuat ber dasarkan uraian diatas yaitu Pola detek si penyerang serangan homograp me ngelabui korban dengan menggunakan tulisan yang serupa dengan web aslinya untuk mengelabui korbanya dengan we b palsu untuk memasukan informasi at au data-data pribadi. Penerapan sanksi pidana bagi pelaku tindak pidana sera ngan *homograph*.

B. Metode Penelitian

Metode penulisan untuk penulisan ini menggunakan penelitian yuridis nor matif (*Legal research*). Penelitian hu kum (*Legal research*) adalah menemu kan kebenaran koherensi, yaitu ada kah aturan hukum sesuai norma hukum dan adakah norma yang berupa perintah ata u larangan itu sesuai dengan prinsip hu kum, serta tindakan (*Act*) sesorang sesu ai dengan *norma hukum* (bukan sesuai aturan hukum) atau *Prinsip hukum.*[7] Pendekatan masalah dalam penelitian ini menggunakan pendekatan Perunda ng - undangan (*Statute Approach)* dan Pendekatan Konseptual (*conceptualap pro ach).* Bahan hukum primer merupa kan bahan hukum yang bersifat auto ritatif, artinya mempunyai otoritas. Ba han hukum primer terdiri dari perun dang-undangan, catatan-catatan resmi a tau risa lah dalam pembuatan undang-undang dan putusan-putusan hakim.[8] A dapun bahan hukum primer yang di gunakan dalam penelitian ini antara lain:

1. KUHP
2. Undang-undang (UU) Nomor 27 Thun 2022 tentang Pelindungan Da ta Pribadi
3. Undang-undang (UU) Nomor 1 Ta hun 2023 tentang Kitab Undang-Undang Hukum Pidana
4. Undang-undang (UU) Nomor 1 Tahun 2024 tentang Perubahan Ke dua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

[7] Peter Mahmud Marzuki, *Penelitian Hukum (Edisi Revisi)*, edisi revisi 2 (Jakarta: PT. Adhitya Andrebina Agung, 2015).

[8] Peter Mahmud Marzuki.

C. Penelitian dan Pembahasan

1. Pola deteksi penyerang serangan homograp mengelabui korban de ngan menggunakan tulisan yang serupa dengan web aslinya untuk mengelabui korbanya dengan we b palsu untuk memasuk kan in formasi atau data-data pri badi.

Pada tahun 2011, serangan homo grap ini dikenal karena stasiun televisi KBOI-TV memiliki domain homograph hic untuk membuat situs web berita pal su. digunakan untuk menyebarkan lelu con Hari April Mop tentang gubernur Id aho yang memutuskan untuk melarang penjualan musik Justin Bieber. Peneliti keamanan Ankit Anbv menemukan sera ngan Homograp IDN pada tahun 2017. Penyerang menggunakan domain adobe .com untuk mengirimkan virus Trojan Betabot.[9]

Serangan homograp sering menar getkan nama domain yang sah karena mereka menggunakan kesalahan penge nalan visual manusia sehingga penggu na tidak menyadari bahwa mereka me ngunjungi situs web yang berbeda. Se rangan ini menggunakan nama domain baru yang terlihat seperti nama domain yang sudah ada dan mengganti bebe rapa karakter dengan nama domain ya ng secara visual serupa.[10]

Penipu menggunakan serangan ho mograp untuk menipu korban dengan menggunakan nama doain yang sangat mirip dengan situs web yang sebenar nya. IDN mudah digunakan dan dapat digunakan oleh semua orang. Ini karena nama domain dapat diakses dalam ber bagai bahasa dengan mengkodekannya dalam format *Unicode*.[11] Untuk menge labui korban, pelaku menggunakan do main *spoofing* dengan homograph IDN yang salah.

Web penyerang, seperti *Web For gery* atau *Web Phising*, adalah situs web yang dimaksudkan untuk menipu peng gunanya. Tampilan awal situs web di modifikasi secara bertahap. Korban ke mudian diminta untuk mengisi formulir yang telah disiapkan pelaku untuk me nunjukkan identitasnya. Data akan di simpan dalam database di situs web se telah korban memberikan identitas pe ngguna dan password. Ini adalah data yang disimpan yang diincar pelaku un tuk disalah gunakan untuk kepentingan nya sendiri.

Berawal dengan pembuatan situs web palsu yang sengaja dirancang un tuk mengelabui korban. Situs ini dibuat dengan cara yang sangat mirip dengan situs resminya dan mengguna kan nama domain yang sangat mirip dengan yang asli.[12] Untuk membuat web palsu, pe

---

[9] Wikipedia, "Serangan Homograf IDN," Wikipedia, n.d., https://en.wikipedia.org/wiki /IDN_homograph_attack#Known_homograph_ attacks.

[10] Yuta Sawabe et al., "Detection Metho d of Homograph Internationalized Domain Na mes with OCR," *Journal of Information Pro cessing* 27 (2019): 536–44, https://doi.org/10. 2197/ipsjjip.27.536.

[11] Greg Baatard Tyson McElroy, Peter Hannay, "The 2017 Homograph Browser Attack Mitigation Survey," *The Proceedings of 15th Australian Information Security Management Conference*, 2017, https://doi.org /10.4225/75/5a84f5a495b4d.

[12] Berlyan Gumay, Ade Hendri Hendrawan, and Fitrah Satrya Fajar Kusumah, "Analisis Dampak Ancaman Cyber Crime Terhadap Data Mahasiswa Pada Serangan Web

nyerang biasanya membuat link yang hampir mirip dengan web aslinya. Ke mudian, penyerang akan melakukan pe nipuan dengan memperdaya korbannya untuk memberikan informasi pribadi nya.

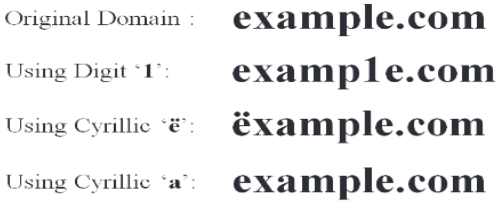
Menurut pemahaman Palmer, ho mograp sendiri berasal dari kata "ho mo", yang berarti "sama", dan "graf" yang berarti "tulisan". Menurut Palmer, homograp adalah kata yang memiliki bentuk atau ejaan yang sama tetapi me miliki bunyi atau pelafalan yang ber beda dan arti yang berbeda. [13]

Serangan homograp biasanya me nggunakan beberapa karakter yang mi rip dengan karakter asli. Sementara beberapa situs web HTTP yang tidak resmi dapat dengan mudah dibobol oleh para hacker, situs web asli yang me minta kredensial (seperti jaringan so sial, portal bank, dll.) menggunakan HTTPS. Situs web yang menggunakan HTTPS bukan berarti Hecker tidak da pat membobolnya, tetapi hanya mem butuhkan waktu untuk melakukannya. Dalam praktiknya, Hecker melakukan nya dengan mengambil keuntungan dari huruf alfabet yang berbeda tetapi sama.

Untuk ilustrasi, korban mengunju ngi situs web bank nasional. Tindak pi dana yang dilakukan oleh pelaku ini menggunakan karakter yang digunakan pada situs web asilnya, seperti menggan ti huruf "o" dengan "0", atau (nol).

Pelaku akan mendaftarkan doma in yang tampaknya mirip dengan situs web yang mereka ingin palsukan, men dapatkan sertifikat untuk mendapatkan domain baru, dan kemudian membuat domain baru dengan cara yang sama. Misalnya, facabook.com mirip dengan domain asli Facebook.com, atau rnerca dolibre.com mirip dengan domain asli mercadolibre.com.

Gambar 1. Contoh nama domain homograp



Berikut merupakan contoh bagai mana alamat domain asli website dan alamat domain palsu untuk mengelabui korban. Alamat domain yang menggu nakan *Cyrillic,* hanya merubah sedikit kata jika korban tidak teliti maka in formasi data pribadinya dapat di curi oleh penyerang.

Serangan phishing menggunakan kerentanan manusia untuk membedakan situs web asli dari palsu. Serangan *phi sing* web ini biasanya menggunakan ber bagai cara, seperti email, web palsu, SMS, dan telepon.

Kita tidak akan menyadari dengan cepat bahwa website tersebut merupa kan *web forgery* atau *web phising* yang menggunakan kata-kata yang mirip dengan website asli. Jika korban tidak

Phising SIAK UIKA," *Infotech Journal* 10, no. 2 (October 13, 2024): 297–305, https://doi.org/10.31949/ infotech.v10i2.11463.

[13] and Agita Misriani. Trisari, Tiara, Ifnaldi Ifnaldi, "Analisis Struktur Berita Dan Pemilihan Diksi Dalam Artikel Berita Online CNN Indonesia (Ferdy Sambo)" (Diss. Institut Agama Islam Negeri Curup, 2023).

hati-hati, beberapa contoh di atas dapat menipu mereka.

Jika korban tidak memperhatikan dengan cermat dan memberikan data pribadi mereka, seperti username dan password, ke situs web palsu Pelaku dapat mencuri data pribadi dan infor masi korban untuk melakukan penipuan atau memberikan pinjaman online.

Jika seseorang membaca domain yang dibuat oleh penyerang berdasar kan penampilannya, mereka akan per caya bahwa domain tersebut sah. Na mun, mereka sebenarnya berada di do main palsu. Seperti yang dilakukan oleh beberapa website judi, mereka meng gunakan metode *spoofing* atau pemal susan untuk menipu *Internet Protocol Address* sehingga mereka tidak dapat dilacak oleh polisi.[14] Penyerang mem buat situs web baru dengan meniru situs web aslinya, biasanya dikombinasikan dengan email *phising* atau *spoofing* yang menarik. Korban akan terkecoh dan memberikan informasi sensitif se perti username, kata sandi, bahkan no mor kartu kredit.

Nama domain internasional homo grap (IDN) digunakan untuk mengganti kan karakter dalam nama domain asli. Penipu menggunakan Unicode dari sis tem penulisan non-latin seperti *Cyrillic* atau *Greek* untuk membuat URL atau nama domain identik dengan versi as linya. Dengan bantuan Punycode, sintak s pengkodean yang memungkinkan kara kter Unicode untuk diterjemahkan ke da lam sting karakter yang lebih terbatas yang kompatibel dengan URL, dan do main yang menggunakan karakter ini dapat didaftarkan, abjad ini mengandu ng karakter yang serupa atau bahkan identik dengan karakter yang kita gu nakan dalam alfabet latin dan di URL.

Penyerang menggunakan huruf Ba hasa non-Latin, seperti *Cyrillic*, untuk menggantikan karakter Latin dalam na ma domain Internasional (IDN). Meng gunakan karakter *Cyrillic a* (*Cyrillic Lo wercase a*) daripada "cek bawah bahasa Inggris a" adalah contohnya. Mereka a kan terlihat sama jika mereka tidak me miliki mata. Namun, komputer akan me ngetahui perbedaan dan mengarahkan pengguna ke situs web berbahaya bi asanya mirip dengan situs web yang mereka inginkan dari pada halaman web yang sah yang mereka inginkan.

Beberapa jenis serangan Homograp yang umum terjadi termasuk: [15]

1. Serangan Homograp IDN: Sera ngan ini menggunakan karakter non-Latin yang mirip dengan ka rakter Latin, seperti huruf *Cyrillic* "O" yang mirip dengan huruf Latin.
2. Serangan Homograp Visual: Se rangan ini menggunakan karakter yang terlihat mirip secara visual, te tapi berbeda secara kode, seperti huruf "l" (kecil) dan "I" (kapital).
3. Serangan homofon: Serangan ini menggunakan kata-kata yang seru pa tetapi ejaan mereka berbeda.

[14] R Muhammad Rayhan Rizky Pratama, "Analisis Yuridis Tindak Pidana Perjudian Online Slot Dan Toto Gelap Online Melalui Website," *Ethics and Law Journal: Business and Notary* 2, no. 1 (January 25, 2024): 224–30, https://doi.org/10.61292/eljbn.118.

[15] Alreza Deva Febriawati, "Serangan-Homograp-Bahaya-Tersembunyi-Di-Balik-Url-Mirip," memorandum, 2024, https://memorandum.disway.id/read/100149/serangan-Homograp-bahaya-tersembunyi-di-balik-url-mirip/15.

"there" dan *"their"* adalah contoh nya.

Bahasa *Cyrillic*, yang biasanya di gunakan dalam serangan homograp, da pat menjadi yang paling mudah disalah gunakan karena banyaknya karkater ya ng sangat mirip dengan huruf Latin. Ke tika serangan homograph menyerang ba nyak bahasa Eropa dan Asia, karakter yang terlihat seperti latin. *Cyrillic*, Yu nani, Armenia, Ibrani, dan Thailand adalah contohnya.

Gambar 2. Contoh karakter Cyrillic

Karakter Cyrillic	Cicipi IDN
l (ibu di i)	google[.]com
y (u kecil)	macys[.]com
e (kekecilan)	aplikasi[.]com
o (kecil o)	microsoft[.]com
p (smaller)	paypal[.]com
c (kecil)	chanel[.]com
x (kecekaru kecil)	foxnews[.]com
ь (tanda lembut huruf kecil)	ьbc[.]com
s (dze kecil)	adida (.)com
j (small je)	nj[.]com

Misalnya, browser menginterpre tasikan domain yang didaftar sebagai "xn--pple-43d.com" sebagai "apple.com ". Namun, karakter Cyrillic "a" (U+ 0430) digunakan daripada karakter ASCII "a" (U+0041). Meskipun kedua karakter mata telanjang terlihat sama, dua karakter ini berbeda untuk browser dan sertifikat keamanan karena me wakili domain yang berbeda. Contoh lain adalah domain "tωitter.com", yang dikodekan menjadi xn--titter-i2e.com di Punycode, dan "gmạil.com", yang diko dekan menjadi xn--gmil-6q5a.com. De ngan menggunakan konverter Unicode ke Punycode, Anda bahkan dapat me nikmati membuat kombinasi unik.

Banyak browser saat ini me nawarkan sistem yang dapat mencegah serangan homograp. Jika sebuah do main mengandung karakter dari sistem penulisan yang berbeda, Firefox dan Chrome menampilkan Punycode yang sesuai daripada Unicode.

Pengguna disarankan untuk meng hindari serangan homograp dengan me meriksa pengirim pesan, memeriksa tau tan ke halaman yang ingin dikunjungi, dan yang paling penting, memastikan bahwa semua tertulis dengan benar dan aman (seperti menggunakan HTTPS) dan memiliki sertifikat keamanan.

Tindakan pencegahan ini, bagai manapun, tidak cukup lagi karena pen jahat dunia maya menggunakan metode yang semakin kompleks untuk menge labui pengguna. Menggunakan HTTPS dan sertifikat bukan lagi masalah bagi peretas. Lagi pula, apa peduli mereka tentang apakah data dienkripsi jika me reka mencuri kredensial.

Intinya, metode ini digunakan un tuk memberi pengguna ilusi keamanan, membuat mereka memasukkan data mereka dengan asumsi bahwa situs ter sebut aman. Mereka kemudian menya rankan pengguna untuk mengikuti reko mendasi berulang-ulang yang menya takan bahwa situs memiliki gembok kecil yang menunjukkan HTTPS, tetapi ini tidak cukup lagi. Mereka juga menyarankan pengguna untuk memper hatikan dengan cermat sertifikat kea manan, menghindari tautan email ke si tus web lebih baik menggunakan tautan langsung atau URL yang dapat diper caya dan menambahkan lapisan per lindungan tambahan ke akun dengan menggunakan dua faktor otentikasi.

2. Penerapan Saksi Pidana bagi Pelaku Tindak Pidana Serangan Homograp.

Serangan homograp melibatkan penyerang yang mengelabui korban de ngan menggunakan tulisan yang serupa dengan situs web aslinya. Jenis sera ngan ini biasanya *menggunakan web forgery* atau *phishing* untuk mengelabui korban dengan memasukkan informasi atau data pribadi. Korban yang tidak berhati-hati dapat menemukan pelaku tindak pidana homograp membobol na ma web dan url web resmi untuk mem bobol data pribadinya untuk menda patkan akses ke perbankan dan sumber daya lainnya.

Serangan homograp mencakup tin dakan seperti *phising* dan *spoofing* yang menggunakan nama domain yang mirip dengan domain asli untuk mencuri data sensitif. Dalam hukum pidana Indone sia, serarangna homograph dapat diguna kan untuk beberapa konsekuensi pida na.

Pasal 35 UU ITE mengatur sanksi bagi pelaku penyerang homograp ini, se mentara Pasal 51 UU ITE mengatur sanksi denda sebesar 12 miliar rupiah dan Pasal 378 KUHP lama dan Pasal 492 KUHP baru untuk tindak pidana penipuan. Serangan homograp sering menggunakan nama domain palsu un tuk mengelabui korban, yang meru pakan penipuan.

Untuk membuat korban mudah mempercayai bahwa situs web tersebut adalah aslinya, penyerang sangat hati-hati membuat situs web palsu dengan nama domain yang menggunakan karak ter *Cyrillic* atau *Greek*. Selain itu, *phi sing* juga melibatkan mendorong kor ban untuk memberikan data pribadi me reka. Dalam hal ini, memenuhi unsur-unsur yang tercantum dalam Pasal 378 KUHP lama dan 492 KUHP baru.

Salah satu unsur dalam Pasal 378 KUHP adalah penipuan dengan tujuan mendapatkan keuntungan. Namun, Pa sal 378 KUHP tidak tepat untuk men cakup unsur-unsur yang berkaitan de ngan informasi elektronik dan/atau do kumen elektronik, seperti yang tercan tum dalam Pasal 35 jo 51 UU ITE, yang dapat digunakan untuk menentukan san ksi yang dikenakan kepada pelaku pe nyerang homograp. Penyerangan me manfaatkan situs web palsu untuk me perdaya korban. Tujuannya ialah mem buat pengguna percaya bahwa situs web berisi informasi yang dapat dipercaya. Teknik manipulasi elektronik diguna kan penyerang untuk mencuri data atau informasi pribadi korban. Pencurian secara fisik atau pencurian secara fisik berbeda dengan tindak pidana konven sional. Transaksi elektronik adalah jenis kejahatan *cyber* atau kejahatan dunia maya yang diatur dalam Undang-un dang ITE. [16]

Pelaku tindak pidana homograp dapat mengelabui korban dan mempe roleh akses mudah ke data pribadi kor ban dengan membuat situs web dengan bentuk tulisan yang sama dengan situs web aslinya, yang dikenal sebagai *web forgery*. Data yang dimasukkan korban, yaitu identitas pengguna dan pasword, akan disimpan di database di situs web tersebut. Dengan demikian, pelaku da

[16] Asmak Ul Aura Nasha Ramadhanti1, Tessa Ayuning Tias2, Erin Dwi Lestari3 and Hosnah, "Cara Operasi Kejahatan Phising Di Ranah Siber Yang Diatur Oleh Hukum Positif Indonesia," *Jurnal Pendidikan Tambusai* 8, no. 1 (2024): 1299–1305, https://doi.org/https://doi.org/10.31004/jptam.v8i1.12549.

pat dengan mudah menggunakan data tersebut untuk kepentingannya.

Pasal 67 UU PDP melarang me nggunakan data pribadi orang lain tanpa izin. Menggunakan data pribadi orang lain dengan sengaja untuk keuntungan diri sendiri atau pihak lain yang menga kibatkan kerugian bagi subjek data pri badi. Pencurian data pribadi dapat me ngakibatkan hukuman penjara lima tahun dan denda maksimal Rp.5.000.000 .000 (lima miliar rupiah). Pelaku juga dapat dikenakan pidana tambahan se perti perampasan keuntungan atau harta yang didapat dari tinak pidana dan kewajiban untuk mengganti kerugian.[17]

Perlindungan preventif dan re presif dapat digunakan untuk melin dungi subjek hukum. Untuk mencegah pelanggaran dan memberikan kepastian hukum kepada pelaku dan korban, perlindungan preventif digunakan. Per lindungan hukum reperesif mencakup sanksi seperti denda, hukuman penjara, sanksi sosial, dan hukuman tambahan sebagai bentuk represif terhadap pela nggaran yang dilakukan oleh individu yang melakukannya. Bagi pelaku penye rangan serangan homograph dapat diper tanggungjawabkan dengan beberapa peraturan perundang-undangan yang be rlaku seperti UU ITE, UU PDP, KUHP.

D. Penutup

Pola deteksi penyerang serangan homograp mengelabui korban dengan menggunakan tulisan yang serupa de ngan web aslinya untuk mengelabui kor banya dengan web palsu atau *Web For gery* atau *Web Phising* untuk mema sukan informasi atau data-data pribadi. Penggunaan situs web palsu yang di buat oleh penyerang dengan membuat seperti web aslinya dengan membuat nama domain dengan menggunakan ka rakter *Cyrillic* atau *Greek* dengan me nggunakan karakter yang mirip dengan alfabet yang sering kita gunakan penye rang membuat semirip mungkin dengan alafabet web aslinya. Jika korban tidak perhatian terhadap web palsu tersebut akan memasukan id user, password, id identitas, nomor kartu kredit, informasi sensitif lainya milik korban. Hal ini akan di manfaatkan penyerang untuk membobol keuangan korban dan data-data lainya untuk disalahgunakan pela ku untuk kepentingan penyerang.

Tindak pidana serangan homo graph ini Sanksi pidana bagi pelaku ho mograp ini sementara di atur di dalam Pasal 35 UU ITE dan mendapatkan san ksi paling lama 12 tahun denda 12 mi liar rupiah terdapat dalam Pasal 51 UU ITE dan Pasal 378 KUHP lama dan Pasal 492 KUHP baru dengan tindak pi dana penipuan. Pembuatan situs websi te dengan menyakan bentuk tulisan ya ng sama dengn website asli makan pe laku tindak pidana homograp ini dapat mengelabui korban dan dapat mudah di aksesnya data pribadi korban atau yang sering disebut dengan *web forgery* membuat web mirip dengan aslinya. Korban masukan user id dan paswor dnya makan data akan tersimpan di data base di situs website tersebut dan pe laku dapat dengan muah menggunakan data

[17] Firmansyah3 Nur Alfiana Alfitri1*, Rahmawati2, "Perlindungan Terhadap Data Pribadi Di Era DigitalBerdasarkan Undang-Undang Nomor 27 Tahun 2022," *Journal Social Society* 4, no. 2 (2024): 92–111, https://doi.org /https://doi.org/10.30605/jss.4.2.2024.511.

tersebut untuk kepentinganya. Bagi pelaku dengan mengakases data pribdai korban yang sudah masuk web palsu tersebut dapat dikenai Pasal 67 UU PDP karena secara melawan hukum me nggunakan data pribadi orang lain tanpa izin.

Adapun saran yang diberikan ada lah masyarakat agar lebih berhati-hati dalam melihat tautan atau website yang akan di kunjungi atau diklik tautan terse but. Perlu ketelitian sebelum mengklik tautan yang tidak jelas dengan membu ka melalui website melalui google deng an menuliskan alamat domain website aslinya untuk mengecek keaslian web site yang dituju. Bagi pelaku tindak pi dana serangan homograp untuk semen tara ini dapat dikenakan sanksi UU ITE, UU PDP agar pelaku dapat dikenakan sanksi terlebih dahulu untuk pencegah an agar pelaku-pelaku yang lain tidak mengikuti tindak pidana serangan homo grap ini dan mendapatkan kepastian hu kum.

Daftar Pustaka

admin. “Phishing Homograph Bisa Men yerang Saat Tidak Cukupnya Kesa daran Pengguna.” bitdefenderindo nesia, 2022. https://bitdefenderin donesia.com/phishing-homograph/ .

Aura Nasha Ramadhanti1, Tessa Ayu ning Tias2, Erin Dwi Lestari3, As mak Ul, and Hosnah. “Cara Opera si Kejahatan Phising Di Ranah Siber Yang Diatur Oleh Hukum Po sitif Indonesia.” *Jurnal Pendidikan Tambusai* 8, no. 1 (2024): 1299–1305. https://doi.org/https://doi.org/10.31004/jptam.v8i1.12549.

Chaer, Abdul. *Linguistik Umum*. Jakarta: Rineka Cipta, 2012.

Erizka Permatasari, S.H. “Jerat Hukum Pelaku Phishing Dan Modusnya.” Hukumonline.com, 2021. https://www.hukumonline.com/klinik/a/jerat-hukum-pelaku-iphishing-i-dan-modusnya-cl5050/.

Febriawati, Alreza Deva. “Serangan-Ho mograp-Bahaya-Tersembunyi-Di-Balik-Url-Mirip.” memorandum, 2024. https://memorandum.disway.id/read/100149/serangan-Homograp-bahaya-tersembunyi-di-balik-url-mirip/15.

Gumay, Berlyan, Ade Hendri Hendra wan, and Fitrah Satrya Fajar Ku sumah. “Analisis Dampak Anca man *Cybercrime* Terhadap Data Mahasiswa Pada Serangan Web Phising SIAK UIKA.” *Info tech Journal* 10, no. 2 (October 13, 2024): 297–305. https://doi.org/10.31949/infotech.v10i2.11463.

Justina Nur Landhiani. “Waspada! Ke tahui Apa Itu Modus Penipuan Ho mograph Attack Yang Semakin Merajalela.” TrenAsia, 2023.

Nur Alfiana Alfitri1*, Rahmawati2, Firmansyah3. “Perlindungan Terha dap Data Pribadi Di Era Digi tal Berdasarkan Undang - Undang No mor 27 Tahun 2022.” *Journal So cial Society* 4, no. 2 (2024): 92–111. https://doi.org/https://doi.org/10.30605/jss.4.2.2024.511.

Peter Mahmud Marzuki. *Penelitian Hu kum (Edisi Revisi)*. Edisi revisi 2. Jakarta: PT. Adhitya Andrebina Agung, 2015.

R Muhammad Rayhan Rizky Pratama. “Analisis Yuridis Tindak Pidana

Perjudian Online Slot Dan Toto Gelap Online Melalui Website." *Ethics and Law Journal: Business and Notary* 2, no. 1 (January 25, 2024): 224–30. https://doi.org/10.61292/eljbn.118.

Rahmawat, Anindia Ayu. "Verbal Humor In The Rio Anima Ted Film And Its Translation In The Indonesian Subtitling," 2013.

Sawabe, Yuta, Daiki Chiba, Mitsuaki A kiyama, and Shigeki Goto. "Detec tion Method of Homograph Internationalized Domain Names with OCR." *Journal of Informa tion Processing* 27 (2019): 536–44. https://doi.org/10.2197/ipsjjip.27.536.

Themes, DarkNews by AF. "Mengulik Tipuan URL Trik Serangan Homo graf." *Prosperita It News*, 2024. https://news.prosperita.co.id/mengulik-tipuan-url-trik-serangan-homograf/.

Trisari, Tiara, Ifnaldi Ifnaldi, and Agita Misriani. "Analisis Struktur Berita Dan Pemilihan Diksi Dalam Arti kel Berita Online CNN Indonesia (Ferdy Sambo)." Diss. Institut Agama Islam Negeri Curup, 2023.

Tyson McElroy, Peter Hannay, Greg Baatard. "The 2017 Homograph Browser Attack Mitigation Sur vey." *The Proceedings of 15th Aus tralian Information Security Mana gement Conference*, 2017. https://doi.org/10.4225/75/5a84f5a495b4d.

Wikipedia. "Serangan Homograf IDN." Wikipedia, n.d. https://en.wikipedia.org/wiki/IDN_homograph_attack#Known_homograph_attacks.