TINJAUAN YURIDIS TERHADAP PERLINDUNGAN DATA PRIBADI DALAM MENGATASI *CYBERCRIME* PADA KASUS *PHISHING* [1]

Oleh :
Aprilia Violita Maramis [2]
Marthin Doodoh [3]
Marthin L. Lambonan[4]

ABSTRAK

Penelitian ini bertujuan untuk mengetahui pengaturan hukum mengenai perlindungan data pribadi dan untuk mengetahui langkah-langkah/strategi pemerintah dalam mengatasi tindak pidana *phishing*. Metode yang digunakan adalah penelitian normatif, dengna kesimpulan yaitu: 1. Pengaturan Hukum mengenai Perlindungan Data Pribadi diatur dalam Undang-Undang Nomor 27 Tahun 2022, yang bertujuan melindungi data pribadi masyarakat di era digital. Undang-Undang ini mencakup berbagai aspek pelindungan data pribadi, yang dimana Data Pribadi didefinisikan sebagai data tentang orang yang dapat diidentifikasi secara langsung maupun tidak langsung. Peraturan ini juga mencakup ketentuan tentang sanksi administratif, larangan penggunaan data pribadi, serta ketentuan pidana. 2. Pemerintah Indonesia telah membentuk lembaga-lembaga yang akan menangani kasus *phishing* dengan menerapkan sejumlah strategi sesuai dengan prosedurnya sendiri, Lembaga tersebut antara lain: BSSN dimulai dari persiapan, identifikasi, pengendalian, pemberantasan, pemulihan, dan Tindak lanjut. Dittipidsiber dan KOMDIGI dimulai dengan pelaporan kasus, penyelidikan, pemblokiran akses konten, kerja sama antar institusi, Tindakan penegakan hukum, dan edukasi masyarakat.

Kata Kunci : *perlindungan data pribadi, cyber crime, phising*

PENDAHULUAN

A. Latar Belakang

Seiring dengan kemajuan zaman dan teknologi yang terus berkembang, kejahatan siber (*cybercrime)* juga telah mengalami pertumbuhan, menciptakan berbagai bentuk kejahatan baru dengan metode-metode inovatif. *Cybercrime* pada dasarnya adalah Kejahatan Siber yang tindak kejahatannya menggunakan teknologi komputer dan jaringan internet untuk melakukan peretasan, pencurian, penipuan, penyebaran virus, dan tindak kriminal digital lainnya. Bentuk-bentuk kejahatan

siber *(cybercrime)* terus mengalami perkembangan dan tidak hanya terbatas pada aktivitas *hacking, cracking,* atau *carding*. Melainkan, juga melibatkan berbagai macam kejahatan yang lebih spesifik seperti Konten Tidak Sah *(Illegal Contents)*, Pemalsuan Data *(Data Forgery)*, Mata-mata *(Cyber Spionase)*, Mencuri *Data (Data Theft)*, Menyalahgunakan Peralatan Komputer *(Misuse of devices)*, *Hijacking, Cyber Terorism,* Akses Tanpa Ijin ke Sistem Komputer *(llegal Access)* dan *Cyber Phishing* (pencurian data pribadi antara lain berawal dari penipuan berupa link/situs website).[5] Perkembangan terus-menerus dalam teknologi menyebabkan serangan *cyber* menjadi semakin rumit dan sulit terdeteksi. Di Indonesia, kejahatan siber juga merupakan isu yang signifikan. Penting untuk terus memperbarui sistem keamanan dan meningkatkan kesadaran pengguna internet akan ancaman *cybercrime.* Kerja sama lintas negara juga penting dalam memberantas kejahatan siber yang sering melibatkan pelaku yang berasal dari berbagai negara. Penanganan kejahatan siber yang semakin kompleks membutuhkan kerja sama dari berbagai pihak. Dalam era internet yang semakin berkembang, penting bagi individu, perusahaan, dan pemerintah untuk mengambil tindakan yang serius untuk melindungi diri dari ancaman *cybercrime* dan bekerjasama untuk menciptakan lingkungan online yang lebih aman.[6]

Seiring dengan kemajuan teknologi, ketergantungan masyarakat dan organisasi terhadap internet dan sistem informasi telah meningkat. Kondisi ini menciptakan peluang baru bagi para pelaku kejahatan untuk mengeksploitasi kerentanan dalam sistem digital. Dalam era digital yang semakin maju, perhatian terhadap perlindungan data pribadi menjadi semakin penting. Semakin banyak data pribadi yang dikumpulkan dan diproses oleh berbagai entitas, termasuk perusahaan, pemerintah, dan organisasi lainnya. Namun, bersamaan dengan kemajuan teknologi juga muncul ancaman baru dalam bentuk

---

[1] Artikel Skripsi
[2] Mahasiswa Fakultas Hukum Unsrat, NIM 20071101754
[3] Fakultas Hukum Unsrat, Magister Ilmu Hukum
[4] Fakultas Hukum Unsrat, Magister Ilmu Hukum
[5] It Dare Blog, "Pengertian Cyber Crime dan Jenis-jenis Cyber Crime", itdare.blogspot.com, di akses dari: https://itdare.blogspot.com/2014/12/pengertian-cyber-crime-dan-jenis-jenis.htm, pada tanggal 01 Februari 2024 pukul 00.28 Wita.
[6] Rian Dwi Hapsari dan Kuncoro Galih Pambayun, *"Ancaman Cybercrime di Indonesia Sebuah Tinjauan Pustaka Sistematis"*, Jurnal Konstituen Vol.5 No. 1, (April, 2023) Hal. 9

FAKULTAS HUKUM UNSRAT

cybercrime, yaitu serangan *phishing*. Istilah resmi phising adalah *phishing*, yang berasal dari bahasa Inggris *"fishing"* yaitu memancing.[7] *Phishing* adalah jenis serangan keamanan siber yang sangat berbahaya dan merugikan yang bertujuan untuk mendapatkan data pribadi, seperti nama pengguna, kata sandi, dan informasi keuangan. Serangan ini dilakukan dengan menyamar sebagai entitas resmi atau menggunakan teknik untuk memancing (mengelabui) korban. Para pelaku *phishing* berupaya membuat korban percaya bahwa mereka berkomunikasi dengan entitas yang sah, seperti bank, perusahaan, atau situs web resmi. Orang yang melakukan kejahatan *phishing* dikenal sebagai *Phisher*.[8] Untuk membuat korban mereka percaya dan mendorong mereka untuk membagikan informasi pribadi mereka, *Phisher* akan menggunakan berbagai strategi, seperti mengirim email palsu atau membuat situs web palsu yang terlihat sangat mirip dengan situs web asli. Penyebab utama dari pencurian data dan serangan siber adalah kekurangan dalam sistem keamanan. Banyak faktor dapat menyebabkan sistem keamanan tidak sempurna, seperti kekurangan sumber daya, ketidaktahuan, dan kesalahan manusia.[9] Ketidakpahaman pengguna terhadap perangkat teknologi informasi yang digunakan menjadi pemicu utama terjadinya *phishing*. Praktik *phishing* dapat muncul di berbagai platform, seperti media sosial, situs web, dan aplikasi. Pada kebanyakan kasus yang terjadi terdapat pada aplikasi WhatsApp yang dimana aplikasi ini menjadi tempat untuk bertukar pesan. Selain itu, ada juga orang yang tidak bertanggung jawab menggunakannya untuk tujuan kriminal. Di WhatsApp, pelaku berusaha mengirimkan pesan ke nomor tertentu. Pesan tersebut mungkin mengandung informasi bahwa nomor tersebut telah terpilih sebagai pemenang lotre, dan ketika pengguna mengklik tautan tersebut, mereka diminta untuk mengonfirmasi melalui tautan tersebut. Pengguna akan diarahkan ke situs web berbahaya yang telah diubah oleh pelaku.

Pengesahan dan implementasi Undang-Undang ITE awalnya dilakukan melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Selanjutnya, Undang-Undang ini mengalami revisi dan perubahan kedua melalui Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, yang berlaku hingga saat ini.

Kejahatan siber dalam bentuk *phishing* di Indonesia saat ini dimungkinkan dapat dikenakan Pasal 35, karena *phishing* melibatkan pembuatan situs palsu yang meniru situs asli yang resmi. Selain itu, *cybercrime phishing* juga dapat dikenakan Pasal 28 ayat (1), karena *phishing* melibatkan tindakan penipuan yang menggunakan kebohongan untuk menyesatkan orang lain. Dalam hal ini, *phishing* mengarahkan individu yang tertipu untuk mengakses suatu tautan yang menuju ke situs palsu, lalu memberikan perintah palsu untuk memperbarui informasi pribadi rahasia ke dalam situs palsu yang dibuat oleh pelaku *phishing*. Akibatnya, informasi pribadi rahasia tersebut terungkap kepada pelaku *phishing* dan menyebabkan kerugian pada korban.[10]

B. Rumusan Masalah

1. Bagaimana pengaturan hukum mengenai Perlindungan Data Pribadi?
2. Bagaimana langkah-langkah/strategi pemerintah dalam mengatasi tindak pidana *phishing*?

C. Metode Penulisan

Jenis Penelitian yang akan digunakan dalam penelitian ini adalah metode yuridis-normatif.

PEMBAHASAN

A. Pengaturan Hukum Mengenai Perlindungan Data Pribadi

Pengaturan Hukum mengenai Perlindungan Data Pribadi diatur dalam Undang-Undang Nomor 27 Tahun 2022. Undang-undang ini ditujukan untuk memberikan perlindungan atas data pribadi masyarakat, sekaligus untuk menghadapi tantangan era digital di mana data pribadi menjadi salah satu aset yang paling berharga. Undang-Undang ini juga membahas mengenai semua yang berkaitan dengan data pribadi dan sistem-sistem

[7] Kementerian Keuangan, "Waspada! Kehajatan Phising Mengintai Anda", djkn.kemenkeu.go.id, diakses dari: https://www.djkn.kemenkeu.go.id/kpknl-purwakarta/baca-artikel/14851/Waspada-Kehajatan-Phising-Mengintai-Anda.html, pada tanggal 03 Februari 2024 pukul 03.05 Wita.

[8] Ananta Fadli Sutarli dan Shelly Kurniawan, *"Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia"*, Jurnal of Social Science Research, Vol. 3 No. 2 (2023) Hal. 3.

[9] Rian Dwi Hapsari dan Kuncoro Galih Pambayun, "*Ancaman Cybercrime di Indonesia Sebuah Tinjauan Pustaka Sistematis",* Jurnal Konstituen Vol.5 No. 1, (April, 2023) Hal. 9

[10] Ardi Saputra Gulo, Sahuri Lasmadi, dan Kabib Nawawi, *"Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik"*, Jurnal of Criminal Law, Vol. 1 No. 2 (2020) Hal. 72.

FAKULTAS HUKUM UNSRAT

perlindungannya.[11] Dalam undang-undang ini terdapat 16 bab dengan 76 pasal yang membahas perihal data pribadi dengan lingkup pengaturan terdiri dari: Ketentuan Umum, Asas, Jenis Data Pribadi, Hak Subjek Data Pribadi, Pemrosesan Data Pribadi, Kewajiban Pengendali Data Pribadi dan Prosesor Data Pribadi dalam Pemrosesan Data Pribadi, Transfer Data Pribadi, Sanksi Administratif, Kelembagaan, Kerja Sama Internasional, Partisipasi Masyarakat, Penyelesaian Sengketa dan Hukum Acara, Larangan dalam Penggunaan Data Pribadi, Ketentuan Pidana, Ketentuan Peralihan, dan Ketentuan Penutup.[12] Dalam Pasal-Pasal awal undang-undang ini membahas mengenai ketentuan umum seputar data pribadi dan pihak yang terlibat dalam pemrosesannya. Sebagaimana diatur dalam pasal 1 ayat 1 undang-undang pelindungan data pribadi menerangkan bahwa Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik. Selanjutnya dalam pasal 1 ayat 2 menerangkan bahwa Pelindungan data pribadi adalah keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi. Dalam undang-undang ini Bab yang membahas Sanksi Administratif terdapat dalam pasal 57 meliputi peringatan tertulis, penghentian sementara kegiatan pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi, dan denda administratif.

Berdasarkan ketentuan Pasal 3 Undang-Undang Pelindungan Data Pribadi menjelaskan beberapa asas yang menjadi dasar perlindungan data pribadi. Ada delapan asas yang menjadi landasan, yaitu:

1. Asas Pelindungan
2. Asas Kepastian Hukum
3. Asas Kepentingan Umum
4. Asas Kemanfaatan
5. Asas Kehati-Hatian
6. Asas Keseimbangan
7. Asas Pertanggungjawaban
8. Asas Kerahasiaan.

Semakin maraknya kasus terkait perlindungan data pribadi di era modern ini tidak hanya terjadi dalam interaksi langsung secara tatap muka, tetapi juga melalui platform digital. Kebocoran data lebih sering terjadi di ranah digital, baik dalam transaksi maupun pengelolaan akun media sosial, yang sering kali disalahgunakan. Oleh karena itu, dengan adanya Undang-Undang Nomor 27 Tahun 2022 ini untuk mengatasi masalah perlindungan data pribadi dalam menghadapi kasus-kasus tersebut.

Kepatuhan terhadap Undang-Undang Pelindungan Data Pribadi (UU PDP) juga telah menjadi fokus utama di lembaga keuangan sejak disahkannya undang-undang tersebut. Lembaga keuangan, terutama perbankan merupakan salah satu yang paling rentan terhadap pencurian data pribadi. Informasi sensitif yang dikelola oleh bank dan lembaga keuangan, seperti informasi identitas, transaksi, dan data keuangan pribadi menjadikannya sasaran utama bagi pelaku kejahatan siber untuk mendapatkan data pribadi. Kepatuhan terhadap UU PDP membantu dalam melindungi data dari penyalahgunaan yang dapat mengancam privasi serta keamanan finansial pelanggan.[13]

Penerapan Undang-Undang Pelindungan Data Pribadi (UU PDP) di industri ini bertujuan untuk memperkuat perlindungan data serta meningkatkan kepercayaan nasabah. Kepercayaan nasabah sangat penting bagi industri perbankan. Kepatuhan bank terhadap UU PDP menunjukkan bahwa mereka sangat berkomitmen untuk melindungi data pribadi, yang pada akhirnya membantu membangun dan mempertahankan kepercayaan nasabah. Ini penting karena pelanggaran data dapat menyebabkan kerugian finansial yang besar bagi bank, baik secara langsung maupun tidak langsung, melalui kerusakan reputasi dan kepercayaan pelanggan.

Perlindungan data pribadi adalah aspek yang sangat penting dalam industri perbankan dan kehidupan masyarakat modern. Dengan diberlakukannya UU Pelindungan Data Pribadi, bank memiliki tanggung jawab untuk menjaga kerahasiaan dan keamanan data nasabah.

FAKULTAS HUKUM UNSRAT

[11] Dzulfahmil Khikam, Skripsi *"Kajian Hukum Perlindungan Data Pribadi dalam Peraturan Perundang-undangan di Indonesia"*, (Semarang: Universitas Islam Sultan Agung). Hal. 51.

[12] Sustainable Indonesia, "Empat Perbuatan Yang Dilarang dan Sanksinya berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)", sustain.id, diakses dari: https://sustain.id/2024/01/16/empat-perbuatan-yang-dilarang-dan-sanksinya-berdasarkan-undang-undang-nomor-27-tahun-2022-tentang-pelindungan-data-pribadi-uu-pdp/#:~:text=UU%20PDP%20mengatur%204%20(empat,Pribadi%20Palsu/Memalsukan%20Data%20Pribadi, pada tanggal 24 September 2024 pukul 17.50 Wita.

[13] Detik News, "Perlindungan Data di Industri Keuangan", news.detik.com, diakses dari: https://news.detik.com/kolom/d-7085737/perlindungan-data-di-industri-keuangan, pada tanggal 24 September 2024 pukul 20.50 Wita.

Sosialisasi, edukasi, serta kerjasama antara perbankan dan otoritas terkait menjadi faktor kunci dalam membangun budaya yang menghargai serta melindungi privasi data. Hal ini diharapkan dapat meningkatkan kepercayaan masyarakat terhadap perbankan dan menjadikan perlindungan data nasabah sebagai prioritas utama bagi semua pihak yang terlibat.[14]

B. Langkah-Langkah / Strategi Pemerintah dalam Mengatasi Tindak Pidana *Phishing*

Di era digital yang terus berkembang, aktivitas online telah menjadi bagian yang tak terpisahkan dari kehidupan manusia. Di tengah pesatnya kemajuan internet, kita sering kali menghadapi penipuan berbasis digital. Meskipun internet memberikan banyak kemudahan dalam kehidupan sehari-hari, ada juga dampak negatif yang perlu diwaspadai. Salah satu ancaman pengguna internet adalah *phishing*.[15] *Phishing* adalah jenis kejahatan siber di mana pelaku berpura-pura sebagai entitas resmi dan menghubungi korban melalui pesan WhatsApp, email, telepon, atau pesan teks, dengan tujuan untuk mendapatkan data sensitif seperti data pribadi (seperti nama, usia, dan alamat), informasi akun (*username* dan *password*), dan informasi keuangan (seperti rincian kartu kredit dan rekening).[16]

Dalam menghadapi maraknya kasus *phishing* yang semakin membahayakan keamanan data pribadi, pemerintah Indonesia telah mengambil berbagai langkah-langkah strategis dimulai dengan pembentukkan Kementerian dan Lembaga-lembaga yang akan menangani kasus *phishing*. Pembentukan Kementerian dan Lembaga-lembaga tersebut dilakukan melalui dasar hukum berupa peraturan pemerintah, peraturan presiden, atau keputusan Kementerian. Kementerian dan Lembaga-lembaga yang dibentuk juga memiliki Standar Operasional Prosedur (SOP) tersendiri dalam menangani kasus phishing. Lembaga-lembaga nasional yang dibentuk juga saling bekerja sama dengan *Forum Internasional* untuk meningkatkan dan memperkuat penanganan kejahatan phishing di Indonesia.

Berikut adalah langkah-langkah dari Kementerian dan lembaga-lembaga yang dibentuk pemerintah untuk mengatasi *Phishing*:

1. Badan Siber dan Sandi Negara (BSSN) Prosedur Penanganan *Phishing*.[17]

Dalam penanganan terhadap serangan *phishing* dilakukan dalam beberapa tahap sebagai berikut:

1. Persiapan
   Tujuan tahap persiapan pada penanganan serangan *phishing* adalah untuk membangun kontak, menentukan prosedur dan mengumpulkan informasi serangan. Tahap persiapan penanganan serangan *phishing*, dilakukan dengan prosedur sebagai berikut:
   a) Membuat daftar semua domain sah yang dimiliki organisasi;
   b) Mempersiapkan satu buah halaman website untuk memperingatkan pengguna tentang terjadinya serangan phising;
   c) Mempersiapkan formulir untuk informasi laporan penyalahgunaan domain.
   d) Membangun kontak dengan pihak-pihak terkait, seperti perusahaan hosting, penyedia domain, penyedia jasa email, *Nasional CERT*;
   e) Meningkatkan kesadaran terhadap serangan phishing, diantaranya:
      1) Tidak mengklik link yang mencurigakan;
      2) Tidak memasukan *username* dan *password* pada situs web yang alamat webnya meragukan;
      3) Merubah penulisan alamat email yang dipublish, dari bentuk @ menjadi "at" atau dalam bentuk gambar, untuk menghindari menjadi target email phising;
      4) Menggunakan *AntiVirus* yang memiliki fitur *Anti Phishing*.
2. Identifikasi
   Tujuan dari proses identifikasi adalah untuk mendeteksi adanya insiden serangan *phishing*, menentukan ruang lingkup, dan melibatkan pihak-pihak yang tepat dalam menangani serangan *phishing*. Tahap identifikasi penanganan serangan *phishing* adalah sebagai berikut:
   a) Memonitor email, social media, web forms dsb pada Organisasi untuk mencari informasi *Phishing*;

[14] Cyber Hub, "Perbankan Wajib Perkuat Perlindungan Data Pribadi", cyberhub.id, diakses dari: https://cyberhub.id/berita/bank-perlindungan-data#!, pada tanggal 25 September 2024 pukul 20.45 Wita.

[15] Diskominfo Kota Bogor, "Awas Tindakan Phising! Ini Dia Langkah-Langkah Agar Tidak Terkena Pesan Berisi Link Phishing", kominfo.kotabogor.go.id, diakses dari: https://kominfo.kotabogor.go.id/index.php/post/single/897, pada tanggal 27 September 2024 pukul 23.50 Wita.

[16] Hukum Online, "Jerat Hukum Pelaku Phishing dan Modusnya", hukumonline.com, diakses dari: https://www.hukumonline.com/klinik/a/jerat-hukum-pelaku-iphishing-i-da%20n-modusnya-cl5050/, pada tanggal 28 September 2024 pukul 04.00 Wita.

[17] BSSN, "Panduan Penanganan Insiden Serangan Phishing".

FAKULTAS HUKUM UNSRAT

b) Memeriksa *URL phishing* dan *hyperlink* yang mencurigakan menggunakan www.virustotal.com dan www.phishtank.com;
c) Melibatkan pihak yang tepat terkait serangan *phishing*. Agar bisa segera di lakukan takedown terhadap web *phishing*. Seperti perusahaan hosting, penyedia domain, penyedia jasa email, *Nasional CERT*;
d) Mengumpulkan bukti bukti terkait adanya serangan *phishing*. Contohnya *screenshoot* halaman web yang terdampak.

3. *Containment* (Pengendalian)
Setelah dipastikan bahwa memang benar telah terjadi serangan *phishing*, maka dilakukan proses mitigasi serangan, agar tidak terjadi kerusakan lebih dalam. Prosedur yang dilakukan pada tahap ini adalah:
a) Menyebarkan *URL phishing* dan konten dari *email phishing* pada pihak *spam reporting website*, misalnya www.phishtank.com;
b) Menginformasikan serangan *phishing* kepada pengguna, agar pengguna mengetahui dan tidak terkena dampak dari serangan tersebut;
c) Memeriksa *source code* dari *website phishing*, jika menggunakan gambar dari website yang anda miliki, anda dapat mengganti gambar dengan tampilan "*Phising Website*"

4. *Eradication* (Pemberantasan)
Proses ini bertujuan untuk mengambil tindakan dalam menghentikan serangan *phishing*. Prosedur untuk melakukan proses ini dapat dilakukan dengan cara berikut:
a) Jika halaman *phishing* di hosting di situs web yang telah disusupi, maka hubungi pemilik dari website tersebut, agar halaman *phishing* dihapus dan dilakukan update security;
b) Untuk percepatan penanganan, hubungi perusahaan hosting dengan mengirim email berisikan informasi *phishing*, serta lakukan kontak telepon perusahaan hosting yang tersedia;
c) Menghubungi perusahaan *hosting* untuk melakukan takedown /penutupan alamat website palsu;
d) Jika takedown terlalu lama, maka hubungi Nasional CERT untuk mengontak CERT lokal yang berada di negara tersebut untuk membantu proses takedown.

5. Pemulihan
Pemulihan merupakan tahap untuk mengembalikan seluruh sistem bekerja normal seperti semula. Prosedur yang dapat dilakukan sebagai berikut:
a) Memastikan bahwa halaman website penipuan sudah tidak dapat diakses;
b) Tetap Memantau URL palsu, untuk memastikan URL palsu tersebut tidak dapat diakses;
c) Menghapus halaman peringatan dari website.

6. Tindak Lanjut
Tahap ini adalah fase di mana semua dokumentasi kegiatan yang dilakukan dicatat sebagai referensi untuk di masa mendatang. Prosedur yang dapat dilakukan adalah sebagai berikut:
a) Menyempurnakan langkah-langkah respon, prosedur penanganan serangan yang diambil selama insiden agar kedepannya dapat menangani insiden secara lebih cepat dan efisien;
b) Memperbaharui daftar kontak yang dimiliki, disertai catatan cara paling efektif untuk menghubungi setiap pihak yang terlibat;
c) Berkolaborasi dengan tim hukum jika diperlukan tindakan hukum;
d) Membuat dokumentasi dan laporan terkait penanganan serangan Phising;
e) Membuat evaluasi dan rekomendasi.

2. Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri

Prosedur Penanganan *Phishing*.[18]

1. Pelaporan Kasus
a) Portal Resmi: Masyarakat yang menjadi korban dapat melaporkan melalui portal resmi seperti Patroli Siber (patrolisiber.id) atau melapor ke kantor polisi terdekat dari lokasi tindak pidana itu terjadi. Misalnya jika berada di suatu kecamatan, maka dapat melapor ke Kepolisian tingkat sektor (POLSEK) terdekat di mana tindak pidana itu terjadi. Tapi, dapat juga melapor ke wilayah administrasi yang berada di atasnya, seperti POLRES, POLDA atau MABES POLRI.
b) Verifikasi dan Dokumentasi**:** Laporan diverifikasi oleh petugas dengan

[18] Patroli Siber, "*Menjaga lanskap digital Indonesia melalui langkah-langkah keamanan siber tingkat lanjut",* patrolisiber.id, diakses dari: https://www.patrolisiber.id/about-us/, pada tanggal 28 November 2024 pukul 19.15 wita

FAKULTAS HUKUM UNSRAT

mengumpulkan bukti awal seperti screenshot percakapan, bukti transaksi finansial, email atau link yang digunakan dalam aksi *phishing.*

2. Penyelidikan Digital
   a) Patroli Siber: Unit patroli siber secara rutin memantau aktivitas mencurigakan di dunia maya untuk mendeteksi ancaman phishing lebih dini.
   b) Analisis Forensik Digital: Dittipidsiber menggunakan teknologi *cyber forensic* untuk melacak jejak digital pelaku, seperti metadata, email, alamat IP, atau data transaksi mencurigakan.
3. Kerja sama antar Institusi
   a) Institusi Perbankan**:** Dalam kasus *phishing* yang melibatkan penipuan keuangan, Dittipidsiber bekerja sama dengan bank untuk memblokir rekening pelaku dan menghentikan aliran dana.
   b) Kolaborasi Internasional: Jika *phishing* melibatkan jaringan internasional, Polri bekerjasama dengan badan penegak hukum global seperti INTERPOL.
4. Tindakan Penegakan Hukum
   a) Setelah bukti cukup, Dittipidsiber melakukan operasi untuk menangkap pelaku dan menyita alat kejahatan seperti perangkat komputer dan server.
   b) Pelaku kemudian dikenakan pasal-pasal terkait tindak pidana siber sesuai dengan UU ITE dan undang-undang lainnya tekait kejahatan siber.
5. Pencegahan Melalui Edukasi
   a) Kampanye Kesadaran Siber**:** Melalui media digital dan seminar, Polri mengedukasi masyarakat tentang bahaya phishing, seperti mengenali email atau pesan mencurigakan.
   b) Publikasi Kasus: Pengungkapan kasus bertujuan memberikan efek jera bagi pelaku serta meningkatkan kewaspadaan public.
6. Tim Respons Cepat
   Dittipidsiber memiliki tim respons cepat yang menangani laporan secara real-time untuk meminimalkan dampak dan mencegah kerugian lebih lanjut bagi korban.

3. Kementerian Komunikasi dan Digital (Komdigi)

Prosedur Penanganan *Phishing.*[19]

1. Penerimaan Laporan
   Kementerian Komunikasi dan Digital (Komdigi) menyediakan situs web *https://aduannomor.id/home*, sebagai website bagi masyarakat untuk melaporkan nomor-nomor yang digunakan dalam kasus penipuan, tawaran judi online, atau iklan spam. Kementerian Komdigi juga menyediakan layanan pengaduan untuk konten penipuan di situs web, platform digital, atau media sosial melalui https://aduankonten.id/.
2. Verifikasi dan Validasi
   Memverifikasi laporan untuk memastikan bahwa situs atau aktivitas yang dilaporkan adalah phishing.
3. Pemblokiran akses konten
   Komdigi dapat memblokir situs web atau aplikasi yang terlibat dalam phishing. Untuk konten di media sosial, Komdigi bekerja sama dengan platform untuk menonaktifkan akun atau konten yang melanggar.
4. Edukasi dan Sosialisasi Literasi Digital
   Komdigi melakukan edukasi kepada masyarakat tentang tanda-tanda *phishing*, seperti tautan yang mencurigakan, email dari pengirim tak dikenal, atau situs tanpa *HTTPS*. Program literasi digital melibatkan kerja sama dengan Kementerian Pendidikan dan Kebudayaan (Kemendikbud), Siberkreasi, dan Facebook untuk memberikan pemahaman yang lebih mendalam mengenai bahaya phishing.[20]

Untuk menangani *phishing* secara efektif, pemerintah juga melakukan kerja sama dengan lembaga luar negeri, salah satunya INTERPOL *(International Criminal Police Organization)*. INTERPOL bekerja sama dengan Kepolisian Indonesia dan mitra internasional lainnya, telah melakukan berbagai operasi untuk menangani kasus phishing, salah satunya adalah operasi terhadap platform *"16shop"*.

Selain Pemerintah, lembaga keuangan terutama perbankan juga memiliki peran penting dalam menangani kasus *phishing*, mengingat mereka sering menjadi sasaran utama kejahatan ini. Beberapa bank telah menjadi target kejahatan siber, di mana serangan ini terus berkembang dan

[19] Direktorat Jenderal Aplikasi Informatika, "Tiga Strategi Kominfo dalam Tangani Hoaks dan Misinformasi", aptika.kominfo.go.id, diakses dari: https://aptika.kominfo.go.id/2020/09/tiga-strategi-kominfo-dalam-tangani-hoaks-dan-misinformasi/, pada tanggal 28 November 2024 pukul 20.42 Wita.

[20] Media Center, "Kominfo Bersama Kemendikbud Ajak Masyarakat Waspadai Phising", mediacenter.rohilkab.go.id, diakses dari: https://mediacenter.rohilkab.go.id/view/kominfo-bersama-kemendikbud-ajak-masyarakat-waspadai-phising, pada tanggal 28 November 2024 pukul 21.00 Wita.

FAKULTAS HUKUM UNSRAT

semakin sulit dideteksi. Otoritas Jasa Keuangan (OJK) memiliki peran penting dalam mengatasi ancaman *phishing*, terutama yang terkait dengan sektor perbankan dan keuangan digital. Berikut adalah langkah-langkah lembaga keuangan dalam mengatasi phishing:

1. Otoritas Jasa Keuangan (OJK)
   OJK memiliki kewajiban untuk melindungi stabilitas sistem keuangan, termasuk mengatasi ancaman seperti *phishing* yang mengancam keamanan transaksi digital.
2. Bank Umum
   Bank wajib menyusun dan menerapkan strategi *anti-fraud* secara efektif. Penyusunan dan penerapan strategi *anti-fraud* yang efektif memiliki pedoman penerapan strategi *anti-fraud*. Penyusunan dan penerapan strategi *anti-fraud* paling sedikit memuat 4 (empat) pilar. 4 (empat) pilar tersebut terdiri dari:[21]
   1) Pencegahan
   2) Deteksi
   3) Investigasi, Pelaporan, dan Sanksi
   4) Pemantauan, Evaluasi, dan Tindak Lanjut

Bank wajib memiliki mekanisme tindak lanjut berdasarkan hasil evaluasi atas kejadian *fraud* untuk memperbaiki kelemahan-kelemahan dan memperkuat sistem pengendalian intern agar dapat mencegah terulangnya kembali *fraud* karena kelemahan yang serupa.

Selain langkah-langkah diatas lembaga keuangan juga secara rutin memberikan edukasi kepada nasabah mengenai berbagai modus phishing yang terus berkembang. Melalui media seperti email, pesan, dan media sosial, bank memberi tahu nasabah cara mengenali dan menghindari pesan mencurigakan yang berusaha mencuri informasi pribadi. Bank juga sering mengirimkan peringatan terkait phishing, terutama ketika terjadi peningkatan kasus penipuan. Nasabah diingatkan untuk tidak memberikan data pribadi melalui email, telepon, atau pesan yang mengaku berasal dari bank, serta disarankan selalu memeriksa URL situs web sebelum login.[22] Bank juga dapat memblokir kartu atau rekening nasabah jika terindikasi bahwa nasabah menjadi korban phising. Tindakan tersebut untuk mencegah akses lebih lanjut oleh pelaku phising. Memblokir kartu atau rekening juga bisa dilakukan oleh nasabah melalui aplikasi mobile banking jika nasabah merasa kartu atau rekening nasabah terkena penipuan. Hal ini lebih praktis karena nasabah tidak perlu datang ke kantor cabang bank.[23]

Dari sekian banyak langkah-langkah sesuai prosedur yang telah dibahas, terdapat kendala atau tantangan dalam melaksanakan prosedur tersebut. Berikut adalah beberapa kendala dalam melaksanakan prosedur mengatasi *phishing*, di antaranya:[24]

1. Kurangnya Literasi Digital Masyarakat
2. Teknik *Phishing* yang terus Berkembang
3. Keterbatasan Teknologi
4. Minimnya Penegakan Hukum

Selain pemerintah dan lembaga keuangan, kita juga sebagai masyarakat harus lebih memahami dan harus jauh lebih waspada lagi dengan kasus phising ini, karena tidak semua orang paham dan memahami kasus tersebut sehingga banyak masyarakat juga yang terjerumus dalam hal ini, maka selain adanya peran dari pemerintah dan lembaga keuangan kita juga harus pandai-pandai dalam menggunakan smartphone, karena dalam smartphone ini semua kejahatan dapat terjadi terutama dalam hal ini yaitu phising. Berikut langkah-langkah yang bisa kita lakukan untuk menghindari tindakan cybercrime phising:[25]

1. Perbarui Perangkat Lunak Secara Teratur
2. Mengubah password secara rutin
3. Waspadai Email dan Pesan Teks yang Mencurigakan
4. Gunakan Aplikasi Keamanan

Ada juga hal yang perlu dilakukan jika terlanjur mengklik link phising:[26]

1. Matikan Saluran Internet atau WiFi
2. Hapus Histori Browser Internet
3. Kumpulkan bukti-bukti dan laporkan kepada pihak berwajib

PENUTUP

[21] Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 39 /Pojk.03/2019 Tentang Penerapan Strategi *anti-fraud* bagi Bank Umum, Pasal 4

[22] Ramadhanti Achlina Tri Putri dan Heru Sugiyono, *"Tanggung Jawab Bank Terhadap Tindakan Phising dalam Sistem Penggunaan E-Banking (Studi: Kasus Phising Pada PT. Bank Rakyat Indonesia (Persero) Tbk)"*, Jurnal Interpretasi Hukum, Vol. 4 No. 3 (Desember, 2023) 5.

[23] Kompas, "Cara Blokir Kartu ATM BRI, BCA, dan BNI Tanpa ke Bank", money.kompas.com, diakses dari: https://money.kompas.com/read/2024/07/22/105550126/cara-blokir-kartu-atm-bri-bca-dan-bni-tanpa-ke-bank, pada tanggal 29 November 2024 Pukul 00.35 Wita.

[24] Baraka, "Tantangan Terbesar dalam Bidang Cyber Security dan Solusi yang Tepat untuk Mengatasinya", baraka.uma.ac.id, diakses dari: https://baraka.uma.ac.id/tantangan-terbesar-dalam-bidang-cyber-security-dan-solusi-yang-tepat-untuk-mengatasinya/, pada tanggal 29 Desember 00.50 Wita.

[25] Privy, "Melawan Ancaman: Cara Mengatasi Phishing di HP Anda", blog.privy.id, diakses dari: https://blog.privy.id/cara-mengatasi-phising-di-hp/, pada tanggal 05 Oktober 2024 pukul 19.48 Wita.

[26] Privy, "Ini yang Perlu Dilakukan Jika Terlanjur Klik Link Phising, Jangan Panik!", blog.privy.id, diakses dari: https://blog.privy.id/langkah-terlanjur-klik-link-phising/, pada tanggal 05 Oktober 2024 pukul 20.19 Wita.

FAKULTAS HUKUM UNSRAT

A. Kesimpulan

1. Pengaturan Hukum mengenai Perlindungan Data Pribadi diatur dalam Undang-Undang Nomor 27 Tahun 2022, yang bertujuan melindungi data pribadi masyarakat di era digital. Undang-Undang ini mencakup berbagai aspek pelindungan data pribadi, yang dimana Data Pribadi didefinisikan sebagai data tentang orang yang dapat diidentifikasi secara langsung maupun tidak langsung. Peraturan ini juga mencakup ketentuan tentang sanksi administratif, larangan penggunaan data pribadi, serta ketentuan pidana. Undang-Undang ini melarang perolehan, pengungkapan, dan penggunaan data pribadi secara ilegal, dengan ancaman hukuman penjara dan denda. Di era modern, kasus kebocoran data pribadi semakin sering terjadi, tidak hanya dalam interaksi langsung tetapi juga melalui media sosial. Maraknya kasus ini menegaskan pentingnya perlindungan data pribadi di ranah digital. Perlindungan data juga sangat penting bagi lembaga keuangan, terutama perbankan. Penerapan Undang-Undang Perlindungan Data Pribadi di industri ini bertujuan memperkuat keamanan data dan membangun kepercayaan nasabah terhadap industri perbankan, yang dimana kepercayaan nasabah sangat penting bagi industri ini.
2. Di era digital yang terus berkembang, aktivitas online telah menjadi bagian dari kehidupan sehari-hari. Namun, kemajuan internet juga sering kali dihadapkan dengan penipuan berbasis digital, termasuk phishing. Untuk menangani masalah ini, pemerintah Indonesia telah membentuk lembaga-lembaga yang akan menangani kasus *phishing* dengan menerapkan sejumlah strategi sesuai dengan prosedurnya sendiri, Lembaga tersebut antara lain: BSSN dimulai dari persiapan, identifikasi, pengendalian, pemberantasan, pemulihan, dan Tindak lanjut. Dittipidsiber dan KOMDIGI dimulai dengan pelaporan kasus, penyelidikan, pemblokiran akses konten, kerja sama antar institusi, Tindakan penegakan hukum, dan edukasi masyarakat. Lembaga keuangan, yang sering menjadi target phishing, turut berperan dengan dimulai pencegahan, deteksi, investigasi, pelaporan, sanksi, pemantauan, evaluasi, dan tindak lanjut. Namun, terdapat kendala dalam pelaksanaan prosedur tersebut, seperti kurangnya literasi masyarakat, teknik phishing yang terus berkembang, dan keterbatasan teknologi. Dengan demikian, langkah-langkah pemerintah sudah sesuai dengan prosedur, tetapi tetap terdapat kendala-kendala dalam melaksanakan prosedur tersebut.

B. Saran

1. Dalam pengaturan hukum diharapkan Undang-Undang Pelindungan Data Pribadi dapat diberlakukan dan lebih diutamakan, terutama terkait dengan sanksi yang harus tegas bagi pelaku tindak pidana phising. Dan juga untuk lembaga keuangan diharapkan dapat mematuhi standar keamanan siber yang ketat untuk mencegah kebocoran data terutama dalam hal pengelolaan keamanan data nasabah. Selain itu, pengawasan dari otoritas keuangan juga perlu diperketat untuk memastikan kepatuhan lembaga keuangan terhadap peraturan perlindungan data pribadi.
2. Pemerintah diharapkan dapat meningkatkan dan memperkuat strategi-strategi agar lebih efektif dan tepat dalam mengatasi tindak pidana *phishing* ini melalui lembaga-lembaga yang telah dibentuk serta diharapkan dapat memberikan sanksi yang lebih tegas guna memberikan efek jera terhadap pelaku-pelaku yang dengan sengaja mendapatkan informasi pribadi seseorang sehingga mengakibatkan kerugian. Dengan strategi yang sudah diterapkan diharapkan dapat meminimalisir risiko kejahatan phishing. Dengan demikian, pemerintah dapat menciptakan lingkungan digital yang lebih aman bagi semua pihak.

DAFTAR PUSTAKA

BUKU

Adji, Indriyanto Seno. 2002. *Korupsi dan Hukum Pidana.* Jakarta: Kantor Pengacara dan Konsultasi Hukum "Prof. Oemar Seno Adji & Rekan.

Effendi, Erdianto. 2014. *Hukum Pidana Indonesia Suatu Pengantar*. Bandung: PT. Refika Aditama.

Hamzah, Andi. 2010. *Asas-Asas Hukum Pidana.* Jakarta: Rineka Cipta.

Huda, Chairul. 2011. *Dari Tiada Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggungjawaban Pidana Tanpa Kesalahan: Tinjauan Kritis Terhadap Teori Pemisahan Tindak Pidana dan Pertanggungjawaban Pidana cet. Ke-4.* Jakarta: Kencana Prenada Media Group.

Maskun. 2022. *Kejahatan Siber (Cyber Crime) Suatu Pengantar*. Jakarta: Kencana.

Prodjodikoro, Wirjono. 1986. *Asas-asas Hukum Pidana di Indonesia.* Bandung: Eresco.

FAKULTAS HUKUM UNSRAT

Sianturi, S.R. 1998. *Asas-Asas Hukum Pidana dan Penerapannya di Indonesia Cetakan Ke-2"*. Jakarta.

Soekanto, S., & Mamuji, S. 2010. *Penelitian Hukum Normatif Suatu Tinjauan* Singkat. Jakarta: Raja Grafindo Persada.

PERATURAN DAN PERUNDANG-UNDANGAN

Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 22 Tahun 2023 Tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan.

Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor. 39/Pojk.03/2019 Tentang Penerapan Strategi anti Fraud bagi Bank Umum.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).

JURNAL

Dewi, Sinta. 2016. Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing di Indonesia. *Jurnal Yustisia Hukum*. 5. (1).

Gulo, Ardi. Lasmadi Sahuri & Nawawi Kabib. 2020. Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *Jurnal of Criminal Law*. 1. (2).

Hapsari, Rian & Pambayun Kuncoro. 2023. Ancaman Cybercrime Di Indonesia Sebuah Tinjauan Pustaka Sistematis. *Jurnal Konstituen*. 5 (1).

Irawan, Dedi. 2020. Mencuri Informasi Penting dengan Mengambil Alih Akun Facebook dengan Metode Phising. *Jurnal Ilmu Komputer & Informatika*. 1. (1).

Kang, Jerry. 1998. Information Privacy in Cyberspace Transactions. *Stanford Law Review*. 50. (1193).

Putri, Ramadhanti & Sugiyono, Heru. Tanggung Jawab Bank Terhadap Tindakan Phising dalam Sistem Penggunaan E-Banking (Studi: Kasus Phising Pada PT. Bank Rakyat Indonesia (Persero) Tbk). *Jurnal Interpretasi Hukum*. 4. (3).

Rahmadi, Putra & Yunita, Hilda. 2020. Implementasi Pengamanan Basis Data dengan Teknik Enkripsi. *Jurnal Cendikia*. XIX.

Sulisrudatin, Nunuk. 2018. Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit. *Jurnal Ilmiah Hukum Dirgantara*. 9. (1).

Supanto dkk. 2023. Pencegahan dan Penanggulangan Kejahatan Teknologi Informasi di Wilayah PDM Kabupaten Klaten Melalui Metode Sosialisasi Interaktif. *Jurnal Gema Keadilan*. 10. (3).

Sutarli, Ananta & Kurniawan Shelly. 2023. Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia. *Jurnal of Social Science Research*. 3. (2).

Wibowo, Mia. 2017. Ancaman Phising Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime. *Jurnal of Education and Information Communication Technology*. 1. (1).

WEBSITE / INTERNET

A. Faradilla. 2023, Desember 04. *Apa Itu Phising? Pengertian, Jenis, dan Cara Mengenalinya*. Diambil Kembali dari hostinger.co.id: https://www.hostinger.co.id/tutorial/phising-adalah#Jenis-Jenis_Phising

Baraka. 2024, Januari 15. *Upaya Pemerintah Dalam Menangani Ancaman Cybercrime di Era Digital*. Diambil Kembali dari baraka.uma.ac.id: https://baraka.uma.ac.id/upaya-pemerintah-dalam-menangani-ancaman-cybercrime-di-era-digital/

Baraka. 2024. *Tantangan Terbesar dalam Bidang Cyber Security dan Solusi yang Tepat untuk Mengatasinya*. Diambil Kembali dari baraka.uma.ac.id: https://baraka.uma.ac.id/tantangan-terbesar-dalam-bidang-cyber-security-dan-solusi-yang-tepat-untuk-mengatasinya/

Center for Indonesian Policy Studies. 2023, Mei 16. *Kolaborasi Penting Dalam Memerangi Kejahatan Digital Keuangan di Indonesia*. Diambil Kembali dari cips-indonesia.org: https://www.cips-indonesia.org/post/kolaborasi-penting-dalam-memerangi-kejahatan-digital-keuangan-di-indonesia?lang=id

Cloudeka, L. 2023, Juni 21. *5 Contoh Phishing yang Harus Diwaspadai*. Diambil Kembali dari cloudeka.id: https://www.cloudeka.id/id/berita/web-sec/contoh-phising/

CNN Indonesia. 2023, November 04. *Kronologi Baim Wong Kena Phising via WA*. Diambil Kembali dari cnnindonesia.com: https://www.cnnindonesia.com/hiburan/202

FAKULTAS HUKUM UNSRAT

31103231916-234-1019881/kronologi-baim-wong-kena-phising-via-wa

Diskominfo Kota Bogor. *Awas Tindakan Phising! Ini Dia Langkah-Langkah Agar Tidak Terkena Pesan Berisi Link Phishing*. Diambil Kembali dari kominfo.kotabogor.go.id: https://kominfo.kotabogor.go.id/index.php/post/single/897

Diskominfo Kota Bogor. *Memahami Two-Factor Authentication (2FA)*. Diambil Kembali dari kominfo.kotabogor.go.id: https://kominfo.kotabogor.go.id/index.php/post/single/838

Financial Crime Academy. 2024, September 27. *Real-Time and Offsite Transaction Monitoring*. Diambil Kembali dari financialcrimeacademy.org: https://financialcrimeacademy.org/real-time-and-offsite/

Gema, Ari Juliano. 2005, Oktober 04. *Cybercrime: Sebuah Fenomena di Dunia Maya*. Diambil Kembali dari arijuliano.blogspot.com: https://arijuliano.blogspot.com/2005/10/cybercrime-sebuah-fenomena-di-dunia.html

Gillin, P. *The History of Phishing*. Diambil Kembali dari verizon.com: https://www.verizon.com/business/resources/articles/s/the-history-of-phishing/

Haekal, M. 2024, Februari 02. *Apa Itu Phising? Cara Kerja, Contoh, dan Cara Menghindarinya*. Diambil Kembali dari mekarisign.com: https://mekarisign.com/id/blog/apa-itu-phising/

Indonesia, Sustainable. 2024, Januari 16. *Empat Perbuatan Yang Dilarang dan Sanksinya berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)*. Diambil Kembali dari sustain.id: https://sustain.id/2024/01/16/empat-perbuatan-yang-dilarang-dan-sanksinya-berdasarkan-undang-undang-nomor-27-tahun-2022-tentang-pelindungan-data-pribadi-uu-pdp/

It Dare Blog, 2014, Desember 22. *Pengertian Cyber Crime dan Jenis-jenis Cyber Crime*. Diambil Kembali dari itdare.blogspot.com: https://itdare.blogspot.com/2014/12/pengertian-cyber-crime-dan-jenis-jenis.html

Justika. 2021, Desember 10. Cara Mengatasi Kejahatan Phising Penting untuk Diketahui. Diambil Kembali dari blog.justika.com: https://blog.justika.com/pidana-dan-laporan-polisi/cara-mengatasi-kejahatan-phising/

KBBI. *Data Pribadi*. Diambil Kembali dari kbbi.kemdikbud.go.id: https://kbbi.kemdikbud.go.id/Beranda/Hukum

Kemenkeu. 2022, Maret 25. *Waspada! Kehajatan Phising Mengintai Anda*. Diambil Kembali dari jkn.kemenkeu.go.id: https://www.djkn.kemenkeu.go.id/kpknl-purwakarta/baca-artikel/14851/Waspada-Kehajatan-Phising-Mengintai-Anda.html

Kutanto, Haronas. 2023, November 15. *Antisipasi Penipuan Online Laporkan Melalui Aduan Nomor*. Diambil Kembali dari djppi.kominfo.go.id: https://djppi.kominfo.go.id/news/antisipasi-penipuan-online-laporkan-melalui-aduan-nomor

Media Center. 2021, Februari 17. *Kominfo Bersama Kemendikbud Ajak Masyarakat Waspadai Phising*. Diambil Kembali dari mediacenter.rohilkab.go.id: https://mediacenter.rohilkab.go.id/view/kominfo-bersama-kemendikbud-ajak-masyarakat-waspadai-phising

Media Center. 2021. *Kominfo Bersama Kemendikbud Ajak Masyarakat Waspadai Phising*. Diambil Kembali dari mediacenter.rohilkab.go.id: https://mediacenter.rohilkab.go.id/view/kominfo-bersama-kemendikbud-ajak-masyarakat-waspadai-phising

Nquiringminds. 2023. *Interpol Shuts Down Phishing-as-a-Service Platform "16shop" with Three Arrests*. Diambil Kembali dari nquiringminds.com: https://nquiringminds.com/cybernews/interpol-shuts-down-phishing-as-a-service-platform-16shop-with-three-arrests/

Nugroho, Andi. 2020, Februari 11. *Anda Mengalami Insiden Siber, Ini Cara Lapor ke BSSN*. Diambil Kembali dari m.cyberthreat.id: https://m.cyberthreat.id/read/5199/Anda-Mengalami-Insiden-Siber-Ini-Cara-Lapor-ke-BSSN

Patroli Siber. 2024. *Menjaga lanskap digital Indonesia melalui langkah-langkah keamanan siber tingkat lanjut.* Diambil Kembali dari patrolisiber.id: https://www.patrolisiber.id/about-us/

Patroli Siber. *Direktorat Tindak Pidana Siber Bareskrim Polri*. Diambil Kembali dari patrolisiber.id: https://patrolisiber.id/contact-us/

FAKULTAS HUKUM UNSRAT

Patroli Siber. *Tentang Unit Patroli Siber*. Diambil Kembali dari patrolisiber.id: https://patrolisiber.id/about-us/

Perangin-angin, Ita Iya Pulina. 2023, November 29. *Panduan untuk Melaporkan Penipuan Online*. Diambil Kembali dari hukumonline.com: https://www.hukumonline.com/klinik/a/panduan-untuk-melaporkan-penipuan-online-lt656758061ec52/

Permatasari, Erizka. 2021. Desember 09. *Jerat Hukum Pelaku Phishing dan Modusnya*. Diambil Kembali dari hukumonline.com: https://www.hukumonline.com/klinik/a/jerat-hukum-pelaku-iphishing-i-da%20n-modusnya-cl5050/

Prestasi Kita. 2024, Januari 06. *Perkembangan Terkini Cyber Security di Indonesia*. Diambil Kembali dari prestasikita.com: https://www.prestasikita.com/2024/01/06/perkembangan-terkini-cyber-security-di-indonesia/

Privy. 2024, Juni 24. Ini yang Perlu Dilakukan Jika Terlanjur Klik Link Phising, Jangan Panik. Diambil Kembali dari blog.privy.id: https://blog.privy.id/langkah-terlanjur-klik-link-phising/

Privy. 2024, Maret 20. *Melawan Ancaman: Cara Mengatasi Phishing di HP Anda*. Diambil Kembali dari blog.privy.id: https://blog.privy.id/cara-mengatasi-phising-di-hp/

PT. BPR Bank Jombang. *Serangan Phishing di Indonesia Terus Meningkat*. Diambil Kembali dari bankjombang.co.id: https://bankjombang.co.id/serangan-phishing-di-indonesia-terus-meningkat-berikut-data-lengkapnya/

Sari, Rita Puspita. 2024, Maret 14. *Perbankan Wajib Perkuat Perlindungan Data Pribadi*. Diambil Kembali dari cyberhub.id: https://cyberhub.id/berita/bank-perlindungan-data#!,

Shaid, Nur Jamal. 2024, Juli 22. *Cara Blokir Kartu ATM BRI, BCA, dan BNI Tanpa ke Bank*. Diambil Kembali dari money.kompas.com: https://money.kompas.com/read/2024/07/22/105550126/cara-blokir-kartu-atm-bri-bca-dan-bni-tanpa-ke-bank

Shinhan Bank. Pengertian Mobile Banking. Diambil Kembali dari shinhan.co.id: https://www.shinhan.co.id/article-listings/read/pengertian-mobile-banking

Tuhu Nugraha, Abdan. 2023, Desember 14. *Perlindungan Data di Industri Keuangan*. Diambil Kembali dari news.detik.com: https://news.detik.com/kolom/d-7085737/perlindungan-data-di-industri-keuangan

UMSU, Fakultas Hukum. 2023. Juli 26. *Tindak Pidana: Pengertian, Unsur dan Jenisnya*. Diambil Kembali dari fahum.umsu.ac.id: https://fahum.umsu.ac.id/tindak-pidana-pengertian-unsur-dan-jenisnya/

Yusuf. 2020. *Tiga Strategi Kominfo dalam Tangani Hoaks dan Misinformasi*. Diambil Kembali dari aptika.kominfo.go.id: https://aptika.kominfo.go.id/2020/09/tiga-strategi-kominfo-dalam-tangani-hoaks-dan-misinformasi/

SUMBER LAIN

Bachtiyar, Achmad. 2023. Implikasi Hukum Pidana dalam Perlindungan Data Pribadi Ditinjau dari Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. (Sarjana, Sekolah Tinggi Ilmu Hukum Biak-Papua).

BSSN. Panduan Penanganan Insiden Serangan Phishing.

IDADX. Laporan Aktivitas Abuse *Domain.Id (Indonesia Anti-Phishing Data Exchange)*.

Khikam, Dzulfahmil. 2023. Kajian Hukum Perlindungan Data Pribadi dalam Peraturan Perundang-undangan di Indonesia. (Sarjana, Universitas Islam Sultan Agung).

Marita, Lita Sari. Cyber Crime dan Penerapan Cyber Law dalam Pemberantasan Cyber Law di Indonesia. (Dosen Tetap AMIK BSI Jakarta).

Pengadilan Negeri Jember. Putusan Nomor 650/Pid.sus/2019/PN.Jmr.

Putusan Pengadilan Negeri Banjarbaru Nomor 85/Pid.Sus/2022/PN.Bjb

Putusan Pengadilan Negeri Sengkang Nomor 30/Pid.Sus/2019/PN.Skg

FAKULTAS HUKUM UNSRAT