Judge : Jurnal Hukum
Volume 06, Number 05, 2025, doi.org/10.54209/judge.v6i05.1901
E.SSN : 2775-4170 (Online - Elektronik)
https://journal.cattleyadf.org/index.php/Judge/index

ANALISIS PENIPUAN DIGITAL MELALUI PANGGILAN PENIPUAN ATAU SCAM CALL YANG MENEROR MASYARAKAT DAN MENGGANGGU KEAMANAN DIGITAL

Lestari Victoria Sinaga[1], Dearma Sariani Sinaga[2], Emmelia A. Ginting[3], Helen Vanhurk Sriwati Ningsih Sitorus [4]
[1,2,3,4]Universitas Darma Agung, Medan, Indonesia
Missthary35@gmail.com , Dearmasinaga2@gmail.com , Emilginting3@gmail.com , Helensitorus41@gmail.com

Article Info
Keywords:
Scam Call, Keamanan Digital, Tindak Pidana Penipuan.

ABSTRACT
Tujuan penelitian ini adalah untuk mengetahui bagaimana mekanisme penipuan online melalui scam call melalui panggilan penipuan yang beredar ditengah masyarakat. Metode penelitian yang digunakan normatif yuridis, dengan menggunakan studi peraturan perundang-undangan diatur dalam Pasal 378 KUHP dan Pasal 28 juncto Pasal 45 Undang-undang Nomor 19 tahun 2016 tentang Informasi dan Transksi Elektronik. Dimana tergantung dari penipuan digital dengan melakukan penanggulangan dari kementrian digital Komdigi melalui pola spoofing, masking, dan penyalahgunaan identitas pelanggan. Scam call atau panggilan penipuan terjadi melalui telepon, SMS, mesengger service, surat elektronik, dan saluran lain. Bahkan sebagai saran, pemerintah diminta membangun infrastruktur dan teknologi anti scam agar panggilan penipuan dengan menggunakan nomor masking, dan memanipulasi identitas nomor. Oleh karena itu, Pemerintah akan meminta operator membangun sistem anti scam dengan memanfaatkan teknologi, termasuk teknologi Kecerdasan Artifisial (Artifical Intelligence/AI), untuk mendeteksi dan melakukan pencegahan secara otomatis.

Corresponding Author:
Lestari Victoria Sinaga
Universitas Darma Agung
Medan, Indonesia
Missthary35@gmail.com

PENDAHULUAN

Hukum cyber merupakan suatu terobosan perkembangan teknologi dan keamanan data pribadi yang menjawab tantangan yang dihadapi pelanggaran hukum orang yang tidak bertanggung jawab, terhadap suatu provider dan perusahaan online untuk dijadikan untuk menipu.

Era digital saat ini sering sekali dijadikan para penipu untuk menguras keuntungan pribadi dengan sering mencaari nomor telepo dan menemukan panggilan yang tidak dikenal. Penipuan yang menggunakan data pribadi seseorang menjadi cara mendapatkan informasi. Penipuan biasanya terjadi ketika seseorang menyerahkan data pribadinya kepada suatu perusahaan yang menggunakan datanya untuk pinjam meminjam, kredit, utang dibank bahkan dalam pembelian pulsa.

Penggunaan Get contact dapat membantu mengidentifikasi dan mencegah modus nomor tidak dikenal. Aplikasi ini memiliki kelemahan tetapi masih memiliki potensi untuk berkembang dan memberikan pengalaman pengguna yang lebih baik di masa mendatang.

Metode User Experience Questionnaire (UEQ) digunakan dalam penelitian aplikasi GetContact untuk mengukur tingkat kepuasan pengguna dengan berbagai kriteria, seperti daya tarik, efisiensi, ketepatan, stimulasi, dan kebaruan. Hasil penelitian menunjukkan bahwa

aplikasi ini memiliki beberapa keuntungan dalam mendeteksi dan menghindari modus penipuan dengan nomor yang tidak dikenal, tetapi ada beberapa kelemahan yang perlu diperbaiki. Dengan nilai sebesar 0.69, ketepatan deteksi nama pada nomor telepon masih dapat ditingkatkan. Selain itu, fitur seperti daya tarik, efisiensi, stimulasi, dan kebaruan aplikasi kurang dari rata-rata. Meskipun aplikasi ini menawarkan kemampuan untuk mengakses informasi dan membantu pengguna menemukan nomor telepon, pengalaman pengguna kurang memuaskan.

Aplikasi GetContact, khususnya dalam hal memantau nomor telepon dengan aman dan mencegah penipuan smartphone. Izin akses yang berbahaya menurut pengalaman beberapa pengguna provider seperti Halo, Telkomsel, XL, Tri terhadap provider-provider yang tidak diberikan perlindungan bahkan penagih utang ilegal yang memblokir akses pinjama online ilegal di playstore.

Sebagai kegiatan sosial, masyarakat menganggap bahwa provider dan kementrian digital saat ini berfungsi sebagai media daya tarik untuk saling mengenal, saling memberi, saling membutuhkan, saling kunjung, dan sebagai media kerukunan. Sedangkan sebagai kegiatan ekonomi, aplikasi get contact sebagai aplikasi yang aman dalam mencegah penipuan smasrtphone. Pada dasarnya, yang terjadi disini adalah hutang piutang.

Namun saat ini kegiatan penipuan dengan cara meneror puluhan kali bukan lagi menjadi suatu kegiatan yang tabu di sebagian besar masyarakat. Dimana, masyarakat banyak mengeluh ditelepon puluhan kali diteror nomor penipu. Banyaknya kasus penipuan digital yang merugikan masyarakat. Dengan memperketat aturan bahwa wajib memverifikasi wajah untuk pendaftaran nomor baru agar pemilik nomor lebih bertanggungjwab.

Dirjen ekosistem digital kementrian komdigi menyebutkan sebesar 65 % pengguna selular mendapatkan SMS hingga telepon penipuan minimal satu minggu sekali pada tahun 2024. Diakui sebagai banyak termakan bujuk rayu penipu sehingga total kerugian dari penipuan mencapai Rp 7.000.000.000.000,- (tujuh triliun) pada tahun 2025. Tetapi yang mereport terjadinya loss dan scam ini diminta Kementrian ini mengambil kebijakan cepat mempersiapkan langkah-langkah mengurangi potensi dari penipuan berbasis seluler ini. Jadi untuk melindungi sampai scall menggunakan masking pakai nomor dalam negeri pakai teknologi SIP trunking keluar masuk lagi dengan nomor ter cover melalui MSS.

Lebih dari tujuh koma lima triliun, rekening diblokir yang berhasil diserang scam di Indonesia. Ironisnya hanya 5,4% nomor rekening yang berhasil dikembalikan. Ini menjadi kejahatan scam yan paling cepat dengan pola spoofing, masking dan penyalahgunaan identitas pelanggan. Penipuan ini terjadi melalui telepon, SMS, *messenger service*, surat elektronik, dan berbagai saluran lain. Pertanyaannya, bagaimana kita dapat mencegah hal ini?"

Pemerintah akan meminta operator membangun sistem anti *scam* dengan memanfaatkan teknologi, termasuk teknologi Kecerdasan Artifisial (*Artifical Intelligence*/AI), untuk mendeteksi dan melakukan pencegahan secara otomatis.

Menurutnya, sistem ini bertujuan untuk menghentikan panggilan palsu yang mengatasnamakan lembaga resmi atau perseorangan sebelum sampai ke pengguna.

"Operator harus melindungi pelanggan mereka. Mereka diminta membangun infrastruktur dan teknologi anti *scam* agar panggilan penipuan, termasuk yang menggunakan nomor *masking*, tidak lagi menjangkau pengguna internet.

Beberapa cara agar terhindar dari penyamaran nomor pelanggan yaitu: pertama cari proses registrasi *SIM card* masih memberi ruang bagi penyalahgunaan Nomor Induk Kependudukan (NIK) dan Nomor Kartu Keluarga (KK). Kedua, mencatat registrasi berbasis pengenalan wajah (*face recognition*) bersama Direktorat Jenderal Kependudukan dan Catatan

Sipil Kementerian Dalam Negeri. Ketiga, memiliki surat perjanjian. Setidaknya ada surat perjanjian antara penyelenggara dan anggota, hal ini dilakukan untuk meningkatkan kepercayaan dan minat bagi yang ingin bergabung.

Pasal 378 KUHP bisa menjadi dasar pengaduan dalam hal terjadi penipuan mengenai kejahatan penipuan secara umum. Pada arisan online, Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yaitu (1) Informasi Elektronik merupakan bukti hukum yang sah. (2) Informasi Elektronik sebagaimana pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia. Mengenai hal-hal yang dilarang dalam Undang-Undang ini terdapat pada Bab VII Pasal 27-37, kemudian ketentuan pidana terdapat pada Bab XI diatur Pasal yaitu Pasal 45-52.

Sistem pembuktian dalam kasus Scam ini menimbulkan kesulitan, dikarenakan lemahnya regulasi pengaturan penipuan arisan online membuat kasus ini semakin banyak terjadi. Selain itu, pemerintah juga masih belum mampu untuk melacak situs yang menjurus kepada penipuan arisan online. Sehingga untuk mengurangi kasus scam sangat sulit dilakukan. Hal lain yang menjadi kesulitan yaitu mencari alat bukti. Untuk mencari alat bukti dalam kasus penipuan arisan online yang menggunakan media elektronik melalui media sosial seperti facebook juga membutuhkan pihak yang kompeten di bidang media elektronik.

Untuk itulah pemerintah Indonesia sebelumnya telah menyusun Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang bertujuan agar pemanfaatan teknologi lebih teratur dan tidak digunakan semena-mena oleh masyarakat. Dalam penerapannya Undang-Undang ini masih dianggap belum maksimal dikarenakan banyaknya tindak pidana *cybercrime* yang diatur masih belum jelas pengaturannya dalam Undang-Undang.

Dalam praktiknya, yang berujung pada penipuan dapat dijerat melalui Pasal 378 KUHP sebagai tindak pidana penipuan. Selain itu, kegiatan arisan online juga kerap dikategorikan sebagai bentuk perhimpunan dana yang bersifat illegal karena tidak berada di bawah pengawasan lembaga keuangan resmi. Sebagaimana Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Tahun 2008 telah diubah menjadi Undang-Undang Nomor 19 Tahun 2016, turut memberikan dasar hukum terhadap tindakan penipuan yang dilakukan secara daring. Pasal 28 ayat (1) UU ITE menyatakan bahwa setiap orang dilarang menyebarkan informasi yang menyesatkan dan merugikan konsumen dalam transaksi elektronik. Hal ini memberikan ruang perlindungan hukum bagi korban arisan online yang dirugikan oleh penyelenggara.

Artikel ilmiah ini akan menjelaskan tentang bagaimana tanggung jawab pidana dan perdata oleh pelaku web phising dan upaya hukum dalam penanggulangan

METODE PENELITIAN

Metode penelitian yang digunakan adalah metode kualitatif yaitu cara menganalisis data yang bersumber dari bahan hukum berdasarkan kepada konsep, teori, peraturan perundang-undangan, doktrin, prinsip hukum, pendapat pakar atau pandangan peneliti sendiri.

HASIL PEMBAHASAN

A. Tanggung jawab Pelaku Penipuan Scam Call atau Penipuan Panggilan Online.

Penipuan online melalui media sosial menjadi salah satu kejahatan yang terjadi di era modern. Modus operandi yang sering dilakukan oleh pelaku kejahatan untuk dimanfaatkan kecanggihan teknologi dan popularitas media sosial sebagai sarana menjebak korban. Dalam

hal ini pelaku bisa berpura-pura sebagai penyelenggara arisan yang sah, namun pada akhirnya malah menipu para anggota dengan tujuan mencari keuntungan pribadi. Tanggung jawab hukum pelaku penipuan ini dapat dilihat dari beberapa aspek hukum antara lain:

1. Tindak pidana penipuan, dalam arisan online dapat dikenakan pasal KUHP yakni pasal 378 tentang penipuan yang menjelaskan bahwa setiap orang yang dengan maksud menguntungkan diri sendiri atau orang lain secara melawan hukum menyebabkan orang lain memberikan sesuatu, agar memperoleh keuntungan yang tidak dapat dikenakan pidana penipuan dan pelaku yang menjanjikan hadiah arisan namun tidak memenuhi janji tersebut dapat dikenakan pasal 378 KUHP yang mengatur tentang penipuan. Hukuman bagi pelaku penipuan berdasarkan pasal adalah penjara maksimal 4 tahun.
2. Tindak pidana penyalahgunaan program media sosial sesuai dengan undang-undang informasi dan transaksi elektronik (UU ITE) khususnya: pasal 27 ayat (3) UU ITE yang mengatur tentang larangan penyebaran informasi yang menyesatkan atau hoaks. Hal ini bisa menjadi dasar untuk menuntut pelaku, pasal 28 ayat (1)UU ITE yang melarang penyebaran berita bohong atau fitnah dapat merugikan pihak lain. Jika pelaku penipuan menyebarkan informasi palsu untuk menarik perhatian korban UU ITE Nomor 19 Tahun 2016 mengatur tentang penyebaran informasi bohong dan transaksi ilegal.

Kejahatan Siber (Cybercrime) atau kejahatan dunia maya merupakan tantangan serius bagi masyarakat dan berbahaya bagi individu atau organisasi yang menjadi korban.4 Kejahatan dunia maya juga dapat merugikan pribadi, organisasi, dan pemerintah, walaupun di satu sisi memberikan manfaat besar dalam hal efisiensi dan efektifitas, tetapi di satu sisi kejahatan dunia maya juga semakin meningkat. Namun bagaimana dengan individu atau perorangan atau pribadi yang menghadapi kejahatan siber atau korban kejahatan siber? Perlu untuk memahami dan meliti bagaimana jenis, analisis dan perkembangan kejahatan siber yang menyerang individu atau perorangan.

Cyber-terorisme merupakan aspek yang paling menonjol dari kejahatan dunia maya di seluruh negara. Dengan demikian keamanan dan keselamatan informasi telah menjadi tantangan utama saat ini. Dengan pertumbuhan pengguna yang pesat, kasus kejahatan dunia maya juga meningkat dan tidak dibatasi oleh batasan geografis atau batas negara di dunia. Ini merupakan masalah yang sangat memprihatinkan karena berdampak negatif langsung pada kehidupan ekonomi dan sosial masyarakat.

Pelanggaran privacy, akan muncul pertanyaan, bagaimana kepastian hukum untuk melindungi privasi seseorang termasuk data pribadinya. Fakta bahwa privasi memiliki hubungan yang sangat erat dengan martabat manusia, kebebasan dan kemerdekaan individu, dan itu semakin ditantang di era teknologi yang cepat perkembangan masyarakat informasi. Termasuk mengenai isu big data yang berhubungan dengan mekanisme pelestarian privasi yang dikembangkan untuk perlindungan privasi pada berbagai tahap (misalnya, pembuatan data, penyimpanan data, dan pemrosesan data) dari siklus hidup big data. Isu lainnya juga terkait dengan prinsip transparansi yang menjadi prinsip dasar untuk pemrosesan data di bawah Undang-undang Pelindungan Data Pribadi

Tabel 1. Perbedaan Spoofing dan phising

Fitur	Spoofing	Phising
Fokus utama	Peniruan identitas teknis. Pelaku berpura-pura menjadi entitas yang sah (misalnya, menggunakan domain	Penipuan untuk mendapatkan informasi sensitif. Pelaku memanipulasi korban melalui rekayasa sosial

	email atau alamat IP palsu) untuk membuat komunikasi terlihat asli	(misalnya, melalui email, SMS, atau telepon) agar memberikan data pribadi atau finansial.
Cara kerja	Menggunakan teknologi untuk membuat identitas palsu agar komunikasi tampak otentik.	Mengandalkan manipulasi psikologis dan emosional untuk membujuk korban agar bertindak.
Contoh	Email yang terlihat dikirim dari atasan Anda, tetapi alamat emailnya sebenarnya palsu.	Email dari "bank" yang meminta Anda mengklik tautan dan memasukkan detail login.
Tindakan korban	Korban mungkin tidak menyadari apa pun jika spoofing terjadi secara pasif. Namun, jika digabungkan dengan phishing, korban akan diminta melakukan tindakan.	Korban secara aktif diminta untuk melakukan tindakan, seperti mengklik tautan, mengunduh lampiran, atau memasukkan data.

Berikut beberapa jenis *phishing* yang perlu kamu waspadai:

1. **Email Phishing**: Mengirimkan email yang mengaku dari perusahaan atau institusi resmi.
2. **Spear Phishing**: Serangan yang ditargetkan secara khusus pada individu tertentu.
3. **Whaling**: Menargetkan individu penting seperti eksekutif perusahaan.
4. **Smishing**: Menggunakan pesan singkat (SMS) untuk menipu korban.
5. **Vishing**: Melakukan panggilan telepon untuk mendapatkan data pribadi korban.

Memahami perbedaan antara *spoofing* dan *phising* membantu kamu untuk lebih waspada. Dengan pengetahuan ini, kamu bisa melindungi diri dan data pribadi dari ancaman kejahatan siber. Kesadaran adalah langkah pertama untuk mencegah diri dari menjadi korban. Jangan mudah percaya dengan email atau pesan mencurigakan, dan selalu pastikan kamu memverifikasi sumber informasi sebelum bertindak.

Table 2. Kejahatan Siber terhadap Individu

Rekayasa sosial dan tipu daya	Pelecehan daring	Kejahatan terhadap identitas	Peretasan (hacking)	Penolaka layanan dan informasi

Ad.1 rekayasa sosial dan tipu daya melibatkan penerapan metode curang untuk memaksa individu dengan berperilaku cara tertentu. Oleh karena itu, penting bagi individu dan organisasi untuk meningkatkan kesadaran tentang serangan rekayasa sosial, mengenali tandatanda peringatan, dan menjaga kehati-hatian dalam berbagi informasi atau melakukan tindakan online.

Ad. 2 Pelecehan Daring serupa dengan jenis, yang lain dan menjelaskan contoh di mana orang yang daring merasa terganggu/dilecehkan dan disiksa oleh orang lain. Pelecehan daring, juga dikenal sebagai pelecehan online atau serangan siber, merujuk pada tindakan tidak pantas, ancaman, intimidasi, atau penindasan yang dilakukan melalui platform digital atau internet. Ini adalah bentuk kejahatan siber yang dapat berdampak negatif secara emosional, psikologis, dan sosial pada korban

Ad 3. Kejahatan Terkait Identitas adalah kejahatan yang dilakukan oleh seorang individu identitasnya dicuri atau disalahgunakan oleh orang lain untuk hal yang jahat atau tidak sah tujuan tertentu (misalnya, penipuan). Meskipun secara tradisional tidak dianggap sebagai kejahatan pribadi yang signifikan.

Ad. 4. Kejahatan Peretasan adalah kegiatan di mana seseorang (yaitu peretas) mengeksploitasi kelemahan dan kerentanan dalam suatu sistem untuk keuntungan atau kepuasan diri sendiri. Dengan semakin berkembangnya pergerakan dunia dari budaya offline ke online seperti aktivitas belanja, perbankan, berbagi informasi akses ke informasi sensitif melalui aplikasi web telah meningkat.

Ad. 5. Penolakan mengakomodasi Informasi merupakan tren baru ransomware yang serupa dengan menolak akses individu ke informasi mereka sendiri. Bagian selanjutnya menganalisis taksonomi dan masingmasing jenis kejahatannya secara rinci

B. Konsekuensi bagi pelaku Tindak Pidana Penipuan Online

Pelaku penipuan online dalam platform media sosial akan menghadapi beberapa konsekuensi hukum baik bentuk pidana maupun sanksi administratif:

1. Tindak pidana penipuan, pelaku bisa dikenai hukuman dalam kitab undang-undang pidana (KUHP) yakni pasal 378 KUHP tentang penipuan. Dengan hukuman penjara maksimal 4 tahun. Jika terbukti melakukan tindak pidana seperti penyebaran informasi palsu.
2. Selain pidana dipenjara, pelaku penipuan diwajibkan membayar ganti rugi kepada korban yang jumlahnya sesuai dengan kerugian dialami oleh korban. Hal ini dapat diajukan dalam gugatan perdata.
3. Pasal 45 A ayat (1) UU ITE menyatakan bahwa setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan dapat dikenakan pidana penjara paling lama 6 tahun atau denda 1 miliar.
4. Pasal 28 ayat 1 junco pasal 45 ayat 2 dengan berbunyi: setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik. Hukuman diberikan kepada pelaku tindak oidana ini dengan UU ITE dengan pidana penjara paling lama 6 tahun atau denda paling banyak 1 miliar.

C. Upaya penanggulangan penipuan online

Modus yang dilakukan dalam penipuan online dengan kedok lowongan kerja paruh waktu. Penelitian ini juga berangkat dari keprihatinan peneliti terhadap salah seorang rekan yang anaknya menjadi korban modus penipuan online berkedok kerja paruh waktu. Dengan kondisi ekonomi yang kekurangan saat ini korban harus menanggung beban hutang mencapai puluhan juta rupiah. Kondisi ini tentu sangat membebani korban, baik secara materil dan psikis. Di luar itu, informasi dalam penelitian ini diharapkan dapat terpublikasi sehingga dapat menambah wawasan masyarakat agar dapat mencegah terjadinya tindak kejahatan penipuan online. Dengan begitu setidaknya jumlah korban penipuan online tidak semakin bertambah.

Dalam menghadapi era keuangan digital ini pengembangan pengetahuan dan literasi keuangan digital menjadi faktor kunci untuk menjadi pribadi yang handal dalam memerangi kejahatan digital. Untuk itu OJK merancang materi edukasi yang dapat menjadi dasar menjadi pribadi yang handal dalam memerangi kejahatan digital.

KESIMPULAN

Jumlah aktivasi nomor baru per hari pada operator seluler rata-rata mencapai 500 ribu hingga satu juta, kebocoran identitas NIK dan Nomor KK masih terjadi, sehingga membuka peluang penyalahgunaan identitas dalam skala besar untuk target aktivasi *SIM card* secara tidak sah. Penipuan scam call melalui media sosial menjadi masalah serius di era modern yang saat ini berkembang pesat dengan pelaku yang menyamar sebagai penyelenggara arisan yang sah untuk menipu korban. Mereka mencari keuntungan pribadi. Tindak pidana penipuan sesuai pasal 378 KUHP yang menyatakan bahwa setiap orang yang dengan maksud menguntungkan diri sendiri menyebabkan orang lain memberikan sesuatu dapat dikenakan hukuman penjara maksimal 4 tahun.

Saran

1. Bagi pengguna layanan baru diharapkan dapat memahami bagaimana mempersiapkan kebijakan mendaftarkan informasi data pribadi nomor baru menggunakan face recognition.
2. Kasus arisan online ini belum ada aturan jelas yang mengatur dalam undang-undang jadi harapan penulis pemerintah bisa membuat aturan yang lebih jelas terhadap kasus ini seperti contohnya merevisi undang-undang ITE yang baru. Namun kasus arisan online ini juga seringkali dipidanakan tanpa memenuhi unsur-unsur pidana jadi harapan penuh juga untuk masyarakat harus lebih memahami unsur-unsur pidana dan perdata terlebih dahulu.

REFERENSI

CST Kansil,2004, Pokok-pokok Hukum Pidana, Pradnya Paramitha, Jakarta

Barda Namawi, Arief, 2001, Masalah Penegakan Hukum dan Kebijakan Penanggulangan Kejahatan, Citra Aditya Bakti, Bandung.

https://www.msn.com/id-id/berita/other/komdigi-ungkap-kerugian-akibat-kejahatan-siber-capai-rp-476-miliar-ai-diperkuat-untuk-cegah-ancaman-pada-ruang-digital/ar-AA1K9XuD?apiversion=v2&noservercache=1&domshim=1&renderwebcomponents=1&wcseo=1&batchservertelemetry=1&noservertelemetry=1#:~:text=Lebih%20lanjut%2C%20Wamen%20Nezar%20menyebut%20bahwa%20penipuan,akibat%20kejahatan%20siber%20mencapai%20Rp%20476%20miliar.

https://portal.komdigi.go.id/kanal-publik/berita-kini/9810

https://blog.unmaha.ac.id/perbedaan-spoofing-dan-phising-yang-perlu-kamu-pahami/#:~:text=Walaupun%20terdengar%20mirip%2C%20ada%20beberapa,tautan%20dan%20memasukkan%20data%20login.

Peraturan perundang-undangan

Kitab Undang-undang Hukum Pidana

Undang-undang Informasi dan Transaksi Elektronik Nomor 19 Tahun 2016