

Analisis Tindak Pidana Penipuan Online dalam Konteks Hukum Pidana Cara Menanggulangi dan Pencegahannya

Jason Aaron Riado Simanungkalit¹, Raihan Hertadi², Asmak ul Hosnah³

Universitas Pakuan, Indonesia

jasonsimanungkalit05@gmail.com¹, raihanheryadi2505@gmail.com²

Submitted: 13th February 2024 | **Edited:** 20th April 2024 | **Issued:** 01st May 2024

Cited on: Simanungkalit, J. A. R., Hertadi, R., & Hosnah, A. U. (2024). Analisis Tindak Pidana Penipuan Online dalam Konteks Hukum Pidana Cara Menanggulangi dan Pencegahannya. *AKADEMIK: Jurnal Mahasiswa Humanis*, 4(2), 281-294.

ABSTRACT

Fraud has been around for more than twenty centuries. The world continues to grapple with the devastating impact of financial crime. In this digital age, financial fraud is more sophisticated than ever. This article discusses the origins of fraud, its development, and technological advances in fraud prevention and security. In simple terms, fraud is deception with the intent to illegally gain financial advantage over a person or an entity. It refers to dishonest acts that deprive a person or entity of money or legal rights. Fraud requires the intentional misrepresentation of facts to convince someone to hand over money or property, unlike outright theft, which requires stealth or force. The crime of fraud is a form of crime that harms society financially and psychologically. This research aims to analyze various aspects related to fraud, including the motives of the perpetrators, the methods used, and the impact on victims and society. The impact of this crime is financially, emotionally, and psychologically detrimental to victims, and can undermine public trust in institutions and individuals. Through an in-depth understanding of the motives, methods, and impacts of fraud, this research contributes to the development of more effective prevention and law enforcement strategies. Preventive measures involving public education on the risks of fraud, increased legal awareness, and enhanced cooperation between law enforcement agencies and the private sector can be the first step in combating this phenomenon. In addition, strict and fair law enforcement against fraud perpetrators is also necessary to ensure justice for victims and minimize the possibility of similar crimes occurring in the future.

Keywords: Crime of Fraud, Fraud Countermeasures, Fraud

PENDAHULUAN

Bentuk-bentuk baru penipuan online telah menjamur, tampaknya dibantu oleh kemajuan teknologi, dan telah berhasil menguras rekening korbannya. Akses terhadap internet semakin mudah diakses akibat menjamurnya gadget elektronik berteknologi tinggi (Zabidin, 2021). Masyarakat di pedesaan atau pedesaan kesulitan mengakses internet dan memahami cara kerja teknologi, sehingga mereka hanya dapat menggunakan internet di kota-kota besar. Artinya, akses internet pada masa lalu sangat terbatas. Saat ini, individu dari semua lapisan masyarakat, baik perkotaan maupun pedesaan, memiliki

akses terhadap internet dan dapat memanfaatkannya untuk berbagai tujuan. Orang-orang dari segala usia, dari balita hingga nenek, kini dapat menemukan sesuatu yang berguna di dalamnya. Terdapat sedikit perbedaan antara penipuan tradisional dan insiden penipuan online. Penggunaan sistem elektronik menjadi satu-satunya pembeda dalam metode tindakannya. Karena tindakan yang dilakukan oleh mereka yang melakukan penipuan online berpotensi menimbulkan kerugian bagi orang lain (Takanjanji, 2020), maka hukum pidana secara tegas menyatakan aturan ini, dan sekali lagi, terdapat konsekuensi yang jelas bagi mereka yang melakukan kejahatan tersebut (Gultom, 2022). Manusia harus mengambil tindakan untuk memberikan gambaran menyeluruh tentang kehidupan manusia, karena hal ini terkait langsung dengan sifat kita sebagai makhluk hidup dan menggerakkan nilai-nilai inti kita.

Pemerintah harus meningkatkan kolaborasinya dengan perusahaan keamanan data, seperti perbankan dan keuangan, untuk memerangi penipuan digital dalam segala bentuknya (Silalahi, et al., 2022). Selain itu, cara terbaik untuk membuat masyarakat memikirkan isu-isu penting adalah dengan meningkatkan membaca dan pendidikan.

LANDASAN TEORI

Penipuan online merupakan salah satu bentuk kejahatan yang semakin marak seiring dengan perkembangan teknologi informasi dan komunikasi (Suardi, et al., 2022). Dalam konteks hukum pidana, penipuan online termasuk dalam tindak pidana yang diatur oleh Kitab Undang-Undang Hukum Pidana (KUHP) di Indonesia. Pasal 378 KUHP mendefinisikan penipuan sebagai tindakan menggunakan nama palsu, keadaan palsu, tipu muslihat, atau rangkaian kebohongan untuk menggerakkan orang lain menyerahkan barang, membuat utang, atau menghapuskan piutang. Dalam kasus penipuan online, modus operandi sering kali melibatkan penggunaan internet untuk menyebarkan informasi palsu atau untuk melakukan transaksi yang tidak sah (Bernoza, et al., 2020).

Penipuan online memiliki berbagai bentuk, termasuk phishing, scam, dan penipuan berkedok jual beli online (Sipahutar, 2021). Phishing adalah upaya mendapatkan informasi sensitif seperti kata sandi dan nomor kartu kredit dengan menyamar sebagai entitas tepercaya dalam komunikasi elektronik (Hasibuan & Sitompul, 2022). Scam biasanya melibatkan penawaran investasi palsu atau hadiah undian yang tidak pernah ada (Lestari, et al., 2023). Penipuan jual beli online sering terjadi di platform e-commerce, di mana

pelaku menawarkan barang dengan harga menarik namun tidak pernah mengirimkan barang tersebut setelah menerima pembayaran. Kejahatan ini sering kali menargetkan individu yang kurang waspada atau tidak memiliki pengetahuan yang cukup tentang keamanan digital (Wibisono & Mahanani, 2023).

Penanggulangan penipuan online memerlukan pendekatan terpadu yang melibatkan pemerintah, penyedia layanan internet, dan masyarakat. Pemerintah perlu memperkuat regulasi dan penegakan hukum terhadap kejahatan siber, termasuk penipuan online (Asriyani & Dwiyaniti, 2022). Selain itu, perlu adanya peningkatan kerja sama internasional mengingat sifat lintas batas dari kejahatan ini. Penyedia layanan internet dan platform e-commerce juga memiliki peran penting dalam mengidentifikasi dan mencegah aktivitas penipuan di platform mereka, serta memberikan edukasi kepada pengguna tentang cara melindungi diri dari penipuan (Rahmanto, et al., 2019).

Pencegahan penipuan online juga memerlukan upaya edukasi yang menyeluruh kepada masyarakat. Kampanye literasi digital yang mengajarkan pengguna internet tentang tanda-tanda penipuan, langkah-langkah pengamanan data pribadi, dan pentingnya verifikasi informasi sebelum melakukan transaksi online sangat penting (Zubaidah, et al., 2023). Selain itu, individu harus didorong untuk selalu menggunakan metode pembayaran yang aman dan waspada terhadap penawaran yang terlalu bagus untuk menjadi kenyataan. Kesadaran dan pengetahuan yang tinggi di kalangan masyarakat dapat secara signifikan mengurangi risiko menjadi korban penipuan online (Wahyudi, et al., 2022).

Secara keseluruhan, penipuan online merupakan tantangan serius dalam era digital yang memerlukan respons yang komprehensif dari berbagai pihak. Peningkatan regulasi, penegakan hukum, kerjasama antarnegara, dan edukasi masyarakat adalah kunci untuk menanggulangi dan mencegah tindak pidana ini. Hanya dengan usaha bersama kita dapat menciptakan lingkungan digital yang lebih aman dan terpercaya bagi semua pengguna.

METODE PENELITIAN

Untuk menggali sudut pandang para partisipan, penelitian kualitatif ini menggunakan taktik yang bersifat partisipatif dan mudah beradaptasi. Mencari tahu apa yang terjadi dari sudut pandang setiap orang merupakan tujuan dari kajian hukum normatif. Penelitian kualitatif adalah penelitian yang peneliti mempelajari keadaan suatu benda alam dengan memusatkan perhatiannya semaksimal mungkin pada hal-hal yang

diperlukan untuk penelitiannya, seperti survei lapangan dan pengamatan terhadap keadaan dinamis di lokasi tersebut. Jenis penelitian yang dipilih penulis adalah penelitian deskriptif. Penelitian deskriptif memungkinkan Anda mengeksplorasi suatu topik secara lebih mendalam dan menjelaskan fenomena dan peristiwa yang terjadi di masyarakat. Penelitian deskriptif juga dapat memberikan dan menjelaskan segala bentuk informasi dan fakta secara sistematis dan akurat.

HASIL PENELITIAN

“Misdrijven tegen de eigendom en de daaruit voortvloeiende zakelijk rechten” (kejahatan terhadap harta benda dan hak-hak lain yang berasal dari harta benda) adalah kata dalam bahasa Belanda yang berarti penipuan. Melakukan penipuan adalah dengan sengaja dan sengaja memanfaatkan kepercayaan orang lain dengan menampilkan diri sendiri secara tidak benar, dengan menggunakan intimidasi atau ancaman agar orang tersebut menyerahkan uang, harta benda, atau barang berharga lainnya (Pasal 378 KUHP)..

Penjahat yang terlibat dalam penipuan online bergantung pada infrastruktur teknologi untuk semua operasi mereka. Seperti bentuk penipuan tradisional, ide dasar di balik penipuan internet adalah seseorang mendapat keuntungan secara tidak sah sementara orang lain dirugikan. Penggunaan sistem elektronik (seperti komputer, internet, dan perangkat telekomunikasi) membedakan penipuan online dari bentuk penipuan yang lebih tradisional.

Penipuan memiliki 2 (dua) pengertian, yaitu: Pertama, adanya pengertian penipuan yang luas yang mencakup seluruh delik yang tercantum dalam KUHP pasal XXV. Kedua, adanya keterbatasan dalam pengertian penipuan yang mengacu pada bentuk utama dan bentuk khusus penipuan, yang umumnya disebut *oplichting*, yang masing-masing dituangkan dalam Pasal 378 dan 379. Pengertian penipuan (*oplichting*) sendiri tertuang dalam Pasal 378. Penipuan ada dalam arti terbatas dalam bentuk mitigasi tertentu, dan rumusan ini merupakan bentuk fundamentalnya. Hal ini dikenai sanksi sebagai penipuan kecil, khususnya berdasarkan Pasal 379, karena adanya fitur mitigasi yang luar biasa.

Penjahat yang terlibat dalam penipuan online bergantung pada infrastruktur teknologi untuk semua operasi mereka. Seperti bentuk penipuan tradisional, ide dasar di balik penipuan internet adalah seseorang mendapat keuntungan secara tidak sah sementara orang lain dirugikan. Penggunaan sistem elektronik (seperti komputer,

internet, dan perangkat telekomunikasi) membedakan penipuan online dari bentuk penipuan yang lebih tradisional. KUHP memperlakukan bentuk-bentuk penipuan tradisional sama dengan penipuan melalui internet. Ada hubungan erat antara perlindungan konsumen dan kejahatan penipuan. Hanya konsumen atau orang lain yang berada dalam situasi serupa yang dapat memperoleh manfaat dari perlindungan yang diberikan oleh Pasal 28 ayat (1).

Riset Nasional “Penipuan Digital di Indonesia: Modus, Medium, dan Rekomendasi” memaparkan realitas kejahatan siber di Indonesia. Studi yang menggunakan metode survei online dengan non-probability sampling ini menyurvei 1.700 orang dari berbagai kelompok demografi di 34 provinsi.

Berdasarkan temuan penelitian, lima bentuk penipuan yang paling umum adalah sebagai berikut: penipuan pinjaman digital (74,8% responden), skema hadiah palsu (91,2% responden), skema penipuan krisis keluarga (59,8% responden), dan penipuan skema investasi (56% responden). Di sisi lain, responden paling kecil kemungkinannya mengalami lima bentuk penipuan berikut: penipuan permohonan sekolah atau beasiswa (19,9%), pembajakan atau peretasan akun dompet digital (20,6%), penipuan bertema percintaan (27,7%), dan penipuan pribadi. pencurian identitas (29,2%).

Karena sering kali dikirimkan secara sembarangan dan dalam jumlah besar melalui berbagai media, terutama melalui fitur yang terkait pada masing-masing ponsel, responden paling sering menerima pesan palsu yang terkesan seperti hadiah (telepon atau SMS).

Evolusi teknik kriminal sejalan dengan kemajuan peradaban manusia pada saat ini. Manusia semakin berinteraksi satu sama lain melalui fasilitas teknologi digital, yang sejalan dengan pertumbuhan masyarakat dan teknologi. Media internet yang menggunakan sistem elektronik digunakan oleh hampir semua aktivitas komersial di dunia. Salah satu aspek kegiatan ekonomi adalah e-commerce, atau perdagangan melalui media online, yang melibatkan transaksi yang dilakukan melalui internet. Berkat kemajuan teknologi, dunia modern baru telah muncul: dunia internet. Di dunia ini, orang tidak lagi harus bertemu langsung secara fisik untuk menjalankan bisnis; sebaliknya, mereka dapat bertransaksi satu sama lain secara elektronik, tanpa memandang kedekatan fisik.

ada banyak cara penipu menipu korbannya. Penjahat sering kali memperoleh informasi sensitif untuk melakukan transaksi keuangan secara online. Sejumlah teknik umum yang digunakan penipu dalam transaksi online dirinci Kementerian Komunikasi dan Informatika (2021).

a. Phishing. Secara teknis, phishing adalah praktik penjahat dunia maya yang menyamarkan sebagai situs web terkemuka untuk mengelabui pengguna agar membocorkan informasi penting (Ghazi-Tehrani dan Pontell, 2021). Pelaku akan menyamarkan sebagai perwakilan resmi dari organisasi yang sah untuk melakukan penipuan jual beli online. Panggilan telepon, email, dan pesan media sosial adalah cara utama penjahat mencoba menghubungi korbannya. Korban phishing rentan informasi sensitifnya dicuri dan dimanfaatkan oleh penipu. Setelah mendapatkan informasi korban, pelaku akan memanfaatkannya untuk melakukan jual beli online.

b. Pharming. Salah satu metode melakukan penipuan, yang dikenal sebagai pharming, melibatkan pemalsuan nama domain situs web untuk mengelabui pengguna agar mengunjungi situs web jahat yang mencuri informasi sensitif (Prasad dan Rohokale, 2020). Dalam kasus ini, penjahat akan membuat nama domain untuk situs web korban yang sangat mirip dengan domain asli organisasi yang sah. Menginfeksi situs web palsu ini dengan malware memungkinkan penipu mencuri informasi pribadi sensitif dari pengguna yang tidak menaruh curiga. Penjahat akan menggunakan informasi yang dicuri untuk melakukan transaksi online palsu, sehingga menyebabkan kerugian pada korban.

c. Sniffing. Sebuah metode serba guna untuk melanggar keamanan jaringan, sniffing melibatkan pengumpulan data sensitif dari jenis lalu lintas jaringan tertentu (Alemayehu, 2021). Sniffing, dalam definisi paling mendasarnya, adalah serangan terhadap data sensitif, seperti penemuan kata sandi atau informasi identitas pribadi lainnya. Korban mungkin mengalami perilaku ini jika mereka menggunakan WiFi publik atau koneksi internet publik lainnya. Penggunaan koneksi internet publik, khususnya untuk transaksi keuangan, membuat korban rentan terhadap serangan sniffing. Untuk melakukan pembelian dan penjualan online menggunakan data yang dicuri, penjahat akan memanfaatkan informasi pribadi korban.

Kasus yang bisa diangkat dari sudut pandang ini antara lain yang melibatkan Satgas Waspada Investasi (SWI) yang membongkar skema penipuan yang menjerat mahasiswa

dan warga di IPB. Penipu menawarkan kerjasama di toko online korban dengan imbalan komisi 10% dari seluruh penjualan.

Tongam L. Tobing, Ketua Satgas Waspada Investasi, mengatakan, Kamis (17/11), pihaknya telah bertemu dengan pejabat IPB dan korban lainnya, termasuk mahasiswa, untuk mendapatkan informasi mengenai strategi penipuan tersebut. Tongam mengklaim bahwa pelaku meminta siswa untuk membeli barang dari toko internet pelaku. Pelaku akan mendesak korban untuk meminjam uang secara online jika kekurangan uang. Penjahat menyimpan hasil pinjaman untuk dirinya sendiri, atau barang tidak pernah sampai ke pelanggan, atau pembeli tidak pernah benar-benar membeli apa pun dari toko online penjahat.

Penjahat membujuk siswa untuk berinvestasi dengan berjanji membayar kembali pembayaran pinjaman pemberi pinjaman. Pelakunya gagal melakukan pembayaran pinjaman seperti yang dijanjikan, sehingga penagih mulai membebankan biaya kepada murid-muridnya sebagai peminjam. "Kasus ini bukan masalah pinjol, tetapi penipuan berkedok toko online dengan pembiayaan pembelian barang yang ternyata barangnya fiktif, tetapi uangnya mengalir ke pelaku," kata Tongam. Satgas Waspada Investasi telah bekerja sama dengan Polres Bogor dan Rektorat IPB untuk mengadili pihak-pihak yang bertanggung jawab atas penipuan ini.

Mengingat hal-hal di atas, sudah ditetapkan secara hukum bahwa perjanjian yang dibuat melalui Internet rentan terhadap penipuan. Hal ini disebabkan, tidak seperti transaksi tatap muka, pihak-pihak yang terlibat dalam transaksi online mungkin tidak saling mengenal sebelum melakukan transaksi. Jika melihat studi kasus di atas, maka hal tersebut termasuk dalam Pasal 1320 BW yang mengatur tentang syarat-syarat sahnya suatu perjanjian, antara lain; kesepakatan, kompetensi, bidang studi tertentu, dan alasan yang tidak dilarang. Oleh karena itu, sesuai dengan Pasal 1320 BW, apabila ada pihak yang melanggarnya, maka akan timbul akibat hukum, misalnya perjanjian itu batal demi hukum dan dapat dibatalkan. Dampak ini melampaui akibat hukum perdata yang telah disebutkan sebelumnya dan juga berdampak pada hukum pidana penipuan dan UU ITE yang berlaku di Indonesia.

Di Indonesia, UU ITE dan hukum pidana terhadap penipuan mempunyai dampak yang baik. Mengingat kejadian-kejadian di atas, jelas bahwa penipuan perjanjian jual beli online dapat dan memang terjadi. Misalnya, dalam kasus seperti ini, pembeli mungkin

sudah membayar barangnya, namun penjual mungkin membutuhkan waktu yang sangat lama atau bahkan tidak pernah sama sekali untuk mengirimkannya. sampai-sampai pembeli memutuskan untuk tidak memanfaatkan barang tersebut karena rusak atau tidak sesuai harapan, padahal barang itu sendiri belum pernah ada. Berdasarkan pertimbangan hukum tersebut di atas, salah satu potensi bahayanya adalah penipuan, yang mungkin timbul karena peserta transaksi jual beli online tidak saling mengenal dan tidak dapat bertemu langsung. Agar para pihak yang melakukan jual beli online tidak berpapasan secara sah, begitu pula dengan barang yang dipertukarkan. Oleh karena itu, ada kemungkinan penipuan saat membeli barang secara online.

Berikut peraturan perundang-undangan yang mengatur jual beli online di Indonesia: UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Peraturan perundang-undangan tersebut diketahui mengatasi permasalahan penipuan dalam perjanjian jual beli online. Namun kenyataannya, meskipun ada batasan hukum, penipuan belanja internet masih lazim terjadi di masyarakat. Hal ini disebabkan oleh kenyataan bahwa pihak berwenang yang berwenang untuk menegakkan undang-undang ini telah gagal total dalam upaya mereka untuk membendung gelombang masalah hukum umum yang mengganggu perdagangan online, terutama masalah penipuan yang banyak terjadi di sektor ini.

Dalam keadaan ini, pengguna yang melakukan penipuan pada forum atau situs belanja online dengan memberikan informasi palsu dan berbohong secara berulang-ulang untuk membeli suatu produk berarti melakukan tindak pidana penipuan dan melanggar ketentuan UU ITE sebagai berikut: “Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.” Dalam Pasal 45 ayat (1) dan (2) Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik diatur bahwa:

1. “Transaksi Elektronik yang dilakukan para pihak memberikan akibat hukum kepada para pihak;
2. Penyelenggaraan Transaksi Elektronik yang dilakukan para pihak wajib memperhatikan:

- a. iktikad baik;
- b. prinsip kehati-hatian;
- c. transparansi;
- d. akuntabilitas; dan
- e. kewajaran.”

Pasal 17–22 UU ITE mengatur tentang transaksi elektronik. UU ITE ini tidak secara khusus membahas persoalan penipuan transaksi elektronik. Namun menurut Pasal 28 ayat (1), pelanggar dapat dikenakan sanksi sebagai berikut “Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik”, “diancam dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1.000.000.000,00 (satu miliar rupiah).” Tujuan undang-undang ini adalah untuk menetapkan bukti-bukti yang dapat diterima untuk penyidikan, penuntutan, dan pemeriksaan pengadilan, dan informasi serta dokumen elektronik memenuhi definisi ini.

PP Nomor 71 Tahun 2019 mengatur tentang penyelenggaraan sistem dan transaksi elektronik, dan UU No. 19 Tahun 2016 mengubah UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang menjadi landasan utama pengaturan jual beli online. Walaupun permasalahan perjanjian jual beli melalui transaksi elektronik mempunyai kepastian hukum, namun peraturan mengenai transaksi elektronik sudah diketahui dengan baik. Meski demikian, masyarakat masih mudah tertipu saat berbelanja online, meski sudah ada undang-undang yang melarangnya. Secara khusus, permasalahan penipuan dalam jual beli online masih terus terjadi karena penegak hukum gagal menerapkan pembatasan hukum secara memadai untuk memperkirakan, mengoptimalkan, atau mengurangi timbulnya permasalahan hukum. Karena maraknya penipuan di pasar internet, penulis merasa terdorong untuk menyuarakan keprihatinan ini.

Masyarakat nampaknya sedang resah dengan maraknya kejadian penipuan akhir-akhir ini. Ada banyak cara untuk melakukan penipuan, dan salah satunya adalah praktik jual beli barang dan jasa secara online yang semakin umum dan meluas. Tampaknya mereka yang melakukan penipuan tidak lagi takut dengan konsekuensi yang mungkin menimpa mereka jika kesalahan mereka terbukti. Kenyataannya, para penipu kini semakin licik dalam melakukan pendekatan terhadap belanja online, dan sering kali mereka terlihat tidak meninggalkan jejak kejahatannya.

Maka dari itu, Berikut ada beberapa tips menghindarinya terutama tentang penipuan online, antara lain:

1. Hindari dan Periksa Panggilan dari Nomor Tidak Dikenal/Terdaftar

Kontak yang tidak terdaftar mungkin telah menghubungi Anda atau terus melakukannya sesekali; ini adalah bagian yang tidak bisa dihindari dalam penggunaan perangkat seluler. Biasanya, penipu akan menggunakan nomor telepon internasional dan menyamar sebagai orang yang dicintai atau rekan kerja untuk menipu Anda.

Jadi, sebaiknya abaikan saja atau tolak panggilan tersebut. Selain itu, penipu sering kali menggunakan identitas perusahaan atau lembaga pemerintah yang sah untuk mengirimkan komunikasi palsu melalui berbagai platform online.

Untuk menghindari hal tersebut, pastikan nomor tersebut milik pihak resmi terkait. Salah satu metode untuk melakukan ini adalah dengan menggunakan aplikasi pemeriksa nomor telepon. Anda bisa mendapatkan detail nomor tersebut melalui aplikasi ini.

Selain itu, Anda juga sering mendapat telepon dari pihak atau instansi resmi yang menggunakan nomor tidak berawalan +62. Tujuannya di sini adalah untuk membuatnya menonjol dari nomor palsu lainnya.

2. Jangan Bagikan Kode OTP Sembarangan

Meminta kata sandi satu kali (OTP) merupakan praktik yang biasa dilakukan saat Anda mendaftar ke layanan seperti jejaring sosial atau rekening bank. Tujuan dari kode One-Time Password (OTP) ini adalah untuk mengonfirmasi bahwa Anda adalah pengguna sah yang mendapatkan akses ke akun tersebut. Pasti ingin tidak ada orang lain yang dapat mengakses akun Anda, bukan? Anda dapat menghindari masalah dengan menyimpan kode OTP untuk Anda sendiri. Tujuan lain dari kode ini adalah untuk mendeteksi upaya tidak sah untuk mengakses akun Anda. Artinya, tidak seorang pun, bahkan kerabat dekat atau rekan kerja, boleh memiliki akses terhadap kode OTP. Kode yang Anda terima melalui email atau telepon datang dengan hati-hati untuk tidak mendistribusikannya karena hal ini.

3. Pasang Keamanan Dua Lapis (2FA)

Saat ini, sebagian besar aplikasi dan situs media sosial menggunakan Autentikasi Dua Faktor, yang menambah tingkat perlindungan ekstra. Tujuan utama dari sistem

keamanan ini adalah untuk menghentikan individu yang ceroboh mendapatkan akses ke akun individu. Agar autentikasi dua faktor ini berfungsi, sidik jari atau pengenalan wajah pengguna yang terdaftar harus dapat diakses. Langkah kedua pemilik akun memasukkan password atau PIN yang didaftarkan.

4. Unduh Aplikasi Resmi

Jika ingin aman saat berbelanja online, selalu unduh aplikasi resmi dari sumber terpercaya seperti App Store atau Google Play. Alasannya adalah karena beberapa taktik menipu saat ini menipu korbannya agar mengunduh aplikasi yang tidak disetujui. Pelaku kejahatan ini sangat kurang ajar bahkan sampai menggunakan nama lembaga pemerintah. Mereka sering menggunakan file APK. Budaya modern penuh dengan cara-cara seperti penipuan file APK melalui surat undangan, denda lalu lintas, dan banyak lagi.

5. Lakukan Pembayaran di Aplikasi Resmi dan Terpercaya

Pastikan untuk selalu membayar di dalam aplikasi saat Anda bertransaksi online, baik melalui e-commerce atau aplikasi lainnya. Jangan mentransfer sejumlah besar uang ke luar aplikasi. Anda menggunakan aplikasi e-commerce Y untuk membeli item X, misalnya. Setelah itu, vendor akan meminta Anda membayar menggunakan nomor non-aplikasi dan kemudian mengirimkan bukti pembelian secara terpisah dari aplikasi. Membatalkan pembelian segera adalah pilihan cerdas dalam situasi ini karena mungkin merupakan tanda penipuan online.

6. Jangan Mengeklik Link Secara Sembarangan

Sejak berkembangnya gadget masa kini, terjadi peningkatan signifikan dalam jenis penipuan online termasuk phishing. Dengan membuat tautan yang diberikan seolah-olah berasal dari situs resmi, metode phishing ini menipu korban agar mengeklik tautan tersebut. Jika Anda mengeklik tautan tersebut, penipu akan dapat mengakses informasi perbankan Anda dan data sensitif lainnya karena akan dikirim langsung ke sistem mereka. Maka dari itu berhati-hatilah dan jangan pernah sembarangan mengklik link yang diberikan oleh nomor atau orang asing ya!

7. Waspada dalam Mengisi atau Memberikan Data Pribadi

Sebagai praktik standar untuk verifikasi akses, pengguna sering kali diminta untuk memasukkan detail pribadi saat melakukan transaksi atau aktivitas online. Alamat email, kata sandi, nomor ID, tanda tangan digital, dan informasi keuangan (seperti

nomor kartu kredit atau kartu debit) adalah bentuk umum informasi identitas pribadi yang dicari. Orang yang rutin berbisnis atau mentransfer surat secara online mungkin akan merasakan manfaatnya. Itu sebabnya Kominfo merekomendasikan penggunaan Privy dan aplikasi bersertifikat lainnya. Pengiriman dokumen yang aman dan pembelian online menjadi mudah dengan fungsi PrivyPass Privy.

8. Gunakan Saluran Internet yang Aman

Area umum yang menyediakan WiFi atau internet gratis merupakan keuntungan besar. Sayangnya, ternyata cara koneksi tersebut seringkali berbahaya dan digunakan oleh para penipu. Sebagian besar jaringan WiFi publik tidak memiliki sistem keamanan yang kuat, sehingga menjadikannya sasaran empuk bagi peretas. Penyusup mungkin saja mengakses informasi pribadi Anda melalui server saat Anda menghubungkan perangkat ke internet dan melakukan transaksi atau aktivitas online lainnya.

9. Rutin Perbarui Sistem Perangkat

Virus atau perangkat lunak berbahaya lainnya dapat menginfeksi perangkat dan melancarkan serangan penipuan online. Karena virus ini mungkin menyulitkan untuk melihat atau bahkan mengambil data pribadi, virus ini dapat menimbulkan ancaman pada perangkat.

10. Kenali Ciri-Ciri Modus Penipuan Online

Terakhir, terus ikuti perkembangan fitur mode penipuan online terkini tanpa ketinggalan. Hal ini diperlukan untuk mencegah pengumpulan data pribadi yang dapat dieksploitasi oleh orang yang ceroboh.

a. Cek Rekening

Situs resmi Kementerian Komunikasi dan Informatika, yaitu rekening giro, berfungsi sebagai database rekening bank yang diyakini terkait dengan kejahatan dunia maya dan transaksi elektronik.

Adapun tahapan untuk melaporkan rekening pelaku penipuan online adalah sebagai berikut:

- Masukkan data nomor rekening yang ingin dilaporkan (dapat berupa nomor bank atau e-wallet).

- Masukkan biodata yang dilaporkan dan kategori tindak pidana yang dapat berupa penipuan online, narkoba dan obat terlarang, pemerasan, prostitusi online, pinjaman online, dan lainnya.
- Masukkan biodata pelapor.
- Jelaskan kronologi kejadian dan unggah bukti kronologi.

b. Aduan Nomor Kominfo

Ketika masyarakat merasa nomor ponselnya dieksploitasi untuk tujuan penipuan, mereka bisa mengunjungi situs resmi Kominfo ini dan mengajukan pengaduan. Tindakan yang mungkin dilakukan meliputi:

- Masukkan nomor seluler yang ingin dilaporkan.
- Pilih kategori pelaporan; apakah termasuk peniruan identitas, penipuan/fraud, investasi online fiktif, atau judi online.
- Isi biodata pelapor.
- Kronologi dan upload bukti kronologi.
- Melaporkan ke kepolisian

Anda dapat mendatangi kantor polisi yang paling dekat dengan TKP. Misalnya, jika Anda berada di suatu kecamatan, Anda dapat menghubungi Kepolisian Sektor (POLSEK) setempat untuk mengajukan pengaduan atas kejadian tersebut. Bisa juga mendatangi Wilayah administratif yang lebih tinggi, seperti POLRES, POLDA, atau MABes POLRI. Kumpulkan semua dokumentasi yang dapat Anda temukan, termasuk tangkapan layar obrolan Anda dengan penipu, gambar, rekaman audio, film, dan bukti pengiriman uang.

KESIMPULAN

Kejahatan di ranah digital merupakan sebuah kemungkinan nyata yang dimungkinkan oleh media baru sebagai teknologi yang memfasilitasi komunikasi melalui digitalisasi. Di antara jenis kejahatan dunia maya yang paling sering terjadi, penipuan keranjang belanja online baru-baru ini muncul sebagai masalah utama. Banyak pihak yang mengalami kerugian akibat penipuan, yang dapat terjadi karena berbagai sebab dan cara yang beragam. Anda dapat melindungi masyarakat dari pelaku penipuan belanja dan penjualan online dengan mempelajari berbagai metode yang mereka gunakan. Terdapat upaya *preventif* (non-penal) dan represif (penal) yang digunakan untuk mengurangi frekuensi penipuan transaksi online. UU ITE yakni Pasal 28 Ayat 1 dan KUHP khususnya

Pasal 378 mengatur tindakan represif dalam hal ini. Sedangkan upaya untuk meminimalisir tindak pidana pencurian dilakukan melalui pencegahan.

DAFTAR PUSTAKA

- Asriyani, A., & Dwiyaniti, A. (2022). Efektivitas kepolisian dalam melakukan penyelidikan tindak pidana penipuan online melalui media elektronik internet. *Jurnal Litigasi Amsir*, 56-60.
- Bernoza, A., Fadlan, F., & Nurkhotijah, S. (2020). Analisis Yuridis Tindak Pidana Penipuan Berbasis Jual Beli Online Di Kota Batam (Studi Penelitian Polresta Barelang). *Zona Hukum: Jurnal Hukum*, 14(3), 1-11.
- Gultom, K. F. (2022). Analisis Kriminologi Terhadap Pelaku Tindak Pidana Penipuan Dengan Modus Arisan Online (Studi Pada Kepolisian Resor Kota Besar Medan). *Jurnal Ilmiah Mahasiswa Hukum [JIMHUM]*, 2(1).
- Hasibuan, M. S., & Sitompul, M. N. (2022). Analisis Tindak Pidana Penipuan Jual Beli Tas Melalui Aplikasi Online (Studi Putusan PN Nomor 149/Pid. B/2017/PN LBP). *Jurnal Pendidikan Tambusai*, 6(1), 3901-3908.
- Lestari, D. N. A. M., Dewi, A. A. S. L., & Mahaputra, I. G. A. (2023). Penerapan Undang-Undang Nomor 11 Tahun 2008 Tentang ITE dalam Tindak Pidana Penipuan Love Scam. *Jurnal Analogi Hukum*, 5(1), 120-125.
- Rahmanto, T. Y., Kav, J. H. R. S., & Kuningan, J. S. (2019). Penegakan Hukum Terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik. *Jurnal Penelitian Hukum De Jure*, 19(1), 31.
- Silalahi, P. R., Daulay, A. S., Siregar, T. S., & Ridwan, A. (2022). Analisis Keamanan Transaksi E-Commerce Dalam Mencegah Penipuan Online. *Profit: Jurnal Manajemen, Bisnis dan Akuntansi*, 1(4), 224-235.
- Sipahutar, E. S. (2021). Analisis Hukum Atas Pertanggungjawaban Tindak Pidana Penipuan Arisan Online Menurut Undang-Undang Nomor 8 Tahun 2011 Tentang Informasi Dan Transaksi Elektronik (Studi Kasus No. 345/Pid. B/2017. Pn Tpg). *Jurnal Normatif*, 1(1), 18-26.
- Suardi, S., Asba, P., & Iksan, M. N. (2022). Penegakan Hukum Terhadap Pelaku Tindak Pidana Penipuan Investasi Melalui Media Internet. *Jurnal Litigasi Amsir*, 10(1), 72-83.
- Takanjanji, J. (2020). Merefleksi Penegakan Hukum Tindak Pidana Penipuan Online. *Widya Pranata Hukum: Jurnal Kajian dan Penelitian Hukum*, 2(2), 75-90.
- Wahyudi, D., Samosir, H. S., & Devi, R. S. (2022). Akibat Hukum Bagi Pelaku Tindak Pidana Penipuan Online Melalui Modus Arisan Online Di Media Sosial Elektronik. *JURNAL RECTUM: Tinjauan Yuridis Penanganan Tindak Pidana*, 4(2), 326-336.
- Wibisono, C. S., & Mahanani, A. E. E. (2023). Analisis Yuridis Terhadap Tindak Pidana Penipuan Dalam Transaksi Elektronik Melalui Media Sosial (Twitter). *JURNAL HUKUM, POLITIK DAN ILMU SOSIAL*, 2(2), 125-146.
- Zabidin, Z. (2021). Analisis Penegakan Hukum Tindak Pidana Penipuan Online Di Indonesia. *SPEKTRUM HUKUM*, 18(2).
- Zubaidah, S., Renggong, R., & Nur, M. (2023). ANALISIS HUKUM TERHADAP PENERAPAN SANKSI TINDAK PIDANA PENIPUAN ARISAN ONLINE DI KOTA MAKASSAR. *Indonesian Journal of Legality of Law*, 5(2), 502-507.