Vol 8 No 3, November 2024
Halaman: 167 – 173

Jurnal Pengabdian Papua
ISSN 2550-0082
e-ISSN 2579-9592

EDUKASI BAHAYA MODUS KEJAHATAN *SOCIAL ENGINEERING*

Thresia Hilda M.Y. Krey*, Winna A.A. Senandi

Fakultas Hukum, Universitas Cenderawasih, Jayapura

Alamat korespondensi:
Fakultas Hukum, Kampus UNCEN-Waena, Jl. Kamp. Wolker Waena, Jayapura Papua. 99358. Email: krey.hilda@gmail.com
*koresponden author

ABSTRACT

Social engineering is a cyber crime that involves the perpetrator using an individual's mistake or carelessness to steal important confidential data or information such as personal information, passwords, financial data, or accessing a computer system in an unauthorized way. Perpetrators usually use psychological tricks so they can easily trick other people and make others unaware even through communication tools because the perpetrators take advantage of someone's reaction when planning their attack. This outreach activity with the title "Education on the Dangers of Social Engineering Crime Modes" was carried out at Abepura Adventist Elementary and Middle School with the target participants being school children and teenagers. This outreach activity is carried out with the target of school children to provide an understanding of the dangers of the social engineering crime mode and the various actions that need to be taken so that we avoid the social engineering crime mode, as well as legal steps that can be taken if we are caught in the social engineering crime mode. During the activity, the enthusiasm of the participants was visible, especially when providing responses during the question and answer session at the end of the activity. It is hoped that this activity will be useful for the participants so that they can act as a relay for other communities to spread and understand the dangers of the social engineering information crime mode, and also as an indirectly useful effort to protect the people in Jayapura City.

Manuskrip:
Diterima: 25 September 2024
Disetujui: 25 Oktober 2024

Keywords: *cybercrime; cyberspace; social engineering; social media; ITE law*

PENDAHULUAN

Era digital yang berkembang pesat saat ini selain memberikan banyak kemudahan dalam berbagai aktivitas digital, juga memberikan ancaman berupa tantangan yang serius bagi keamanan informasi dan privasi pengguna. Salah satu ancaman siber yang semakin meresahkan adalah kejahatan dengan modus social engineering. Kejahatan ini melibatkan teknik psikologi dan rekayasa sosial untuk memanipulasi seseorang dengan tujuan memperoleh akses tanpa izin atau informasi rahasia. Maraknya serangan social engineering memunculkan kekhawatiran baru dalam dunia siber, mengingat modus ini menargetkan beberapa orang tertentu yang rentan terhadap manipulasi (Universitas Bakrie, 2024).

Dalam SANS InfoSec Reading Room, Social Engineering merupakan ancaman yang sering diabaikan namun dapat dieksploitasi setiap saat, untuk mengambil kesempatan dari adanya kelemahan di dalam sebuah jaringan keamanan, yaitu manusia atau pengguna dari sistem itu sendiri. Dimana dari dulu manusia atau pengguna dianggap sebagai bagian terlemah dalam sebuah keamanan jaringan (Allen, 2007). Seperti yang juga dikemukakan oleh Prof. Richardus Eko Indrajit, Kepala ID-SIRm, bahwa dalam dunia keamanan jaringan ada prinsip yang berbunyi "kekuatan sebuah rantai tergantung dari atau terletak pada sambungan yang terlemah" atau dalam bahasa asingnya "*the strength of a chain depends on the weakest link*". Pada berbagai buku keamanan jaringan juga selalu mengemukakan "*People is the weakest link*" atau "manusia adalah komponen yang terlemah" (Rafizan, 2011).

Social engineering adalah suatu teknik pencurian data atau informasi penting dan

berharga dari seseorang dengan menggunakan pendekatan interaksi sosial. Dengan kata lain social engineering adalah suatu teknik serangan yang mengeksploitasi kelemahan manusia. Social Engineering terbagi menjadi dua, yaitu berbasis interaksi sosial dan berbasis interaksi komputer. Pada jenis berbasis interaksi sosial, penyerang menggunakan teknik komunikasi yang sangat baik untuk menipu korbannya. Pada jenis yang berbasis interaksi komputer penyerang biasanya menggunakan beberapa metode seperti Phishing, Malvertising, dan Phone scams (Indrajit, 2016).

Kelemahan manusia yang dieksploitasi pada modus kejahatan social engineering biasanya berupa :

1) Rasa Takut– jika seorang pegawai atau karyawan dimintai data atau informasi dari atasannya, polisi atau penegak hukum yang lain, biasanya yang bersangkutan akan langsung memberikan tanpa merasa sungkan;
2) Rasa Percaya– jika seorang individu dimintai data atau informasi dari teman baik, rekan sejawat, sanak saudara, atau sekretaris, biasanya yang bersangkutan akan langsung memberikannya tanpa harus merasa curiga;
3) Rasa Ingin Menolong– jika seseorang dimintai data atau informasi dari orang yang sedang tertimpa musibah, dalam kesedihan yang mendalam, menjadi korban bencana, atau berada dalam duka, biasanya yang bersangkutan akan langsung memberikan data atau informasi yang diinginkan tanpa bertanya lebih dahulu (Ahmadian & Sabri, 2021).

Social engineering dilakukan dengan menggunakan kesalahan atau kecerobohan individu untuk mencuri data atau informasi penting yang konfidensial. Para pelaku social engineering dengan mudah bisa memperdaya orang lain dan membuat orang lain tidak sadar bahkan melalui alat komunikasi sehingga orang bisa secara tidak sadar memberikan informasi penting, menyebarkan sesuatu yang tidak seharusnya, atau bahkan memberi akses ke sistem alat komunikasi yang digunakan.

Pelaku menggunakan trik psikologi untuk memanipulasi korban sehingga korban melakukan hal yang diinginkan dengan memanfaatkan reaksi korban. Teknik ini didasarkan pada pemanfaatan sifat manusia yang rentan terhadap pengaruh sosial dan emosional, seperti rasa percaya, ketergantungan, atau kurangnya kewaspadaan. Serangan social engineering biasanya dilakukan untuk mencuri informasi pribadi, kata sandi, data keuangan, atau mengakses sistem komputer dengan cara yang tidak sah. Modus social engineering bisa melibatkan komunikasi secara langsung, seperti percakapan telepon atau tatap muka, atau melalui komunikasi digital seperti email, pesan teks, atau media sosial.

Beberapa contoh kejahatan modus social engineering yang sering terjadi di Indonesia, antara lain:

1) Undangan Pernikahan Palsu dan Surat Tilang berbentuk File APK, yaitu modus penipuan yang terjadi melalui permintaan untuk mengklik sebuah file undangan pernikahan berformat APK melalui aplikasi chat WhatsApp (WA). Melalui aplikasi bodong (tidak resmi) tersebut, membuat korban dengan sadar memberikan persetujuan untuk mengizinkan aplikasi tersebut mengakses SMS dan apilikasi lain di handphone. Kejahatan pun dapat terjadi karena data transaksi perbankan (kode OTP) yang bersifat pribadi dan rahasia dikirimkan melalui sms. Sehingga transaksi perbankan dapat berjalan dengan sukses.
2) Iklan Palsu di Sosial Media, yaitu modus akun palsu di media sosial yang mengatasnamakan bank yang membagikan iklan dengan ciri-ciri seperti, nama akun tidak lazim dan tidak centang biru; tampilan visual tidak kredibel mulai dari kualitas gambar yang buruk, penulisan tidak profesional, serta link bio mencurigakan. Jika meng-klik link tercantum akan diarahkan untuk mendaftar dan mengisi data-data perbankan yang bersifat rahasia seperti nomor kartu, PIN, OTP, dan sebagainya.
3) Link Modus Perubahan Tarif, yaitu modus penipuan jenis ini biasanya menggunakan platform WhatsApp (WA). Bedanya, file yang dikirimkan berupa pengumuman/pemberitahuan agar nasabah melakukan perubahan tarif. Biasanya dalam pengumuman tersebut berisi ancaman yang membuat nasabah resah/takut sehingga langsung mengklik file APK yang dikirimkan. File APK itu kemudian terinstall dalam ponsel korban sehingga pelaku dapat mencuri semua informasi yang terdapat dalam ponsel korban.
4) File foto berbentuk APK Bodong, yaitu layaknya modus undangan pernikahan dan surat tilang, namun kali ini berbentuk image atau gambar yang berupa file APK. Biasanya

pelaku mengaku sebagai kurir pengantar paket dan seakan-akan memberi informasi paket dapat terlihat setelah meng-klik file yang berformat APK namun terlihat seperti file foto tersebut (Kompas.com, 2023).

Pentingnya memberikan pemahaman mendalam kepada masyarakat terkait akan bahaya modus kejahatan social engineering yang marak beredar di tengah msyarakat karena:

1) Masih banyak orang yang terjebak dengan modus kejahatan social engineering;
2) Masih ada orang yang belum memahami cara pencegahan agar terhindar dari modus kejahatan social engineering;
3) Orang yang terjebak dalam modus kejahatan social engineering belum memahami langkah yang sebaiknya segera dilakukan untuk mengamankan informasi ataupun langkah hukum untuk menjerat pelaku.

Sehingga nantinya kegiatan ini dapat memberi manfaat untuk mengedukasi masyarakat agar terhindar dari pencurian informasi maupun data pribadi dengan modus kejahatan social engineering. Kegiatan ini juga menjadi upaya yang secara tidak langsung dapat melindungi masyarakat dari kejahatan siber yang semakin banyak.

METODE PELAKSANAAN

Kegiatan ini dilakukan dalam bentuk penyuluhan hukum tentang “Edukasi Bahaya Modus Kejahatan Social Engineering” kepada siswa-siswi SD-SMP Advent Abepura.

Gambar 1. Pemaparan materi pengabdian.

Metode yang digunakan adalah ceramah dengan melakukan pemaparan materi dan diskusi dengan peserta penyuluhan. Metode ini digunakan untuk memberikan pemahaman yang lengkap kepada peserta penyuluhan.

Sebelum sebelum sosialiasi dilakukan, para peserta diberikan pertanyaan terkait definisi modus kejahatan social engineering untuk melihat sejauh mana mereka memahami materi penyuluhan yang akan disampaikan. Setelah itu, tim penyuluh mulai memberikan pemahaman mengenai modus kejahatan social engineering secara mendalam berikut cara pencegahan agar terhindar dari modus kejahatan ini. Selain itu, tim penyuluh juga memberikan edukasi mengenai tindakan yang dapat dilakukan apabila sudah terlanjur terjebak dalam modus kejahatan social engineering, serta aturan hukum yang berlaku guna melawan modus kejahatan ini.

Gambar 2. Salah satu peserta sedang bertanya

Kegiatan ini merupakan upaya preventif terhadap modus kejahatan social engineering yang saat ini marak tersebar di seluruh platform media sosial yang dapat menjadi jebakan sehingga merugikan penggunanya. Dengan menanamkan edukasi mengenai bahaya modus kejahatan social engineering sejak dini kepada anak dan remaja, diharapkan mereka dapat bergerak menjadi penerus informasi ini kepada lingkungan sekitarnya, baik teman, keluarga, ataupun masyarakat di lingkungannya sehingga semakin banyak orang yang dapat memahami dan mengerti akan bahaya dari modus kejahatan social engineering.

HASIL DAN PEMBAHASAN

Kegiatan penyuluhan hukum di SD-SMP Advent Abepura dilaksanakan pada hari Kamis

sesudah ibadah pagi dalam rangka ulang tahun sekolah dengan peserta siswa-siswi SD kelas 4 hingga kelas 6 serta siswa-siswi SMP kelas 7 hingga kelas 9.

Materi diberikan dalam bentuk seminar dengan alat bantu Powerpoint yang berisikan materi dan contoh-contoh sehingga peserta menjadi tertarik dan bersemangat mengikuti kegiatan penyuluhan tersebut. Selain itu tim penyuluh juga menunjukkan berbagai sanksi hukum yang dikenakan pada pelaku sesuai dengan peraturan perundang-undangan yang berlaku. Materi selama kegiatan dapat diterima dengan baik oleh para peserta. Hal ini ditunjukkan dengan sikap antusiasme mereka selama mengikuti kegiatan penyuluhan hukum dengan memberikan tanggapan dan respon yang positif.

Hal tersebut menjadi indikator bahwa peserta penyuluhan memahami bahwa edukasi mengenai bahaya modus kejahatan social engineering sangat dibutuhkan karena apabila kurang berhati-hati maka dengan mudah siapa saja bisa terjebak dengan modus kejahatan ini.

Berikut ini adalah pokok materi penyuluhan yang diberikan kepada peserta, yaitu :

A. Bahaya Modus Kejahatan Social Engineering

Social engineering adalah suatu metode memanupulasi psikologis korban yang dilakukan oleh hacker atau penyerang dengan bertujuan untuk mendapatkan akses atau rahasia individu, organisasi bisnis, maupun perangkat atau sistem endpoint. Lain hal dengan peretasan yang menggunakan metode teknis seperti virus komputer malware dan sebgainya, social engineering lebih mengedepankan sisi interaksi terhadap sesama manusia serta memanfaatkan alamiah manusia untuk mempercayai atau memberikan informasi pribadi. Penyerang yang menggunakan social engineering akan berusaha memanipulasi si korban dengan cara-cara tertentu, seperti memanfaatkan rasa takut si korban, mudah percaya, atau ketidaktahuan si korban (Prima Cyber Solusi, 2024).

Otoritas Jasa Keuangan menyebut dalam wawancaranya dengan CNBC Indonesia bahwa Social Engineering menggunakan manipulasi psikologis, dengan memengaruhi pikiran korban melalui berbagai cara dan media yang persuasif dengan cara membuat korban senang atau panik sehingga korban tanpa sadar akan menjawab atau mengikuti instruksi pelaku (CNBC, 2023).

Gambar 3. Foto bersama seluruh peserta kegiatan.

Tujuan utama dari serangan social engineering adalah mendapatkan akses ke informasi rahasia, seperti kata sandi, nomor kartu kredit, atau data identitas pribadi. Penyerang menggunakan informasi ini untuk kepentingan pribadi, seperti pencurian identitas, penipuan finansial, atau akses ilegal ke sistem komputer. Serangan social engineering mengandalkan kelemahan manusia dalam hal kepercayaan dan pola pikir. Penyerang biasanya mencoba membangun hubungan percaya dengan korban mereka, seringkali dengan menyamar sebagai seseorang yang berwenang atau memiliki kebutuhan mendesak. Mereka menggunakan manipulasi emosi dan teknik psikologis untuk mengendalikan tindakan korban dan memperoleh informasi yang mereka cari (Elitery, 2024).

Penyerang merencanakan strategi dengan mengumpulkan informasi tentang latar belakang dan tempat kerja korban, kemudian menyusup dengan menjalin hubungan atau memulai interaksi, dimulai dengan membangun kepercayaan korban. Kemudian, penyerang akan mengeksploitasi korban setelah kepercayaan terbentuk dan kelemahan mereka terlihat. Setelah korban dieksploitasi, penyerang akan memutuskan hubungan setelah korban melakukan tindakan yang diinginkan. Proses ini dapat berlangsung dalam satu kali interaksi email atau selama berbulan-bulan dalam serangkaian obrolan di media sosial. Namun, pada akhirnya, serangan akan diakhiri setelah

korban melakukan tindakan yang diharapkan penyerang. Hal itu seperti membagikan informasi pribadi atau memaparkan malware pada sistem device mereka.

Modusnya bisa bermacam-macam, salah satu yang paling sering adalah dengan menelepon calon korban dan mengatakan kalau salah satu anggota calon korban tersebut tertimpa masalah entah itu tertangkap karena narkoba, kecelakaan dan lain sebagainya, sehingga membutuhkan uang. Contoh lainnya adalah, penipu menelpon calon korban dan mengaku sebagai karyawan bank dan menawarkan hadiah tertentu. Syaratnya, korban harus memberitahukan informasi-informasi penting, seperti nomor kartu kredit, nomor ATM, username hingga PIN (Prima Cyber Solusi, 2024).

Beberapa jenis modus kejahatan social engineering, antara lain:

1) Phishing, yaitu pengiriman pesan palsu yang tampaknya berasal dari sumber tepercaya untuk memancing informasi pribadi atau mengarahkan pengguna untuk mengklik tautan berbahaya, seperti menggunakan SMS, WhatsApp, dan sosial media lainnya.
2) Pretexting, yaitu modus kejahatan yang dilakukan penyerang dengan menciptakan alasan atau skenario palsu untuk meminta informasi rahasia dari korban. Pretexting biasanya dilakukan dengan membuat cerita palsu/fiksi untuk mendapatkan informasi dari korban, seperti menyamar sebagai orang terdekat seperti teman semasa kecil atau saudara jauh yang sudah lama tidak berkomunikasi.
3) Impersonation, yaitu teknik manipulasi social engineering dengan teknik menyamar sebagai salah seorang yang memiliki otoritas atau status dengan tujuan untuk mendapatkan akses informasi penting si korban. Contohnya adalah pelaku mengaku sebagai polisi atau aparat yang berwenang. Modusnya adalah menginformasikan bahwa terjadi sesuatu terhadap keluarga dekat sang korban –seperti kecelakaan, ditangkap polisi, dll, serta harus segera mengirimkan sejumlah uang untuk dapat diselamatkan.
4) Quid Pro Quo, yaitu kejahatan yang dilakukan penyerang dengan menawarkan imbalan atau bantuan palsu kepada korban dalam pertukaran informasi rahasia. Misalnya, penyerang dapat mengklaim bahwa mereka adalah staf teknis yang membantu memperbaiki masalah komputer, tetapi sebenarnya mereka mencoba mendapatkan akses ke jaringan korban. Atau berpura-pura menyamar sebagai karyawan dari suatu bank dan meminta informasi pribadi perbankan si korban, dengan imbalan apabila si korban sukarela memberikan informasinya, akan diberikan hadiah yang tidak sebanding dengan informasi pribadi yang berharga milik si korban.
5) Baiting, yaitu kejahatan dengan melibatkan penggunaan insentif atau daya tarik untuk memikat korban melakukan tindakan yang tidak aman. Misalnya, penyerang dapat meninggalkan USB drive yang terinfeksi dengan malware di tempat umum dan menunggu seseorang untuk menghubung-kannya ke komputer mereka.
6) Dumpster Diving, yaitu kejahatan melibatkan penyerang yang mencari informasi rahasia atau bahan yang tidak aman dengan menjelajahi sampah atau dokumen yang dibuang oleh sebuah organisasi. Informasi seperti faktur, surat, atau catatan penting sering kali dibuang secara sembarangan dan dapat dimanfaatkan oleh penyerang.

Adapun dampak dan risiko dari modus kejahatan Social Engineering, adalah sebagai berikut:

1) Kehilangan Data Pribadi: Penyerang dapat menggunakan informasi pribadi yang diperoleh dari serangan untuk melakukan pencurian identitas atau penipuan finansial.
2) Kompromi Keamanan Sistem: Jika penyerang berhasil mendapatkan akses ke sistem, mereka dapat mencuri atau merusak data penting, mengakibatkan kerugian finansial atau reputasi yang serius.
3) Penipuan Finansial: Informasi keuangan korban dapat digunakan untuk melakukan transaksi yang tidak sah atau mengakses rekening bank mereka.

Berdasarkan data OJK, sejak tahun 2013 hingga 31 Mei 2023, OJK telah menerima aduan terkait modus penipuan berupa skimming, phising, social engineering dan sniffing sebanyak 72.618 (6,5% dari seluruh aduan yang masuk sebanyak 1.116.175 layanan. Adapun untuk investasi illegal, kerugian yang dialami masyarakat akibat investasi ilegal sejak 2018 hingga 2022 telah mencapai Rp126 triliun (OJK, 2023).

B. Cara Menghindari Jebakan Modus Kejahatan Social Engineering

Beberapa cara yang dapat dilakukan agar tidak terjebak dalam modus kejahatan Social Engineering, antara lain:

1) Tidak memberikan informasi sensitif dan informasi rahasia pribadi secara berlebihan ke dunia maya, khususnya media sosial.
2) Berhati-hati dan tidak mudah mengklik tautan yang mencurigakan, baik itu di email maupun internet secara umum.
3) Langsung menghubungi pihak bank melalui kontak official yang tersedia apabila memiliki pertanyaan maupun keluhan. Banyak penipu yang berpura-pura menjadi pihak bank untuk menghubungi korban yang komplain melalui media sosial.
4) Tidak menanggapi telepon spam dari nomor yang tidak dikenal.
5) Selalu mengkonfirmasi kepada individu terkait apabila ada teman mengirimkan pesan permohonan peminjaman uang dalam jumlah besar. (Lintasarta, 2023)

C. Langkah Hukum apabila Terjebak Modus Kejahatan Social Engineering

Apabila sudah terjebak atau menjadi korban dari modus kejahatan Social Engineering, maka yang perlu dilakukan untuk meminimalisir kerugian yang diderita, yaitu:

1) Segera lapor ke Bank terkait apabila ada transaksi yang tak dikenal di rekening anda. Bisa datang langsung ke Bank, atau telepon call-center Bank terkait untuk memblokir rekening sementara.
2) Lapor polisi untuk diproses lebih lanjut.
3) Ajukan pengaduan di website https://aduannomor.id/home terkait nomor telepon yang digunakan dalam penipuan online maupun iklan spam.
4) Ajukan pelaporan melalui https://cekrekening.id untuk melapor rekening bank yang digunakan penipu. (Kompas.com, 2022).

Adapun sanksi hukum yang dapat dikenakan kepada pelaku tindak pidana modus kejahatan Social Engineering, yaitu:

1) Pasal 378 Kitab Undang-Undang Hukum Pidana, yaitu:

"Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan menggunakan nama palsu atau martabat palsu; dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang maupun menghapuskan piutang, diancam, karena penipuan, dengan pidana penjara paling lama 4 tahun".

2) Pasal 45A Ayat 1 Undang-Undang ITE, yaitu:

"Setiap orang yang dengan sengaja mendistribusikan dan/atau mentransmisikan informasi elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan yang mengakibatkan kerugian materiel bagi konsumen dalam transaksi elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu milyar rupiah).

KESIMPULAN

Modus kejahatan social engineering perlu diwaspadai karena apabila sudah terlanjur terjebak, maka dapat membahayakan dan merugikan korban, yaitu; korban dapat kehilangan data pribadi, sistem keamanan terancam, dan dapat tertipu jebakan finansial.

Jangan memberikan informasi sensitif dan rahasia pribadi ke dunia maya, serta selalu waspada dan berhati-hati apabila menerima pesan yang mencurigakan. Tidak perlu menanggapi telepon spam dari nomor yang tidak dikenal. Segera hubungi pihak berwajib, baik bank ataupun polisi, apabila terdapat transaksi mencurigakan, dan selalu lakukan konfirmasi kepada individu terkait apabila ada teman atau kenalan mengirimkan pesan mencurigakan.

UCAPAN TERIMA KASIH

Puji syukur kami panjatkan kepada Tuhan Yang Maha Esa, atas terselesainya kegiatan pengabdian yang berjudul "Edukasi Bahaya Aplikasi Pinjaman Online Ilegal". Untuk itulah kami memberikan ucapan terima kasih dan penghargaan yang tulus kepada:

1. Ibu Prof. Dra. Rosye H.R. Tanjung, M.Sc.,Ph.D, selaku Ketua Lembaga Penelitian dan Pengabdian Kepada Masyarakat (LPPM) Universitas Cenderawasih;
2. Bapak Prof. Dr. Frans Reumi, S.H., M.A., M.H. selaku Dekan Fakultas Hukum Universitas Cenderawasih;

3. Ibu Erlin Suebu, S.Pd. selaku kepala sekolah SD-SMP Advent Abepura.

DAFTAR PUSTAKA

Ahmadian, H., dan Sabri, A. 2021. Teknik Penyerangan Phishing pada Social Engineering mengunakan SET dan Pencegahannya. *Jurnal Dharmawangsa Djtechno: Journal of Information Technology Research,* 2(1), 13-20.

Allen, M. 2007. Social Engineering: A Means to Violate a Computer System. https://www.sans.org/white-papers/529/

CNBC Indonesia. 2022. Bahaya Soceng! OJK Warning Jangan Balas Whatsapp dan SMS Ini, https://www.cnbcindonesia.com/tech/20221104071529-37-385076/bahaya-soceng-ojk-warning-jangan-balas-whatsapp-dan-sms-ini

Indrajit, P.R. 2016. Keamanan Informasi dan Internet. Penerbit Preinexus. Yogyakarta.

Kitab Undang-Undang Hukum Pidana

Kompas.com. 2023. Kenali Modus-Modus Penipuan Social Engineering dan Tips Mencegahnya, https://www.kompas.tv/ekonomi/436458/kenali-modus-modus-penipuan-social-engineering-dan-tips-mencegahnya?page=all

Listasarta Cloudeka. 2023. Social Engineering: Pengertian, Jenis, dan Cara Pencegahan, https://www.cloudeka.id/id/berita/teknologi/social-engineering-adalah/#:~:text=Social%20engineering%20adalah%20tindakan%20kejahatan,pada%20pencurian%20dan%20penyalahgunaan%20data

Otoritas Jasa Keuangan. 2023. Waspada Modus Penipuan Gaya Baru, https://www.ojk.go.id/ojk-institute/id/capacitybuilding/upcoming/2746/waspada-modus-penipuan-gaya-baru.

Universitas Bakrie. 2024. Waspada! Ini 4 Social Engineering Attacks yang bisa Menyerangmu, https://bakrie.ac.id/articles/587-waspada-ini-4-social-engineering-attacks-yang-bisa-menyerangmu.html#:~:text=Jika%20dulunya%20'hipnotis'%20hanya%20dilakukan,sistem%20alat%20komunikasi%20yang%20digunakan

Prima Cyber Solusi. 2024. Mengenal Lebih Jauh apa itu Serangan Social Engineering dan Cara Mencegahnya, https://www.primacs.co.id/post/mengenal-lebih-jauh-apa-itu-serangan-social-engineering-dan-cara-mencegahnya.

Rafizan, O. 2011. Analisis Penyerangan Social Engineering, https://www.neliti.com/publications/233773/analisis-penyerangan-social-engineering.

Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik.