JOURNAL OF ACCOUNTING, MANAGEMENT, AND FINANCIAL (JAMFI)
Vol. 01, Issue. 02, December 2024, Pp: 140–149
Available online at: https://pub.ruangrosadi.com/jurnal-ilmiah/index.php/jamfi/index

Pencegahan Jebakan Digital: Upaya Bank BCA Mengatasi Modus *Social engineering* di Media Sosial

Nisrina Khalda Zahirah[1], Anisa Maulina[2], Nazwa Maulida G[3], Ines Nur Irawan[4], Rendika Vhalery[5]
[1,2,3,4,5]Universitas Indraprasta PGRI, Jakarta, Indonesia
[1]nisrinazahirah19@gmail.com, [2]maulinaanisa15@gmail.com, [3]nzwamlda2@gmail.com,
[4]ineznurirawan@gmail.com, [5]rendikavhalery31@gmail.com

Received: 11 Jul 2025
Revised: 15 Agu 2025
Accepted: 23 Agu 2025

Abstract

Era digitalisasi telah mengubah lanskap keuangan, memicu perkembangan pesat dalam layanan perbankan elektronik dan digital. Bank Central Asia (BCA) telah berinovasi dengan layanan seperti Blu by BCA untuk meningkatkan efisiensi dan kenyamanan nasabah. Namun, kemajuan ini juga membuka celah bagi modus kejahatan siber, terutama *Social engineering* (Soceng) atau "Jebakan Digital", yang memanfaatkan manipulasi psikologis untuk mencuri data pribadi. Penelitian ini menganalisis upaya pencegahan yang dilakukan BCA dalam mengatasi modus Soceng di media sosial, dengan pendekatan kualitatif melalui observasi dan analisis konten terhadap materi edukasi BCA di situs web dan platform seperti Instagram, Twitter, dan TikTok. Hasil penelitian menunjukkan bahwa BCA secara aktif memberikan informasi komprehensif mengenai ciri-ciri dan pencegahan Soceng, termasuk peringatan tentang tautan berbahaya dan pentingnya menjaga kerahasiaan data pribadi. Wawancara dengan narasumber dari Otoritas Jasa Keuangan (OJK) dan mahasiswa mengkonfirmasi urgensi edukasi terkait Soceng, termasuk modus baru seperti *sniffing* melalui *file* APK. Meskipun BCA telah melakukan sosialisasi ekstensif, masih ditemukan celah pemahaman di kalangan masyarakat. Oleh karena itu, penelitian ini menyimpulkan bahwa edukasi berkelanjutan dan peningkatan literasi digital adalah kunci utama dalam melindungi nasabah dari ancaman Soceng yang terus berkembang.

Keywords: *social engineering* , literasi digital, BCA, pencegahan kejahatan siber

(*) Corresponding Author: nisrinazahirah19@gmail.com

INTRODUCTION

Dunia saat ini berada di era Society 5.0 , di mana *cyber space* dan *physical space* terintegrasi. Hal ini menunjukkan bahwa bagaimana masyarakat memanfaatkan teknologi digital dalam berbagai aspek kehidupan (Umar *et al*., 2024). Digitalisasi adalah proses yang menggantikan metode tradisional dengan teknologi digital untuk meningkatkan efisiensi dan produktivitas (Herlambang dkk, 2023). Banyak sektor, seperti layanan pemerintah, keuangan, perizinan, dan pendidikan, sudah beralih ke digital.

Di dunia keuangan, digitalisasi telah mengubah transaksi tradisional menjadi digital. Salah satu contoh yang paling jelas adalah kehadiran *financial technology,* yang memberikan akses lebih mudah ke layanan keuangan. Masyarakat kini dapat mengajukan kredit dengan mudah tanpa perlu pergi ke lembaga keuangan, berkat layanan seperti *peer-to-peer lending* (Share *et al.,* 2023). Selain itu, layanan Beli Sekarang, Bayar Nanti memungkinkan konsumen membeli barang dan membayarnya nanti dengan cicilan, bahkan

tanpa kartu kredit. Perkembangan ini menunjukkan kemajuan signifikan yang dibawa oleh digitalisasi di sektor keuangan.

Seiring berkembangnya era digital, bank merasakan dampak yang signifikan. Bank tradisional kesulitan bersaing jika tidak beradaptasi dengan teknologi digital. Kepercayaan sangat penting bagi bank, dan jika masyarakat kehilangan kepercayaan, penarikan dana dalam jumlah besar dapat merugikan bank. Kemajuan pesat dalam teknologi informasi dan globalisasi memungkinkan bank untuk meningkatkan layanan, menjadikannya lebih aman, lebih nyaman, dan lebih efektif. Salah satu solusinya adalah perbankan elektronik (*e-banking*), yang memudahkan nasabah mengakses informasi dan bertransaksi menggunakan media elektronik. Perbankan digital merupakan bagian dari *e-banking* yang bertujuan untuk memberikan pengalaman yang lebih cepat dan lebih sesuai dengan kebutuhan nasabah.

Bank telah meluncurkan beragam layanan perbankan elektronik, seperti ATM, EDC, *Point of Sales, phone banking*, SMS *banking*, *internet banking*, dan *mobile banking***.** Sedangkan layanan perbankan digital merupakan evolusi dari perbankan elektronik, yang memanfaatkan data nasabah untuk operasionalnya. Salah satu contoh bank digital yang marak di masyarakat ialah Blu by BCA. Tujuan utama digitalisasi ini adalah untuk meningkatkan efisiensi, dan kenyamanan bagi nasabah, memungkinkan transaksi yang lebih cepat dan akurat, serta meningkatkan daya saing sektor perbankan. Gibbs (2020) mengatakan meningkatnya kejahatan siber disebabkan pesatnya perkembangan teknologi.

Banyak laporan menyoroti penipuan terorganisir di perbankan karena teknologi yang memudahkan transaksi tetapi juga mempermudah penipuan. Sebagian besar penipuan disebabkan oleh kelalaian konsumen dan buruknya pemahaman keuangan mereka sendiri. Penipu beroperasi secara daring atau secara langsung memengaruhi psikologis target untuk mengeksploitasi kelemahan keamanan (Andriyanto, 2022).

Saat ini, salah satu modus kejahatan yang sering terjadi dalam dunia perbankan digital adalah *Social engineering (Soceng)* atau biasa dikenal dengan Jebakan Digital**.** Chetioui et al. (2022) menjelaskan bahwa *social engineering* adalah teknik mempengaruhi seseorang dengan cara tertentu agar mau memberikan informasi rahasia, seperti kata sandi, alamat, atau data penting lainnya yang berkaitan dengan bank. Soceng merupakan tipu daya yang memanfaatkan interaksi sosial dan manipulasi psikologis untuk mencuri data atau informasi korban. Pelaku mendekati korban dengan cara yang tampak wajar, sehingga korban sulit menyadari bahwa mereka ditipu untuk membagikan informasi rahasia. Cara ini sangat efektif karena menyasar kelemahan manusia seperti rasa takut, rasa percaya, dan keinginan untuk menolong. Soceng dapat dilakukan dengan berbagai cara, seperti mengirimkan tautan berbahaya untuk mencuri uang atau menyebarkan *malware* yang disamarkan sebagai dokumen penting. Soceng juga dapat dilakukan melalui panggilan telepon palsu dari orang yang mengaku sebagai petugas bank, dengan tujuan untuk mendapatkan informasi pribadi secara ilegal guna mengakses rekening perbankan digital. Karena Soceng memanfaatkan rasa percaya, rasa ingin tahu, dan kecerobohan, korban sering kali tidak menyadari bahwa mereka telah menjadi sasaran skema ini.

Banyak laporan modus penipuan yang terorganisir di sektor perbankan, seperti di bank BCA. Penipuan ini terjadi karena kemajuan teknologi yang mempermudah transaksi, tetapi juga memudahkan pelaku penipuan. Menurut Hasan dan Febrian tahun 2021 mencatat peningkatan kejahatan finansial seiring dengan perkembangan digital. Oleh karena itu, diperlukan langkah-langkah pencegahan dan penanganan, termasuk edukasi kepada nasabah oleh bank untuk mengurangi penipuan. Edukasi tentang kejahatan siber dapat meningkatkan

kewaspadaan masyarakat dan dapat diberikan melalui media sosial dan situs resmi perusahaan, sehingga nasabah dan masyarakat dapat mengenali berbagai modus penipuan.

Satu kasus penting terjadi di Bank Central Asia (BCA), di mana terdapat hampir 2.000 kejadian serangan siber setiap bulan pada tahun 2022. Menurut Nisaputra Rezkiana (2022), mayoritas korban adalah nasabah berusia 30-an. Rekayasa sosial, juga dikenal sebagai soceng, adalah teknik utama yang digunakan oleh penjahat siber. Dalam pendekatan ini, pelaku menyamar sebagai kurir paket, perwakilan layanan nasabah bank, pengirim surat undangan pernikahan, atau penyedia penawaran peningkatan layanan nasabah prioritas. Untuk mengelabui korban agar mengungkapkan informasi sensitif, seperti kata sandi, PIN, dan OTP, mereka mengirim tautan melalui saluran media sosial seperti WhatsApp. Korban penipuan semacam ini sebagian besar adalah perempuan berusia antara 21 dan 35 tahun, sehingga sangat merugikan. Selain itu, laki-laki berusia antara 36 dan 50 tahun lebih mungkin tertipu oleh penipuan soceng, yang melibatkan penawaran peningkatan layanan kepada nasabah prioritas. Selain itu, strategi ini juga meluas ke sektor *e-commerce*, dengan fokus pada lima barang yang paling sering menjadi sasaran penipuan *online* : ponsel pintar, mobil, pakaian, tas tangan, dan sepeda motor. Menurut Rahayu Isna Rifka Sri dan Pratama Akhdi Martin Pratama (2023), mayoritas korban adalah perempuan muda yang tergiur dengan tawaran barang murah dan berkualitas tinggi.

Mayoritas masyarakat Indonesia juga belum sepenuhnya memahami *soceng*, menganggapnya sebagai kasus baru. Oleh karena itu, penelitian ini bertujuan untuk memberikan pemahaman yang jelas kepada masyarakat mengenai *soceng* dan ancamannya, serta menganalisis pola-pola sosialisasi pencegahan modus *soceng* oleh BCA melalui media *website* dan media sosial Twitter.

METHODS

Penelitian ini menggunakan pendekatan kualitatif. Penelitian kuantitatif secara sistematis mengukur variabel, menganalisis data angka, dan menggeneralisasi temuan ke populasi yang lebih besar, menggunakan statistik untuk memastikan hasil yang objektif dan andal (Gnawali,Y. P.2022). Penelitian ini bermaksud untuk menganalisis pencegahan jebakan digital upaya Bank BCA mengatasi modus *social engineering* di *social* media. Penulis mengumpulkan informasi secara lengkap dan menganalisis mengenai pencegahan jebakan digital upaya Bank BCA mengatasi modus *social engineering* melalui *social* media diantaranya Instagram, Twitter, dan Tiktok.

Selanjutnya, Teknik pengumpulan data merupakan tahap pertama dalam proses penelitian berlangsung, karena tujuan utama penelitian adalah mendapatkan data yang valid dan sah. Teknik pengumpulan data dilakukan dengan dua cara yaitu observasi dan analisis konten. Penelitian ini menggunakan data dari literatur dan dokumen, tanpa batasan variabel yang ketat (Asyari dkk, 2021). Analisis ini menggunakan kerangka teoritis komunikasi pemasaran yang menyoroti elemen-elemen seperti daya tarik pesan, relevansi informasi, dan efek emosional terhadap audiens (Belch & Belch, 2020).

RESULTS & DISCUSSION

Bank BCA telah mengambil langkah aktif dalam mencegah penipuan digital dengan menyediakan informasi lengkap tentang ciri-ciri *social engineering* dan langkah pencegahannya di situs resmi mereka. Edukasi ini meliputi cara mengenali akun resmi bank, menghindari tautan mencurigakan, serta tidak membagikan data pribadi seperti PIN dan OTP kepada siapapun.

Gambar 1.
Tips Terhindar Dari Kejahatan Perbankan Skimming
Sumber: https://bca.co.id/

Gambar 2.
Tips Terhindar Dari Kejahatan Perbankan Phishing
Sumber: https://bca.co.id/

Berdasarkan hasil observasi terbaru terhadap kejahatan siber skimming dan phishing, penulis menemukan modus penipuan yang jauh lebih berbahaya. Modus ini melibatkan peretas yang telah berhasil menyusup ke aplikasi e-channel Bank BCA, yaitu *mobile banking*. Masyarakat, khususnya nasabah setia BCA, dihimbau untuk selalu ekstra hati-hati setiap kali menggunakan aplikasi mobile banking. Jangan pernah mengeklik tombol atau tautan apa pun

jika muncul peringatan atau indikasi bahwa ponsel Anda telah diserang virus trojan, terutama jika itu terlihat seperti pesan dari aplikasi mobile banking. Modus penipuan baru ini menunjukkan tingkat kecanggihan yang lebih tinggi, sehingga kewaspadaan nasabah menjadi sangat krusial untuk menghindari kerugian finansial.

Gambar 3.
Modus Penipuan Terbaru Melalui *Mobile Banking*
Sumber: https://bca.co.id/

BCA menghimbau nasabah untuk lebih berhati-hati dengan rekening bank dan saat menggunakan mobile banking. Sangat penting untuk mewaspadai tautan berbahaya, terutama dengan teknologi yang terus berkembang. BCA telah membagikan peringatan ini di situs web resmi dan saluran media sosialnya. Selalu periksa kembali sumber informasi apa pun sebelum Anda memercayai atau membagikannya. Anda dapat menemukan informasi resmi BCA di situs web mereka (www.bca.co.id), WhatsApp resmi mereka (cari tanda centang hijau), Instagram (@GoodLifeBCA), Twitter (@HaloBCA), dan TikTok (@BankBCA).

Profil Narasumber :

Identitas Narasumber:

Narasumber 1 : Ibu Friderica Widyasari Dewi (Kepala Eksekutif Pengawas Perilaku Pelaku Usaha Jasa Keuangan, Edukasi, dan Perlindungan Konsumen Otoritas Jasa Keuangan).

Hasil Wawancara:

Siaran Pers Jakarta, 24 Mei 2025

Perkembangan pesat di era digitalisasi ini mendorong sektor jasa keuangan untuk lebih optimal dalam menyediakan layanan. Namun, hal ini juga membawa tantangan, di mana semua pihak, mulai dari regulator, pelaku usaha jasa keuangan, hingga masyarakat, perlu senantiasa waspada terhadap kejahatan digital**.**

Salah satu jenis kejahatan digital yang sedang marak adalah penipuan *Social engineering* (Soceng)**.** Selain itu, ada juga modus terbaru bernama *Sniffing***,** di mana pelaku mengirimkan tautan palsu berupa paket kurir atau undangan pernikahan melalui WhatsApp. Tautan ini biasanya dalam bentuk *file* APK (Android *Package* Kit), yang jika dibuka bisa membahayakan perangkat korban.

Sniffing dan *link* APK adalah modus penipuan *online* di mana penjahat siber (*hacker*) mencegat komunikasi internet. Tujuannya adalah untuk mencuri data dan informasi sensitif korban, seperti *username* dan *password* m-*banking*, detail kartu kredit, dan data penting lainnya. Modus penipuan ini biasanya terjadi ketika pelaku mengirimkan pesan chat yang meminta korban mengunduh lampiran. Lampiran ini sebenarnya adalah aplikasi berbahaya

(umumnya berformat .APK) yang sering kali disamarkan sebagai "foto" atau *file* lain yang tidak berbahaya. Jika korban tidak waspada dan mengunduh lampiran tersebut, aplikasi tersebut akan terinstal di perangkat *smartphone* mereka dan mampu mencuri data sensitif, termasuk informasi terkait *mobile banking*.

Penipuan *online* semakin marak, tapi juga bisa menghindarinya dengan beberapa tips pencegahan sederhana, diantaranya. Waspada Unduh Aplikasi dan Tautan: Jangan asal mengunduh aplikasi atau mengklik tautan yang dikirimkan lewat SMS, WhatsApp, atau email, apalagi jika pengirimnya tidak jelas. Modus ini sering dipakai penipu untuk menyebarkan *malware* atau *phishing*. Verifikasi Kontak Mencurigakan**:** Jika menerima telepon, SMS, atau WhatsApp yang mencurigakan mengatasnamakan perusahaan atau lembaga tertentu, segera verifikasi keasliannya dengan menghubungi *call center* resmi mereka. Jangan mudah percaya pada nomor yang tidak dikenal.

Aktifkan Notifikasi Transaksi: Aktifkan notifikasi transaksi untuk semua rekening. Dengan begitu, bisa langsung tahu jika ada aktivitas mencurigakan dan bisa segera mengambil tindakan. Cek Rekening dan Ganti Kata Sandi Berkala: Periksa mutasi rekeningmu secara rutin dan ganti kata sandi akun-akun penting secara berkala. Ini akan mempersulit penipu yang mungkin sudah mendapatkan akses ke akun.

Hindari Wifi Publik untuk Transaksi Keuangan: Jaringan Wifi publik seringkali tidak aman dan rentan disusupi. Sebisa mungkin, jangan gunakan Wifi publik saat melakukan transaksi keuangan atau mengakses informasi sensitif. Otoritas Jasa Keuangan (OJK) menghimbau seluruh masyarakat, agar meningkatkan kewaspadaan terhadap ancaman penipuan *online* yang semakin banyak muncul di dunia digital. Modus kejahatan yang perlu diwaspadai antara lain *social engineering* , *sniffing*, dan tindak kejahatan digital sejenis.

“Sektor jasa keuangan di Jakarta menunjukkan pertumbuhan yang positif dan stabil. Ini terlihat dari kenaikan kredit dan aset perbankan. Tak hanya itu, jumlah Single Investor Identification (SID) di pasar modal juga meningkat dibandingkan periode sebelumnya. Otoritas Jasa Keuangan (OJK) telah melayani 226.267 permintaan informasi dan pengaduan melalui berbagai saluran. Dari total layanan tersebut, 10.109 di antaranya merupakan pengaduan dari masyarakat. Hampir setengah dari seluruh pengaduan, tepatnya 49,5%, berasal dari sektor perbankan. Sektor Industri Keuangan Non-Bank (IKNB) menyumbang jumlah pengaduan yang sedikit lebih banyak, yaitu 50%. Sisanya merupakan pengaduan terkait layanan di sektor pasar modal.

Kepala OJK menghimbau masyarakat untuk waspada terhadap penipuan *online* atau *social engineering* (soceng) yang semakin marak. Selain berupaya menjaga pertumbuhan sektor jasa keuangan, OJK juga berkomitmen meningkatkan literasi dan inklusi keuangan bagi mahasiswa, ASN, komunitas, serta masyarakat di lingkungan pemerintahan kota dan kabupaten di Indonesia.” (Uyu Septiyati Liman, 2025)

Lampiran Wawancara Eksternal

Profil Narasumber

Identitas Narasumber:

Narasumber 2 : Avi Putri (Mahasiswa Strata 1 Bisnis Digital)
Narasumber 3 : Ainayah Adinda (Mahasiswa Strata 1 Ilmu Komunikasi)
Narasumber 4 : Siti Aisyah (*Freshgraduate* Strata 1 Akutansi)

Hasil Wawancara

Apakah Saudari tahu apa itu *Social engineering* ?

Narasumber 2 : Saya tahu *Social engineering* itu isu yang menjadi ancaman bagi keamanan

data pribadi yang patut diwaspadai.

Narasumber 3 : Sedikit tahu, menurut Saya *Social engineering* ialah tindakan penipuan yang memanfaatkan berbagai taktik untuk mendapatkan data pribadi atau informasi rahasia kita.

Narasumber 4 : Ya secara umum saya sedikit tahu terkait *Social engineering* .

Apakah Saudari sudah familiar dengan macam-macam bentuk dari *Social engineering* ?

Narasumber 2 : Setahu saya, salah satu bentuk *Social engineering* itu kayak penipuan yang dilakukan dengan menggali informasi pribadi korban, biasanya dengan iming-iming hadiah. Namanya pretexting kalau tidak salah mba.

Narasumber 3 : Ada beberapa jenis *social engineering* yang saya tahu, misalnya phishing sama spear phishing**.** Phishing itu melibatkan pengiriman email atau pesan teks berisi tautan ke situs web palsu. Sementara, spear phishing mirip sama phishing, tapi jauh lebih terperinci dan ditargetkan pada pihak tertentu, dengan pesan yang disesuaikan menggunakan informasi yang sangat detail.

Narasumber 4 : Saya memiliki sedikit tahu tentang bentuk *Social engineering* . Saya pernah membaca buku berjudul "The Art of Human Hacking", yang menjelaskan perkembangan teknologi dan juga seluk-beluk *Social engineering* . Oleh karena itu, saya jadi sedikit mengerti mengenai topik ini.

Dari mana Anda mendapat informasi tentang *Social engineering* ?

Narasumber 2 : Media sosial mba soalnya gen z cenderung mengakses media sosial dibanding menonton televisi.

Narasumber 3 : Saya sudah tak asing dengan *Social engineering* , karena sebagai mahasiswa, saya selalu mengikuti perkembangan teknologi dan informasi di lingkungan sosial saya.

Narasumber 4 : Saya tahu soal ini dari media sosial, karena belakangan ini kasus *Social engineering* lagi marak terjadi.

Apakah menurut Saudari isu *Social engineering* ini ancaman yang berbahaya?

Narasumber 2 : Sosial Engineering sangat berbahaya bagi masyarakat mba, karena dapat merugikan bagi orang yang belum paham ataupun awam. Sebab *Social engineering* dapat menyerang siapa saja dan dari kalangan manapun.

Narasumber 3 : Buat saya, *Social engineering* itu tidak terlalu mengancam. Tapi, bagi mereka yang awam atau belum paham betul, *Social engineering* bisa sangat merugikan dan membahayakan, karena dampaknya bisa menyerang siapa saja dari berbagai kalangan.

Narasumber 4 : Berbahaya karena sangat merugikan korban.

Pernahkah Saudari atau orang terdekat Anda mengalami penipuan *Social engineering* ?

Narasumber 2 : Pernah mba, Orang tua saya sering dihubungi oleh pihak tak dikenal yang mengaku dari BCA, meminta informasi pribadi. Ini jelas modus penipuan, karena pihak BCA tidak pernah menanyakan data pribadi nasabah melalui telepon.

Narasumber 3 : Secara pribadi, saya atau keluarga saya belum pernah menjadi korban *social engineering* . Namun, ada teman saya yang pernah tertipu; dia menerima pesan

SMS atau WhatsApp yang menjanjikan hadiah dan kemudian diminta menyerahkan data pribadi seperti KTP dan nomor rekeningnya.

Narasumber 4 : Pernah suatu ketika, saya menjadi korban penipuan berkedok rekrutmen kerja dari sebuah perusahaan yang sebelumnya memang saya lamar. Modusnya, mereka mengirimkan pesan berisi undangan wawancara dan meminta saya mengunggah berkas-berkas persyaratan melalui tautan yang mereka berikan.

Menurut Saudari, seberapa mendesak atau pentingkah edukasi terkait *Social engineering* saat ini?

Narasumber 2 : Penting banget mba untuk memberikan edukasi, karena tidak ada batasan usia dalam penggunaan media digital saat ini. Dengan begitu, kita bisa meminimalkan ancaman *Social engineering* .

Narasumber 3 : Menurut saya, edukasi tentang *Social engineering* sangat penting di era perkembangan teknologi yang pesat ini. Banyak anak muda, yang mungkin kurang tertarik mencari informasi, tidak menyadari apa itu *social engineering* dan potensi kerugian yang bisa ditimbulkannya. Oleh karena itu, saya berharap ada lebih banyak edukasi mengenai hal ini.

Narasumber 4 : Edukasi mengenai *Social engineering* itu hal yang esensial, terutama di era teknologi yang terus maju ini di mana semua kalangan dan usia bisa mengakses berbagai informasi.

Upaya apa yang Saudari lakukan untuk menghindari dari *Social engineering* ?

Narasumber 2 : Untuk menghindari *Social engineering* , saya akan menjaga kerahasiaan data pribadi dengan tidak mudah percaya atau tergiur iming-iming hadiah yang tidak masuk akal. Saya akan selalu berhati-hati dalam memberikan informasi pribadi dan memastikan tujuannya jelas. Selain itu, saya akan aktif mencari informasi dan mendengarkan masukan dari berbagai sumber untuk meningkatkan kewaspadaan.

Narasumber 3 : Kalau Saya tidak mudah percaya dan selalu memverifikasi kiriman dari orang yang tidak saya kenal. Saya juga akan menolak atau memblokir email dan pesan dari pengirim yang tidak dikenal.

Narasumber 4: Saya selalu mewaspadai bujukan dari pihak yang tidak dikenal dan memperbanyak dalam menggali informasi dari berbagai sumber di media sosial.

Di tengah pesatnya perkembangan teknologi digital, ancaman kejahatan siber seperti *social engineering* (Soceng) semakin meningkat. Ibu Friderica Widyasari Dewi, Kepala Eksekutif Pengawas Perilaku Pelaku Usaha Jasa Keuangan, Edukasi, dan Perlindungan Konsumen Otoritas Jasa Keuangan (OJK), menekankan pentingnya kewaspadaan terhadap modus-modus penipuan *online* seperti *sniffing*, di mana pelaku menyebarkan tautan berbahaya berkedok paket kurir atau undangan pernikahan via WhatsApp. Tautan tersebut seringkali berupa file APK yang dapat membahayakan perangkat korban dan mencuri data sensitif.

Ibu Friderica juga menyoroti tingginya jumlah pengaduan terkait kejahatan digital di OJK. Data menunjukkan bahwa hampir setengah dari pengaduan berasal dari sektor perbankan dan IKNB. Hal ini menunjukkan betapa pentingnya edukasi dan literasi digital bagi masyarakat. OJK sendiri aktif memberikan edukasi dan himbauan kepada masyarakat untuk

meningkatkan kewaspadaan terhadap penipuan *online*.

Pandangan serupa disampaikan oleh para mahasiswa yang diwawancarai. Avi Putri, : Ainayah Adinda, dan Siti Aisyah, masing-masing mahasiswa Bisnis Digital, Ilmu Komunikasi, dan Akuntansi, mengakui bahaya *social engineering* . Mereka memahami berbagai modus penipuan *online*, seperti *phishing* dan *spear phishing*, dan mendapatkan informasi tersebut terutama dari media sosial. Ketiganya sepakat bahwa edukasi tentang *social engineering* sangat penting, mengingat akses mudah terhadap teknologi digital oleh semua kalangan usia. Ancaman *social engineering* merupakan isu serius yang membutuhkan perhatian bersama. Edukasi dan literasi digital yang intensif, serta kewaspadaan individu, menjadi kunci utama dalam melindungi diri dari kejahatan siber ini. Baik regulator seperti OJK maupun masyarakat sendiri perlu berperan aktif dalam upaya pencegahan.

CONCLUSION

Penelitian ini menyimpulkan bahwa *Social engineering* (Soceng) atau jebakan digital merupakan ancaman serius di era digital, khususnya di sektor perbankan seperti BCA. Modus penipuan ini memanfaatkan manipulasi psikologis korban untuk mencuri data pribadi, yang dapat berujung pada kerugian finansial. BCA telah proaktif melakukan upaya pencegahan melalui edukasi intensif di situs web dan media sosial mereka, mengedukasi nasabah tentang ciri-ciri penipuan, bahaya tautan mencurigakan, dan pentingnya menjaga kerahasiaan data pribadi. Meskipun demikian, masih banyak masyarakat yang belum sepenuhnya memahami bahaya Soceng, sehingga edukasi berkelanjutan menjadi sangat krusial.

REFERENCES

Andriyanto, T. (2022). Komunikasi Termediasi Penipuan dengan Modus Business Email Compromise. *Jurnal Riset Komunikasi*, 5(2), 220-243.

Asy'ari, R., Dienaputra, R. D., Nugraha, A., Tahir, R., Rakhman, C. U., & Putra, R. R. (2021). Kajian Konsep Ekowisata Berbasis Masyarakat Dalam Menunjang Pengembangan Pariwisata : Sebuah Studi Literatur. Pariwisata Budaya. *Jurnal Ilmiah Agama Dan Budaya*, 6(1), 9. https://doi.org/10.25078/pba.v6i1.1969

Badan Siber dan Sandi Negara. (2020). Rekap serangan siber (januari-april2020). Diakses melalui https://bssn.go.id/rekap-serangan-siber-januari-april-2020/

Belch, G. E., & Belch, M. A. (2020). Advertising and Promotion: An Integrated Marketing Communications Perspective. McGraw-Hill Education

Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of *social engineering* attacks on social networks. Procedia Computer Science, 198(2021), 656–661.

Gibbs, T. (2020). Seeking economic cyber security: A middle eastern example. Journal of Money Laundering Control, 23(2), 493–507.

Gnawali, Y. P. (2022). Ganeshman Darpan Use of Mathematics in Quantitative Research. Ganeshman Darpan, 7(1), 1.

Hasan, A., & Febriany, L. (2021). Identifikasi Tindakan Pengawasan Dan Pencegahan Terhadap Kejahatan Finansial Perbankan Syariah Selama Masa Pandemi COVID19. *Jurnal Ilmiah Akuntansi Dan Keuangan*, 4(4), 1089–1090.

https://doi.org/26222191

Herlambang, Y. T., & Abidin, Y. (2023). Pendidikan Indonesia Dalam Menyongsong Dunia Metaverse : Telaah Filosofis Semesta Digital dalam Perspektif Pedagogik Futuristik Program Studi. Pendidikan Guru Sekolah Dasar , *Universitas Pendidikan Indonesia Kampus Cibiru.*

Nisaputra, R. (2022). Laporan kasus serangan siber pada nasabah BCA. *BCA Annual Report.*

Rahayu, I. R. S., & Pratama, A. M. P. (2023). Penipuan jual-beli *online* dengan modus soceng. *Jurnal Keuangan Digital*.

Sahare, Ni Wayan Nitya Varshini, and Utami, Putu Devi Yustisia, "Peer to Peer (PP2p Lending: Upaya Mengatasi Layanan Pinjaman *Online* Ilegal Terhadap Keamanan Data Pribadi", Kertha Semaya, 11.06. (2023), 1373-1383, h. 1374.

Umar, Muhammad Abdullah. "Penggunaan Shopee Paylater Di Era Society 5.0 Perspektif Hukum Ekonomi Syariah." *Journal of Islamic Economic and Law (JIEL)* 1.2 (2024): 25-32. H.26.

Uyu Septiyati Liman. (2025). *OJK: Kejahatan sektor perbankan tetap dapat terjadi jika nasabah lalai*. Antara News. https://www.antaranews.com/berita/4856553/ojk-kejahatan-sektor-perbankan-tetap-dapat-terjadi-jika-nasabah-lalai

We are social. (2022).Indonesian digital report 2022. In we are social (p. 113). Diakses melalui https://datareportal.com/reports/digital-2021-indonesia.