JURNAL RISET SISTEM INFORMASI
Halaman Jurnal: https://journal.smartpublisher.id/index.php/jissi
Halaman UTAMA Jurnal : https://journal.smartpublisher.id

DOI: https://doi.org/10.69714/8b7xtv35

ANALISIS DAN PENCEGAHAN SERANGAN SOSIAL ENGGINERING PADA JARINGAN KOMPUTER STUDI KASUS PENIPUAN INVESTASI CRYPTO

Rahmat Eka Putra R Palaloi [a*], Rakhmadi Rahman [b]
[a] Sistem Informasi, rahmat.palaloy@gmail.com, Institut Teknologi Bacharuddin Jusuf Habibie, Parepare Sulawesi Selatan
[b] Information System Department, rakhmadi.rahman@ith.ac.id, Institut Teknologi Bacharuddin Jusuf Habibie, Parepare Sulawesi Selatan
[*]Korespondensi

ABSTRACT

The study investigates cryptocurrency investment fraud practices in Indonesia that use social engineering. Fast-growing digital technology presents opportunities and challenges, including an increasing risk of cybercrime. An APJII survey in 2024 showed that there are 221 million people in Indonesia who use the Internet. On the other hand, Kemenkeu predicts the digital economy will grow eightfold by 2030. Cryptocurrency investment scams often use social engineering attacks such as phishing and identity theft. Qualitative descriptive methods are used in this research to conduct literary analysis of various journal articles. The results show that crypto investment fraud has psychological and social consequences in addition to financial losses. To address this problem, the authors suggest increased digital literacy, tighter security policies, and government-industry collaboration to reduce risk and increase public confidence in blockchain and cryptocurrency technologies.

Keywords: social engineering, investment fraud, cryptocurrency, social engineering prevention.

Abstrak

Studi ini menyelidiki praktik penipuan investasi cryptocurrency di Indonesia yang menggunakan rekayasa sosial. Teknologi digital yang berkembang pesat menimbulkan peluang dan tantangan, termasuk meningkatnya risiko kejahatan siber. Survei APJII tahun 2024 menunjukkan bahwa ada 221 juta orang di Indonesia yang menggunakan internet. Di sisi lain, Kemenkeu memperkirakan ekonomi digital hendak berkembang delapan kali lipat ditahun 2030. Penipuan investasi cryptocurrency sering menggunakan serangan rekayasa sosial seperti phishing dan pencurian identitas. Tekhnik deskriptif kualitatid dipakai pada penelitiannya guna melakukan analisis literatur dari berbagai artikel jurnal. Hasil menunjukkan bahwa penipuan investasi kripto memiliki konsekuensi psikologis dan sosial selain kerugian finansial. Untuk mengatasi masalah ini, penulis menyarankan peningkatan literasi digital, kebijakan keamanan yang lebih ketat, dan kolaborasi pemerintah-industri untuk mengurangi risiko dan meningkatkan kepercayaan publik terhadap teknologi blockchain dan cryptocurrency.

Kata Kunci: social engineering penipuan investasi, cryptocurrency, pencegahan social engineering

1. PENDAHULUAN

Di dunia yang dinamis dan bergerak, Indonesia adalah salah satu negara yang menikmati kemajuan teknologi. Menurut survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah orang Indonesia yang menggunakan internet pada tahun 2024 akan mencapai 221.563.479 orang, dari 278.696.200 orang pada tahun 2023[1]. Pada tahun 2021, Kementerian Keuangan Republik Indonesia (Kemenkeu) memperkirakan bahwa hingga tahun 2030, ekonomi digital Indonesia akan meningkat hingga delapan kali lipat[2]. Menurut Tjendrawinata, Kevin(2022) Tidak diragukan lagi bahwa dinamika perkembangan era digital di Indonesia memiliki pengaruh yang signifikan, baik secara positif maupun negatif. Perkembangan

Received Juni 2, 2024; Revised Juni 12, 2024; Accepted Juli 2, 2024; Published juli 10, 2024

digital memiliki kelemahan bahwa data tersebar luas dan dapat digunakan oleh pihak yang tidak berkepentingan atau bahkan digunakan untuk merencanakan kriminalitas di dunia siber.

Salah satu dampak negative dalam perkembangan era digital adalah sosial engineering menurut ade nepila (2023) Serangan dengan social engineering dapat dikombinasikan dengan serangan teknis seperti spyware dan trojan yang lebih efektif, tetapi hanya sedikit yang dapat dikategorikan sebagai serangan non-teknis[3]. Memanipulasi manusia sangat mudah untuk memberikan informasi yang mungkin bermanfaat bagi hacker. Saat ini, sebagian besar perusahaan dan bank bergantung pada teknologi seperti smartphone dan internet. Salah satu kasus social engineering yang marak terjadi saat ini adalah kasus penipuan investasi crypto.

Sebuah penelitian yang dilakukan pada bulan Desember 2020 oleh Association of Certified Fraud Examiners (ACFE) menemukan bahwa 85% orang yang disurvei mengakui skema fraud siberx[4]. Menurut Federal Bureau of Investigation(2023) dalam laporannya "internet crime report" mencatatkan rekor pengaduan kejahatan siber dengan potensi kerugian US$ 12,5 miliar atau setara dengan 880.418 pegaduan. Dalam setahun terakhir berdasarkan hasi pelacakan Crime complaint center (IC3) menunjukan jenis kejahatan yang paling merugikan adalah penipuan investasi[5].

Berbagai jenis fraud siber dapat terjadi jika sistem, prosedur, atau sumber daya manusia bocor atau tidak berfungsi seperti yang seharusnya. Salah satu jenis fraud siber ini disebabkan oleh Social Engineering, yang bergantung pada intuisi manusia untuk melakukan tindakan tertentu daripada sistem.

Oleh karna itu penulis ingin menganalisis salah satu kasus sosial engineering yag marak terjadi saat ini yaitu kasus penipuan investasi crypto. penulis juga ingin memberikan wawasan kepada pembaca agar dapat terhindar dari sosial engineering.

2. TINJAUAN PUSTAKA

2.1. Perkembangan Teknologi dan Ekonomi Digital di Indonesia

Indonesia mengalami kemajuan pesat dalam menggunakan teknologi, terutama internet. Menurut survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), populasi pengguna internet di Indonesia diperkirakan mencapai 221.563.479 pada tahun 2024, dari 278.696.200 yang ada pada tahun 2023. Selain itu, Kementerian Keuangan Republik Indonesia memperkirakan pertumbuhan ekonomi digital Indonesia hingga delapan kali lipat hingga tahun 2030. Perkembangan ini memiliki efek baik dan buruk, termasuk kemungkinan penyalahgunaan data dan kejahatan siber.

2.2. Social Engineering dalam Kejahatan Siber

Serangan social engineering adalah salah satu ancaman besar bagi era digital. Manipulasi psikologis digunakan dalam social engineering untuk mengelabui orang untuk memberikan informasi atau melakukan tindakan tertentu yang merugikan mereka. Meskipun pada dasarnya adalah serangan non-teknis, Ade Napila (2023) mengatakan bahwa serangan ini dapat menjadi lebih efektif jika dikombinasikan dengan serangan teknis seperti spyware dan trojan. Karena ketergantungan mereka pada internet dan teknologi, sosial engineering sering menargetkan karyawan bisnis dan lembaga keuangan.

2.3. Penipuan Investasi Cryptocurrency

Penipuan investasi cryptocurrency telah menjadi salah satu kasus social engineering yang marak terjadi. Sebuah penelitian oleh Association of Certified Fraud Examiners (ACFE) pada Desember 2020 menemukan bahwa 85% responden mengakui adanya skema penipuan siber . Laporan Federal Bureau of Investigation (FBI) pada tahun 2023 mencatatkan rekor pengaduan kejahatan siber dengan potensi kerugian sebesar US$12,5 miliar, dimana penipuan investasi merupakan jenis kejahatan yang paling merugikan .

2.4. Dampak dan Pencegahan Social Engineering

2.4.1. Dampak Social Engineering

Sosial engineering dapat menyebabkan banyak hal, seperti kehilangan data, infeksi malware, kerusakan sistem, hilangnya kepercayaan, dan kerusakan lingkungan. Serangan seperti ini dapat menyebabkan kerugian psikologis dan moneter bagi individu dan organisasi.

2.4.2. Dampak Penipuan Investasi Cryptocurrency

Penipuan investasi cryptocurrency dapat menyebabkan kerugian finansial yang signifikan, stres psikologis, kehilangan kepercayaan pada teknologi blockchain, dan penurunan aktivitas ekonomi di industri yang relevan.

2.4.3. Pencegahan Social Engineering

Pendidikan, teknologi, peraturan, dan kebijakan perusahaan yang kuat adalah langkah pencegahan. Untuk mengurangi risiko penipuan, orang dapat meningkatkan literasi digital, menggunakan verifikasi dua faktor (2FA), dan menjadi skeptis terhadap tawaran investasi yang terlalu bagus untuk menjadi kenyataan. Pemerintah dan lembaga keuangan juga harus menetapkan aturan yang ketat untuk mengawasi platform investasi crypto dan melindungi investor.

3. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan menganalisis literatur secara sistematis. Tujuan dari penelitian ini adalah untuk memberikan gambaran lengkap dan memahami fenomena yang diteliti. Metode ini akan memungkinkan peneliti untuk mengumpulkan dan menganalisis berbagai artikel jurnal nasional dan internasional yang berkaitan dengan kejahatan cyber mengenai kasus pembobolan data kominfo oleh bjorka yang menggunakan sistem biometrik. Untuk melakukan review, database literatur Google Scholar digunakan melalui aplikasi Publish or Perish. Artikel penelitian menggunakan periode 2019–2024.

4. HASIL DAN PEMBAHASAN

4.1 Pembahasan sosial engginering

Social engineering adalah seni memaksa pengguna untuk mengkompromikan sistem informasi. Alih-alih serangan teknis terhadap sistem, sosial enginer menargetkan manusia dengan akses ke informasi, memanipulasi mereka untuk mengungkapkan informasi rahasia atau bahkan melakukan serangan berbahaya mereka melalui pengaruh dan persuasi. Tindakan perlindungan teknis biasanya tidak efektif terhadap jenis serangan ini. Selain itu, orang umumnya percaya bahwa mereka baik dalam mendeteksi serangan semacam itu. Penelitian, bagaimanapun, menunjukkan bahwa orang tampil buruk dalam mendeteksi kebohongan dan penipuan[6].

4.1.1. Jenis-jenis sosial engineering

a. Tailgating
   Tindakan mengikuti orang yang tidak dikenal yang memiliki akses legal ke ruang terbatas dikenal sebagai tajil.

b. Impersonating(meniru)
   Untuk melakukan tindakan, penyerang menggunakan identitas palsu. Penyerang berusaha mendapatkan akses fisik ke lokasi yang aman dengan melakukan peniruan untuk mendapatkan izin dari orang yang memiliki akses yang sah. Serangan ini sebagian besar berfokus pada menciptakan situasi yang masuk akal untuk dilakukan kepada individu yang terpilih. Untuk menghindari kecurigaan, metode ini membutuhkan kisah yang dapat dipercaya. Oleh karena itu, sangat penting untuk melakukan penelitian pada target tersebut terlebih dahulu.

c. Melalui telepon
   Serangan sosial engineering seperti ini biasanya terjadi melalui telepon. Penipu akan menelpon seseorang yang berkuasa dan menirunya, kemudian mengumpulkan informasi dari orang yang menjawab. Desk bantuan adalah contoh mudah dari serangan seperti ini. Hacker dapat menggunakan operator interkom atau interkom untuk berpura-pura menelepon dari perusahaan. Salah satu contoh trik interkom adalah dengan mengatakan, "Selamat siang, saya adalah petugas reparasi jaringan telepon."

d. Eavesdropping(menguping)
   Karyawan perusahaan dapat berbicara tentang rahasia dengan mudah. Pelaku social engineering hanya dapat memanfaatkan pelanggaran keamanan seperti ini karena berada di tempat yang tepat pada waktu yang tepat. Namun, pencuri juga dapat mendengarkan saluran komunikasi seperti telepon dan e-mail secara proaktif.

e. Shouldersurfing
   menggambarkan proses pengamatan langsung yang dilakukan dengan tujuan untuk mengumpulkan informasi; biasanya digunakan untuk mengekstraksi data otentikasi

f. Dhumpsterdiving
   Mengacak tong sampah adalah teknik sosial engineering lainnya yang populer. Sampah perusahaan dapat mengumpulkan banyak data penting. Bagan organisasi, memo, petunjuk kebijakan perusahaan,

jadwal pertemuan, kegiatan, manual sistem, disket, tape, kertas surat perusahaan, formulir memo, dan perangkat keras yang usang adalah beberapa contoh kebocoran keamanan yang mungkin terjadi di tong sampah, menurut "The LAN Times."

g. Reverse socialengineering
Metode pengumpulan data paling baru adalah reverse social engineering. Serangan reverse social engineering yang direncanakan dan dilaksanakan dengan baik dapat memberi hacker kesempatan yang jauh lebih besar untuk mendapatkan data karyawan jika seorang hacker berpura-pura menjadi seseorang yang memiliki otoritas. Namun, metode ini memerlukan banyak hacking, studi, dan persiapan. Seorang pencuri menyabotase jaringan, menyebabkan masalah.

4.1.2. Dampak sosial engginering

a. Kehilangan Data: Penyerang dapat mencuri data pribadi seperti nomor telepon, informasi akun, dan lain-lain dan kemudian menjualnya di dark web atau digunakan untuk tujuan yang tidak sah.
b. Infeksi Malware: Social engineering dapat digunakan untuk menginfeksi sistem dengan malware, virus, atau ransomware, yang dapat menyebabkan kerusakan sistem dan data serta meminta tebusan.
c. Kerusakan Sistem: Serangan social engineering dapat menyebabkan kerusakan sistem, seperti menghapus atau mengenkripsi file, yang dapat merugikan perusahaan.
d. Kehilangan Kepercayaan: Social engineering dapat merusak kepercayaan masyarakat dan reputasi organisasi, yang dapat berdampak pada kualitas bisnis.
e. Kerusakan Lingkungan: Social engineering dapat digunakan untuk mengubah cara masyarakat bertindak untuk menyelamatkan lingkungan, yang dapat mengancam kelestarian ekosistem.

4.2 Pembahasan kasus investasi crypto

Kasus penipuan kripto adalah ketika seseorang atau kelompok menggunakan metode yang melanggar hukum untuk mengambil keuntungan dari orang lain melalui mata uang kripto. Penipuan ini seringkali memanfaatkan ketidaktahuan atau ketidakwaspadaan korban terhadap teknologi dan sistem keamanan cryptocurrency. Mata uang kripto seperti Bitcoin dan Ethereum telah menjadi alat investasi dan transaksi digital yang semakin populer. Namun, karena popularitasnya yang meningkat, muncul berbagai skema penipuan yang menargetkan orang yang tidak berpengalaman atau tidak waspada[7]. Penipuan kripto dapat datang dalam berbagai bentuk, dan penipu menggunakan metode manipulasi psikologis canggih untuk mengeksploitasi korban. Untuk membujuk korban untuk mengungkapkan informasi sensitif atau menginvestasikan uang mereka dalam skema palsu, mereka sering menciptakan situasi yang tampaknya benar. Selain itu, pelaku yang mahir dalam teknik hacking dan social engineering masih dapat menggunakan teknologi blockchain yang mendasari cryptocurrency, meskipun aman.

4.2.1. Jenis-jenis penipuan crypto

a. Aset Fiktif
Keuntungan besar menjanjikan dari aset digital yang tidak didaftarkan oleh otoritas pengatur. Namun, aset ini tidak disekuritisasi oleh perusahaan atau didaftarkan oleh otoritas pengatur. Tidak adanya prospektus terdaftar yang mengesahkan keamanan, informasi manajemen, atau laporan keuangan menurunkan kredibilitas aset yang dijual ke publik. Kami berharap regulator akan memperketat peraturan ICO untuk melindungi kepentingan investor mengingat banyaknya penerbitan sekuritas kripto dan kurangnya pemahaman publik tentang industri dan masalahnya. Sebagai contoh, pertimbangkan keputusan Komisi Perdagangan Berjangka Komoditi dan Komisi Cryptocurrency pada Februari 2018. Komisi tersebut menyatakan bahwa hingga saat ini, semua ICO yang diawasi SEC dianggap sebagai sekuritas, kecuali Bitcoin dan baru-baru ini, yang tidak dianggap sebagai sekuritas.

b. Dana Investasi Palsu
Banyak dana investasi kripto mencoba memikat investor dengan keuntungan besar yang tidak berdasar, karena manajemen aset menjadi salah satu pendorong pertumbuhan. Sebagian besar program ini didasarkan pada program pemasaran berjenjang yang mendorong investor untuk meningkatkan keuntungan bisnis selain berkontribusi pada program. Dengan terdaftar di CME dan CFE, pasar dapat bertaruh pada kenaikan harga Bitcoin berjangka, yang meningkatkan minat investor terhadap aset tersebut. Dimasukkannya Bitcoin di 4,444 bursa terkemuka mendorong investor untuk membeli aset tersebut dengan asumsi bahwa itu adalah aset yang sah. Karena mata uang kripto secara eksplisit dikategorikan sebagai sekuritas, otoritas yang bertanggung jawab atas klasifikasi tersebut berada di bawah yurisdiksi regulator sekuritas.

c. Pertukaran Crypto yang Tidak Diatur
Manipulasi pasar berarti dengan sengaja membuat harga barang, keamanan, komoditas, atau mata uang palsu. Karena portal yang tidak terikat dengan banyak regulasi investor, aset yang diperdagangkan di sana dapat terkena berbagai manipulasi pasar. Di masa lalu, banyak kasus di mana manipulasi pasar—jika bukan perdagangan curang—dilakukan di portal, termasuk ramping dan churning. Ini berbeda dengan bursa komoditas atau sekuritas biasa.

d. Keamanan Cyber
Karena memilikinya, semakin banyak orang yang ingin menyimpannya. Istilah "tukaran" mengacu pada dompet desktop, aplikasi seluler, dan dompet online tempat cryptocurrency dan data pribadi disimpan dengan aman. Penyedia Exchange menyimpan data terenkripsi atas nama pemiliknya, meskipun Exchange dianggap sebagai metode penyimpanan yang paling rentan terhadap pencurian dan penipuan dan mungkin tidak tunduk pada pengawasan peraturan.

4.2.2. Dampak penipuan investasi crypto

Penipuan investasi crypto memiliki dampak yang luas dan mendalam, mempengaruhi individu, masyarakat, dan industri secara keseluruhan. Dampak ini dapat dikategorikan menjadi beberapa aspek utama:

a. Dampak Finansial
1) Kerugian Uang: Investor kripto sering kehilangan banyak uang karena penipuan. Karena transaksi kripto anonim dan tidak dapat dipulihkan, dana yang hilang hampir tidak mungkin dikembalikan.
2) Kerugian Aset: Korban dapat kehilangan aset kripto lainnya atau uang tunai mereka. Dalam situasi tertentu, seluruh portofolio crypto korban dapat lenyap.

b. Dampak Psikologis
1) Stres dan Kecemasan: Korban penipuan investasi dapat mengalami stres dan kecemasan yang signifikan, terutama ketika kehilangan uang memengaruhi kehidupan mereka secara signifikan.
2) Rasa Malu dan Kehilangan Kepercayaan Diri: Korban mungkin merasa malu dan tidak percaya diri lagi dalam membuat keputusan finansial di masa depan karena tertipu.
3) Depresi: Dalam kasus yang lebih parah, kehilangan uang dapat menyebabkan depresi dan masalah kesehatan mental lainnya.

c. Dampak Sosial
1) Kehilangan Kepercayaan: Penipuan investasi kripto dapat merusak kepercayaan masyarakat terhadap teknologi blockchain dan cryptocurrency. Orang mungkin ragu untuk berinvestasi atau menggunakan mata uang kripto karena hal ini.
2) Hubungan Sosial: Kehilangan uang dapat memengaruhi hubungan pribadi, menimbulkan konflik dengan teman dan keluarga.

d. Dampak pada Industri Crypto
1) Menurunkan Reputasi: Penipuan cryptocurrency dapat merusak reputasi industri crypto secara keseluruhan. Ini mungkin menghalangi adopsi teknologi baru dan inovasi di ruang blockchain.
2) Regulasi yang Lebih Ketat: Penipuan yang meluas dapat mendorong pemerintah dan regulator untuk memberlakukan peraturan yang lebih ketat terhadap industri crypto. Ini dapat menghambat pertumbuhan dan inovasi.

e. Dampak Ekonomi
1) Kehilangan Investasi: Penipuan crypto dapat menyebabkan penurunan investasi dalam industri kripto dan teknologi blockchain secara keseluruhan. Investor mungkin menjadi lebih berhati-hati dan menghindari investasi dalam proyek-proyek baru.
2) Pengurangan Aktivitas Ekonomi: Penipuan yang signifikan dapat menyebabkan pengurangan aktivitas ekonomi di sektor terkait, mempengaruhi berbagai layanan yang bergantung pada transaksi dan investasi kripto.

4.3 Pencegahan sosial engginering

Untuk mencegah social engineering, ada banyak langkah yang harus diambil, termasuk teknologi, kebijakan keamanan, pendidikan, dan sikap skeptis yang sehat. Pelatihan rutin meningkatkan kesadaran risiko dan tanda-tanda social engineering. Penggunaan teknologi canggih dan kebijakan keamanan yang kuat dapat melindungi data sensitif dan mendeteksi aktivitas mencurigakan. Untuk mencegah penipuan, sikap skeptis dan verifikasi identitas saat menerima permintaan informasi atau tindakan tertentu juga

penting. Pendekatan holistik ini dapat membantu orang dan organisasi menghindari serangan social engineering dan melindungi diri dari ancaman baru.

a. Pencegahan sosial engginering pada kasus penipuan investasi crypto
   Pendidikan, teknologi, peraturan, dan kebijakan perusahaan yang kuat dapat mencegah penipuan investasi kripto yang memanfaatkan teknik social engineering. Pertama dan terpenting, meningkatkan literasi digital sangat penting. Sangat penting bagi masyarakat untuk mempelajari dasar-dasar cryptocurrency, bagaimana investasi crypto, dan tanda-tanda penipuan. Pelatihan, workshop, dan kampanye kesadaran publik melalui media sosial, seminar, dan sumber pendidikan lainnya dapat membantu masyarakat lebih memahami bahaya dan cara menghindari penipuan ini. Selain itu, sangat penting untuk memberikan pendidikan tentang keamanan siber yang mencakup pengetahuan dasar seperti penggunaan kata sandi yang kuat, mengidentifikasi email phishing, dan pentingnya menjaga kerahasiaan informasi pribadi.

   Teknologi harus mendorong penggunaan verifikasi dua faktor (2FA) untuk mengamankan akun crypto karena menambah lapisan keamanan tambahan, menghalangi penipu untuk mengakses akun korban. Selain itu, menggunakan dompet kripto yang aman, seperti dompet hardware atau penyimpanan dingin, dapat melindungi aset kripto lebih baik daripada menggunakan dompet online. Untuk melindungi terhadap kerentanan keamanan yang diketahui, penting untuk selalu memperbarui perangkat lunak dan aplikasi crypto ke versi terbaru.

   Verifikasi dan skeptisisme adalah kunci untuk menghindari penipuan. Investor cryptocurrency harus memastikan platform mereka memiliki proses verifikasi identitas yang ketat dan reputasi yang baik. Untuk menghindari penipuan, lakukan penelitian independen sebelum berinvestasi, periksa ulasan, dan periksa rekam jejak perusahaan. Selain itu, sangat penting untuk berhati-hati terhadap tawaran investasi yang menjanjikan keuntungan besar dalam waktu singkat karena itu mungkin merupakan penipuan.

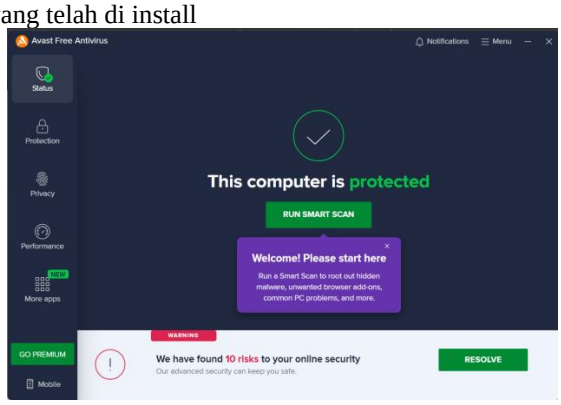
   Pemerintah dan otoritas keuangan harus menerapkan peraturan yang ketat untuk mengawasi platform investasi crypto dan melindungi investor. Pemerintah juga harus membuat dan menegakkan peraturan yang melindungi investor dari penipuan dan mendorong masyarakat untuk melaporkan insiden dan upaya penipuan kepada otoritas berwenang. Pelaporan yang cepat dapat mencegah penipuan lebih lanjut dan melindungi korban potensial lainnya.

b. Aplikasi yang dapat digunakan untuk mencegah sosial engginering
   Avast Free Antivirus adalah perangkat lunak keamanan dengan berbagai fitur yang melindungi komputer pengguna dari ancaman internet seperti virus, malware, spyware, ransomware, dan serangan phishing. Sebagai salah satu produk antivirus gratis paling populer, Avast Free Antivirus menawarkan perlindungan yang komprehensif tanpa biaya, menjadikannya pilihan yang populer bagi pengguna yang membutuhkan solusi keamanan yang efisien.

4.4 Penggunaan avast free anti virus

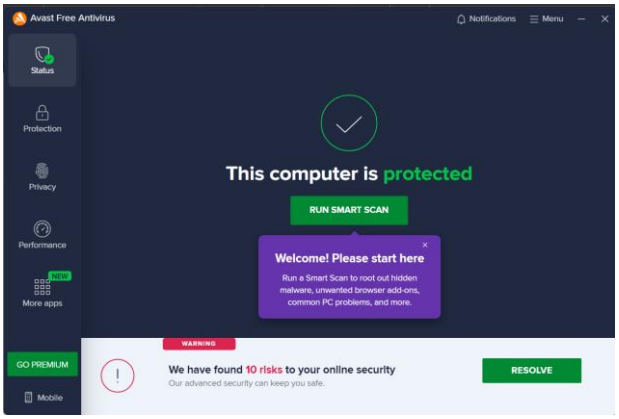
Avast Free Antivirus sukup baik dalam membantu menangani sosial engginering, Rekayasa sosial seringkali melibatkan manipulasi psikologis untuk memperoleh informasi atau akses yang tidak sah. Pada avast free anti virus terdapat 3 fitur utama yang berguna untuk mencegah sosial engginering yaitu web shield, mail shield, dan file shield berikut adalah cara untuk mengaktifkan fitur-fitur tersebut

a. Masuk ke aplikasi avast yang telah di install



Gambar 1 Masuk Ke avast

b. Klik protection lalu buka core shield



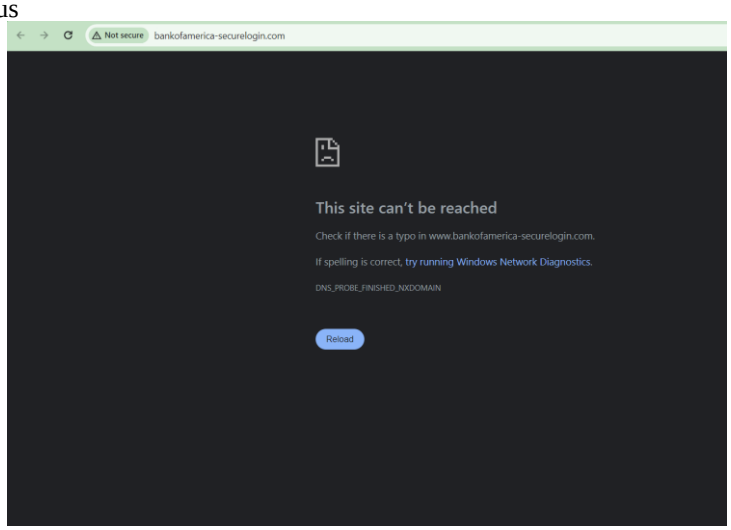
Gambar 2 klik protection

c. Aktifkan ketiga fitur shield yang di butuhkan

Gambar 3 Aktifkan fitur shield

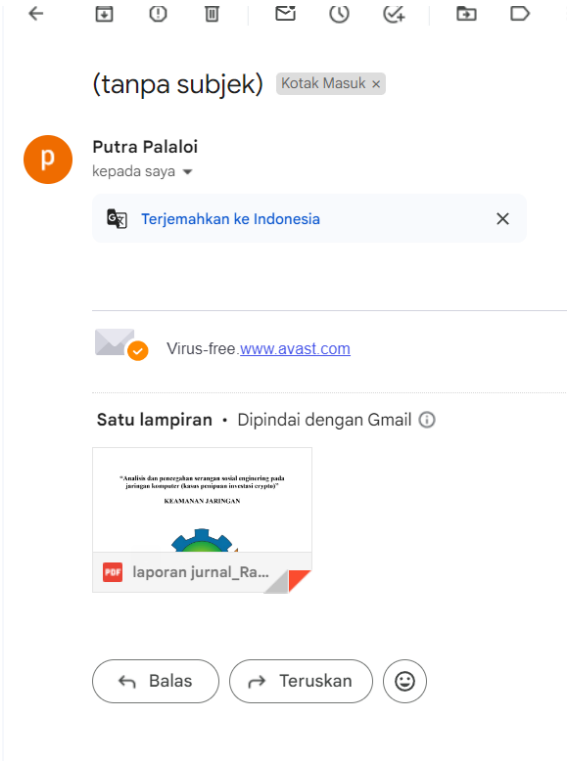
Setelah selesai mengaktifkan ketiga fitur yang dibutuhkan Langkah selanjutnya adalah percobaan apakah fitur tersebut berfungsi dengan benar berikut adalah penjelasan singkat tentang fitur tersebut serta percobaan penggunaannya.

d. Avast Free Antivirus memiliki fitur Web Shield yang memindai situs web untuk mendeteksi ancaman dan menghalangi akses ke situs yang mencurigakan atau berbahaya. Ini penting untuk mencegah pengguna dari mengunjungi situs web phishing yang sering digunakan dalam serangan rekayasa sosial untuk mencuri informasi pribadi. Berikut adalah tampilan website yang terindikasi berbahaya oleh avast free anti virus



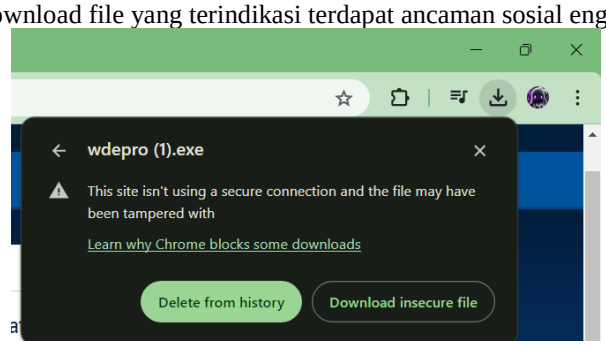
Gambar 4 website yang terindikasi berbahaya

e. Avast Free Antivirus memiliki fitur mail Shield yang memindai email yang dikirim ke pengguna untuk mendeteksi ancaman dan menghalangi yang mencurigakan atau berbahaya. Ini penting untuk mencegah pengguna dalam menerima sebuah email phishing yang sering digunakan dalam serangan rekayasa sosial untuk mencuri informasi pribadi. Berikut adalah tapilan email yang telah di pindai oleh avast free anti virus



Gambar 5 email yang telah di pindai

f. Avast Free Antivirus memiliki fitur file Shield yang memindai file yang akan di download oleh pengguna untuk mendeteksi ancaman yang mencurigakan atau berbahaya. Ini penting untuk mencegah pengguna dalam mendownload file yang terindikasi terdapat ancaman sosial engginering.



Gambar 6 Fitur file shield avast

5. KESIMPULAN DAN SARAN

Setelah melakukan penelitian saya sebagi penulis menyimpulkan bahwa penipuan investasi cryptocurrency dengan menggunakan rekayasa sosial menjadi ancaman serius di era digital saat ini. Teknik rekayasa sosial seperti phishing, pencurian identitas, dan manipulasi emosional telah terbukti efektif dalam membujuk korban untuk mengungkapkan informasi sensitif atau berinvestasi dalam skema penipuan. Dampak dari penipuan ini tidak terbatas pada kerugian finansial tetapi juga mencakup konsekuensi psikologis dan sosial yang signifikan, seperti stres, kecemasan, dan hilangnya kepercayaan masyarakat terhadap teknologi blockchain dan mata uang kripto.

Untuk menjawab tantangan ini, beberapa usulan strategis dapat diajukan. Pertama, penting untuk meningkatkan pendidikan dan kesadaran masyarakat tentang mata uang kripto dan risiko penipuan

investasi, melalui program pendidikan masyarakat yang komprehensif dan kampanye kesadaran di seluruh jaringan sosial. Kedua, ada kebutuhan untuk memperkuat kebijakan keamanan perusahaan dan platform investasi mata uang kripto untuk melindungi data sensitif dan mendeteksi aktivitas mencurigakan dengan lebih efektif. Selain itu, pelatihan rutin bagi karyawan dan pengguna platform tentang tanda-tanda serangan rekayasa sosial serta peningkatan peraturan di sektor mata uang kripto juga wajib dilakukan. Terakhir, kolaborasi aktif antara pemerintah, regulator, dan industri untuk memerangi penipuan investasi mata uang kripto dan penelitian berkelanjutan untuk memahami evolusi teknik rekayasa sosial dapat membantu Sangat bermanfaat dalam meminimalkan risiko dan memperkuat kepercayaan pada ekosistem mata uang kripto. Dengan menerapkan rekomendasi ini secara komprehensif, kami berharap dapat mengurangi dampak negatif penipuan investasi mata uang kripto rekayasa sosial dan meningkatkan perlindungan investor di masa depan.

DAFTAR PUSTAKA

[1] S. Sadya, “APJII: Pengguna Internet Indonesia 215, 63 Juta pada 2022-2023. DataIndonesia. Id.” 2023.

[2] K. K. R. Indonesia, “Ekonomi digital Indonesia diprediksi tumbuh delapan kali lipat di tahun 2030.” hal. 27, 2021.

[3] A. Napila dan A. Hidayat, “Social Engineering: Menghindari Kejahatan Saat Menggunakan Sosial Media di Pondok Pesantren Nafidatunnajah,” *J. Penelit. Sist. Inf.*, no. 1, hal. 44–48, 2023.

[4] K. Tjendrawinata, “Social Engineering: Crisis in Humanity,” *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 3, hal. 2085–2095, 2022, doi: 10.35957/jatisi.v9i3.2206.

[5] federal burau of Investigation(FBI), “Internet Crime Report,” 2023.

[6] E. M. Safitri, Z. Ameilindra, dan R. Yulianti, “Analisis Teknik Social Engineering Sebagai Ancaman Dalam Keamanan Sistem Informasi: Studi Literatur,” *J. Ilm. Teknol. Inf. dan Robot.*, vol. 2, no. 2, hal. 21–26, 2020, doi: 10.33005/jifti.v2i2.26.

[7] Z. H. Bik, “Manajemen Resiko, Tantangan dan Ketidakpastian Regulasi Investasi Cryptocurrency dalam Pandangan Ekonomi Syariah,” *J. Kewarganegaraan*, vol. 6, no. 3, hal. 6466–6478, 2022.

[8] Asry, D. W., Siswanto, E., Kurniawan, D., & Huda, H. I. (2023). Deteksi Malware Statis Menggunakan Deep Neural Networks Pada Portable Executable. *Teknik: Jurnal Ilmu Teknik dan Informatika*, *3*(1), 19-34.

[9] Asry, D. W., Siswanto, E., Kurniawan, D., & Huda, H. I. (2023). Deteksi Malware Statis Menggunakan Deep Neural Networks Pada Portable Executable. *Teknik: Jurnal Ilmu Teknik dan Informatika*, *3*(1), 19-34.

[10] Sunarto, M. W., Kurniawan, D., Siswanto, E., & Huda, H. I. (2021). Deteksi Anomali Menggunakan Extended Isolation Forest (Eif). *Teknik: Jurnal Ilmu Teknik dan Informatika*, *1*(2), 96-111.