Pubarama
Jurnal Publikasi Pengabdian Kepada Masyarakat
Volume 6 Nomor 2, Juni 2026

e-ISSN : 2798-8880
p-ISSN : 2798-9976

Workshop SCAM in The AI Eras pada Kegiatan Sadar Digital: AI SCAM Safety Seminar

Hendra[1*], Awan[2], Benny[3], Waisen[4], Wilianto[5], Yudi[6]
[1]Fakultas Sains dan Teknologi, Teknik Informatika, Universitas IBBI, Medan, Indonesia
[2]Fakultas Sains dan Teknologi, Sistem Informasi, Universitas IBBI, Medan, Indonesia
[3]Fakultas Sains dan Teknologi, Teknik Informatika, Universitas IBBI, Medan, Indonesia
[4]Fakultas Sains dan Teknologi, SistemInformasi, Universitas IBBI, Medan, Indonesia
[5]Fakultas Sains dan Teknologi, Teknologi Informasi, Universitas IBBI, Medan, Indonesia
[6]Fakultas Sains dan Teknologi, Sistem Informasi, Universitas IBBI, Medan, Indonesia

Email: [1]hendra.soewarno@gmail.com, [2]one.awan@gmail.com, [3]bennyshen77@gmail.com, [4]whisen@gmail.com, [5]wiliantogan@gmail.com, [6]yudifanggawa@gmail.com
(*: coressponded author)

Abstrak− Praktik penipuan (*scam*) telah eksis sejak awal peradaban manusia dan terus berevolusi mengikuti perkembangan zaman. Di era digital dan perkembangan kecerdasan buatan (AI) membawa dilema baru; pada satu sisi memberikan efisiensi masif, namun di sisi lain mengamplifikasi modus penipuan berbasis AI-generated yang makin menyakinkan melalui manipulasi teks, klon suara, hingga video deepfake. Berdasarkan data dari Otoritas Jasa Keuangan (OJK) pada tahun 2025, kerugian akibat aktivitas keuangan ilegal dan scam di Indonesia adalah mencapai Rp4,6 triliun. Fenomena ini menegaskan urgensi edukasi publik guna meningkatkan literasi siber masyarakat. Kegiatan Pengabdian kepada Masyarakat (PKM) ini bertujuan untuk membekali masyarakat dengan pemahaman teoritis dan praktis dalam mengidentifikasi dan memitigasi risiko penipuan berbasis AI. Metode pelaksanaan PKM ini diawali dengan penyusunan materi workshop melalui studi literatur, berita dan wawancara mendalam dengan korban scam. Hasil penyusunan diwujudkan ke dalam materi presentasi taktis dan diseminasi hasil melalui pelaksanaan workshop bertajuk "*Scam in the AI Eras*" yang diintegrasikan dalam seminar "Sadar Digital: AI Scam Safety Seminar". Kegiatan ini dilaksanakan di Universitas IBBI dan dihadiri oleh lebih dari 500 peserta yang terdiri dari siswa SMA, mahasiswa, dosen, serta masyarakat umum. Melalui edukasi ini, para peserta dibekali dengan pemahaman psikologi dan protokol keamanan mandiri untuk mengenali manipulasi digital, sehingga diharapkan dapat menekan angka korban siber dan menciptakan ruang digital yang lebih aman serta resilien.

Kata Kunci: Kecerdasan Buatan, Deepfake, Literasi Digital, Pengabdian kepada Masyarakat, Scam.

Abstract− *Fraudulent practices (scams) have existed since the beginning of human civilization and continue to evolve with the times. The digital era and the development of artificial intelligence (AI) present a new dilemma: on the one hand, they provide massive efficiency, but on the other, they amplify increasingly convincing AI-generated fraud schemes through text manipulation, voice cloning, and deepfake videos. According to data from the* Otoritas Jasa Keuangan *(OJK), losses due to illegal financial activities and scams in Indonesia are expected to reach IDR 4.6 trillion by 2025. This phenomenon underscores the urgency of public education to improve cyber literacy. This Community Service (PKM) activity aims to equip the public with theoretical and practical understanding in identifying and mitigating the risks of AI-based fraud. The PKM implementation method begins with the development of workshop materials through literature studies, news reports, and in-depth interviews with scam victims. The results are then translated into tactical presentation materials and disseminated through a workshop titled "Scam in the AI Era," which is integrated into the "Sadar Digital: AI Scam Safety Seminar" seminar. This activity was held at IBBI University and attended by over 500 participants, including high school students, university students, lecturers, and the general public. Through this education, participants were equipped with an understanding of psychology and self-security protocols for recognizing digital manipulation, which is expected to reduce the number of cyber victims and create a safer and more resilient digital space.*

Keywords: *Artificial Intelligence, Deepfake, Digital Literacy, Community Service, Scam.*

1. PENDAHULUAN

Praktik scam terus berevolusi secara historis seiring dengan perkembangan peradaban dan teknologi manusia. Mulai dari manipulasi alkimia pada Abad Pertengahan, lahirnya skema Ponzi oleh Charles Ponzi (1920), hingga skema penipuan investasi berskala masif oleh Bernie Madoff yang runtuh saat krisis *subprime mortgage* tahun 2008 karena banyak nasabah mencairkan investasi pada saat yang sama. Memasuki abad ke-21, lompatan teknologi komunikasi lintas batas yurisdiksi sempat memfasilitasi penipuan massal tanpa tatap muka lintas negara. Kehadiran kecerdasan buatan (AI) membawa dilema baru yang jauh lebih mengkhawatirkan. Teknologi *AI-generated* mampu memanipulasi teks, email, klon suara, hingga *video deepfake* dengan tingkat kemiripan sangat tinggi dengan biaya produksi yang rendah. Akibatnya, masyarakat menjadi sangat rentan terhadap ancaman siber mutakhir seperti *phishing*, *scamming*, *smising*, *vishing* sampai *love scam.* Dampak dari eskalasi ini tercermin

e-ISSN : 2798-8880
p-ISSN : 2798-9976

laporan Otoritas Jasa Keuangan (OJK) per Agustus 2025 pada kegiatan Kampanye Nasional Berantas *Scam*, yang melaporkan adanya 225.281 laporan kasus dengan total kerugian dana korban di Indonesia mencapai Rp4,6 triliun, dan hanya Rp349.3 milyar yang berhasil diblokir.

Merespons urgensi dan besarnya potensi kerugian tersebut, tim dosen Universitas IBBI hadir menjadi kontributor pada kegiatan Pengabdian kepada Masyarakat (PKM) dalam bentuk workshop yang bertajuk "*Scam in the AI Eras*" yang merupakan bagian dari rangkaian kegiatan pada "Sadar Digital: *AI Scam Safety Seminar*". Kegiatan ini secara umum bertujuan untuk memberikan pemahaman yang menjembatani aspek teoritis dan praktis kepada masyarakat mengenai pemanfaatan AI sebagai instrumen penipuan baru. Melalui program edukasi ini, tim PKM berkomitmen untuk tidak sekadar mengenalkan teknologi AI yang berpotensi disalahgunakan, melainkan juga membangun benteng pertahanan psikologis dan digital bagi audiens, sekaligus menggeser paradigma keliru bahwa korban penipuan adalah individu yang kurang cerdas secara intelektual. Sebaliknya, kegiatan ini bertujuan mengedukasi publik bahwa penipuan era AI adalah murni memanipulasi psikologis dan emosi manusia, memanfaatkan rasa percaya terhadap figur publik atau otoritas tertentu, serta menciptakan situasi darurat yang sengaja mengincar orang normal saat berada dalam kondisi lengah, seperti ketika sedang sibuk, panik, atau terlalu gembira.

Secara spesifik, luaran dan target capaian yang ingin diwujudkan melalui kegiatan PKM ini meliputi empat poin utama. Pertama, meningkatkan kapasitas audien dalam mengidentifikasi modus baru kejahatan berbasis AI seperti *deepfake*, *voice cloning*, dan *generative text*. Kedua, mendekonstruksi pemahaman masyarakat terkait sisi psikologi korban agar kewaspadaan dapat ditingkatkan tanpa adanya stigma sosial. Ketiga, memperkenalkan dan melatih implementasi kerangka kerja PAUSE sebagai protokol keamanan mandiri untuk menunda keputusan saat emosional, membangun penalaran kritis terhadap bukti *audio-visual*, serta memanfaatkan alat digital untuk verifikasi informasi. Keempat, menumbuhkan kewaspadaan kolektif masyarakat sebagai lini pertahanan terakhir dalam ekosistem digital demi mewujudkan ruang siber yang lebih aman dan resilen.

2. KERANGKA TEORI

Materi *workshop* disusun dengan mengambil referensi dari berbagai sumber informasi yang kemudian dikembangkan secara runut sesuai dengan psikologi dari hasil wawancara dengan beberapa narasumber yang pernah mengalami pengalaman upaya *scam*. Pendekatan ini dilakukan bertujuan agar para peserta *workshop* dapat mengikuti, memahami, dan merasakan secara langsung kondisi psikologi korban jika mereka berada pada situasi yang sama, kemudian membahas taktik operandi pelaku, hingga berakhir pada pembahasan metode proteksi diri guna terhindar menjadi korban.

2.1. Penipuan di Internet

Penipuan di internet yang dikenal dengan istilah *scam* dalam perspektif psikologi bukan sekedar tindakan kriminal yang mengekploitasi kelemahan sistem komputer sebagaimana yang dilakukan oleh *cracker* pada umumnya, melainkan sebuah bentuk manipulasi psikologi tingkat tinggi yang dikenal dengan istilah rekayasa sosial (*social engineering*). *Scam* bertujuan mengambil keuntungan finansial ataupun mengambil data sensitif korban dengan cara memanipulasi kesadaran korban.

Scam tidak menyerang IQ seseorang, tetapi lebih kepada ekploitasi kelemahan dari sisi emosional manusia. Kelompok yang rentan akan tindakan penipuan mencakup kepada orang yang sibuk, berada pada kondisi psikologi ekstrem seperti terlalu panik atau terlalu senang, serta mereka yang terlalu percaya kepada visual maupun figur otoritas tertentu (Modic & Lea, 2012)

2.2. Modus Operandi Penipuan

Modus operandi kejahatan digital direncang secara taktis melalui beberapa tahapan psikologi untuk memperdaya emosional korban. Pola ini dapat dianalisis melalui struktur interaksi yang diawali dengan memberikan umpan penipuan (*The Bait*) dengan menawarkan iming-iming stimulus ekonomi yang sangat menarik yang dapat berupa hadiah, tawaran investasi, pemberian barang gratis secara terbatas sampai kepada membangun hubungan pribadi (*love scam*) untuk memicu ketertarikan korban dan meruntuhkan kewaspadaan korban. Untuk lebih menyakinkan korban mereka akan melakukan rekayasa konteks fiktif dengan mencatut identitas tokoh publik atau tokoh terkenal yang memiliki rekam jejak dan reputasi yang luar biasa sehingga korban menyakini bahwa penawaran tersebut sah dan kredibel ataupun terlalu kecil dilakukan oleh tokoh dengan reputasi yang tinggi dan kedermawanannya. Kemudian melakukan manipulasi transaksional ringan, dimana korban digiring untuk

e-ISSN : 2798-8880
p-ISSN : 2798-9976

merasa bahwa mereka hanya menanggung konsekuensi ringan dibandingkan dengan janji hasil yang bakal didapatkan.

Pada contoh studi kasus *Video Giveaway* Le Creuset, penipu menampilkan video aktris Taylor Swift sedang menawarkan *giveaway* produk dapur premium Le Creuset kepada para penggemarnya. Dalam video deepfake tersebut, nampak seakan-akan Taylor Swift menyebutkan bahwa akibat adanya kesalahan pengemasan, terdapat 3.000 set *cookware* Le Creuset akan dibagikan secara gratis. Peminat hanya diminta untuk mengisi formulir kuisioner dan membayar ongkos kirim dengan kartu kredit. Untuk memberikan efek mendesak, penawaran tersebut dibatasi sebelum hari berakhir dengan bersifat *first-come-first-serve*, serta didukung oleh tampilan manipulatif pada situs palsu yang menunjukkan kuota barang yang terus menipis demi memicu kepanikan psikologis korban (CBS News, 2024).

2.3. Penyalahgunaan AI Deepfake

Kehadiran teknologi AI meningkatkan lanskap ancaman siber secara radikal. Salah satu produk turunan AI terkini yang banyak digunakan dalam dunia penipuan adalah media sintesis (Deepfake). Deepfake merupakan materi video, audio, atau gambar hasil rekayasa AI tingkat lanjut yang membuat seseorang tampak mengatakan atau melakukan sesuatu yang sebenarnya tidak pernah mereka katakan atau lakukan secara realitas (Merriam-Webster, n.d.)

Dewasa ini banyak tersedia sofware yang dapat diperoleh secara berbayar ataupun cuma-cuma untuk membuat materi *deepfake* baik secara *offline* maupun *realtime online* sebagaimana yang didemokan video call online yang menggunakan avatar tokoh terkenal seperti Taylor Swift untuk mengelabui mata atau persepsi audiens, sehingga memangkas skeptisisme visual secara alami yang dimiliki manusia.

2.3. Fraud Diamond

Untuk memahami dinamika interaksi antara kapasitas pelaku kriminal dan kondisi psikologis korban, kejahatan siber berbasis AI dapat dibedah menggunakan teori Fraud Diamond.

Dari sisi pelaku, perkembagan AI secara signifikan meningkatkan kapabilitas pelaku dimana teknologi AI memangkas batasan teknis, mempermudah dan mempercepat pembuatan konten palsu beresolusi tinggi yang tampak sangat nyata dan professional. Keberadaan sosial media membuat materi yang telah disiapkan dapat didistribusikan secara massal kepada target korban dengan memanfaatkan algoritma platform sosial media yang mempelajari perilaku audien sehingga iklan scam secara efektif ditampilkan kepada target konsumen yang tepat dengan *preferensi brand* atau tokoh tertentu tanpa membutuhkan verifikasi identitas pelaku secara ketat. Pelaku melakukan rationalisasi membenarkan tindakan kriminal yang dilakukannya melalui pembelaan moral internal, seperti menganggap bahwa tindakan yang dilakukan hanya mengambil sejmulah uang kecil dari korban yang pada dasarnya memiliki sifat tamak, terlalu mudah percaya ataupun ceroboh (Wolfe & Hermanson, 2004).

Kemudian dari sisi korban, mereka dipengaruhi oleh pressure dan urgensi yang dibangkitkan oleh skema pelaku yaitu korban dijebak oleh psikologi kelangkaan melalui "*Giveaway* berlaku hari ini saja, kuota adalah terbatas dan *count down first-come-first-serve* palsu yang menunjukan sisa kuota yang semakin menurun", kondisi ini memicu kepanikan situasional yang dikenal sebagai *Fear of Missing Out* (FOMO). Kemudian karena adanya knowledge gap menyebabkan korban terjebak dengan mengasumsikan penawaran tersebut *legit* karena melibatkan figur publik yang mereka kenal (Sari & Sary, 2020)

2.4. Konflik Neurosains

Fenomena mengapa korban berkecerdasan tinggi dengan pendidikan tinggi tetap dapat menjadi korban scam adalah dapat dijelaskan melalui cara kerja anatomi otak manusia (Goleman, 1995). Sistem limbik (Otak Reptil & Mamalia) merupakan bagian otak yang berfungsi mengendalikan emosi, rasa takut, kesenangan, dan insting otomatis. Pada saat melihat penawaran hadiah menarik yang tampak legit, sistem limbik akan aktif secara impulsive, sedangkan Neo-Cortex(Otak Logis) merupakan bagian otak yang bertanggung jawab atas proses berpikir logis, analitis, kritis. Penipu sengaja menciptakan situasi urgen, sistem limbik mengalami luapan emosi ekstrem yang secara efektif melumpuhkan fungsi kerja Neo-Cortex, akibatnya otak kehilangan kesempatan untuk memproses dan memverifikasi informasi secara rasional.

2.5. Protokol Keamanan Mandiri

Untuk benteng pertahanan kognitif, masyarakat dapat mengadopsi protocol taktis P-A-U-S-E secara konsisten guna memutus rantai manipulasi psikologis penipu secara mandiri.

e-ISSN : 2798-8880
p-ISSN : 2798-9976

P - Pause (Jeda): Berhenti sejenak dan jangan mengambil tindakan atau keputusan transaksional apa pun ketika berada dalam kondisi emosi yang meluap seperti rasa terlalu senang maupun terlalu panik. Jeda ini krusial untuk menurunkan tensi sistem limbik dan memberikan waktu yang cukup membangkitan kendali logis otak (Goleman, 1995).

A - Authenticate (Autentikasi): Lakukan verifikasi dan konfirmasi mandiri melalui kanal atau nomor telepon resmi institusi yang bersangkutan. Jika dihubungi oleh pihak yang mencurigakan, segera putuskan panggilan dan hubungi kembali nomor resmi lembaga terkait. Jika menerima tautan, hindari melakukan klik secara langsung dan ketik URL resmi institusi secara manual pada peramban (Jakobsson & Myers, 2006).

U - Use Skepticism (Gunakan Skeptisisme): Bangun paradigma berpikir kritis dan kewaspadaan tinggi bahwa di era kecerdasan buatan, bukti visual berbentuk video maupun rekaman suara, tokoh ataupun otoritas tertentu tidak lagi dapat dijadikan jaminan kebenaran mutlak (Vaccari & Chadwick, 2020).

S - Search (Pencarian Informasi): Lakukan mitigasi dan penelusuran informasi secara independen melalui mesin pencari Google, lakukan pemeriksaan kepemilikan domain situs, atau manfaatkan alat bantu AI untuk menguji apakah nomor telepon, identitas, atau URL yang diterima berstatus legal atau terindikasi sebagai entitas penipuan (Wineburg & McGrew, 2019).

E - Educate (Edukasi Berkelanjutan): Membangun komitmen personal maupun kolektif untuk terus memperbarui literasi digital, memahami regulasi keamanan siber yang berlaku, serta mengikuti perkembangan tren modus penipuan berbasis teknologi terbaru secara konsisten (Purkait, 2012).

3. METODE PENGABDIAN KEPADA MASYARAKAT

Pelaksanaan kegiatan Pengabdian kepada Masyarakat (PKM) ini dirancang melalui empat tahapan utama yang terintegrasi, yaitu analisis karakteristik target audiens, eksplorasi tren penyalahgunaan fitur AI, investigasi empiris kasus penipuan, serta perumusan instrumen edukasi taktis. Mengingat topik utama yang diangkat adalah "Scam in The AI Eras", metode pelaksanaan difokuskan untuk membedah bagaimana lompatan teknologi generatif bergeser menjadi instrumen kriminalitas baru.

Tahap awal difokuskan pada pemetaan profil dan karakteristik calon peserta workshop. Mengingat audiens seminar "Sadar Digital" bersifat heterogen, tim PKM melakukan identifikasi terhadap tingkat literasi digital awal kelompok sasaran, kesenjangan pengetahuan (knowledge gap) antar-generasi mengenai eksistensi AI, serta potensi kerentanan spesifik yang dihadapi dalam aktivitas siber sehari-hari. Hasil analisis ini menjadi jangkar bagi tim untuk menyusun strategi penyampaian materi yang membumi, komunikatif, dan bebas dari jargon-jargon teknis komputer yang sulit dipahami oleh masyarakat umum.

Tahap kedua berfokus pada studi literatur dan penelusuran data sekunder mengenai fitur-fitur AI terkini yang sedang tren disalahgunakan oleh para pelaku kejahatan. Eksplorasi ini menitikberatkan pada mekanisme media sintetis Tim menganalisis bagaimana fitur-fitur komersial AI yang mudah diakses publik diadopsi oleh penipu untuk menciptakan narasi palsu yang sangat persuasif, murah, cepat, dan terpersonalisasi dalam skala masif.

Tahap ketiga dilakukan dengan mengumpulkan studi kasus riil dari berbagai pemberitaan media massa, media online seperti Channel News Asia (CNA), talk show lainnya yang menghadirkan pakar cyber crime dan cyber security dan melakukan pendekatan empiris melalui wawancara. Tim mengompilasi berita-berita internasional dan nasional mengenai fenomena scam berbasis deepfake—seperti kasus penyalahgunaan identitas dan suara pesohor dunia dalam iklan giveaway palsu, hingga manipulasi video tokoh publik untuk *endorse* investasi bodong. Data berita tersebut kemudian ditriangulasi dengan hasil wawancara mendalam dengan beberapa korban lokal yang pernah mengalami percobaan social engineering maupun korban phishing, guna memetakan titik kelengahan psikologis korban di dunia nyata.

Tahap akhir dari metode ini adalah sintesis data, di mana tim dosen memadukan profil audiens, tren fitur AI yang disalahgunakan, dan anatomi kasus deepfake dari lapangan. Berdasarkan evaluasi tersebut, tim menyusun materi workshop non-teknis yang adaptif. Output dari tahap ini adalah perumusan modul taktis berupa langkah-

e-ISSN : 2798-8880
p-ISSN : 2798-9976

langkah proteksi mandiri—seperti kerangka kerja protokol PAUSE—sebagai benteng pertahanan kognitif demi membangun human firewall yang kuat di tengah masifnya ancaman penipuan berbasis kecerdasan buatan.

4. HASIL

Setelah materi workshop disusun, kami melaksanakan workshop pada 31 Januari 2026 di ruang serba guna Lantai 7 kampus Universitas IBBI yang dihadiri lebih dari 500 peserta yang terdiri dari siswa SMA dari berbagai sekolah, mahasiswa dari berbagai kampus, dosen dan masyarakat umum.

Kegiatan workshop diawali dengan menayangkan Video Giveaway Le Creuset, dimana 3000 kitchen set Le Creuset yang mengalami masalah pada pengemasan akan dibagikan secara cuma-cuma, penawaran berlaku hanya sampai akhir hari ini dan bersifat first-come-first-serve. Peserta yang tertarik cukup mengisi formulir online dan membayar ongkos kirim. Setelah video pemantik awal ditayangkan, pembicara secara interaktif menanyakan kepada para peserta, jika video ini muncul pada sosial media anda hari ini, apakah anda tertarik untuk mengikuti program giveaway tersebut? Kira-kira 85% peserta mengangkat tangan menyatakan tertarik.

Soulmantra menggelar kegiatan dalam program Sadar Digital (Dok. Soulmantra)

Gambar 1. Peserta Kegiatan Sadar Digital: AI SCAM SAFETY SEMINAR
(Sumber: *Waspada Online. 2026)*

Pemaparan sesi pemaparan materi, para pembicara menampilkan video realtime call yang menggunakan teknologi deepfake dan menekankan satu poin krusial bahwa efektivitas praktik scam tidak hanya bertumpu pada kecanggihan eksploitasi teknologi, melainkan pada manipulasi kerentanan psikologis manusia. Berdasarkan analisis siber, para pelaku kejahatan umumnya memanfaatkan kombinasi antara elemen tekanan, peluang, dan pembenaran diri yang dialami oleh targetnya. Akibatnya, kelengahan dan penurunan kewaspadaan sesaat dapat dengan mudah mengubah calon korban menjadi korban penipuan seutuhnya (Wacana, 2026). Fenomena ini dipertegas oleh salah satu narasumber yang menyatakan bahwa:

> “Scam dilakukan dengan pendekatan psikologi, bukan teknologi. Yang diserang itu manusianya, bukan sistemnya. Jika manusianya berhasil diserang, maka sistem tidak lagi mampu melindungi dengan cepat.”

e-ISSN : 2798-8880
p-ISSN : 2798-9976

Pemateri Sares Wari saat menyampaikan materi dalam kegiatan *Campus Talk* di Auditorium UCSN IBBI, Sabtu (31/1/2026). | Hasrina Arum Maulida

Gambar 1. Pemaparan Materi dan Talk Show
(Sumber: *Wacana, 2026)*

Lebih lanjut, para narasumber mengupas berbagai isu strategis yang relevan dengan lanskap digital saat ini. Pembahasan mencakup identifikasi bentuk-bentuk ancaman digital yang umum terjadi, eskalasi risiko penipuan berbasis kecerdasan buatan (AI), hingga pentingnya menumbuhkan etika serta sikap kritis dalam memanfaatkan teknologi secara bertanggung jawab (Waspada Online, 2026).

Tingginya urgensi materi yang dibawakan berbanding lurus dengan antusiasme yang ditunjukkan oleh para peserta. Hal ini terlihat dari dinamisnya sesi diskusi melalui pengajuan berbagai pertanyaan berbobot, khususnya yang berfokus pada instrumen keamanan digital, indikator taktis untuk mengenali hoaks dan scam, serta langkah-langkah praktis dalam melindungi data pribadi di dunia maya (XPRESI, 2026).

Pembicara memperkenalkan metode PAUSE yang terdiri dari pause, authenticate, use skepticisn, search dan educate yang bertujuan memberikan kesempatan kepada neo-cortex untuk bangkit melakukan evaluasi untuk penawaran yang diberikan, memeriksa keaslian informasi, pengajukan pertanyaan skeptis, melakukan pencarian untuk menjawab skeptis dan senantiasa untuk meningkatkan pengetahuan untuk menghindari gap pengetahuan.

Pada akhir sesi presentasi, pembicara secara interaktif menanyakan kepada para peserta, jika video ini muncul pada sosial media anda hari ini, apakah anda tertarik untuk mengikuti program giveaway tersebut? dan tidak ada perserta yang menyatakan tertarik.

Keberhasilan dan kelancaran penyelenggaraan kegiatan edukasi skala besar ini tidak lepas dari adanya sinergi yang kuat antar-lembaga. Sebagaimana diwartakan oleh IDN Times Sumut (2026), kegiatan PKM ini dapat terselenggara berkat dukungan penuh dan kolaborasi strategis dari berbagai mitra serta sponsor lintas sektor, yang meliputi U.S. Embassy, Universitas IBBI Medan, Yayasan Bangsa Cerdas Indonesia, Batik Fractal Indonesia, dan PT Next Level Cipta.

5. KESIMPULAN

Aktifitas *scam* merupakan bagian dari peradaban manusia, dimana para penipu melakukan eksploitasi terhadap psikologi korban yang berada pada situasi lengah, seperti ingin mendapatkan solusi cepat dari tekanan tertentu atau ingin mendapatkan keuntungan besar dan cepat dengan pengorbanan ataupun resiko yang relative kecil dalam waktu yang terbatas ataupun pihak yang terlalu percaya kepada otoritas tertentu tanpa melakukan evaluasi terhadap umpan yang diberikan.

e-ISSN : 2798-8880
p-ISSN : 2798-9976

Penipuan tidak menyerang tingkat kecerdasan (IQ), melainkan menyerang sisi emosional dengan membangkitkan tekanan dan urgensi yang menyebabkan sistem limbik aktif secara impulsive yang secara efektif melumpuhkan fungsi kerja Neo-Cortex, dan akibatnya otak kehilangan kesempatan untuk memproses dan memverifikasi informasi secara rasional.

Metode PAUSE dapat diadopsi untuk memberikan kesempatan kepada neo-cortex untuk bangkit melakukan evaluasi atas tawarn yang diberikan, memeriksa keaslian informasi, pengajukan pertanyaan skeptis, melakukan pencarian di internet dan senantiasa untuk meningkatkan pengetahuan diri untuk menghindari gap pengetahuan.

DAFTAR PUSTAKA

CBS News (2024). *AI-generated ads using Taylor Swift's likeness dupe fans with fake Le Creuset giveaway. Diakses dari: https://www.cbsnews.com/news/taylor-swift-le-creuset-ai-generated-ads/*

Goleman, D. (1995). *Emotional intelligence: Why it can matter more than IQ. Bantam Books.*

IDN Times Sumut. (2026). Soulmantra Gelar Sadar Digital: Perkuat Literasi Keamanan Digital. Diakses dari: https://sumut.idntimes.com/news/sumatra-utara/soulmantra-gelar-sadar-digital-perkuat-literasi-keamanan-digital-00-fj96j-92wcrm.

Jakobsson, M., & Myers, S. (2006). *Phishing and countermeasures: Understanding the increasing problem of electronic identity theft. Wiley-Interscience.*

Merriam-Webster.com Dictionary. *S.v. "deepfake." Accessed May 18, 2026. https://www.merriam-webster.com/dictionary/deepfake.*

Modic, D., & Lea, S. E. (2012). *Scam compliance and the charm of persuasion. Academic Research International, 2(2), 117–129.*

Otoritas Jasa Keuangan (2026). Marak Penipuan Keuangan, OJK Bersama Pemerintah Luncurkan Kampanye Nasional Berantas SCAM dan Aktivitas Keuangan Ilegal. Diakses dari: https://ojk.go.id/id/berita-dan-kegiatan/siaran-pers/Pages/OJK-Bersama-Pemerintah-Luncurkan-Kampanye-Nasional-Berantas-Scam-dan-Aktivitas-Keuangan-Ilegal.aspx

Purkait, S. (2012). *Phishing counter measures as content literacy: An educational paradigm. Information Management & Computer Security*, 20(2), 132–145. https://doi.org/10.1108/09685221211235642

Sari, R. P., & Sary, M. P. (2020). Analisis faktor psikologis dan perilaku korban penipuan berbasis siber (Cyber fraud). Jurnal Kriminologi Indonesia, 16(2), 45–56.

Vaccari, C., & Chadwick, A. (2020). *Deepfakes and disinformation on social media: The effects of synthetic media on political trust and disinformation shares. Journal of Communication*, 70(6), 747–772. https://doi.org/10.1093/joc/jqaa031

Wacana (Badan Otonom Pers Mahasiswa). (2026). Soulmantra dan IBBI Gelar Campus Talk Bahas Deepfake dan Psikologi Scam. Diakses dari: https://wacana.org/ibbi-gelar-campus-talk-bahas-deepfake-dan-psikologi-scam/

Waspada Online. (2026). Soulmantra Gelar Program Sadar Digital, Edukasi Keamanan AI dan Data Pribadi bagi Anak Muda Sumatera. Diakses dari: https://redaksi.waspada.co.id/v2024/soulmantra-gelar-program-sadar-digital-edukasi-keamanan-ai-dan-data-pribadi-bagi-anak-muda-sumatera/

Wineburg, S., & McGrew, S. (2019). *Lateral reading on the open web: A comparison of university students and professional fact-checkers. Stanford History Education Group Working Paper.* https://doi.org/10.2139/ssrn.3446623

e-ISSN : 2798-8880
p-ISSN : 2798-9976

Wolfe, D. T., & Hermanson, D. R. (2004). *The fraud diamond: Considering the four elements of fraud. CPA Journal, 74(12), 38–42.*

XPRESI (Tabloid Media Kreasi dan Interaksi). (2026). Seminar "Sadar Digital" : Cerdas Menanggapi Kebohongan Dunia Maya. Diakses dari: https://xpresi.id/seminar-sadar-digital-cerdas-menanggapi-kebohongan-dunia-maya/