JURNAL ADAM : JURNAL PENGABDIAN MASYARAKAT
E. ISSN 2829-744X
Available at https://jurnal.spada.ipts.ac.id/index.php/adam
Vol. 3 No. 2
Edisi Agustus
2024

KEUANGAN DIGITAL: DIBALIK KEMUDAHANNYA, WASPADAI PULA POTENSI KEJAHATANNYA SERI KEGIATAN PENGABDIAN MASYARAKAT (GURU & ORANG TUA SISWA TK TAMAN INDRIA BANDUNG)

Aldi Akbar[1*], Aditya Wardhana[2], Budi Rustandi Kartawinata[3]
[1*, 2, 3] Program Studi Administrasi Bisnis, Fakultas Ekonomi Bisnis, Universitas Telkom

*Email: aldiakb@telkomuniversity.ac.id

DOI: 10.37081/adam.v3i2.1960

Abstrak

Kejahatan digital keuangan telah menjadi masalah yang mendesak dalam masyarakat berteknologi saat ini. Dengan meningkatnya ketergantungan pada transaksi digital dan pesatnya pertumbuhan ekonomi digital, para pelaku kejahatan telah menemukan peluang baru untuk mengeksploitasi kerentanan dalam sistem keuangan digital Kejahatan digital keuangan mencakup berbagai aktivitas terlarang yang menargetkan sistem keuangan, institusi, dan individu seperti internet, perangkat seluler, dan sistem pembayaran elektronik. Kegiatan pengabdian masyarakat ini sejatinya merupakan bentuk dari rencana berupa seri penyuluhan keuangan digital sehingga akan dirancang relevansi antar satu kegiatan dengan kegiatan lainnya. Dengan demikian masih terbuka untuk seri pengabdian selanjutnya dengan cakupan bukan hanya masyarakat sasar yang sama melainkan jejaring dari masyarakat sasar itu sendiri dalam hal ini lembaga-lembaga pendidikan lain yang masuk dalam jejaring TK Taman Indria (menginduk pada Taman Siswa) di sekitar kota Bandung, sehingga target literasi keuangan digital bisa lebih luas segmentasinya. Hasil workshop ini menunjukkan bahwa 87 % para peserta puas dengan materi literasi kejahatan keuangan digital dan berharap dilakukan berkala dengan topik-topik terkini.
Kata kunci: keuangan digital, skimming, phising

Abstract

Financial digital crime has become a pressing issue in today's technological society. With the increasing reliance on digital transactions and the rapid growth of the digital economy, criminals have found new opportunities to exploit vulnerabilities in the digital financial system Digital financial crime includes a variety of illicit activities targeting financial systems, institutions, and individuals such as the internet, mobile devices, and electronic payment systems. This community service activity is actually a form of a plan in the form of a digital financial counseling series so that relevance will be designed between one activity and another. Thus it is still open for the next series of community service with the scope of not only the same target community but the network of the target community itself, in this case other educational institutions included in the Taman Indria Kindergarten network (based on Taman Siswa) around the city of Bandung, so that the target of digital financial literacy can be more broadly segmented. The results of this workshop showed that 98% of the participants were satisfied with the digital financial crime literacy material and hoped that it would be conducted periodically with the latest topics.
Keywords: Digital financ, skimming, phising

1. PENDAHULUAN

Kejahatan digital keuangan telah menjadi masalah yang mendesak dalam masyarakat berteknologi maju saat ini. Dengan meningkatnya ketergantungan pada transaksi digital dan pesatnya pertumbuhan ekonomi digital, para pelaku kejahatan telah menemukan peluang baru untuk mengeksploitasi kerentanan dalam sistem keuangan digital (Anderson, 2020; Rebovich & Byrne, n.d.) Kejahatan digital keuangan mencakup berbagai aktivitas terlarang yang menargetkan sistem keuangan,

institusi, dan individu. Kejahatan ini mengeksploitasi teknologi digital, seperti internet, perangkat seluler, dan sistem pembayaran elektronik, untuk melakukan aktivitas penipuan (Smith, 2018). Berikut ini adalah beberapa jenis kejahatan digital keuangan yang menonjol: (1) Phishing dan Spoofing: Phishing melibatkan penipuan terhadap individu untuk mengungkapkan informasi keuangan yang sensitif melalui email atau situs web palsu yang meniru institusi yang sah (Alkhalil, Hewage, Nawaf, & Khan, 2021). Spoofing, di sisi lain, melibatkan pemalsuan identitas pengirim untuk menipu penerima agar percaya bahwa mereka berinteraksi dengan entitas tepercaya (Nadeem et al., 2023); (2) Pencurian Identitas: Pencurian identitas terjadi ketika penjahat mencuri informasi pribadi, seperti nomor jaminan sosial, detail kartu kredit, atau kredensial rekening bank, dan menggunakannya untuk melakukan penipuan keuangan. Hal ini dapat mengakibatkan kerugian finansial yang signifikan dan merusak reputasi korban; (3) Penipuan Perbankan Online: Penipuan perbankan online melibatkan akses tidak sah ke akun perbankan individu, yang sering kali difasilitasi melalui malware atau teknik rekayasa sosial. Penjahat dapat mentransfer dana, melakukan transaksi yang tidak sah, atau bahkan memanipulasi saldo rekening, menyebabkan kerugian finansial yang parah bagi korban; (4) Kejahatan yang berhubungan dengan mata uang digital: Seiring dengan semakin populernya mata uang digital, para penjahat mulai mengeksploitasi kerentanan dalam sistem mata uang digital. Hal ini termasuk penipuan Initial Coin Offerings (ICO), skema Ponzi, dan peretasan bursa mata uang digital, yang menyebabkan kerugian finansial yang besar.

Kejahatan digital keuangan memiliki implikasi yang sangat besar bagi individu, bisnis, dan masyarakat secara keseluruhan. Beberapa implikasi utama meliputi: (1)Kerugian Finansial: Korban kejahatan digital keuangan dapat mengalami kerugian finansial yang signifikan, yang menyebabkan kesulitan pribadi dan ekonomi. Kerugian ini dapat berkisar dari pembobolan rekening bank individu hingga serangan siber perusahaan berskala besar; (2) Erosi Kepercayaan dan Keyakinan: Kejahatan digital keuangan yang terjadi berulang kali dapat mengikis kepercayaan dan keyakinan terhadap sistem keuangan digital, sehingga menghalangi individu dan bisnis untuk sepenuhnya menggunakan transaksi digital. Hal ini dapat menghambat pertumbuhan ekonomi dan inovasi; (3) Tantangan Hukum dan Regulasi: Kejahatan digital keuangan menghadirkan tantangan bagi lembaga penegak hukum dan badan pengatur. Sifat kejahatan yang terus berkembang sering kali melampaui pengembangan kerangka hukum dan kemampuan penegakan hukum yang sesuai, sehingga sulit untuk menangkap dan menuntut pelaku secara efektif.

Untuk memerangi kejahatan digital keuangan secara efektif, diperlukan pendekatan multi-segi yang melibatkan berbagai pemangku kepentingan seperti individu, lembaga keuangan, dan pemerintah. Beberapa tindakan penanggulangan yang penting meliputi: (1) Kesadaran dan Pendidikan Publik: Meningkatkan kesadaran masyarakat tentang risiko kejahatan digital keuangan dan strategi pencegahannya sangatlah penting. Kampanye edukasi dapat memberdayakan individu untuk mengenali dan menghindari potensi ancaman, seperti upaya phishing atau aktivitas online yang mencurigakan (Sharma & Thapa, 2023); (2) Memperkuat Tindakan Keamanan Siber: Lembaga keuangan harus berinvestasi pada infrastruktur keamanan siber yang kuat untuk melindungi data pelanggan dan sistem keuangan. Hal ini termasuk menerapkan otentikasi multi-faktor, enkripsi, dan audit keamanan rutin untuk mendeteksi dan memitigasi kerentanan (Kafi & Akter, 2023); (3) Kolaborasi dan Berbagi Informasi: Meningkatkan kolaborasi di antara lembaga keuangan, pemerintah, dan organisasi internasional dapat memfasilitasi pembagian intelijen ancaman siber dan praktik terbaik. Upaya kolektif ini dapat membantu mengidentifikasi ancaman yang muncul dan merancang tindakan pencegahan yang efektif (Samtani, Abate, Benjamin, & Li, 2020); (4) Kerangka Kerja Legislatif dan Regulasi: Pemerintah harus memberlakukan undang-undang yang komprehensif untuk mengatasi kejahatan digital keuangan secara efektif (Mugarura & Ssali, 2021). Kerangka kerja ini harus mencakup ketentuan untuk mengadili pelaku kejahatan, menegakkan peraturan perlindungan data, dan mendorong kerja sama internasional dalam memerangi kejahatan dunia maya (Anwary, 2022).

Indonesia telah menyaksikan lonjakan berbagai bentuk kejahatan siber yang menargetkan sektor keuangan antara lain: (1) Meningkatnya penipuan perbankan online (Erdiyanto, 2023) penipuan perbankan online telah muncul sebagai bentuk kejahatan keuangan digital yang paling umum di Indonesia. Penjahat menggunakan teknik-teknik canggih seperti phishing, malware, dan rekayasa sosial

untuk mendapatkan akses tidak sah ke rekening bank individu; (2) Penipuan pembayaran seluler (Rumampuk, 2007).

Kejahatan digital keuangan merupakan ancaman yang signifikan bagi individu, bisnis, dan ekonomi global. Seiring dengan perkembangan teknologi, para pelaku kejahatan akan mengeksploitasi kerentanan baru, sehingga memerlukan adaptasi dan peningkatan tindakan pencegahan yang berkelanjutan. Berdasarkan fenomena dan latar belakang di atas, maka perlu kiranya edukasi di lapisan masyarakat mengenai pentingnya aspek-aspek keamanan berkaitan dengan penggunaan aplikasi keuangan digital. Hal ini guna memitigasi terjadinya jebakan hutang (debt trap) atau modus penipuan berkedok investasi online dan atau penyalahgunaan data pribadi oleh pihak-pihak yang tidak bertanggung jawab. Melalui upaya kecil inilah maka dirumuskan tema penyuluhan yaitu "Keuangan Digital: Dibalik Kemudahannya, Waspadai pula Potensi Kejahatannya" yang bertempat di aula TK Taman Indria Pandanwangi Kelurahan Cijawura Kecamatan Buahbatu Kota Bandung yang akan dilaksanakan pada akhir April – Awal Mei 2024.

Melalui seri penyuluhan kegiatan pengabdian masyarakat ini difokuskan pada fitur-fitur yang terkait pada kemananan keuangan digital seperti penggunaan anti spam ware, analisa singkat terhadap penawaran investasi bodong/ pinjaman online yang menjerat, dan lain-lain yang berkenaan dengan aplikasi keuangan digital. Kegiatan ini diharapkan dapat mengedukasi para guru dan stakeholders di lingkungan TK Taman Indria sebagai masyarakat sasar sehingga dapat lebih memahami, bijak dan peduli dalam mengakses produk-produk keuangan berbasis digital. Para guru, orang tua murid dan pihak terkait lainnya di TK Taman Indria sebagai ujung tombak pelaku pendidikan tentunya diharapkan manakala telah mengikuti penyuluhan kegiatan pengabdian masyarakat ini dapat mengkomunikasikan kembali di lingkungan mereka masing-masing mengenai pentingnya kehati-hatian dalam memilih produk keuangan digital serta memahami risiko di balik kemudahan yang ditawarkan. Setidaknya para peserta memiliki peningkatan dalam pemahaman terkait literasi keuangan digital dari perspektif cyber-security.

Perlu diketahui bahwa masyarakat sasar dalam hal ini TK Taman Indria merupakan lembaga pendidikan anak usia dini yang telah berdiri sejak tahun 1987 dengan Nomor Pokok Sekolah Nasional (NPSN) 20254758, berlokasi di Komplek Pandanwangi F.23 Kelurahan Cijawura Kecamatan Buahbatu Kota Bandung. Visi yang diembang yaitu "MENJADIKAN ANAK YANG CERDAS CERIA DAN KAYUNGYUN", adapun misi yang dijalankan antara lain: (1) Membangun akhlak anak yang bertaqwa kepada allah swt sejak dini; (2) Membangun anak yang berkarakter baik; (3) Membantu peran orang tua dalam mendidik anak; (4) Menyiapkan anak untuk masuk ke jenjang selanjutnya. Saat ini jumlah peserta didik ada 17 siswa yang terbagi ke dalam dua rombongan belajar dan diampu oleh dua guru dan satu tenaga pendidik. Namun demikian kegiatan yang akan dilaksanakan turut melibatkan kepesertaan dari orang tua siswa agar manfaat dari kegiatan ini juga dirasakan oleh masyarakat sekitar.

2. METODE PENGABDIAN

Kegiatan pengabdian masyarakat ini berupa penyuluhan dan pendidikan kepada masyarakat sasar yang terbagi dalam dua tahap. Adapun masyarakat sasar yang dimaksud adalah para guru/ tenaga pendidik dan orang tua siswa di TK Taman Indria. Tahap pertama yaitu perencanaan berupa koordinasi antar penyelenggara dengan masyarakat sasar diawali dengan kelengkapan administrasi seperti form rekomendasi dan surat kesediaan masyarakat sasar yang memuat peran, tugas, pokok dan fungsi. Dalam tahap ini ditentukan pula tanggal pelaksanaan, jumlah peserta, serta teknis pelaksanaan lainnya.

Tahap kedua yaitu pelaksanaan berupa penyuluhan yang disampaikan secara luring (luar jaringan) yang bertempat di aula sekolah tersebut. Adapun teknis pelaksanaan antara lain: (1) Opening atau sambutan; (2) Penyampaian materi penyuluhan; (3) Tanya jawab; (4) Closing atau penutup berupa rangkuman kegiatan.

Run down rencana kegiatan:

JURNAL ADAM : JURNAL PENGABDIAN MASYARAKAT
E. ISSN 2829-744X
Available at https://jurnal.spada.ipts.ac.id/index.php/adam
Vol. 3 No. 2
Edisi Agustus
2024

Gambar 1. *Rundown kegiatan workshop*

Total durasi keseluruhan kegiatan adalah 45 menit dengan rincian Pendahuluan dan Materi masing-masing berturut-turut adalah 5 menit dan 10 menit. Adapun sesi tanya jawab diberi durasi yang lebih panjang yaitu 28 menit, dan untuk ringkasan kegiatan cukup 2 menit.

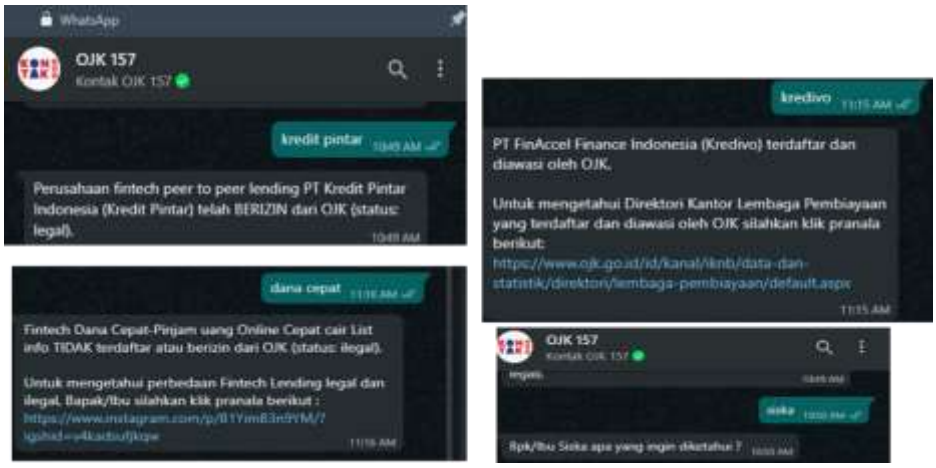
3. HASIL DAN PEMBAHASAN

Seri program pengabdian masyarkat ini dilakukan secara *onsite* sebanyak 16 peserta yang terdiri dari guru dan orang tua siswa TK Taman Indria, dimulai dari pukul 10.00 hingga pukul 12.00 WIB. Kegiatan terbagi empat agenda terdiri dari pemberian materi, tanya jawab, penutup, dan diakhiri oleh sesi foto bersama. Pemberian materi di awali dengan isu-isu terkini yang marak terjadi di masyarakat terkait dengan platform keuangan digital. Banyak peserta yang belum menyadari bahwasannya platform digital yang mereka miliki saat ini apakah berupa *internet/mobile banking* dan atau *e-wallet* ternyata berpotensi disalah gunakan oleh pihak yang tidak bertanggung jawab. Akses untuk melakukan kejahatan ini salah satunya adalah melalui perilaku dari *user* itu sendir. Salah satu kejahatan digital keuangan yang baru-baru ini terjadi adalah mengirimkan file berekstensi aplikasi (apk) melalui platform *instant messaging* seperti Whatsapp, Telegram, dll yang ekstensi file tersebut disamarkan menjadi seolah-olah berupa undangan suatu kegiatan, berkamuflase foto paket dari layanan *e-commerce*, file yang disamarkan berupa sertifikat, danlain sebagainya. Bagi *user* yang kurang berhati-hati tentunya akan langsung mengakses file tersebut dan tanpa sadar memberikan otorisasi sesuai permintaan dari file tersebut saat instalasi berlangsung. Alhasil dalam waktu tidak terlampau lama, data sensitif *user* telah dikuasai oleh pihak ketiga.

Dalam workshop ini diberikan solusi berupa betapa pentingnya kewaspadaan situasional akan perangkat digital yang dimiliki serta dipandu pula beberapa kiat untuk antisipasi agar tidak terjebak sebagai korban kejahatan keuangan digital. Kejahatan keuangan digital di tahun 2023 saja telah tercatat hampir 4000 aduan yang dilayangkan ke OJK (Annur, 2023), semisal modus investasi ilegal, pada pembiayaan online atau lebih dikenal dengan istilah pinjaman online (pinjol). Ciri-ciri modusnya antara lain (1) Tidak memiliki ijin resmi; (2) Pemberian pinjaman sangat mudah; (3) akses seluruh data di ponsel nasabah; (4) Identitas pengurus dan alamat lembaga tidak jelas, dll. Modus seperti ini biasanya aplikator berbentuk badan hukum dan untuk mengantisiapsinya adalah melakukan kroscek apakah lembaga tersebut telah berijin dan terdaftar di OJK. Caranya bisa mengetahui atau menanyakan langsung melalui beberapa kanal informasi yang disediakan salah satunya yang paling populer adalah melalui platform pesan singkat atau instant messaging yaitu Whatsapp. Nomor kontak yang diberikan oleh OJK adalah Kontak OJK di nomor 081157157157, cukup mengetik nama lembaga yang ingin diketahui statusnya apakah terdaftar dan diawasi oleh OJK atau sebaliknya (Gambar 2).

Salah satu bentuk kejahatan digital yang tidak disadari oleh calon korban adalah Social engineering. Yaitu tindakan memanipulasi psikologis korban dengan tujuan memperoleh data pribadi yang selanjutnya digunakan untuk membobol akun keuangan korban (Nicholls, Kuppa, & Le-Khac, 2021). Di tengah masyarakat saat ini tidak sedikit menerima pesan dari (misal) Whatsapp yang seolah-olah pengirim pesan tersebut dari institusi perbankan ternama. Isi pesannya adalah peraturan transfer yang semula dikenakan biaya Rp 6500 per transaksi akan berubah menjadi Rp 150.000 dan ini akan berlaku mulai bulan depan. Jika tidak setuju dengan kebijakan baru ini maka silakan mengisi link yang telah disediakan. Tentu saja si calon korban tidak bersedia dengn kebijakan baru tersebut dan buru-buru mengakses link yang telah disediakan untuk menolak kebijakan baru tersebut. Selanjutnya bisa ditebak bahwasannya link palsu tersebut meminta informasi sensitif dari si calon korban. Modus yang demikian ini disebut Phising yaitu tindakan meminta (memancing) korban untuk mengungkapkan informasi akun keuangan dengan cara mengirimkan pesan penting pelaku (Hasham, Joshi, & Mikkelsen, 2019).

JURNAL ADAM : JURNAL PENGABDIAN MASYARAKAT
E. ISSN 2829-744X
Available at https://jurnal.spada.ipts.ac.id/index.php/adam
Vol. 3 No. 2
Edisi Agustus
2024



Gambar 2. Tampilan Kontak OJK 157 (sumber: (Akbar, Kartawinata, & Wardhana, 2023)

Pada sesi kedua kegiatan ini diisi berupa diskusi atau tanya jawab untuk saling bertukar pikiran dan pengalaman antar pemateri dan peserta.

Gambar 3. Antusiasme peserta dalam workshop Kejahatan Keuangan Digital

Dari hasil diskusi, ternyata terungkap bahwa mayoritas peserta sering menerima Phising dan juga Packet Analyzer (packet sniffer), Modus baru yang dikenal dengan istilah sniffing dengan memanfaatkan aplikasi yang berfungsi untuk mendapatkan seluruh informasi seseorang dan meneruskannya tanpa sepengatuhan pengguna untuk mencuri data pengguna (Siahaan, 2017).

JURNAL ADAM : JURNAL PENGABDIAN MASYARAKAT
E. ISSN 2829-744X
Available at https://jurnal.spada.ipts.ac.id/index.php/adam
Vol. 3 No. 2
Edisi Agustus
2024

Gambar 4. Sesi diskusi peserta dan pemateri

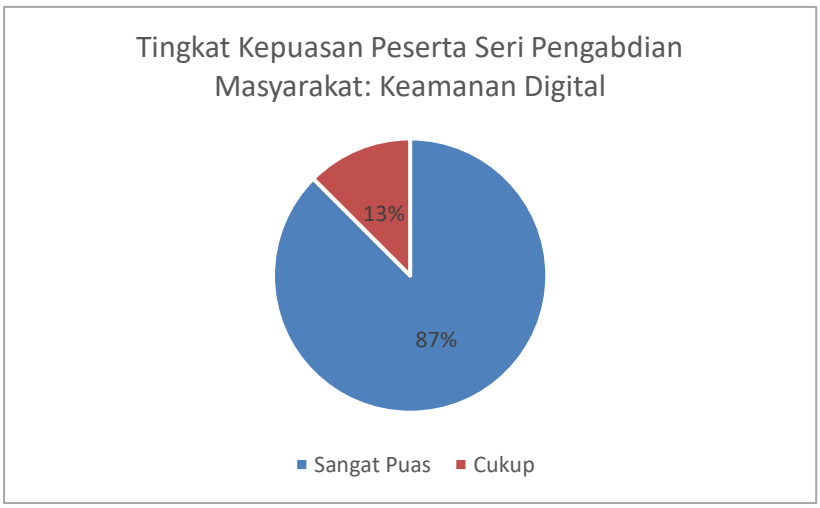
Beruntungnya, para peserta tidak ada yang menjadi korban dari beberapa modus yang telah dijelaskan, namun demikian dengan pemaparan dan penjelasan dari materi yang diberikan setidaknya mereka menjadi lebih *aware* dengan beragamnya modus-modus baru praktek kejahatan digital ini. Penting untuk disampaikan bahwa tindakan antisipasi yang harus dilakukan agar terhindar dari praktek-praktek ilegal yang dimaksud antara lain : (1) Jangan memberikan PIN (Personal Identification Number)/ OTP (One Time Password); (2) Menghindari akses WIFI publik; (3) Rutin memantau notifikasi yang muncul; (4) Mengunduh dan mengakses aplikasi internet banking pada situs dan platform resmi; (5) Jangan memberikan data apapun kepada orang/ oknum yang mengaku dari pihak bank atau operator, dll (OJK, 2021).

Selain itu pul penting untuk selalu memindai aplikasi yang terinstal di gawai masing-masing, jika *smartphone*-nya berbasis Android maka bisa menggunakan aplikasi *on device protection* seperti Google Play Protect. Aplikasi ini tidak perlu diinstal ke gawai yang ada, cukup langsung memindai perangkat kita.

Gambar 5. Tampilan Google Play Protect (Sumber: google.com)

Dengan diberikannya tutorial berupa cara mencegah pencurian data pada perangkat ponsel yang dimiliki memberikan wawasan dan menambah rasa aman dan nyaman bagi peserta workshop. Namun ini perlu dukungan dari para peserta itu sendiri berupa pentingnya kesadaran akan keamana data digital yang dimiliki karena di era serba digital ini, data adalah aset atau harta yang karenya perlu untuk dilindungi.

Umpan balik hasil kegiatan pengabdian masyarakat ini tersaji dalam bentuk mini survey yang meliput kebutuhan dan kesesuaian materi, waktu pelaksanaan, pelayanan, dan harapan kegiatan serupa di masa mendatang. Dan hasilnya 87% menyatakan puas dengan kegiatan ini serta sisanya (13%) menyatakan cukup.



Gambar 6. Survey kegiatan pengabdian masyarakat mengenai kejahatan keuangan digital di TK Taman Indria

4. SIMPULAN

Kesimpulan dari terlaksananya kegiatan ini adalah bahwa mayoritas para peserta mengikuti perkembangan berita terkini terkait dengan maraknya korban kejahatan keuangan digital. Namun mayoritas peserta belum mengetahui dari sisi modus operandi para pelaku tersebut. Bahwa kejahatan keuangan digital di Indonesia telah mengalami eskalasi yang signifikan selama lima tahun terakhir, yang menimbulkan ancaman besar bagi stabilitas keuangan dan keamanan warganya, maka penting dilakukan sosialisasi hingga ke tingkat organisasi di masyarakat yaitu berupa keluarga dan juga komunitas-komunitas di lingkungan warga. Pemaparan kasus-kasus riil sangat penting disampaikan kepada peserta workshop agar selalu tetap waspada dan mampu menerapkan langkah-langkah keamanan yang kuat, dan tetap terus saling mengingatkan di level keluarga masing-masing untuk selalu mengikuti perkembangan terbaru dalam keamanan siber.

5. DAFTARPUSTAKA

Akbar, A., Kartawinata, B. R., & Wardhana, A. (2023). PENYULUHAN# SERI3: PAYLATER DALAM E-COMMERCE (MEMBANTU ATAU MENJEBAK?). *Jurnal ADAM: Jurnal Pengabdian Masyarakat*, *2*(1), 167–172.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, 563060.

Anderson, R. (2020). *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons.

Annur, C. M. (2023). *Ada 3,9 Ribu Aduan Kasus Pinjol Ilegal sejak Awal 2023, Ini Tren Bulanannya*. Retrieved from https://databoks.katadata.co.id/datapublish/2023/06/14/ada-39-ribu-aduan-kasus-pinjol-ilegal-sejak-awal-2023-ini-tren-bulanannya

Anwary, I. (2022). The Role of Public Administration in combating cybercrime: An Analysis of the Legal Framework in Indonesia. *International Journal of Cyber Criminology*, *16*(2), 216–227.

Erdiyanto, R. P. (2023). PENIPUAN MENGATASNAMAKAN BANK BERBENTUK PHISING. *Jurnal Inovasi Global*, *1*(2), 71–79.

Hasham, S., Joshi, S., & Mikkelsen, D. (2019). Financial crime and fraud in the age of cybersecurity. *McKinsey & Company*, *2019*.

Kafi, M. A., & Akter, N. (2023). Securing financial information in the digital realm: case studies in cybersecurity for accounting data protection. *American Journal of Trade and Policy*, *10*(1), 15–26.

Mugarura, N., & Ssali, E. (2021). Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system. *Journal of Money Laundering Control*, *24*(1), 10–28.

Nadeem, M., Zahra, S. W., Abbasi, M. N., Arshad, A., Riaz, S., & Ahmed, W. (2023). Phishing Attack, Its Detections and Prevention Techniques. *International Journal of Wireless Security and Networks*, *1*(2), 13-25p.

Nicholls, J., Kuppa, A., & Le-Khac, N.-A. (2021). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *Ieee Access*, *9*, 163965–163986.

OJK. (2021). *Financial Technology - P2P Lending*. Jakarta. Retrieved from https://www.ojk.go.id/id/kanal/iknb/financial-technology/default.aspx

Rebovich, D., & Byrne, J. M. (n.d.). Te New Technology of Financial Crime.

Rumampuk, T. (2007). Penipuan dengan Menggunakan Telepon Seluler Ditinjau dari KUHP. *Unisia*, (63), 81–94.

Samtani, S., Abate, M., Benjamin, V., & Li, W. (2020). Cybersecurity as an industry: A cyber threat intelligence perspective. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 135–154.

Sharma, R., & Thapa, S. (2023). Cybersecurity awareness, education, and behavioral change: strategies for promoting secure online practices among end users. *Eigenpub Review of Science and Technology*, *7*(1), 224–238.

Siahaan, A. P. U. (2017). Network Forensic Application in General Cases.

Smith, R. (2018). *Crime in the digital age: Controlling telecommunications and cyberspace illegalities*. Routledge.