JURNAL ADAM : JURNAL PENGABDIAN MASYARAKAT
E. ISSN 2829-744X
Available at https://jurnal.spada.ipts.ac.id/index.php/adam

Vol. 3 No. 1
Edisi Februari
2024

KEJAHATAN KEUANGAN DIGITAL: MODUS & CARA ANTISIPASI SERI KEGIATAN PENGABDIAN MASYARAKAT PERSATUAN WREDATAMA REPUBLIK INDONESIA (PWRI) PEMPROV JAWA BARAT

Oleh:
Aldi Akbar[1*], Amalina Dewi Kumalasari[2], Nurafni Rubiyanti[3], Sherly Artadita[4], Yulia Nur Hasanah[5], Anita Silvianita[6], Fitriani Nur Utami[7], Romat Saragih[8]
[1*,2, 3,4,5,6,7,8] Program Studi Administrasi Bisnis, Fakultas Komunikasi Bisnis, Universitas Telkom

*Email: aldiakb@telkomuniversity.ac.id

DOI: 10.37081/adam.v3i1.1750

Article info:
Diterima:08/01/24 Disetujui:21/01/24 Publis: 08/02/24

Abstrak

Kegiatan workshop ini bertujuan untuk memberikan informasi dan langkah antisipasi terkait semakin maraknya penggunaan platform digital keuangan dan masih banyaknya celah-celah keamanan yang sering diabaikan oleh penggunanya. Subjek penelitian ini adalah para aparatur sipil negara yang telah purna tugas khususnya dari instansi Pemerintah Provinsi Jawa Barat yang tergabung dalam wadah Persatuan Wredatama Republik Indonesia (PWRI). Sebanyak 40 peserta antusias selama kegiatan berlangsung terlihat dari banyaknya peserta yang berbagi pengalaman dan pertanyaan-pertanyaan yang diajukan kepada pemateri. Istilah-istilah keuangan digital seperti skimming, phising, dan social engineering selain menambah wawasan juga diberikan infomasi celah-celah yang sering dilakukan oleh pelaku kejahatan guna mendapatkan informasi individu. Hasil workshop ini menunjukkan bahwa 95 % para peserta puas dengan materi literasi kejahatan keuangan digital dan menginginkan kegiatan serupa dilakukan berkala dengan topik-topik lain yang berkaitan dengan literasi dan inklusi platform keuangan digital.
Kata kunci: Kejahatan keuangan digital, skimming, phising, social engineering

Abstract

This workshop activity aims to provide information and anticipatory steps related to the increasingly widespread use of digital financial platforms and the many security gaps that are often ignored by its users. The subjects of this study were state civil servants who had retired, especially from the West Java Provincial Government agency who were members of the Persatuan Wredatama Republik Indonesia (PWRI). A total of 40 participants were enthusiastic during the activity as seen from the number of participants who shared their experiences and questions asked to the speaker. Digital financial terms such as skimming, phishing, and social engineering in addition to adding insight are also given information on the gaps that are often done by criminals to obtain individual information. The results of this workshop showed that 95% of the participants were satisfied with the digital financial crime literacy material and wanted similar activities to be carried out periodically with other topics related to digital financial platform literacy and inclusion.
Keywords: Digital finance crime, skimming, phising, social engineering

JURNAL ADAM : JURNAL PENGABDIAN MASYARAKAT
E. ISSN 2829-744X
Available at https://jurnal.spada.ipts.ac.id/index.php/adam
Vol. 3 No. 1
Edisi Februari
2024

1. PENDAHULUAN

Kejahatan keuangan digital telah menjadi ancaman yang meluas di dunia yang saling terhubung saat ini. Selama lima tahun terakhir, banyak negara telah menyaksikan lonjakan aktivitas kejahatan siber yang menargetkan lembaga keuangan dan individu. Artikel ini bertujuan untuk memberikan gambaran ringkas tentang tren kejahatan keuangan digital di berbagai negara, menyoroti insiden-insiden utama dan merujuk pada sumber-sumber terpercaya. Di beberapa negara maju seperti Amerika Serikat telah mengalami peningkatan yang signifikan dalam kejahatan keuangan digital, dengan contoh pelanggaran data, serangan ransomware, dan pencurian identitas yang menjadi berita utama. Insiden penting termasuk pembobolan data Equifax pada tahun 2017 (McCrank, John; Finkle, 2018) dan peretasan Capital One pada tahun 2019 (Berthelsen;Christian & Turton, 2019). Di Inggris juga menghadapi banyak kejahatan keuangan digital, termasuk penipuan perbankan online, penipuan phishing, dan penipuan terkait mata uang kripto. Serangan siber Tesco Bank pada tahun 2016 (BBC, 2016) dan pelanggaran data British Airways pada tahun 2018 (Jasper Jolly, 2018) adalah contoh yang menonjol. Negara berkembang terbesar di dunia sekaligus sebagai salah satu ekonomi digital terkemuka di dunia, Cina telah menjadi sasaran penjahat siber yang canggih. Aktivitas penipuan yang melibatkan platform pembayaran seluler, skema investasi palsu, dan upaya peretasan terhadap lembaga keuangan telah menjadi hal yang lazim. Penipuan WeChat Pay pada tahun 2018 dan peretasan pertukaran mata uang kripto di Cina pada tahun 2019 adalah insiden yang patut dicatat (Zhang, 2021). Sementara di India terjadi lonjakan kejahatan keuangan digital, terutama yang berkaitan dengan penipuan perbankan online, skema pinjaman palsu, dan serangan phishing. Pembobolan data kartu debit tahun 2016 dan serangan malware WhatsApp tahun 2019 adalah contoh yang signifikan (Cornish, 2023). Dalam beberapa tahun terakhir, Australia menghadapi peningkatan kejahatan keuangan digital, dengan penjahat siber yang menargetkan individu, bisnis, dan organisasi pemerintah. Insiden yang terjadi meliputi penipuan perbankan online, pencurian identitas, dan penipuan terkait pajak. Pelanggaran data My Health Record tahun 2018 dan serangan siber tahun 2019 terhadap Parlemen Australia adalah contoh penting (Webber, 2023).

Kejahatan keuangan digital tidak mengenal batas dan menimbulkan ancaman signifikan bagi individu dan ekonomi di seluruh dunia. Contoh-contoh yang diberikan dari Amerika Serikat, Inggris, Cina, India, dan Australia menunjukkan beragamnya jenis kejahatan siber yang terjadi selama lima tahun terakhir.

Bagaimana dengan Indonesia? Setali tiga uang, selama lima tahun terakhir, 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), dengan adopsi platform pembayaran seluler yang cepat, penipu telah mengalihkan fokus mereka untuk mengeksploitasi kerentanan dalam sistem ini. Kasus penipuan pembayaran mobile telah meningkat dalam beberapa tahun terakhir, dengan para penjahat menggunakan taktik seperti penukaran kartu SIM, aplikasi mobile palsu, dan transaksi yang tidak sah (BUANA, 2022); (3) Penipuan mata uang kripto, popularitas mata uang kripto di Indonesia telah menarik perhatian para penjahat yang ingin mengeksploitasi para investor yang naif. Skema ponzi, penawaran koin perdana (ICO) palsu, dan penipuan investasi mata uang kripto telah meningkat. Otoritas Jasa Keuangan (OJK) telah memperingatkan masyarakat tentang risiko yang terkait dengan investasi mata uang kripto yang tidak teregulasi (Atmojo & Fuad, 2023); (4) Pembobolan data dan pencurian identitas, pembobolan data telah menjadi mimpi buruk yang berulang bagi masyarakat Indonesia, yang menyebabkan peningkatan kasus pencurian identitas yang mengkhawatirkan. Penjahat siber menargetkan database informasi pribadi bank, platform e-commerce, dan lembaga pemerintah untuk mendapatkan data sensitif. Badan Siber dan Sandi Negara (BSSN) melaporkan peningkatan mengejutkan sebesar dalam insiden pembobolan data dalam beberapa tahun terakhir (Kusuma & Rahmani, 2022; Rizaldi, 2022); (5) Pencucian uang dan pendanaan teror, kejahatan keuangan digital juga telah dikaitkan dengan kegiatan pencucian uang dan pendanaan terorisme di Indonesia. Penjahat mengeksploitasi platform online untuk mentransfer dana ilegal, sehingga menyulitkan pihak berwenang untuk mendeteksi dan mencegah kegiatan tersebut. Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) telah secara aktif berkolaborasi dengan mitra internasional untuk memerangi pencucian uang di ranah digital (Fajarini, Widyantara, & Sutama, 2022; Hidayat & Jatikusumo, 2019). Jadi dapat

JURNAL ADAM : JURNAL PENGABDIAN MASYARAKAT
E. ISSN 2829-744X
Available at https://jurnal.spada.ipts.ac.id/index.php/adam
Vol. 3 No. 1
Edisi Februari
2024

dikatakan bahwa kejahatan keuangan digital di Indonesia telah mengalami eskalasi yang signifikan selama lima tahun terakhir, yang menimbulkan ancaman besar bagi stabilitas keuangan negara dan keamanan warganya. Contoh-contoh yang disebutkan di atas menyoroti beragamnya jenis kejahatan ini, mulai dari penipuan perbankan online hingga pencucian uang. Sangat penting bagi pemerintah Indonesia, lembaga keuangan, dan individu untuk tetap waspada, menerapkan langkah-langkah keamanan yang kuat, dan terus mengikuti perkembangan terbaru dalam keamanan siber untuk memitigasi risiko yang terkait dengan kejahatan keuangan digital.

Salah satu upaya untuk mereduksi tindakan kejahatan keuangan digital khususnya dampak ekonomi dan juga psikis nasabah maka perlu adanya tindakan pencegahan berupa edukasi terus menerus di kalangan masyarakat. Karena pada umumnya banyak sekali para pelaku kejahatan digital keuangan ini menyasar langsung pada *end user* yang notabene minim pemahaman atau literasi keuangan khususnya platform digital. Untuk itu, kegiatan ini dikhususkan bagi para masyarakat terlebih bagi mereka yang telah non aktif atau purna tugas di kalangan instansi pemerintahan (Provinsi Jawa Barat). Melalui upaya kecil inilah maka dirumuskan tema penyuluhan yaitu **Workshop Peningkatan Kejahatan Keuangan Digital** yang bertempat di gedung Persatuan Wredatama Republik Indonesia Provinsi Jawa Barat Kota Bandung pada tanggal 7 Desember 2023.

2. METODE PENGABDIAN

Kegiatan pengabdian masyarakat ini berupa penyuluhan dan pendidikan kepada masyarakat sasar yaitu pensiunan aparat sipil negara (ASN) Provinsi Jawa Barat yang terbagi dalam dua tahap. Tahap pertama yaitu perencanaan berupa koordinasi antar penyelenggara dengan masyarakat sasar diawali dengan kelengkapan administrasi seperti form presensi, ramah tamah, sambutan dari Ketua Persatuan Wredatama Republik Indonesia Provinsi Jawa Barat, serta penjelasan mengenai *run down* acara dan aspek-aspek teknis selama workshop berlangsung. dan surat kesediaan masyarakat sasar yang memuat peran, tugas, pokok dan fungsi. Tahap kedua (Gambar 1) yaitu pelaksanaan berupa penyuluhan yang disampaikan secara interaktif dengan pokok kegiatan sebagai beikut: (1) Pendahuluan/ Latar belakang; (2) Materi inti workshop yaitu tipe kejahatan keuangan digital dan teknik antisipasi; (3) Tanya jawab; (4) Resume atau rangkuman kegiatan.

Gambar 1. *Rundown kegiatan workshop*

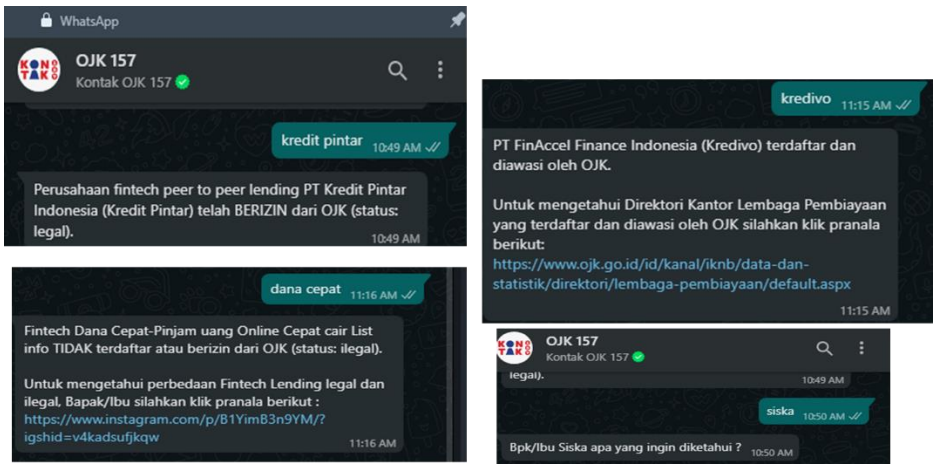
Total durasi keseluruhan kegiatan adalah 45 menit dengan rincian Pendahuluan dan Materi masing-masing berturut-turut adalah 5 menit dan 10 menit. Adapun sesi tanya jawab diberi durasi yang lebih panjang yaitu 28 menit, dan untuk ringkasan kegiatan cukup 2 menit.

3. HASIL DAN PEMBAHASAN

Dalam pelaksanaan program pengabdian masyarkat ini peserta yang hadir secara *onsite* sebanyak 40 wredatama, dimulai dari pukul 09.00 hingga pukul 12.00 WIB. Pemberian materi di awali dengan isu-isu terkini yang marak terjadi di masyarakat terkait dengan platform keuangan digital. Materi awal berupa investasi online, dengan makin beragamnya aplikasi investasi online yang ditawarkan tentunya semakin

JURNAL ADAM : JURNAL PENGABDIAN MASYARAKAT
E. ISSN 2829-744X
Available at https://jurnal.spada.ipts.ac.id/index.php/adam
Vol. 3 No. 1
Edisi Februari
2024

memudahkan calon investor untuk menjatuhkan pilihannya pada instrumen keuangan yang cocok untuk berinvestasi di samping juga tidak perlu datang ke kantor fisik lembaga keuangan yang dimaksud. Namun ternyata dengan kemudahan yang ditawarkan tidak sedikit yang berupa jebakan alias penipuan berkedok investasi. Menurut Otoritas Jasa Keuangan/ OJK (2021), ciri-ciri investasi ilegal antara lain: (1) Menjanjikan keuntungan tidak wajar dalam waktu cepat; (2) Menjanjikan bonus dari perekrutan anggota baru "member get member"; (3) Memanfaatkan tokoh masyarakat/ tokoh agama/Public Figure untuk menarik minat berinvestasi; (4) Klaim tanpa risiko (free risk); dan (5) Legalitas tidak jelas seperti tidak adanya ijin usaha dan ijin kelembagaan. Penyebab munculnya investasi ilegal ini bisa ditinjau dari dua sisi, pertama, dari sisi pelaku berupa kemudahan membuat aplikasi, web dan penawaran melalui media sosial serta banyak server di luar negeri. Kedua, dari sisi masyarakat itu sendiri yang mudah tergiur tingkat pengembalian yang tinggi dan juga minimnya pemahaman mengenai investasi. Dalam workshop ini langsung diberikan solusinya berupa beberapa kiat untuk antisipasi terjebak dalam investasi ilegal yaitu 2L, legal dan logis. Legal, artinya dari sisi perijinannya jelas dan terang (status berbadan hukum). Logis, artinya imbal hasil yang ditawarkan dalam rentang kewajaran dan juga memiliki risiko. Usai pemaparan investasi ilegal, dilanjutkan dengan uraian mengenai kejahatan digital berupa pembiayaan online. Tercatat hampir 4000 aduan yang dilayangkan ke OJK mengenai kejahatan pembiayaan online ini di awal 2023 lalu (Annur, 2023). Seperti halnya modus investasi ilegal, pada pembiayaan online atau lebih dikenal dengan istilah pinjaman online (pinjol), modusnya pun mirip dengan ciri-ciri 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. Antisipasi agar tidak terjerat pinjol ini antara lain adalah rutin mengetahui lembaga-lembaga mana yang 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).



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

Usai pemaparan pinjaman online, dilanjutkan dengan materi kejahatan keuangan digital lainnya. Pada uraian ini ditekankan pada tindakan seperti apa yang biasa dilakukan oleh pelaku kejahatan dalam melakukan aksinya.

JURNAL ADAM : JURNAL PENGABDIAN MASYARAKAT
E. ISSN 2829-744X
Available at https://jurnal.spada.ipts.ac.id/index.php/adam
Vol. 3 No. 1
Edisi Februari
2024

Gambar 3. Antusiasme peserta dalam workshop Kejahatan Keuangan Digital

Skimming, yaitu tindakan pencurian data kartu debit dengan cara menyalin (membaca atau menyimpan) informasi yang terdapat pada strip magnetis secara illegal (Satriana & Dewi, 2022). Phising, Tindakan meminta (memancing) korban untuk mengungkapkan informasi akun keuangan dengan cara mengirimkan pesan penting pelaku (Hasham, Joshi, & Mikkelsen, 2019). Social engineering, Tindakan memanipulasi psikolgis korban untuk mendapatkan data pribadi untuk membobol akun keuangan korban (Nicholls, Kuppa, & Le-Khac, 2021). 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). Tentunya, perlu diinformasikan tindakan antisipasi yang harus dilakukan agar terhindar dari praktek-praktek ilegal yang dimaksud. Menurut OJK (2021) tindakan antisipasinya adalah (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.

Dalam workshop ini juga diberikan langkah-langkah dalam mengunduh dan menginstal aplikasi tambahan untuk mencegah terjadinya malware pada perangkat ponsel yang dimiliki agar meminimalisir peluang terjadinya tindakan pencurian data pribadi. Dari banyaknya aplikasi yang ditawarkan oleh beberapa vendor cyber security, pada workshop ini hanya satu saja yang diambil sebagai contoh simulasi. Adapun platform aplikasi anti malware yang dimaksud adalah Sophos Intercept X.

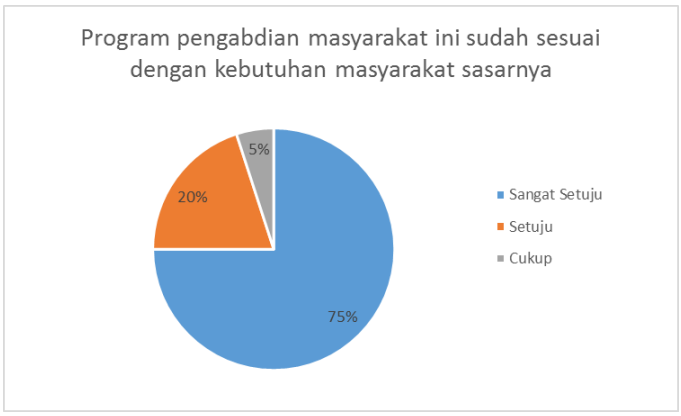
Gambar 4. Proses instalasi aplikasi anti malware pada perangkat ponsel berbasis Android

JURNAL ADAM : JURNAL PENGABDIAN MASYARAKAT
E. ISSN 2829-744X
Available at https://jurnal.spada.ipts.ac.id/index.php/adam
Vol. 3 No. 1
Edisi Februari
2024

Gambar 5. Tampilan hasil scanning oleh aplikasi anti malware Sophos Intercept X pada perangkat ponsel berbasis Android

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 demikian, para pelaku kejahatan akan selalu memunculkan modus-modus baru yang tetap akan menyasar para end user itu sendiri. Karenanya literasi keamanan dalam bertransaksi menggunakan platform digital tetap rutin dilakukan.

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 95% menyatakan puas dengan kegiatan ini serta sisanya (5%) menyatakan cukup.



Gambar 6. Survey kegiatan pengabdian masyarakat mengenai kejahatan keuangan digital di PWRI Provinsi Jawa Barat

4. SIMPULAN

Berdasarkan kegiatan workshop ini serta adanya sharing session selama kegiatan berlangsung maka dapat disimpulkan 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. Contoh-contoh yang disebutkan di atas menyoroti beragamnya jenis kejahatan ini, mulai dari penipuan perbankan online hingga pencucian uang. Sangat penting bagi individu peserta workshop untuk tetap waspada, menerapkan langkah-langkah keamanan yang kuat, dan terus mengikuti perkembangan terbaru dalam keamanan siber untuk memitigasi risiko yang terkait dengan kejahatan keuangan digital.

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.

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

Atmojo, R. N. P., & Fuad, F. (2023). Upaya Perlindungan Hukum Bagi Para Konsumen Pemegang Aset Kripto di Indonesia. *Jurnal Hukum To-Ra: Hukum Untuk Mengatur Dan Melindungi Masyarakat*, *9*(2), 254–276.

BBC. (2016, November 7). Tesco Bank blames “systematic sophisticated attack” for account losses. *BBC*. Retrieved from https://www.bbc.com/news/business-37891742

Berthelsen;Christian, & Turton, M. D. W. (2019). Capital One Says Breach Hit 100 Million Individuals in U.S. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2019-07-29/capital-one-data-systems-breached-by-seattle-woman-u-s-says

BUANA, S. E. W. (2022). Perlindungan Hukum Terhadap Data Pribadi Kepada Pemilik Data Pribadi Dalam Penyelenggaraan Jasa Fintech Peer To Peer Lending.

Cornish, C. (2023, November). India fights back against soaring digital fraud. *Www.Ft.Com*. Retrieved from https://www.ft.com/content/4c384149-bdb1-4bad-87ec-05b7fdec418d

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

Fajarini, A. P. M., Widyantara, I. M. M., & Sutama, I. N. (2022). Peran Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) dalam Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme. *Jurnal Konstruksi Hukum*, *3*(1), 104–109.

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

Hidayat, R. R., & Jatikusumo, D. (2019). Monitoring Sistem Berbasis Web Keamanan Transaksi Pengiriman Uang Pada Penyelenggara Transfer Dana Dengan Menggunakan Peraturan Bank Indonesia Anti Pencucian Uang & Pencegahan Pendanaan Terorisme.

Jasper Jolly. (2018). No TitleBritish Airways: 185,000 more passengers may have had details stolen. *The Guardian*. Retrieved from https://www.theguardian.com/business/2018/oct/25/british-airways-data-breach-185000-more-passengers-may-have-had-details-stolen

Kusuma, A. C., & Rahmani, A. D. (2022). Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia). *SUPREMASI: Jurnal Hukum*, *5*(1), 46–63.

McCrank, John; Finkle, J. (2018, March 3). Equifax breach could be most costly in corporate history. *Www.Reuters.Com*. Retrieved from https://www.reuters.com/article/idUSKCN1GE2JO/

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

Rizaldi, A. (2022). PENGEMBANGAN CYBER SECURITY INDONESIA DALAM UPAYA MENGHADAPI ANCAMAN CYBER CRIME MELALUI BADAN SIBER DAN SANDI NEGARA (BSSN). Universitas Muhammadiyah Malang.

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

Satriana, I., & Dewi, N. M. L. (2022). Law Enforcement in The Process of Investigation on The Crime of Skimming by Foreign Nationals. *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)*, *11*(1), 13–27.

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

Webber. (2023). *The Complete List of Data Breaches In Australia For 2018 – 2023*. Retrieved from https://www.webberinsurance.com.au/data-breaches-list

Zhang, J. (2021, November 28). China fines Caifutong, Tencent's WeChat Pay operator, for breaking foreign exchange rules. *SCMP*. Retrieved from https://www.scmp.com/tech/big-tech/article/3157665/china-fines-caifutong-tencents-wechat-pay-operator-breaking-foreign