E-ISSN: 2655-0865
DOI: https://doi.org/10.38035/rrj.v6i4
Received: 24 Mei 2024, Revised: 10 Juni 2024, Publish: 13 Juni 2024

Ranah Research :
Journal of Multidisciplinary Research and Development
+62 821-7074-3613 ranahresearch@gmail.com https://jurnal.ranahresearch.com/

Strategi Pencegahan Kejahatan *Sniffing* di *M-banking* melalui WhatsApp oleh Lembaga Perbankan

Rista Azimatul Musyayadah[1], Monica Margaret[2]
[1] Universitas Budi Luhur, Jakarta, Indonesia, 2043501192@student.budiluhur.ac.id
[2] Universitas Budi Luhur, Jakarta, Indonesia, monica.margaret@budiluhur.ac.id

Corresponding Author: 2043501192@student.budiluhur.ac.id

Abstract: *WhatsApp has become one of the most widely used modern communication media globally, including in Indonesia. The numerous benefits provided by WhatsApp have also attracted cybercriminals, making it a medium for trapping victims in various cybercrimes, such as attacks on mobile banking. One of the methods used by criminals in WhatsApp-based cybercrimes is sniffing, which focuses on stealing personal and financial data. The purpose of this study is to understand the prevention strategies implemented by banking institutions in combating sniffing crimes in m-banking that use WhatsApp to trap victims. This research employs a descriptive qualitative method, with data derived from interviews and literature studies. The study found that user ignorance is one of the factors contributing to sniffing. Therefore, education through socialization can be considered effective in preventing this crime. Nevertheless, the security and detection systems in banking institutions must be enhanced and regularly checked to ensure their reliability.*

Keyword: *Situational Crime Prevention, Sniffing, Mobile Banking, Whatsapp, Banking Institutions.*

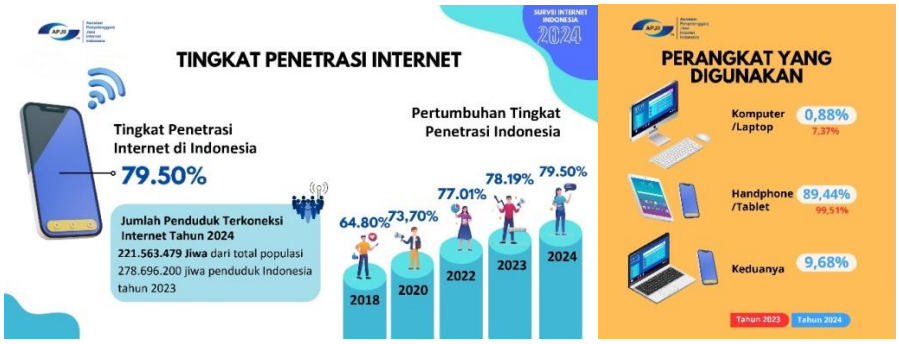
Abstrak: WhatsApp telah menjadi salah satu media komunikasi terkini yang digunakan di seluruh dunia, termasuk Indonesia. Banyaknya manfaat yang diberikan WhatsApp turut menarik pelaku kejahatan siber dan menjadikannya sebagai media untuk menjebak korban dalam berbagai kejahatan siber, seperti serangan terhadap *mobile banking.* Salah satu metode yang digunakan pelaku dalam kejahatan dengan menggunakan WhatsApp adalah *sniffing*, yang berorientasi pada pencurian data pribadi dan keuangan. Tujuan penelitian ini adalah untuk mengetahui bagaimana strategi pencegahan yang dilakukan oleh lembaga perbankan dalam menghadapi kejahatan *sniffing* di *m-banking* yang menggunakan WhatsApp untuk menjebak korbannya. Penelitian ini menggunakan metode kualitatif deskriptif, data yang diolah bersumber dari hasil wawancara dan studi kepustakaan. Penelitian ini menemukan bahwa ketidaktahuan pengguna merupakan salah satu faktor terjadinya *sniffing.* Oleh karena itu, edukasi melalui sosialisasi dapat dikatakan efektif dalam mencegah terjadinya kejahatan

ini. Meskipun demikian, keamanan dan sistem deteksi pada Lembaga Perbankan tetap harus ditingkatkan dan dilakukan pengecekan secara berkala sehingga keamanannya terjamin.

Kata Kunci: Strategi Pencegahan Kejahatan Situasional, *Sniffing*, *Mobile Banking*, Whatsapp, Lembaga Perbankan.

PENDAHULUAN

Perubahan merupakan keniscayaan dalam kehidupan manusia yang bersifat dinamis, hal ini tercermin dari adanya revolusi dari waktu ke waktu yang timbul akibat dari manusia yang selalu mencari cara untuk beraktifitas dengan mudah dan efisien (Puslitbang Aptika dan IKP, 2019) Sejalan dengan itu, dalam beberapa dekade terakhir, perkembangan teknologi dan transformasi digital telah memberikan dampak yang luas dalam berbagai sektor kehidupan manusia, termasuk komunikasi, transportasi, kesehatan, pendidikan, dan industri. Indonesia sebagai negara berkembang sudah ikut andil dalam perkembangan internet, hal ini tercermin dari pertumbuhan akses internet, peningkatan penggunaan *smartphone*, dan adopsi teknologi digital yang menjadi bagian penting dari perkembangan teknologi informasi di Indonesia. Dilansir dari laporan survei yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) terkait tingkat penetrasi internet di Indonesia dan perangkat yang digunakan, bahwa:



Sumber: Asosiasi Penyedia Jasa Internet Indonesia

Gambar 1. Grafik Tingkat Penetrasi Internet dan Perangkat yang Digunakan

Jumlah pengguna internet di Indonesia telah mencapai 221 juta jiwa, jumlah itu setara dengan 79,50% dari total populasi Indonesia yang berjumlah 278,6 juta jiwa di tahun 2023. Tingkat penetrasi internet menunjukkan peningkatan secara signifikan dalam lima tahun terakhir. Terhitung sejak 2018 secara berturut-turut mencapai 64,8%, 73,7% di 2020, 77,01% di 2022, 78,19% di 2023, dan 79,50% di 2024. Sebanyak 89,44% pengguna internet di Indonesia menggunakan *handphone/*tablet untuk mengakses internet, 0,88% memilih komputer/laptop, dan 9,68% memilih menggunakan kedua perangkat tersebut (APJII, 2024). Rata-rata pengguna menghabiskan 7 jam 38 menit setiap harinya untuk aktivitas *online* (Laporan DataReportal via slice.id, 2024). Fenomena ini menunjukkan bagaimana *smartphone* telah menjadi perangkat utama untuk melakukan aktivitas *online*, termasuk komunikasi dan aktivitas perbankan melalui layanan *m-banking*.

WhatsApp merupakan salah satu aplikasi pesan instan utama di banyak negara, termasuk Indonesia. Jumlah pengguna WhatsApp di Indonesia mencapai angka 112 juta jiwa (Laporan Q1 dari *Business of Apps* via dataindonesia.id, 2023), dan menyentuh angka 97, 86% sebagai media chat yang sering digunakan (APJII, 2024), hal ini menunjukkan pentingnya platform tersebut dalam komunikasi dan penyebaran informasi. Sedangkan *m-banking* merupakan layanan keuangan yang memudahkan penggunanya untuk mengakses

dan melakukan transaksi cukup dengan perangkat *smartphone* atau perangkat elektronik lainnya yang memiliki akses internet (Otoritas Jasa Keuangan, 2016).

Kecepatan penyebaran informasi dan banyaknya pengguna WhatsApp telah menjadikannya sebagai media yang rentan dimanfaatkan oleh para peretas dalam melakukan serangan terhadap layanan *m-banking*. Para peretas menggunakan berbagai metode, salah satunya melalui *sniffing*, yaitu salah satu jenis kejahatan siber yang dapat memantau atau memeriksa aliran paket data yang ditujukan untuk mesin tertentu dan ditujukan kepada mesin tertentu pula (kapersky.com). Modus operandi yang umum digunakan adalah dengan mengirimkan file berbahaya melalui WhatsApp yang disamarkan menjadi undangan pernikahan. Korbannya pun berasal dari berbagai jenjang pendidikan dan berusia muda hingga tua. Polri memperkirakan kerugian dalam kasus *sniffing* mencapai Rp12 miliar dengan 483 korban (economicreview.id). Upaya penyamaran melalui berbagai modus operandi, termasuk pengiriman resi paket dan surat panggilan dari kepolisian.

Pada konteks di atas, sejarah komunikasi manusia telah melalui perjalanan panjang hingga era teknologi informasi saat ini, dengan layanan seperti *m-banking* dan aplikasi seperti WhatsApp yang membawa kemudahan namun juga menimbulkan bahaya keamanan seperti serangan *sniffing*. Bahkan dengan adanya perlindungan keamanan, selalu ada celah akibat kelalaian pengguna dan modus operandi peretas yang terus berubah. Oleh karena itu, diperlukan strategi pencegahan yang efektif yang mampu memberikan perlindungan proaktif dan adaptif bagi pengguna layanan *m-banking* dari serangan siber seperti *sniffing*.

METODE

Penelitian ini menggunakan metode kualitatif, yaitu metode yang digunakan untuk menyelidiki fenomena dan paradigma alami. Tujuannya adalah untuk memahami apa, bagaimana, dan mengapa suatu fenomena dapat terjadi (Saleem, 2010, dalam Susilo, 2018) Menurut Bogdan dan Biklen (dalam Anggito & Setiawan, 2018), penelitian kualitatif lebih bersifat deskriptif. Peneliti harus menuangkan kutipan-kutipan data yang berupa fakta mengenai suatu objek, fenomena, maupun *setting* sosial ke dalam tulisan yang bersifat naratif. Adapun penggunaan metode ini dilakukan guna menjelaskan secara mendalam mengenai bagaimana dan mengapa *sniffing* di *m-banking* melalui WhatsApp sebagai medianya dapat terjadi, serta apa dan bagaimana strategi pencegahan kejahatan yang dilakukan oleh lembaga perbankan dalam menghadapi kejahatan *sniffing* pada *m-banking* yang menggunakan WhatsApp sebagai media untuk menjebak korbannya. Data primer diperoleh melalui wawancara langsung dengan narasumber terkait kejahatan *sniffing* di *m-banking* melalui WhatsApp, sedangkan data sekunder diperoleh melalui studi kepustakaan.

HASIL DAN PEMBAHASAN

Landasan Teori

Pencegahan Kejahatan Situasional merupakan paradigma kriminologi terapan yang menggabungkan dua konsep situasi kriminal yang saling melengkapi. Pendekatan pertama berfokus pada *rational choice* dan pandangan *routine activity*, di mana situasi kriminal dianggap sebagai peluang yang dievaluasi secara rasional oleh pelaku. Sementara itu, pendekatan kedua berasal dari psikologi sosial dan perilaku, menekankan bahwa situasi dapat mempengaruhi perilaku secara tidak sadar (Smallbone, 2013). Pencegahan Kejahatan Situasional berfokus pada langkah-langkah pengurangan peluang seseorang atau kelompok dalam melakukan pelanggaran atau kejahatan dengan meningkatkan resiko atau tingkat kerumitan dan mengurangi keuntungan atau penghargaan bagi pelaku (Clarke, 1997). Cornish dan Clarke mengklasifikasikan bentuk intervensi ke dalam 25 teknik pencegahan situasional dan membaginya menjadi lima kelompok (Bullock, 2010, dalam Sudiadi, 2015):

Tabel 1. Teknik Strategi Pencegahan Kejahatan Situasional

Increase the effort	Increase the risks	Reduce the rewards	Reduce provocation	Remove excuses
Target harden	Extend guardianship	Conceal targets	Reduce frustrations and stress	Set rules
Control access to facilities	Assist natural	Remove targets	Avoid disputes	Post instruction
Screen exits	Reduce anonymity	Identify property	Reduce emotional arousal	Alert conscience
Deflect offenders	Use place managers	Disrupt markets	Neutralize peer pressure	Assist compliance
Control tools/weapons	Strengthen formal surveillance	Deny benefits	Discourage imitation	Controlling drugs and alcohol

Secara praktis, pencegahan kejahatan dapat dicapai dengan mengurangi peluang kejahatan dan menghilangkan kondisi pemicu perilaku masalah tertentu. Pencegahan kejahatan situasional efektif untuk masalah yang sangat spesifik, dan pendekatan ini memerlukan analisis situasional tingkat mikro untuk merancang intervensi yang sesuai dengan setiap masalah dan pengaturan khusus. Intervensi ini dirancang untuk membuat tindakan yang dilakukan menjadi lebih berisiko, sulit dijalankan, kurang memuaskan, kurang diperbolehkan, dan kurang menggoda dengan mengubah lingkungan fisik dan interaksi manusia dengan lingkungan tersebut (Smallbone, 2013). Dapat disimpulkan bahwa pencegahan kejahatan situasional bertujuan untuk melakukan intervensi terhadap pelaku kejahatan agar kesulitan dalam mengakses target kejahatan mereka, serta mengurangi nilai atau keuntungan yang akan mereka peroleh dari tindakannya tersebut.

Fenomena *Sniffing* di *M-banking* melalui WhatsApp

Kejahatan *Sniffing* pada *m-banking* yang menggunakan WhatsApp sebagai media untuk menjebak korbannya marak terjadi dalam beberapa tahun terakhir. *Sniffing* merupakan proses menangkap, mendekode, memeriksa, dan menafsirkan data dari paket-paket yang dikirim melalui saluran transmisi, seperti jaringan *transmission control/internet protocol*. Proses *sniffing* dilakukan menggunakan perangkat khusus yang disebut *packet sniffer* (Prabadevi & Jeyanthi, 2018). *Sniffer* dikenal juga sebagai monitor jaringan atau penganalisis jaringan. Administrator jaringan atau sistem dapat menggunakan *sniffer* secara sah guna memantau dan memecahkan lalu lintas jaringan, di mana melalui informasi yang ditangkap oleh *sniffer* dapat digunakan sebagai pengidentifikasi paket yang salah dan data tersebut dapat digunakan untuk menunjukkan adanya hambatan dan memberikan bantuan, serta menjaga transmisi data dan jaringan yang efisien (swissen.in).

Kejahatan siber seperti *sniffing* dapat ditimbulkan oleh beberapa faktor (Umbara & Setiawan, 2022), diantaranya:

1. Sosialiasi dan edukasi yang kurang terkait manfaat internet, sehingga rawan disalahgunakan.
2. Kesenjangan sosial yang semakin besar karena kemajuan sebuah negara tidak diimbangi dengan kesejahteraan masyarakatnya.
3. Kian marak sosial media menjadikan manusia semakin terikat dengan akses internet dalam hidupnya.
4. Berkaitan dengan gaya hidup.
5. Kelalaian pengguna.
6. Keinginan validasi dari orang lain.
7. Kemajuan teknologi dan aksesibilitas internet yang luas.

Sedangkan motifnya dapat diklasifikasikan menjadi dua kelompok (Umbara & Setiawan, 2022), yaitu:

1. Motif intelektual, dapat dikatakan bahwa kejahatan yang dilakukan adalah untuk menunjukkan bahwa dirinya hebat dan semata-mata untuk kesenangan pribadi. Motif ini umumnya dilakukan secara individu.
2. Motif ekonomi, politik, dan kriminal, yang berarti dilakukan untuk mendapatkan keuntungan dan memberikan kerugian pada korbannya baik secara ekonomi maupun politik, Motif ini umumnya dilakukan secara kolektif.

Pada era saat ini, masyarakat dipaksa untuk bergantung pada internet dan teknologi digital. *M-banking* merupakan layanan perbankan yang memudahkan penggunanya dalam melakukan transaksi finansial dan non finansial, dimana pengguna cukup menggunakan perangkat telepon seluler ataupun perangkat elektronik lainnya yang memiliki akses internet (Otoritas Jasa Keuangan, 2016) Sedangkan WhatsApp merupakan media chat yang memberikan berbagai kemudahan dalam menyampaikan pesan melalui fitur-fiturnya, pesan yang diterima lebih cepat sampai, serta pemakaian aplikasi yang tergolong murah (Ahmad, Susanti, & Muzid, 2022). Berdasarkan wawancara dengan korban dan saksi dari kejahatan *sniffing*, mereka mengaku menggunakan WhatsApp sebagai media untuk memudahkan komunikasi, sedangkan penggunaan *m-banking* digunakan untuk mempermudah transaksi agar tidak harus datang lagi ke ATM. Dimana semakin bertambahnya nasabah yang memanfaatkan layanan *internet banking* turut memberikan kesempatan bagi pelaku kejahatan siber dalam melakukan tindakannya (Hidayatullah, 2023). Selain itu, korban berinisial A menggunakan *e-commerce* untuk berjualan turut menjadi korban dari kejahatan ini.

Pelaku dalam kejahatan siber seperti *sniffing* umumnya merasa terdorong karena berpikir bahwa mereka memiliki kesempatan untuk melakukan tindakannya dengan melihat bahwa kurangnya pengawasan, mengingat sifat anonimitas internet dan luasnya aksesibilitas sehingga sulit untuk mengatur dan mengawasi aktivitas yang terjadi di dalamnya. Hal ini diperparah dengan ketidaktahuan dan ketidakpedulian masyarakat terhadap kejahatan siber yang berpotensi melahirkan keuntungan bagi para pelaku kejahatan (Palinggi, Palelleng, & Allolinggi, 2020). Adapun saksi berinisial AK menjelaskan bagaimana ayahnya menjadi korban dari kejahatan *sniffing* yang menguras tabungan ayahnya dengan total kerugian mencapai 58 juta rupiah. Kejadian tersebut berawal dari pesan undangan pernikahan yang dikirim oleh teman ayah AK di grup rombongan jamaah haji, namun dengan ketidaktahuan korban akhirnya file tersebut diklik. Di sisi lain, korban berinisial A kehilangan saldonya sebesar 5 juta rupiah di akun *m-banking* dan *e-wallet*nya setelah membuka pesan yang dikira adalah daftar barang yang ingin dibeli pelanggannya. Kedua korban mengaku belum pernah mendengar maupun melihat kejahatan *sniffing* sebelumnya.

Ketidaktahuan para korban merupakan cerminan dari edukasi dan sosialiasi yang kurang. Jika ditelusuri di internet dapat pula terlihat bahwa sebagian masyarakat acuh dengan keamanan pada dunia digital, beberapa dari mereka merasa biasa saja walaupun pernah tanpa sadar mengklik file berisi *malware* tersebut karena tidak memiliki *m-banking*, padahal data pribadi lain milik mereka bisa saja terancam dicuri. Diketahui pula bahwa para pelaku turut mengambil alih akun WhatsApp korbannya, seperti yang terjadi dengan ayah AK. Akun tersebut kemudian digunakan untuk mencari keuntungan lebih banyak dengan cara membagikan pesan dalam bentuk file yang dapat menginfeksi perangkat siapa saja yang mengklik pesan tersebut. Lain halnya dengan korban A yang foto pribadinya digunakan oleh pelaku pada aplikasi Bumblee.

Implementasi Strategi Pencegahan Kejahatan Situasional oleh Lembaga Perbankan

Kejahatan *sniffing* ini muncul akibat kurangnya sistem deteksi dan pencegahan pada pengguna, perangkat yang digunakan, maupun pada keamanan bank. Kelalaian dan ketidaktahuan pengguna dalam menjaga keamanan data pribadi mereka, seperti menggunakan kata sandi yang lemah dan mengunduh aplikasi di luar *Google Playstore*, sering dijadikan

celah bagi pelaku kejahatan siber. Selain itu, perangkat yang tidak diperbaharui secara bekala menjadikannya semakin rentan terhadap serangan siber. Di lain sisi, sistem deteksi dini dan pencegahan bank yang kurang efektif dapat menjadi sasaran empuk bagi serangan siber, sehingga memungkinkan pelaku kejahatan melakukan transaksi ilegal.

United Nations Office on Drugs and Crime mendefinisikan pencegahan kejahatan mencakup strategi dan langkah-langkah yang bertujuan untuk mengurangi resiko terjadinya kejahatan, serta dampak berbahaya potensialnya terhadap individu dan masyarakat, termasuk rasa takut akan kejahatan, dengan melakukan intervensi untuk mempengaruhi berbagai penyebabnya. Pursuit (dalam Sudiadi, 2015) berpendapat bahwa strategi pencegahan kejahatan merupakan serangkaian kegiatan terorganisir untuk mencegah perilaku kriminal atau meminimalisir perilaku tersebut sehingga menghindari campur tangan polisi. Strategi pencegahan dengan pendekatan situasional berupaya mengurangi peluang terjadinya kejahatan, baik oleh individu maupun kelompok. Pendekatan ini didasarkan pada anggapan bahwa pelaku kejahatan bertindak secara rasional dan memanfaatkan kesempatan yang ada (Gunawan & Margaret, 2022) Teknik-teknik strategi pencegahan situasional melibatkan beberapa aspek, seperti meningkatkan usaha yang diperlukan untuk melakukan kejahatan, meningkatkan risiko tertangkap, mengurangi keuntungan yang dapat diperoleh, mengurangi provokasi, dan menghilangkan alasan pelaku dalam melakukan tindakannya.

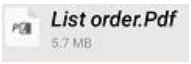
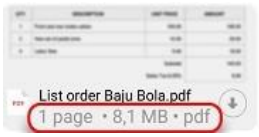
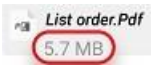
Pada aspek meningkatkan usaha, langkah-langkah yang dilakukan adalah dengan memperkokoh sasaran melalui edukasi atau sosialisasi kepada nasabah guna meningkatkan kewaspadaan terhadap kejahatan perbankan serta memberikan kiat-kiat aman bertransaksi melalui *website* Bank dan media *online* seperti Facebook, YouTube, Twitter, dan Instagram. Untuk mengendalikan akses ke dalam fasilitas maka digunakan autentikasi 2 faktor yang dapat berbentuk kode *one time password*, tautan, kolom isi, kode, maupun *biometric scan* yang diterima melalui *e-mail* maupun *software* khusus (bca.co.id). Selain itu, termasuk pula satuan kerja yang berkoordinasi dengan unit kerja di Cabang, Wilayah, maupun Kantor Pusat dalam melakukan pengidentifikasian, pengukuran, pemantauan, serta pengendalian resiko yang tujuannya adalah untuk menilai potensi resiko terjadinya *fraud*. *Update reguler* melalui *threat intelligence* dan pelaksanaan *cyber drilling* secara berkala juga penting untuk mengantisipasi risiko siber. Bank menerapkan kombinasi sistem dan proses untuk mendeteksi aktivitas yang terindikasi *fraud*, termasuk penggunaan *Fraud Detection System* yang mampu mendeteksi anomali transaksi pada nasabah (*Direktur Information Technology* Bank Mandiri dalam keuangan.kontan.co.id). Kemudian, untuk menghindari pelaku dapat dilakukan dengan cara memperhatikan dan berhati-hati dalam mengklik pesan berisi *file*, terutama jika *file* tersebut berformat .apk. Waspada pada setiap pesan berisi *file* yang masuk, karena pelaku *sniffing* kerap kali mengambil alih akun WhatsApp korban-korbannya dan menyebarkan pesan tersebut kepada grup maupun kontak yang ada pada WhatsApp korbannya. Selain itu, hindari penggunaan WiFi di tempat umum dalam melakukan transaksi perbankan karena dapat menjadi salah satu pintu masuk kejahatan seperti *sniffing*.

Pada aspek meningkatkan resiko, upaya pencegahan yang dilakukan adalah dengan memperluas penjagaan melalui dibentuknya satuan kerja atau biro khusus yang dapat memantau transaksi nasabah dan menerima pengaduan nasabah 24 jam dalam 7 hari secara *real-time*, seperti divisi manajemen risiko dan biro *anti-fraud*. Dalam memanfaatkan manajer tempat, dilakukan pengawasan aktif oleh Dewan Komisaris dan Direksi guna memastikan bahwa kebijakan dan prosedur dijalankan secara disiplin dan konsisten, serta untuk menjamin efektivitas kontrol internal. Adapun dalam memperkuat pengawasan formal dilakukan dengan pengawasan oleh lembaga-lembaga terkait seperti Bank Indonesia dan Otoritas Jasa Keuangan dalam mengawasi kepatuhan Bank terhadap regulasi keamanan siber, manajemen risiko, keamanan infrastruktur teknologi informasi, penanganan masalah siber, evaluasi keamanan, pelaporan dan pengungkapan, serta berkoordinasi sebagai upaya pencegahan serta

penegakan hukum terkait kejahatan siber yang dilakukan oleh kepolisian untuk melakukan proses hukum.

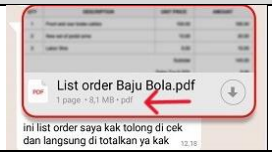
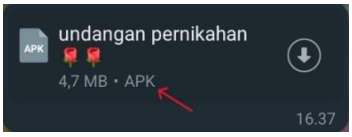
Pada aspek mengurangi keuntungan, bank melakukan kegiatan terkait literasi keuangan digital. Salah satunya dilakukan melalui kerjasama OJK dalam program edukasi yang disajikan dalam bentuk modul sosialisasi, buku elektronik, video animasi, dan permainan-permainan. Dalam aspek mengurangi provokasi, dicegah dengan memperhatikan perbedaan *file* asli dengan *file* tipuan. Pelaku *sniffing* umunya mengirimkan *file* degan format .apk, namun ada juga yang menggunakan format .pdf. Dilansir dari *website* BCA, berikut adalah bagaimana membedakan file pdf asli dan tipuan:

Tabel 1. Perbandingan file dengan format .pdf asli dan palsu

Asli		Palsu	
	Terlihat tampilan dokumen		Tidak memiliki tampilan dokumen
	Logo file berwarna putih dan tulisan PDF berwarna merah		Logo file berwarna putih dan tulisan PDF berwarna hitam atau abu.
	Memiliki detail dokumen yang terperinci, terdapat format file dibawah judul file, serta ukurannya yang tidak sebesar file palsu		Tidak memiliki detail dokumen (seperti jumlah halaman), tidak memiliki format file, dan berukuran besar.

Sumber: bca.com

Tabel 2. Perbandingan file asli dan palsu dalam format .apk dan .pdf

File Asli	File Palsu	
		

Sumber: bca.com dan dokumentasi pribadi

File dengan format .pdf harus diperhatikan dengan lebih cermat karena terkadang lebih sulit dibedakan daripada *file* berformat .apk. Selain itu, file berformat .pdf juga dikaitkan dengan dokumen yang sah dan digunakan sehari-hari oleh kalangan tertentu, sehingga orang cenderung mempercayai dan mengklik tanpa curiga. Adapun pada aspek menghilangkan alasan pelaku untuk mengurungkan niatnya dalam melakukan *sniffing* di *m-banking* melalui WhatsApp dapat dicegah dengan menetapkan peraturan dari lembaga-lembaga terkait hingga peraturan perundang-undangan. Selain itu, untuk meningkatkan kewaspadaan maka pengguna wajib curiga jika ada yang mengirimkan pesan berisi *file.* Demikian dalam mencegah terjadinya kejahatan serupa, lembaga perbankan dapat saling berbagi informasi agar dapat mempelajari kejahatan dengan modus-modus baru, tujuannya adalah agar dapat dilakukan pencegahan lebih awal sebelum menyebar ke bank lainnya, sebagaimana yang dikatakan oleh Timothy Utama selaku *Direktur Information Technology* Bank Mandiri (keuangan.kontan.co.id).

KESIMPULAN

Strategi pencegahan kejahatan yang dilakukan oleh Lembaga Perbankan sudah cukup mencegah kejahatan *sniffing* di *m-banking* melalui WhatsApp terutama adanya kerja sama dengan instansi-instansi terkait dalam mengedukasi atau menyebarkan *awareness* kepada

pengguna. Penulis berpendapat bahwa edukasi merupakan faktor yang paling memberi pengaruh dalam upaya pencegahan kejahatan ini, karena dalam kasus kejahatan *sniffing* di *m-banking* melalui WhatsApp pengguna sebagai pintu utama. Selain itu, pembaharuan *update system* pada *device* sebaiknya diperhatikan karena dapat meminimalisir celah pada keamanan, hindari juga mengunduh aplikasi yang tidak resmi atau di luar *Google Play*. Meskipun demikian keamanan dan sistem deteksi pada Lembaga Perbankan tetap harus ditingkatkan dan dilakukan pengecekan secara berkala agar keamanannya terjamin.

REFERENSI

Ahmad, F. S., Susanti, N., & Muzid, S. (2022). Implementasi Teknologi WhatsApp pada ADINDA. *Jurnal Sistem Informasi dan Teknologi*, 57-64.

Alfarizki. (2023, 3 1). *Economic Review*. Diambil kembali dari economicreview.id: https://economicreview.id/cybersecurity-marak-kasus-peretasan-sniffing-melalui-file-apk-begini-tips-cara-mencegahnya/

Anggito, A., & Setiawan, J. (2018). *Metodologi Penelitian Kualitatif.* Sukabumi: CV. Jejak.

APJII. (2024). *Press Conference Survei Penetrasi Internet Indonesia 2024.* Jakarta: Asosiasi Pengguna Jasa Internet Indonesia.

B, P., & N, J. (2018). A Review on Various Sniffing Attacks and Its Mitigation Techniques. *Indonesian Journal of Electrical Engineering and Computer Science*, 1117-1125.

Bank Central Asia. (2022, 3 10). *BCA*. Diambil kembali dari bca.co.id: https://www.bca.co.id/id/informasi/Edukatips/2022/03/10/08/00/mengenal-lebih-jauh-tentang-otp

Clarke, R. V. (1997). *Situational Crime Prevention: Successful Case Studies.* New York: Harrow and Heston.

Gunawan, E., & Margaret, M. (2022). Situational Crime Prevention terhadap Pelecehan Seksual di Mass Rapid Transit (MRT) Jakarta. *Jurnal Anomie*, 1-10.

Hidayatullah, C. (2023). Jenis dan Dampak Cyber Crime. *Prosiding SAINTEK: Sains dan Teknologi*, 216-221.

Hutauruk, D. M., & Mahadi, T. (2021, 12 25). *Kontan*. Diambil kembali dari keuangan.kontan.co.id: https://keuangan.kontan.co.id/news/begini-upaya-bank-mandiri-cegah-kejahatan-perbankan-di-tengah-digitalisasi

kapersky. (t.thn.). *Kapersky*. Diambil kembali dari kapersky.com: https://www.kaspersky.com/resource-center/definitions/what-is-a-packet-sniffer?_x_tr_hist=true

Otoritas Jasa Keuangan. (2016). *Seri Literasi Keuangan - Perbankan.*

Palinggi, S., Palelleng, S., & Allolinggi, L. R. (2020). Peningkatan Rasio Kejahatan Cyber dengan Pola Interaksi Sosio Engineering pada Periode Akhir Era Society 4.0 di Indonesia. *Jurnal Ilmiah Dinamika Sosial*, 145-163.

Puslitbang Aptika dan IKP. (2019). *Perkembangan Ekonomi Digital di Indonesia.* Jakarta: Puslitbang Aptika.

Rizaty, M. A. (2023, 5 17). *dataindonesia.id*. Diambil kembali dari dataindonesia.id: https://dataindonesia.id/internet/detail/pengguna-whatsapp-global-capai-245-miliar-hingga-kuartal-i2023

slice.id. (2024, 3 18). *slice*. Diambil kembali dari slice.id: https://www.blog.slice.id/blog/tren-pengguna-media-sosial-dan-digital-marketing-indonesia-2024

Smallbone, S. (2013). Situational Crime Prevention. *NOTA Policy Committee.* North West England: National Organisation for the Treatment of Abuse.

Sudiadi, D. (2015). *Pencegahan Kejahatan di Perumahan.* Jakarta: Yayasan Pustaka Obor Indonesia.

Susilo, W. H. (2018). *Penelitian Kualitatif.* Surabaya: CV. Garuda Mas Sejahtera.

swissen.in. (t.thn.). *swissen.in*. Diambil kembali dari swissen.in.

Umbara, A., & Setiawan, D. A. (2022). Analisis Kriminologis Terhadap Peningkatan Kejahatan Siber di Masa Pandemi Covid-19. *Jurnal Riset Ilmu Hukum*, 81-88.

United Nations Office on Drugs and Crime. (t.thn.). *United Nations Office on Drugs and Crime*. Diambil kembali dari unodc.org: https://www.unodc.org/unodc/justice-and-prison-reform/cpcj-crimeprevention-home.html