Kabilah: Journal of Social Community Print-ISSN: 2502-9649 Online-ISSN: 2503-3603
Terakreditasi Nasional SK No.14/E/KPT/2019 Vol. 8 No.1 Juni 2023

PENCEGAHAN *FRAUD* PADA KEJAHATAN SIBER PERBANKAN

Nanang Setiawan, Imam Wahyudi
Institut Agama Islam Al-Fatimah Bojonegoro
Universitas Islam Madura Pamekasan
Email: nanang.setiawan@iai-alfatimah.ac.id
hectorsmaga@gmail.com

Abstrak:
Tulisan ini bertujuan untuk menjelaskan realita kasus kejahatan dunia maya pada internet banking di Indonesia dan memberikan alternatif pencegahan untuk meminimalisir terjadinya kejahatan dunia maya pada internet banking di Indonesia. Artikel ini menggunakan metode kualitatif deskriptif dengan pendekatan studi pustaka. Cyber-crime merupakan kejahatan kerah putih, pelakunya adalah orang-orang terpelajar yang memiliki rasa ingin tahu yang besar terhadap teknologi komputer yang melihat peluang kelalaian dari pengguna komputer (khususnya akses perbankan) dan juga lemahnya sistem keamanan jaringan dan rasionalisasi yang didapat. manfaat besar dengan risiko rendah. Tindakan preventif untuk menghindari kejahatan dunia maya adalah dengan senantiasa meningkatkan pengetahuan tentang modus kejahatan dunia maya dan cara penanggulangannya, ekstra hati-hati dalam setiap transaksi dan akses perbankan baik melalui seluler maupun komputer, ekstra hati-hati dengan setiap data, password, PIN dan kode perbankan lainnya serta melakukan perubahan secara berkala, dan tidak mudah tergoda oleh orang yang tidak bertanggung jawab

Kata Kunci: *pencegahan penipuan, kejahatan dunia maya, perbankan internet*

Abstract:
This paper is aimed to explain the reality of cybercrime cases on internet banking in Indonesia and provide alternative prevention to minimize the occurrence of cyber-crimes on internet banking in Indonesia. This article uses a descriptive qualitative method with a literature study approach. Cyber-crime is a white-collar crime, the perpetrators are educated people who have a great curiosity about computer technolo-gy who see the opportunity for negligence from computer users (especially access to banking) and also a weak network security system and rationalization get a large benefit with low risk. Preventive actions to avoid cyber-crime are to constantly in-crease knowledge of the modus of cyber-crime and how to deal with it, to be extra careful in every transaction and access to banking either through cellular or comput-ers, be extra careful with every data, passwords, PINs and other banking codes and make changes regularly, and not easily tempted from irresponsible people

Keywords*: fraud prevention, cyber-crime, internet banking*

Pendahuluan

Perkembangan teknologi yang melaju cepat saat ini menyebabkan banyaknya inovasi terkait dengan teknologi, di antaranya adalah teknologi internet. Internet merupakan jaringan dari jutaan komputer yang saling terhubungkan (Fuady, 2005)[1]. Dengan internet, setiap orang di seluruh dunia dapat berkomunikasi hanya dengan menekan *keyboard* dan *mouse* di hadapannya. Informasi apapun yang dibutuhkan tersedia, karena kemudahan yang ditawarkan itulah banyak individu yang menggunakannya. Tabel 1 menunjukkan data 10 negara dengan pengguna internet terbesar di dunia tahun 2020, dan Indonesia menempati urutan ke-6 dengan jumlah internet user sebanyak 102,8 juta user dari total 258,3 juta penduduk.

Teknologi internet telah digunakan dalam berbagai aspek kehidupan dan salah satunya adalah pada dunia perbankan dengan teknologi *internet banking. Internet banking* adalah suatu bentuk pemanfaatan media internet oleh bank untuk mempromosikan dan sekaligus melakukan transaksi secara online, baik dari produk yang sifatnya konvensional maupun yang baru (Aini & Taman, 2020) [2].

Trend penggunaan transaksi perbankan semakin meningkat, tansaksi pembayaran yang dilakukan masyarakat tidak lagi dilakukan secara konvensional melainkan sudah beralih secara *online banking* melalui *mobile banking, internet banking*, maupun *online store*. Bank memperoleh keunggulan kompetitif dan peningkatan produktivitas melalui penerapan perbankan online. Pelanggan bank menikmati perbankan online karena menyediakan pengalaman perbankan kapan saja dan di mana saja.

Tabel 1. Daftar 10 Negara dengan Pengguna Internet Terbesar di Dunia Tahun 2020 (Dickson, 2021)[3]

No	Negara	Jml Penduduk	Jml Internet User	Rasio
1	China	1,373,541,278	700,100,000	51%
2	India	1,266,883,598	283,800,000	22%
3	Amerika Serikat	323,995,528	264,900,000	82%
4	Brazil	205,823,665	119,800,000	58%
5	Jepang	126,702,133	104,500,000	82%
6	Indonesia	258,316,051	102,800,000	40%
7	Rusia	142,355,415	91,400,000	64%
8	Meksiko	123,166,749	70,700,000	57%
9	Nigeria	186,053,386	69,100,000	37%
10	Jerman	80,722,792	62,500,000	77%

Fasilitas *internet banking* yang memberikan banyak manfaat dan kemudahan bagi nasabah seperti pengurangan biaya, perluasan pasar dan peningkatan kecepatan layanan, memunculkan terjadinya jenis kejahatan baru baik kejahatan tradisional terorganisir maupun pelanggaran keamanan siber dengan

[1] Fuady, M. E. (2005). "Cybercrime" Fenomena Kejahatan melalui Internet di Indonesia. *Mediator*, *6*(2), 255–264.
[2] Aini, P. N., & Taman, A. (2020). *Jurnal Pendidikan Akuntansi Indonesia, Vol. 18, No. 1, Tahun 2020*. *18*(1), 48–65.
[3] Dickson. (2021). *10 Negara dengan Pengguna Internet Terbesar di Dunia*. https://ilmupengetahuanumum.com/

menggunakan media computer dan internet, termasuk di dalamnya adalah memanfaatkan teknologi *internet banking*, di mana kejahatan tersebut dikenal dengan istilah kejahatan siber (*cyber-crime*). Bagi sebagian besar masyarakat yang terbiasa menggunakan media teknologi komunikasi (telekomunikasi), *cyber-crime* bukanlah istilah yang asing didengar. *Cyber-crime* adalah kejahatan yang dihasilkan komputer yang mencakup semua akses tidak sah atas data dan kerusakan perangkat elektronik keamanan, privasi, PIN, sandi, dan lain-lain dengan penggunaan teknologi (Singh et al., 2021)[4].

(Fuady, 2005; Sheetz, 2007)[5] menerangkan terdapat berbagai versi kejahatan dunia maya seperti: a) hacker orang yang ahli dan menguasai computer, gemar mempelajari seluk-beluk sistem computer dan bereksperimen dengannya untuk kemudian melakukan tindakan menyusup ke dalam jaringan komunikasi suatu institusi di dunia maya, b) *Cracker* adalah tindakan sisi gelap seorang hacker yang secara illegal melakukan penyusupan dan perusakan terhadap situs, website, dan sistem keamanan jaringan internet untuk memperoleh kesenangan dan keuntungan, c) *Carder* adalah orang yang melakukan cracking terhadap kartu kredit untuk mencuri nomor kartu orang lain dan menggunakannya untuk kepentingan pribadi, d) *Deface* adalah tindakan menyusup ke suatu situs lalu mengubah tampilan halaman dari situs dengan tujuan tertentu, e) *Phreaker* adalah orang yang melakukan cracking terhadap jaringan telepon, sehingga dapat menelepon secara gratis ke daerah manapun yang dituju.

Cyber-crime dapat dikategorikan ke dalam 2 (dua) bidang, yaitu: 1) *Computer related crime*, di mana computer menjadi target oleh pelaku untuk setiap perilaku ilegal dan kriminal dengan memproses data sistem computer dengan cara yang tidak sah untuk melakukan kejahatan computer, 2) Computer *generated crime*, di mana computer menjadi alat/senjata yang digunakan oleh pelaku untuk perilaku ilegal untuk merusak atau mencuri beberapa privasi dan data sistem (Singh et al., 2021) [6].

Cyber-crime yang selama ini terjadi pada dunia perbankan diantaranya adalah adanya akses illegal pada akun perbankan nasabah, pemalsuan data nasabah yang tersimpan melalui internet (*cloud*) serta adanya kejahatan memanfaatkan jaringan internet untuk memata-matai. Di samping itu juga terdapat kejahatan yang ditujukan terhadap data pribadi nasabah yang tersimpan dalam komputer. Data pribadi nasabah tersebut seperti PIN, nomor rekening dan lain-lain, serta melakukan transaksi dengan kartu kredit ataupun kartu debet milik orang lain. Dalam kejahatan perbankan, seorang *hackers* dapat masuk ke dalam suatu sistem jaringan perbankan untuk mencuri informasi nasabah yang terdapat di dalam server mengenai *database* rekening bank tersebut, karena dengan adanya

[4] Singh, A., Singh, S. K., Nayak, S. K., & Singh, N. (2021). *Cyber-Crime and Digital Forensic : Challenges Resolution*. *January*

[5] Fuady, M. E. (2005). "Cybercrime" Fenomena Kejahatan melalui Internet di Indonesia. *Mediator*, *6*(2), 255–264, Sheetz, M. (2007). Computer Forensics, An Essential Guide for Accountants, Lawyers, and Managers. In *John Wiley & Sons, Inc*. John Wiley & Sons, Inc. https://doi.org/10.1002/9781119202011

[6] Singh, A., Singh, S. K., Nayak, S. K., & Singh, N. (2021). *Cyber-Crime and Digital Forensic : Challenges Resolution*. *January*

e-banking jaringan tersebut menjadi terbuka serta dapat diakses oleh siapa saja (Golose, 2006)[7].

(Golose, 2006) menyebutkan terdapat beberapa bentuk potensi cyber-crime dalam kegiatan perbankan antara lain: 1) *Typo Site* yaitu Pelaku membuat nama situs palsu yang sama persis dengan situs asli dan membuat alamat yang mirip dengan alamat situs asli. Pelaku menunggu kesempatan jika korban salah mengetikkan alamat dan masuk ke situs palsu buatannya. Jika hal ini terjadi maka pelaku akan memperoleh informasi user dan password korbannya dan dapat dimanfaatkan untuk merugikan korban. 2)*Keylogger/Keystroke Logger* merupakan kajahatan yang sering terjadi pada tempat mengakses internet umum seperti warnet. Program ini akan merekam karakter-karakter yang diketikkan oleh user dan berharap akan mendapatkan data penting seperti user ID maupun password. Semakin sering mengakses internet di tempat umum, semakin rentan pula terkena modus operandi. 3) *Sniffing* adalah saha untuk mendapatkan user ID dan password dengan jalan mengamati paket data yang lewat pada jaringan komputer. 4) *Bruce Force Attacking* merupakan usaha untuk mendapatkan password atau key dengan mencoba semua kombinasi yang mungkin. 5) *Web Deface* merupakan tindakan *Exploitation system* dengan tujuan mengganti tampilan halaman muka satu situs. 6) *Email Spamming* merupakan tindakan mengirimkan junk email berupa iklan produk dan sejernisnya pada alamat email seseorang. 6) *Daniel of Service* yaitu membanjiri data dalam jumlah sangat besar dengan maksud untuk melumpuhkan sistem sasaran. 7) *Virus Worm, Trojan* tindakan yang dilakukan dengan *m*enyebarkan virus worm maupun Trojan dengan tujuan untuk melumpuhkan sistem komputer, memperoleh data-data dari sistem korban dan untuk mencemarkan nama baik pembuat perangkat lunak tertentu.

Potensi pencurian data yang dilakukan sering kali tidak dapat dibuktikan secara kasat mata karena tidak ada data yang hilang tetapi dapat diketahui telah diakses secara illegal dari sistem yang dijalankan. Kejahatan *cyber-crime* ini akan berdampak besar pada perbankan yang bersangkutan, dan dampaknya akan mempengaruhi diantaranya adalah adanya kepercayaan pelanggan yang berkurang atau lebih sering dikenal dengan adanya risiko reputasi, dan dibutuhkan adanya upaya untuk melakukan perbaikan asset dan perbaikan fisik amat besar. Banyak penelitian yang sudah dilakukan terkait dengan realita terjadinya *cyber-crime* dalam industri perbankan. Wang (2020) di dalam penelitiannya menyatakan bahwa terdapat 4 (empat) jenis kejahatan siber yang paling signifikan dalam industri perbankan, yaitu: 1) infeksi virus, *worm* dan *trojan*, 2) email spam elektronik, 3) peretasan, dan 4) *cyberstalking* atau pelecehan online[8].

Dampak dari *cyber-crime* dalam perbankan adalah: 1) hilangnya pendapatan, 2) kerusakan reputasi, 3) kehilangan pelanggan, dan 4) sanksi peraturan (Wang et al., 2020). Fokus dari sebagian besar penelitian yang telah direview mengenai *cyber-crime* adalah pada perspektif keuangan sektor perbankan dan persepsi

[7] Golose, P. R. (2006). Perkembangan CyberCrime dan Upaya Penanganannya di Indonesia oleh Polri. *Buletin Hukum Perbankan Dan Kebanksentralan*, *4*(2).

[8] Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice*, *62*(June), 100415. https://doi.org/10.1016/j.ijlcj.2020.100415

nasabah terhadap layanan perbankan, yaitu implikasi *cyber-crime* terhadap persepsi nasabah dan jasa keuangan (Akinbowale et al., 2020)[9]. Gelombang kejahatan siber yang meningkat yang berdampak negatif pada pertumbuhan ekonomi lembaga keuangan, secara tidak langsung melalui kurangnya kepercayaan pada infrastruktur digital dan internet atau secara langsung melalui penipuan dan pemerasan. Untuk mengurangi kejahatan dunia maya, seseorang harus mempertimbangkan pengembangan pendekatan multi-disiplin untuk gangguan yang efektif terhadap infrastruktur penjahat dunia maya melalui berbagi intelijen tanpa kompromi dan kerja sama yang erat antara penegak hukum dan badan investigasi kejahatan untuk pengumpulan intelijen yang cepat (Akinbowale et al., 2020).

Makalah ini ditujukan untuk menjelaskan fenomena dan berbagai jenis *cyber-crime*, bagaimana perkembangan kasus *cyber-crime* dalam perbankan (*internet banking*) di Indonesia, melakukan analisa penyebab-penyebab terjadinya *cyber-crime*, menjelaskan bagaimana modus operandi yang umumnya dilakukan oleh pelaku *cyber-crime* dan memberikan alternatif pencegahan (*fraud prevention*) untuk menghindari atau meminimalisir terjadinya *cyber-crime* dalam *internet banking* di Indonesia.

Metode Penelitian

Artikel ini menggunakan metode kualitatif deskriptif dengan pendekatan studi literatur. Penelitian kualitatif deskriptif adalah penelitian yang ditujukan untuk memahami fenomena tentang apa yang dialami oleh subjek penelitian dengan cara deskripsi dalam bentuk kata-kata dan bahasa untuk memberikan pemahaman dan penjelasan agar dapat dipahami dengan baik oleh pembaca (Moleong, 2017)[10]. Adapun pendekatan studi literatur ditujukan untuk membantu pembaca dalam memahami seluruh tubuh penelitian yang tersedia tentang suatu topik yang dibahas yang didapatkan dari berbagai sumber data dan literatur, menginformasikan pembaca tentang kelebihan dan kekurangan studi atas topik tersebut (Rhoades, 2011).

Rhoades (2011) menyebutkan langkah-langkah yang dilakukan dalam studi literatur dalam artikel ini adalah: pertama, menentukan topik atau pertanyaan riset; kedua, mengidentifikasi informasi yang relevan berupa kriteria atau kata kunci penyertaan/pengecualian; ketiga, melakukan pencarian literatur dengan kata kunci yang teridentifikasi; keempat, menyaring semua dan mengecualikan studi yang tidak relevan; kelima, meneliti studi yang relevan; keenam, mensintesiskan temuan; dan ketujuh, mengembangkan kesimpulan dan rekomendasi[11].

[9] Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using the balanced score card: a survey of literature. *Journal of Financial Crime*, *27*(3), 945–958. https://doi.org/10.1108/JFC-03-2020-0037

[10] Moleong, L. J. (2017). *Metodologi Penelitian Kualitatif* (Revisi). Remaja Rosdakarya.

[11] Rhoades, E. A. (2011). Commentary: Literature reviews. *Volta Review*, *111*(1), 61–71. https://doi.org/10.17955/tvr.111.1.677

Pembahasan dan Hasil Penelitian

Cyber-crime tergolong kepada jenis kejahatan kerah putih (*white collar crime*). Pelaku *cyber-crime* umumnya adalah kaum terpelajar yang sudah mahir dalam mengoperasikan computer. Terdapat 4 (empat) kategori pelaku *cyber-crime*, yaitu (Fuady, 2005) [12]:

a. *Organizational Occupational Crime*

Dalam kategori ini, pelaku *cyber-crime* merupakan para eksekutif, yang melakukan perbuatan illegal dan merugikan pihak lain melalui jaringan internet demi kepentingan atau keuntungan korporasi.

b. *Government Occupational Crime*

Dalam kategori ini, pelaku *cyber-crime* merupakan pejabat atau birokrat yang melakukan perbuatan illegal melalui internet atas persetujuan atau perintah pemerintah, meski dalam banyak kasus hal itu akan disangkal.

c. *Professional Occupational Crime*

Dalam kategori ini, pelaku cyber-crime merupakan pelaku professional dari berbagai profesi yang melakukan kejahatan secara sengaja (*malpractice)*.

d. *Individual Occupational Crime*

Dalam kategori ini, pelaku *cyber-crime* merupakan perorangan dari kalangan pengusaha, pemilik modal atau orang-orang independen lainnya yang memilih jalan yang menyimpang yang melanggar hukum atau merugikan pihak lain.

Modus operandi *cyber-crime* yang banyak dilakukan oleh pelaku dalam menjalankan operasinya adalah sebagai berikut (Arifah, 2011)[13]:

a. *Unauthorized Access to Computer System and Service*

Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer. Kejahatan ini semakin marak dengan berkembangnya teknologi intranet. Kita tentu belum lupa ketika masalah Timor Timur sedang hangat-hangatnya dibicarakan di tingkat internasional, beberapa website milik pemerintah RI dirusak oleh *hacker*.

b. *Illegal Contents*

Kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya, pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain. Hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah dan sebagainya.

c. *Data Forgery*

Kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scripless document melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen e-commerce dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku karena

[12] Fuady, M. E. (2005). "Cybercrime" Fenomena Kejahatan melalui Internet di Indonesia. *Mediator*, *6*(2), 255–264

[13] Arifah, D. A. (2011). Kasus Cybercrime di Indonesia Indonesia's Cybercrime Case. *Jurnal Bisnis Dan Ekonomi (JBE)*, *18*(2), 185–195.

korban akan memasukkan data pribadi dan nomor kartu kredit yang dapat saja disalahgunakan.

d. Cyber Espionage

Kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data pentingnya (*database*) tersimpan dalam suatu sistem yang *computerized* (tersambung dalam jaringan komputer).

e. Cyber Sabotage and Extortion

Kegiatan ini dilakukan dengan membuat gangguan perusakan atau penghancuran terhadap suatu data, program computer atau system jaringan yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Misalnya dengan penyebaran virus komputer saat korban melakukan browsing di internet.

f. *Offence Against Intellectual Property*

Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Sebagai contoh, peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di Internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.

g. Infringements of Privacy

Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara computerized, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.

Berikut ini beberapa penyebab terjadinya cyber-crime yang marak terjadi dan akhir-akhir ini semakin banyak hingga meresahkan masyarakat. Penyebab tersebut adalah diantaranya (Umamit, 2017)[14]:

1. Akses internet yang tidak terbatas.
2. Kelalaian pengguna komputer. Hal ini merupakan salah satu penyebab utama kejahatan komputer.
3. Mudah dilakukan dengan alasan keamanan yang kecil dan tidak diperlukan peralatan yang super modern. Walaupun kejahatan komputer mudah untuk dilakukan tetapi akan sulit untuk melacaknya, sehingga ini mendorong para pelaku kejahatan untuk terus melakukan hal ini.
4. Para pelaku merupakan orang yang pada umumnya cerdas, mempunyai rasa ingin tahu yang besar dan fanatik akan teknologi komputer. Pengetahuan pelaku kejahatan komputer tentang cara kerja sebuah komputer jauh di atas operator komputer.

[14] Umamit, Z. (2017). *Cyber Crime*. Kompasiana.Com. https://www.kompasiana.com/zulkifliumamit/593803914f4edb085912cea2/cyber-crime?page=all

5. Sistem keamanan jaringan yang lemah dan kurangnya perhatian masyarakat. Masyarakat dan penegak hukum saat ini masih memberi perhatian sangat besar terhadap kejahatan konvensional. Pada kenyataanya pelaku kejahatan komputer masih terus melakukan aksi kejahatannya

Cyber-crime merupakan salah satu jenis kejahatan di dunia maya yang terkait dengan tindakan kriminal dan upaya (penipuan) *fraud*. Dalam kajian tentang fraud, terdapat teori yang menjelaskan tentang penyebab terjadinya fraud yang dikenal dengan *Fraud Triangle Theory* (Cressey, 1950)[15]. Cressey menjelaskan ada 3 penyebab utama terjadinya fraud, yaitu: niat/tekanan (*pressure)*, peluang (*opportunity*) dan rasionalisasi tindakan (*rasionalization*). Tanpa 3 (tiga) sebab tersebut maka tindakan fraud akan sulit terjadi, demikian juga dengan *cyber-crime*. Dalam kasus *cyber-crime* umumnya terjadi dikarenakan adanya niat/tekanan (pressure) dari pelaku berupa tuntutan kebutuhan hidup baik dari diri pribadi atau tuntutan dari orang lain, ditambah dengan adanya peluang (*opportunity*) untuk melakukan tindakan fraud berupa kelalaian pengguna computer (korban) dan juga melihat adanya sistem keamanan yang lemah, dan juga dengan rasionalisasi (rasionalization) atau pembenaran atas tindakannya bahwa tindakannya bukan merupakan tindakan melanggar hukum atau dengan banyaknya pelaku yang sama yang lolos dari jeratan hukum. Rasionalisasi yang lain adalah berdasarkan perhitungan untung rugi *(cost and benefit*) dari pelaku atas tindakannya dengan membandingkan antara potensi pendapatan atas kejahatannya dibandingkan dengan biaya yang ditimbulkan atau resiko yang akan dihadapi termasuk di dalamnya adalah resiko jeratan hukum dan hukuman tahanan. Jika masih besar pendapatan yang akan dihasilkan, maka secara rasionalisasi pelaku akan melanjutkan tindakan fraud, apalagi kejahatan berupa cyber-crime dalam perbankan dengan target para nasabah dengan rekening gemuk, maka sangat besar sekali potensi keuntungan (*benefit*) yang akan didapatkan. Hal inilah yang menjadi alasan penyebab terbesar kenapa cyber-crime masih marak terjadi dan sulit untuk dihentikan.

Banyak penulis telah mengusulkan berbagai solusi untuk mengatasi masalah keamanan perbankan online tetapi sementara beberapa hanya berfokus pada otentikasi klien, yang lain hanya memikirkan keamanan saluran transfer data. Tom mengusulkan protokol otentikasi berbasis biometrik yang dapat dibatalkan yang menjamin otentikasi timbal balik yang aman, privasi pelanggan dan menawarkan transmisi end-to-end data transaksi pelanggan yang aman (Tom et al., 2020)[16]. Protokol ini dirancang dengan menggunakan biohashing, suatu teknik proteksi template biometrik dan algoritma kriptografi ganda yang menggabungkan algoritma *Advanced Encryption Standard* (AES) dan *algoritma Data Encryption Standard* (Tom et al., 2020). Arifah (2011) mengusulkan beberapa upaya

[15] Cressey, D. R. (1950). The Criminal Violation of Financial Trust. *American Sociological Review*, *15*(6), 738–743.

[16] Tom, J., Alese, B. K., & Thompson, A. (2020). A Cancelable Biometric Based Security Protocol for Online Banking System Cloud Computing Security View project Computer Security View project. *Article in International Journal of Computer Science and Information Security*, *June*. https://sites.google.com/site/ijcsis/

pencegahan (prevention) bagi masing-masing individu yang bisa dilakukan untuk mengurangi terjadinya *cyber-crime* yaitu (Arifah, 2011)[17] :

a. *Educate User*, yaitu memberikan pengetahuan baru terhadap *cyber-crime* dan dunia internet.
b. *Use Hacker's Perspective*, yaitu menggunakan pemikiran dari sisi *hacker* untuk melindungi sistem
c. *Patch System*, yaitu menutup lubang-lubang kelemahan pada sistem
d. *Policy*, yaitu menentukan kebijakan-kebijakan dan aturan-aturan yang melindungi sistem dari orang-orang yang tidak berwenang
e. *Firewell*, yaitu sistem yang didesain khusus untuk mencegah akses mencurigakan masuk ke dalam jaringan pribadi
f. *Antivirus*, yaitu program komputer yang digunakan untuk mencegah, mendeteksi, dan menghapus *malware*.

Untuk menghindari dan meminimalisir terjadinya *cyber-crime* dalam perbankan khususnya dalam transaksi *internet banking*, berikut ini terdapat beberapa hal yang bisa dilakukan, yaitu (Wahyuningsih, 2020)[18]:

a. Input URL alamat bank secara benar, pastikan ada tanda gembok
b. Tidak membagikan PIN/password/kode OTP kepada siapapun
c. Rajin mengupdate dan merubah password/PIN secara berkala
d. Memastikan selalu *logout* setelah selesai melakukan transaksi perbankan di ponsel/laptop
e. Rajin membersihkan *history internet* di ponsel/laptop
f. Menghindari sembarangan *download* software/aplikasi
g. Menghindari transaksi dengan menggunakan WiFi umum, VPN gratis dan ponsel orang
h. Tidak mudah tergiur dengan godaan (iming-iming) oknum yang tidak bertanggungjawab
i. Selalu rutin melakukan cek saldo dan mutasi rekening

Dalam *scope* yang lebih luas, berikut ini langkah preventif yang harus dilakukan oleh pemangku kebijakan (dalam hal ini adalah pemerintah) dalam penanggulangan *cyber-crime* adalah (Arifah, 2011)[19]:

a. Melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut.
b. Meningkatkan sistem pengamanan jaringan computer nasional sesuai standar internasional.
c. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan *cyber-crime*.

---

[17] Arifah, D. A. (2011). Kasus Cybercrime di Indonesia Indonesia's Cybercrime Case. *Jurnal Bisnis Dan Ekonomi (JBE)*, *18*(2), 185–195.
[18] Wahyuningsih, R. (2020). *Waspadai Modus Cyber Crime, Ini Cara Aman Transaksi Internet Banking*. Cermati.Com. https://www.cermati.com/artikel/waspadai-modus-cyber-crime-ini-cara-aman-transaksi-internet-banking
[19] Arifah, D. A. (2011). Kasus Cybercrime di Indonesia Indonesia's Cybercrime Case. *Jurnal Bisnis Dan Ekonomi (JBE)*, *18*(2), 185–195

d. Meningkatkan kesadaran warga negara mengenai masalah *cyber-crime* serta pentingnya mencegah kejahatan tersebut terjadi.
e. Meningkatkan kerjasama antar negara, baik bilateral, regional maupun multilateral, dalam upaya penanganan *cyber-crime*, antara lain melalui perjanjian ekstradisi dan *mutual assistance treaties*.

Penutup

Cyber-crime merupakan kejahatan kerah putih (*white collar crime*), pelakunya adalah kaum terpelajar yang mempunyai rasa ingin tahu yang besar terhadap teknologi komputer yang melihat adanya *opportunity* kelalaian dari pengguna computer (terutama akses perbankan) dan juga sistem keamanan jaringan yang lemah dan dengan rasionalisasi mendapatkan benefit yang cukup besar atas tindakannya dengan resiko yang rendah. Hal-hal yang perlu dilakukan agar terhindar dari kejahatan *cyber-crime* adalah senantiasa meningkatkan pengetahuan terhadap modus operandi *cyber-crime* dan cara menanggulanginya, ekstra berhati-hati pada setiap transaksi dan akses perbankan baik melalui media ponsel maupun komputer (laptop), ekstra berhati-hati terhadap setiap data, password, PIN dan kode perbankan lainnya dan melakukan perubahan secara berkala, serta tidak mudah tergiur dengan godaan (iming-iming) dari oknum yang tidak bertanggungjawab.

Penelitian selanjutnya dilakukan kepada lembaga keuangan non perbankan untuk mendapatkan kecukupan informasi bagaimana modus operandi dan bagaimana solusi untuk menanggulanginya. Ucapan terima kasih kepada semua pihak yang telah membantu penelitian ini baik secara langsung maupun tidak secara langsung. Semoga penelitian ini bermanfaat dalam pengembangan keilmuan *digital forensic* khususnya dalam pencegahan *cyber-crime*.

DAFTAR PUSTAKA

Aini, P. N., & Taman, A. (2020). *Jurnal Pendidikan Akuntansi Indonesia, Vol. 18, No. 1, Tahun 2020*. *18*(1), 48–65.

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using the balanced score card: a survey of literature. *Journal of Financial Crime*, *27*(3), 945–958. https://doi.org/10.1108/JFC-03-2020-0037

Arifah, D. A. (2011). Kasus Cybercrime di Indonesia Indonesia's Cybercrime Case. *Jurnal Bisnis Dan Ekonomi (JBE)*, *18*(2), 185–195.

Cressey, D. R. (1950). The Criminal Violation of Financial Trust. *American Sociological Review*, *15*(6), 738–743.

Dickson. (2021). *10 Negara dengan Pengguna Internet Terbesar di Dunia*. https://ilmupengetahuanumum.com/

Fuady, M. E. (2005). "Cybercrime" Fenomena Kejahatan melalui Internet di Indonesia. *Mediator*, *6*(2), 255–264.

Golose, P. R. (2006). Perkembangan CyberCrime dan Upaya Penanganannya di Indonesia oleh Polri. *Buletin Hukum Perbankan Dan Kebanksentralan*, *4*(2).

Lokadata. (2021). *Jenis Kejahatan Siber di Indonesia*. https://lokadata.beritagar.id/

Moleong, L. J. (2017). *Metodologi Penelitian Kualitatif* (Revisi). Remaja Rosdakarya.

Rhoades, E. A. (2011). Commentary: Literature reviews. *Volta Review*, *111*(1), 61–71. https://doi.org/10.17955/tvr.111.1.677

Sheetz, M. (2007). Computer Forensics, An Essential Guide for Accountants, Lawyers, and Managers. In *John Wiley & Sons, Inc*. John Wiley & Sons, Inc. https://doi.org/10.1002/9781119202011

Singh, A., Singh, S. K., Nayak, S. K., & Singh, N. (2021). *Cyber-Crime and Digital Forensic : Challenges Resolution*. *January*.

Tom, J., Alese, B. K., & Thompson, A. (2020). A Cancelable Biometric Based Security Protocol for Online Banking System Cloud Computing Security View project Computer Security View project. *Article in International Journal of Computer Science and Information Security*, *June*. https://sites.google.com/site/ijcsis/

Umamit, Z. (2017). *Cyber Crime*. Kompasiana.Com. https://www.kompasiana.com/zulkifliumamit/593803914f4edb085912cea2/cyber-crime?page=all

Wahyuningsih, R. (2020). *Waspadai Modus Cyber Crime, Ini Cara Aman Transaksi Internet Banking*. Cermati.Com. https://www.cermati.com/artikel/waspadai-modus-cyber-crime-ini-cara-aman-transaksi-internet-banking

Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice*, *62*(June), 100415. https://doi.org/10.1016/j.ijlcj.2020.100415