BANCA ISLAMICA: JURNAL PERBANKAN SYARIAH

Available at https://ejournal.binamuda.info/banca-islamica

ANCAMAN SIBER PADA *MOBILE BANKING* DAN PENCEGAHANNYA

Sandy Maulana Yusuf [1, *]

[1]Program Studi Perbankan Syariah, Sekolah Tinggi Ekonomi Islam Bina Muda Bandung

Abstrak: Dunia perbankan sudah mulai memasuki era digital yang berpengaruh terhadap layanan perbankan. Dengan adanya perbankan digital, nasabah diberikan kemudahan untuk melakukan kegiatan transaksi secara *online* dengan cepat dan mudah salah satunya melalui *mobile banking*. Namun, dengan berkembangnya perbankan digital, terdapat kekhawatiran adanya ancaman siber pada *mobile banking*. Tujuan penelitian untuk memaparkan ancaman siber pada *mobile banking* dan pencegahannya. Metode penelitian yang digunakan pada penelitian ini adalah *library research* dengan menggunakan data sekunder yang diperoleh dari buku, jurnal penelitian terdahulu, dan *website*. Dari hasil penelitian ditemukan bahwa ancaman siber pada *mobie banking* adalah pencurian data, penyalahgunaan hak guna akses pada *mobile banking*, serangan *phishing* pada nasabah, kerentanan *mobile banking* terhadap kesalahan pengelolaan dan kerentanan *mobile banking* terhadap *malware*. Terdapat beberapa upaya untuk mencegah kejahatan siber pada *mobile banking* baik dari pihak perbankan maupun nasabah. Dari pihak perbankan yaitu dengan menerapkan, *two factor authentication, ssl secured website,* dan *automatic timeout sessions.* Sedangkan dari pihak nasabah pencegahan yang dapat dilakukan adalah dengan mengunduh aplikasi resmi dari bank, serta waspada menggunakan fasilitas atau jaringan publik. Dengan adanya pencegahan yang dilakukan oleh pihak perbankan maupun nasabah bisa mengurangi ancaman siber pada *mobile banking*.

Kata kunci: kejahatan siber, *mobile banking*, bank, nasabah.

Abstract: *The banking industry has entered the digital era, significantly influencing banking services. With the advent of digital banking, customers are provided with the convenience of conducting transactions online quickly and easily, particularly through mobile banking. However, alongside the growth of digital banking, concerns about cyber threats targeting mobile banking have emerged. The purpose of this study is to highlight cyber threats to mobile banking and their prevention measures. The research method employed in this study is library research, utilizing secondary data sourced from books, previous research journals, and websites. The study's findings reveal that cyber threats to mobile banking include data theft, misuse of access rights to mobile banking, phishing attacks on customers,*

Citation: Yusuf, S. M. (2025). Ancaman Siber pada *Mobile Banking* dan Pencegahannya. *Banca Islamica: Jurnal Perbankan Syariah, 1*(2), 39-49.

Article History:
Received: 29 Juli 2025
Revised: 26 Agustus 2025
Accepted: 28 Agustus 2025
Published: 31 Agustus 2025

Korespondensi penulis:
sandymaulanayusuf044@gmail.com

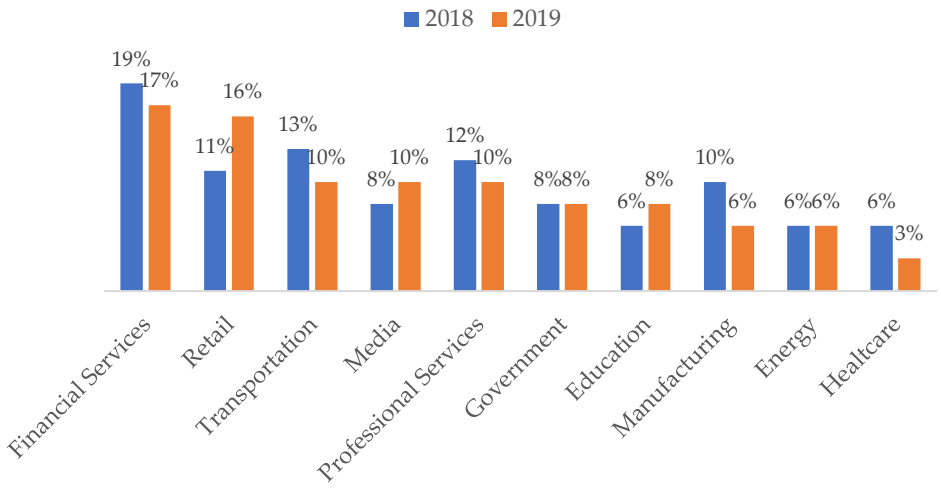
vulnerabilities in mobile banking due to management errors, and susceptibility to malware. Several measures can be taken to prevent cyber-crimes targeting mobile banking, both by banks and customers. Banks can implement measures such as two-factor authentication, SSL-secured websites, and automatic session timeouts. On the customer's side, preventive actions include downloading official banking applications and exercising caution when using public facilities or networks. By implementing these preventive measures, both banks and customers can reduce cyber threats to mobile banking.

Keywords: *cybercrime, mobile banking, bank, customer.*

1. Pendahuluan

Dengan berkembangnya era digital, perbankan harus mengubah secara perlahan bentuk pelayanan konvensional menuju digital. Perbankan digital atau digital *banking* merupakan layanan perbankan yang menggunakan teknologi digital seperti internet, aplikasi *mobile*, dan perangkat lunak untuk memfasilitasi transaksi keuangan. Otoritas Jasa Keuangan (OJK) mendorong digitalisasi perbankan dengan pengeluarkan peraturan OJK No.12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum. Peraturan yang dikeluarkan oleh OJK ini menyebutkan layanan perbankan digital adalah layanan perbankan berbasis elektronik yang bisa memberikan kepuasan kepada nasabahnya, karena perbankan bisa memberikan pelayanan kepada nasabah secara digital yang bisa dilakukan dimana saja secara cepat, mudah dan sesuai dengan kebutuhan nasabah (OJK, 2018**)**. Dengan adanya tekonologi, perbankan harus mulai melakukan layanan digital yang bisa diakses secara cepat dan mudah bagi nasabahnya. *Mobile banking* adalah salah satu contoh dari perkembangan teknologi informasi, yang digunakan perbankan dalam memanfaatkan perkembangan di era digital ini (Wardhana, 2015).

Namun demikian, layanan perbankan yang sudah masuk ke era digital memiliki risiko yang cukup berbahaya. Gambar 1 memperlihatkan laporan kejahatan siber yang sering terjadi di industri tahun 2018-2019.



Gambar 1. Industri yang paling sering terkena siber
Sumber: BSSN, 2020 (data diolah)

Pada Gambar 1, *financial services* (sektor keuangan) merupakan yang sering terkena kejahatan siber. Selama 2 tahun terakhir kejahatan siber pada lembaga keuangan

merupakan kejahatan yang paling rentan dibanding dengan industri lainnya. Semua ini bisa terjadi karena sektor keuangan umumnya sektor perbankan sudah mulai masuk ke era digital yang membuat peluang adanya kejahatan siber terbuka lebar. Kejahatan siber dapat mengancam berbagai layanan perbankan salah satunya layanan pada *mobile banking.* Kejahatan siber pada *mobile banking* pada dasarnya memiliki tujuan yang sama dengan kejahatan pada layanan konvensional yaitu untuk mendapatkan informasi rekening, kartu kredit, serta meretas sistem basis data bank serta merampok bank (Widayanti, 2022).

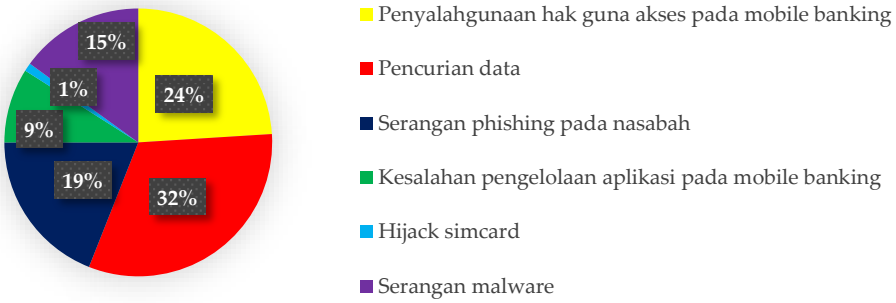
Pada penelitian ini akan dipaparkan apa saja ancaman siber pada *mobile banking* dan bagaimana pencegahannya. Informasi yang akan dipaparkan dalam penelitian ini diharapkan menjadi sebuah informasi yang bermanfaat bagi pengguna *mobile banking* sehingga mengetahui berbagai ancaman siber pada *mobile banking* dan mempersiapkan langkah pencegahannya.

2. Metode Penelitian

Penelitian ini termasuk ke dalam jenis penelitian studi kepustakaaan *library research* yang merupakan penelitian dengan memanfaatkan sumber kepustakaan untuk mendapatkan data penelitian (Zed, 2004). Pendekatan yang dilakukan dalam penelitian ini menggunakan metode deskriptif kualitatif yaitu metode pengolahan informasi dengan cara menganalisa melalui sumber-sumber yang berkaitan dengan objek penelitian. Sumber data yang digunakan dalam penelitian ini adalah data sekunder, yakni data-data berupa dokumen tertulis yang berasal dari buku, jurnal, dan *website* yang berkaitan dengan penelitian

3. Hasil dan Pembahasan

Mobile banking adalah suatu layanan perbankan yang memungkinkan nasabah untuk mengakses dan melakukan transaksi perbankan melalui perangkat *mobile* seperti ponsel pintar atau tablet. Dengan menggunakan aplikasi perbankan yang khusus dirancang untuk perangkat *mobile* atau melalui akses web *mobile*, pelanggan dapat melakukan berbagai aktivitas perbankan seperti cek saldo, transfer dana, pembayaran tagihan, pembelian produk atau layanan, mengelola investasi, dan banyak lagi langsung dari perangkat *mobile* mereka (Simatupang, 2021).



Gambar 2. Kejahatan yang sering muncul pada *mobile banking*
Sumber: BSSN, 2020 (data diolah)

Mobile banking menjadi semakin populer karena kemudahan dan kenyamanannya. Dalam era digital saat ini, banyak orang memiliki akses ke perangkat *mobile* yang terhubung dengan internet, sehingga mereka dapat mengelola keuangan mereka dengan mudah tanpa harus pergi ke bank fisik atau menggunakan komputer (Laksana, Astuti, & Dewantara, 2015). Akan tetapi adanya *mobile banking* ini tentunya memeliki risiko tindak kejahatan pada *mobile banking* seperti pencurian data, penyalahgunaan hak guna akses, serangan *phishing* pada nasabah, serangan *malware*, kesalahan pengelolaan aplikasi pada *mobile banking*. Gambar 2 menunjukkan ancaman siber yang sering terjadi pada *mobile banking.*

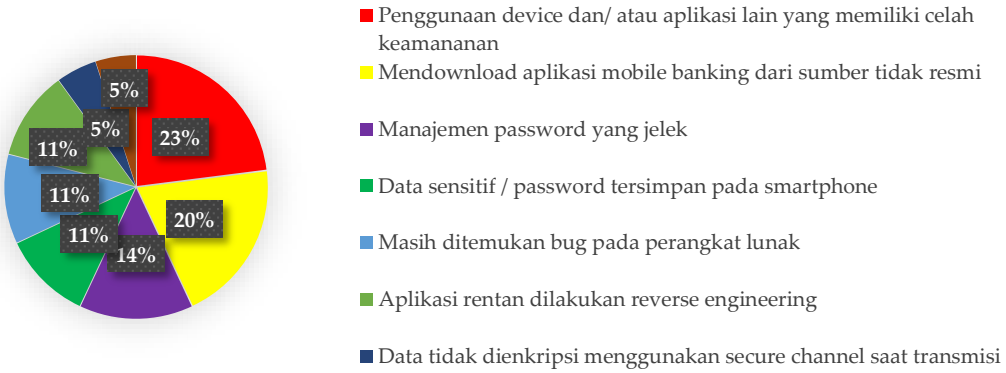
Pada Gambar 2, ada 6 (enam) ancaman siber yang sering terjadi pada *mobile banking* selama tahun 2020 antara lain pencurian data sebesar 32%, kemudian penyalahgunanan hak akses sebesar 24%, serangan *phishing* sebesar 19%, serangan *malware* sebesar 15%, kesalahan pengelolaan aplikasi sebesar 9%, dan yang paling terkecil adalah *hijack simcard* sebesar 1%. Pencurian data merupakan ancaman terbesar yang ditemukan pada *mobile banking* selama tahun 2020. Pencurian data menjadi ancaman terbesar pada *mobile banking* karena informasi penting seperti nomor rekening, *password*, dan nomor kartu kredit dapat diambil oleh pihak yang tidak berwenang melalui serangan keamanan pada aplikasi *mobile banking*. Pihak yang melakukan pencurian data dapat mengakses rekening pengguna, melakukan transaksi yang tidak diizinkan, atau bahkan mencuri uang secara langsung. Oleh karena itu, keamanan pada aplikasi *mobile banking* sangat penting untuk mencegah terjadinya pencurian data.

3.1 Ancaman Siber pada Mobile Banking

Mobile banking memiliki risiko terkait ancaman siber yang perlu diwaspadai. Berikut adalah beberapa ancaman siber pada *mobile banking.*

a. Kerentanan terbesar pada *mobile banking* terhadap pencurian data

Pencurian data pada *mobile banking* merujuk pada aksi mencuri atau mendapatkan akses tidak sah terhadap informasi sensitif pengguna yang terkait dengan layanan perbankan melalui perangkat *mobile.* Data yang dapat dicuri meliputi informasi login, nomor rekening, kata sandi, nomor kartu kredit, dan data keuangan pribadi lainnya. Pencurian data pada *mobile banking* dapat terjadi melalui berbagai metode, seperti serangan malware, serangan *phishing*, pencurian perangkat, atau eksploitasi kerentanan pada aplikasi *mobile banking*. Penyerang yang berhasil mencuri data pribadi pengguna dapat menyalahgunakannya untuk melakukan penipuan, transfer dana ilegal, atau mengakses informasi sensitif lainnya (Rumlus & Hartadi, 2020).



Gambar 3. Pencurian data pada *mobile banking*
Sumber: BSSN, 2020 (data diolah)

Pencurian data merupakan ancaman terbesar yang ditemukan pada *mobile banking* selama tahun 2020. Hal ini menggambarkan bahwa tidak hanya finansial yang menjadi sasaran utama hacker melainkan data nasabah juga menjadi target utama. Namun apabila terjadi pencurian data maka ancaman siber lainnya bisa saja terjadi dari dampak pencurian data yang ditimbulkan, misalnya terjadinya penyalahgunaan hak akses pada *mobile banking*, penipuan, dan lain-lain. Bisa dilihat pada Gambar 3 kerentanan terbesar pada *mobile banking* terhadap pencurian data.

Pencurian data merupakan ancaman siber terbesar pada *mobile banking* selama tahun 2020. Dari hasil penelitian diketahui ada 8 (delapan) kerentanan terbesar yang relevan terhadap ancaman pencurian data pada mobile banking antara lain disebabkan oleh penggunaan *device* dan/atau aplikasi lain yang memiliki celah keamanan dengan persentase sebesar 23%, unduh aplikasi *mobile banking* dari sumber yang tidak resmi sebesar 20%, manajemen kata sandi yang buruk sebesar 14%, data sensitif/*password* tersimpan pada *smartphone* nasabah, masih ditemukan bug pada perangkat lunak, dan aplikasi rentan dilakukan *reverse engineering* masing-masing sebesar 11%, data tidak dienkripsi menggunakan *secure channel* saat transmisi serta *hard coded secret key* pada penggunaan algoritma kriptografi tersimpan di aplikasi masing-masing sebesar 5%.

Selain peran dari industri perbankan, nasabah mempunyai peran besar untuk meminimalisir kerentanan-kerentanan tersebut. Pilih aplikasi resmi pastikan untuk mengunduh aplikasi *mobile banking* resmi dari penyedia layanan keuangan yang sah. Gunakan sumber yang terpercaya seperti toko aplikasi resmi seperti *google play store* atau *apple app store*. Jaga kerahasiaan informasi pribadi jangan pernah memberikan informasi pribadi atau rincian akun anda kepada pihak yang tidak tepercaya. Pastikan untuk tidak membagikan informasi seperti *username, password*, atau nomor PIN dengan siapapun, termasuk melalui pesan teks, *email*, atau telepon, juga menjadi peluang bagi para hacker untuk melakukan pencurian data dengan mudah. serta ketidaktahuan nasabah atau hindari akses melalui *Wifi* publik jangan menggunakan jaringan *Wifi* publik saat mengakses *mobile banking*. Lebih baik menggunakan jaringan data seluler atau jaringan *Wifi* pribadi yang lebih aman.

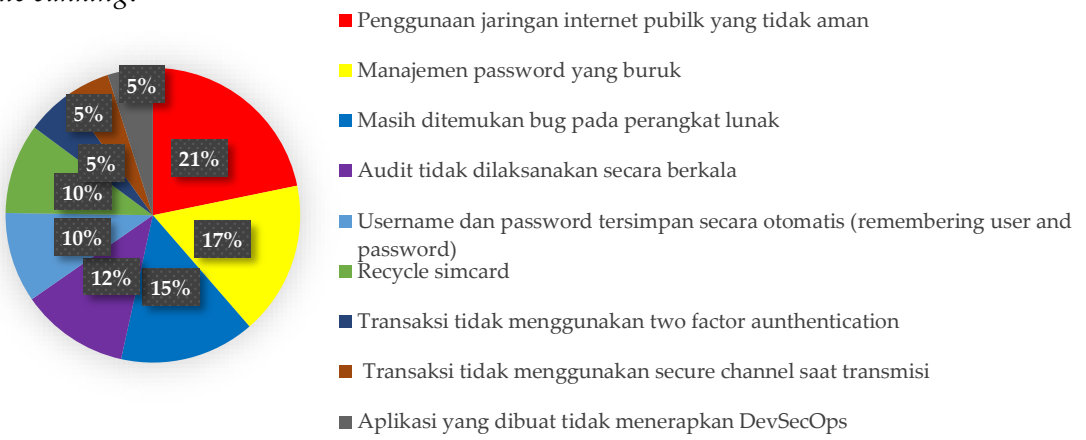
b. Penyalahgunaan hak guna akses pada *mobile banking*

Ancaman keamanan pada *mobile banking* kedua adalah penyalahgunaan hak akses. Penyalahgunaan hak akses terjadi ketika seseorang yang tidak berwenang memperoleh atau menggunakan hak akses yang seharusnya hanya dimiliki oleh nasabah atau pihak yang sah. Ini dapat terjadi melalui berbagai metode, termasuk serangan *malware*, aplikasi berbahaya, atau penyerangan terhadap jaringan perbankan. Penting bagi nasabah dan penyedia layanan perbankan untuk tetap waspada terhadap ancaman penyalahgunaan hak akses. Menjaga perangkat *mobile* yang digunakan, mengunduh aplikasi resmi dari sumber yang tepercaya, dan mengaktifkan fitur keamanan seperti otentikasi ganda dapat membantu meminimalisir risiko penyalahgunaan hak akses pada *mobile banking* (Situmeang 2021). Gambar 4 menunjukkan penyalahgunaan hak guna akses pada *mobile banking.*

Penyalahgunaan hak akses merupakan ancaman siber terbesar kedua setelah pencurian data yang ditemukan pada *mobile banking* selama tahun 2020. Dari hasil penelitian diketahui terdapat 9 (sembilan) kerentanan yang relevan terhadap ancaman penyalahgunaan hak akses pada *mobile banking* yang disebabkan oleh penggunaan jaringan internet publik yang tidak aman dengan persentase sebesar 22%, manajemen *password* yang buruk sebesar 17%, masih ditemukan bug pada perangkat lunak sebesar

14%, audit tidak dilaksanakan secara berkala sebesar 12%, *username* dan *password* tersimpan secara otomatis (*remembering user and password*) serta *recycle simcard* masing-masing sebesar 10%, aplikasi yang dibuat tidak menerapkan *DevSecOps* dan transaksi tidak menggunakan *secure channel* saat transmisi, serta transaksi tidak menggunakan *two factor authentication* masing-masing sebesar 5%.

Nasabah dan pihak internal perbankan sama-sama mempunyai peranan besar untuk meminimalisir kerentanan-kerentanan tersebut. Kurangnya *security awareness* nasabah sehingga menggunakan jaringan internet publik yang tidak aman, menggunakan sandi yang kuat, gunakan sandi yang kuat dan unik untuk akun *mobile banking*. Kombinasikan huruf besar dan kecil, angka, dan simbol untuk meningkatkan keamanan sandi. Hindari menggunakan sandi yang mudah ditebak, seperti tanggal lahir atau nama lengkap. Ketika menggunakan *password* yang lemah otomatis hacker bisa melakukan penyalahgunaan hak akses. Begitu pula dengan kerentanan-kerentanan yang ditemukan di aplikasi seperti tidak diterapkannya *two factor authentication* juga menjadi peluang hacker dalam menyalahgunakan hak akses. Dengan begitu aktifkan fitur otentikasi dua faktor (2FA), aktifkan fitur otentikasi dua faktor yang disediakan oleh aplikasi *mobile banking*. Fitur ini akan menambahkan lapisan keamanan tambahan dengan memerlukan kode verifikasi yang dikirimkan melalui SMS, *email*, atau aplikasi *mobile banking*.



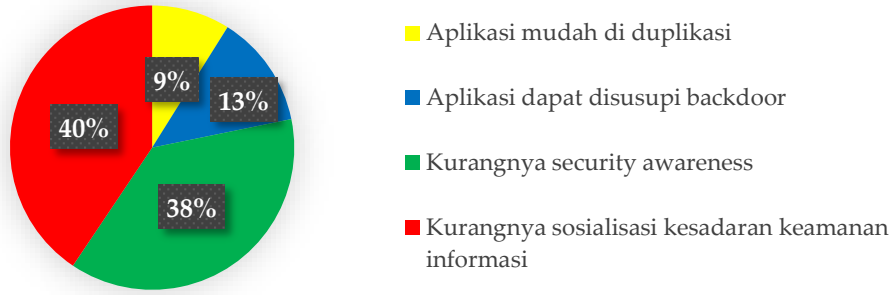
Gambar 4. Penyalahgunaan hak guna akses pada *mobile banking*
Sumber: BSSN, 2020 (data diolah)

c. Kerentanan terbesar pada *mobile banking* terhadap serangan *phishing* nasabah

Ancaman keamanan pada *mobile banking* ketiga adalah kerentanan terbesar pada *mobile banking* terhadap serangan *phishing* nasabah adalah salah satu metode penipuan di mana penyerang mencoba untuk mendapatkan informasi sensitif pengguna melalui pesan teks, *email* palsu, atau situs web palsu yang meniru tampilan aplikasi *mobile banking* yang sah. Tujuan utama penyerang dalam serangan *phishing* adalah untuk mencuri akses *login*, nomor kartu kredit, nomor rekening bank, atau informasi pribadi lainnya yang dapat mereka gunakan untuk melakukan penipuan atau pencurian identitas (Radiansyah et al., 2016). Gambar 5 menunjukkan kerentanan terbesar pada *mobile banking* terhadap serangan *phishing* nasabah.

Nasabah merupakan ancaman siber terbesar ketiga setelah pencurian data dan penyalahgunaan hak akses, yang ditemukan pada *mobile banking* selama tahun 2020. Dari data diketahui terdapat 4 (empat) kerentanan yang relevan terhadap ancaman serangan *phishing* nasabah pada *mobile banking* yaitu kurangnya sosialisasi kesadaran

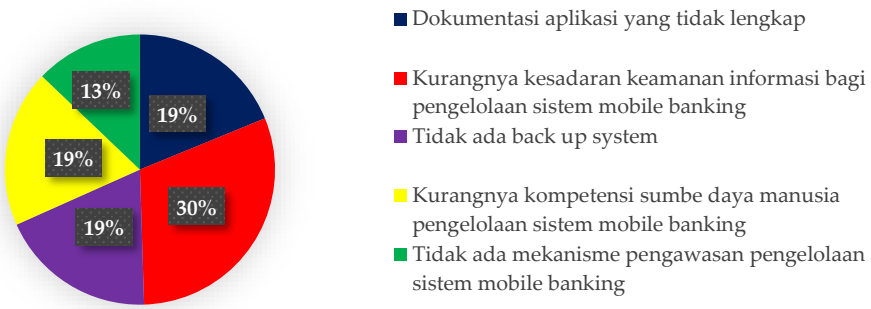
keamanan informasi dengan persentase sebesar 40%, kurangnya *security awareness* sebesar 38%, aplikasi dapat disusupi *backdoor* sebesar 13%, dan aplikasi mudah diduplikasi sebesar 9%. Untuk meminimalisir risiko yang disebabkan kerentanan-kerentanan tersebut dibutuhkan peranan dari pihak internal untuk memastikan keamanan aplikasi agar tidak mudah disusupi oleh *backdoor* dan tidak mudah diduplikasi, serta dibutuhkan peranan nasabah untuk meningkatan *security awareness.* Kurangnya *security awareness* nasabah yang menyebabkan terjadinya *phishing* juga dapat memiliki dampak di ancaman lainnya, diantaranya pencurian data, penyalahgunaan hak akses, dan sebagainya.



Gambar 5. Serangan *phishing* pada nasabah
Sumber: BSSN, 2020 (data diolah)

Nasabah memiliki peran penting untuk meminimalisir terhadap kejahatan phishing ini seperti, jangan menanggapi pesan teks, *email*, atau panggilan telepon yang meminta pengguna memberikan informasi pribadi atau rahasia keuangan. Bank atau lembaga keuangan yang sah tidak akan meminta informasi tersebut melalui komunikasi yang tidak diminta, gunakan aplikasi resmi dari sumber yang terpercaya pastikan penggguna mengunduh aplikasi *mobile banking* resmi dari toko aplikasi yang sah, seperti *google play store* atau *apple app store*. Hindari mengunduh aplikasi dari sumber yang tidak terpercaya., selalu perbarui perangkat lunak dan aplikasi perbankan *mobile* ke versi terbaru (Muftiad et al., 2022).

d. Kerentanan terbesar pada *mobile banking* terhadap kesalahan pengelolaan



Gambar 6. Kerentanan *mobile banking* terhadap kesalahan pengelolaan
Sumber: BSSN, 2020 (data diolah)

Ancaman keamanan pada *mobile banking* keempat adalah kerentanan terbesar pada *mobile banking* terhadap kesalahan pengelolaan dapat mencakup berbagai aspek, termasuk kebijakan keamanan yang lemah, kekurangan perlindungan data, kurangnya pembaruan perangkat lunak, atau pelanggaran privasi, pengelola *mobile banking* yang tidak memiliki kebijakan keamanan yang kuat dan terkini dapat meningkatkan risiko

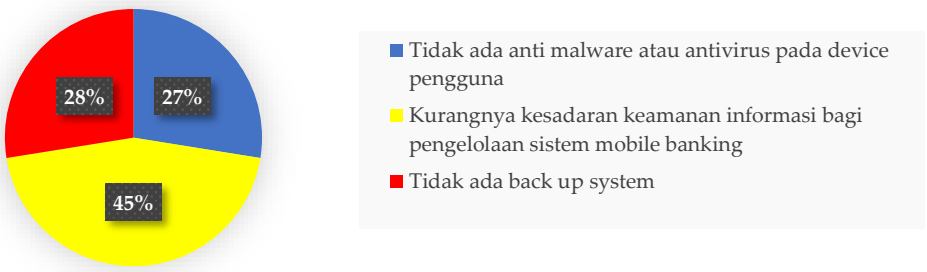
serangan dan pencurian data. Ini dapat mencakup kebijakan lemah terkait penggunaan kata sandi, autentikasi dua faktor, enkripsi data, dan manajemen akses (BSSN 2020). Bisa dilihat pada Gambar 6 kerentanan terbesar pada *mobile banking* terhadap kesalahan pengelolaan.

Pengelolaan kesalahan *mobile banking* mejadi ancaman keempat terbesar. Hasil data diketahui terdapat 5 (lima) kerentanan yang relevan terhadap ancaman kesalahan pengelolaan pada *mobile banking*. Kurangnya kesadaran keamanan informasi memang menjadi isu kerentanan yang paling sering ditemukan termasuk terhadap ancaman kesalahan pengelolaan *mobile banking*. Dari data tahun 2020 kurangnya kesadaran keamanan informasi bagi pengelola sistem *mobile banking* memiliki persentase paling besar yaitu 30%. Kemudian diikuti dengan kerentanan akan kurangnya kompetensi sumber daya manusia pengelola sistem, tidak ada *back up* sistem, dan dokumentasi yang tidak lengkap dengan persentasi masing masing sebesar 19%. Serta tidak ada mekanisme pengawasan pengelolaan sistem *mobile banking* sebesar 13%. Pihak internal perbankan memiliki peranan besar untuk meminimalisir kerentanan-kerentanan tersebut terhadap ancaman kesalahan pengelolaan *mobile banking*. Pihak perbankan perlu melakukan langkah antisipasi dengan melakukan dokumentasi aplikasi secara lengkap, menerapkan mekanisme pengawasan pengelolaan sistem, menyediakan *back up* sistem, meningkatkan kompetensi dan kesadaran keamanan informasi bagi pengelola sistem *mobile banking.*

Pihak perbankan memeliki peran dalam meminimalisir dalam menangani kerentanan kesalahan pengelolaan, seperti, pengelola *mobile banking* harus memiliki kebijakan keamanan yang kuat dan terkini. Ini termasuk kebijakan yang mengatur penggunaan kata sandi yang kuat, autentikasi dua faktor, enkripsi data, manajemen akses yang tepat, dan pemantauan keamanan secara proaktif. data pengguna harus dilindungi secara efektif menggunakan enkripsi yang memadai. Pengelola mobile banking juga harus memiliki kebijakan untuk mengelola dan menyimpan data dengan aman serta mengatur akses ke data tersebut.

e. Kerentanan terbesar pada *mobile banking* terhadap *malware*

Ancaman keamanan pada *mobile banking* kelima adalah kerentanan terbesar pada *mobile banking* terhadap *malware*, *malware* singkatan dari *malicious software* adalah perangkat lunak yang dirancang untuk merusak, mengganggu, atau mencuri informasi dari sistem komputer atau perangkat lainnya tanpa persetujuan pengguna. *Malware* dapat beragam bentuk dan tujuannya, termasuk mencuri data sensitif, mengendalikan perangkat, merusak sistem, atau menyebarkan diri ke perangkat lain (Faridi, 2018). Gambar 7 menunjukkan kerentanan terbesar pada *mobile banking* terhadap *malware.*



Gambar 7. Kerentanan *mobile banking* terhadap *malware*
Sumber: BSSN, 2020 (data diolah)

Dari Gambar 7 diketahui terdapat 3 (tiga) kerentanan yang relevan terhadap ancaman serangan malware pada mobile banking. Tidak ada anti *malware* atau antivirus pada *device* pengguna menjadi isu kerentanan paling tinggi dengan persentase sebesar 50%. Hal ini tentunya karena pihak perbankan tidak dapat mengontrol secara penuh *device* yang digunakan oleh pengguna sehingga dibutuhkan kesadaran dari nasabah itu sendiri. Selanjutnya kurangnya *security awareness* juga menjadi isu pada ancaman serangan *malware* dengan persentase sebesar 31%. Hacker biasanya memanfaatkan kelemahan, ketidaktahuan, dan ketidaksadaran nasabah terkait keamanan informasi untuk melakukan serangan *malware*. Kerentanan yang terakhir adalah sistem tidak update dengan persentase sebesar 19%. Kerentanan ini juga memiliki potensi dan peluang untuk hacker melakukan serangan *malware*.

Selain peran dari industri perbankan, nasabah mempunyai peran besar untuk meminimalisir kerentanan-kerentanan tersebut pastikan sistem operasi perangkat *mobile* dan aplikasi *mobile banking* pengguna selalu diperbarui dengan versi terbaru. Pembaruan ini seringkali memperbaiki kerentanan keamanan yang dapat dimanfaatkan oleh *malware, h*indari mengklik tautan atau membuka lampiran yang mencurigakan dalam email, pesan teks, atau pesan media sosial yang terkait dengan *mobile banking*. Tautan atau lampiran tersebut dapat mengarahkan pengguna ke situs web yang berbahaya atau mengunduh *malware* ke perangkat pengguna.

3.2 Pencegahan Siber pada Mobile Banking

Untuk mencegah ancaman siber pada *mobile banking*, berikut adalah beberapa langkah pencegahan yang dapat dilakukan oleh pihak perbankan maupun nasabah:

a. Aspek keamanan sisi penyedia layanan (perbankan)

Pihak perbankan pertama menerapkan *two factor aunthencation* ini sangat dibutuhkan untuk memastikan bahwa transaksi keuangan yang berjalan dilakukan oleh nasabah/pengguna yang sah. Pemindaian sidik jari dapat dijadikan sebagai metode verifikasi tambahan pada aplikasi perbankan. Aplikasi juga mengharuskan ponsel dilindungi oleh kata sandi (*password*), jika ingin menggunakan pemindaian sidik jari. Kedua *ssl secured website* pihak perbankan menggunakan situs website atau aplikasi perbankan yang menjadi tempat terjadinya transaksi keuangan harus memiliki jalur komunikasi yang aman sehingga informasi yang diteruskan antara server bank dan browser nasabah tetap terjaga keamanannya. Ketiga *automatic timeout sessions* pihak perbankan harus menutup kegiatan transaksi nasabah yang tidak aktif dalam beberapa menit untuk menghindari timbulnya kejahatan siber (PBI 2020).

b. Aspek keamanan sisi penyedia layanan (nasabah)

Nasabah mempunyai peran penting dalam mengurangi ancaman siber pada *mobile banking* seperti, mengunduh aplikasi resmi dari bank nasabah diharuskan mengunduh aplikasi *mobile banking* disitus atau layanan yang resmi seperti dari *google play store.* Jangan mengunduh aplikasi dari *website* ataupun jejaring sosial lainnya bisa saja itu terdapat kejahatan siber. Kedua waspada penggunaan fasilitas dan jaringan publik saat menggunakan layanan *mobile banking* nasabah jangan menggunakan perangkat komputer yang bukan miliknya begitu juga menggunakan jaringan internet berupa *wifi* publik. Hal ini agar menghindari adanya penyadapan atau perekaman terhadap akun pengguna *mobile bankking.* Penggunaan *antivirus* pada perangkat pengguna dapat mencegah terjadinya ancaman siber pada *mobile banking* selain itu, update terhadap

penggunaan sistem operasi terbaru pada perangkat nasabah juga turut meningkatkan aspek keamanan pada perangkat pengguna layanan *mobile banking* (PBI, 2020).

4. Kesimpulan

Berdasarkan hasil dan pembahasan di atas, kemajuan teknologi digital bagi dunia perbankan sangat berpengaruh. Namun, kemajuan teknologi digital tersebut masih rentan terhadap ancaman kejahatan siber pada *mobile banking* seperti kerentanan terbesar pada *mobile banking* terhadap pencurian data, penyalahgunaan hak guna akses pada *mobile banking*, kerentanan terbesar pada *mobile banking* terhadap serangan *phishing* nasabah, kerentanan terbesar pada *mobile banking* terhadap kesalahan pengelolaan, dan kerentanan terbesar pada *mobile banking* terhadap *malware.* Pencurian data menjadi ancaman terbesar pada *mobile banking* karena terdapat informasi keuangan dan data pribadi yang menjadi sasaran utama penebar siber. Dan untuk keempat kejahatan siber lainnya itu bisa terjadi karena kurangnya *security awareness*, mengunduh aplikasi bukan disitus resmi perbankan, ketika melakukan kegiatan transaksi pada *mobile banking* pastikan menggunakan data internet atau *wifi* pribadi jangan menggunakan *wifi* publik, karena ketika mengakses menggunakan *wifi* umum itu bisa timbul terjadinya kejahatan siber ini.

Ada beberapa upaya yang dapat dilakukan oleh pihak perbankan maupun nasabah di pihak perbankan dengan menerapkan *two factor aunthencation*, *ssl secured website,* dan *automatic timeout sessions* Nasabah juga memeliki peranan penting dalam mengurangi kejahatan *mobile banking* ini seperti, Nasabah diharuskan mengunduh aplikasi *mobile banking* disitus atau layanan yang resmi seperti dari *google play store* atau *apple app store*, hindari menggunakan jaringan publik atau *wifi* ketika melakukan transaksi menggunakan layanan *mobile banking.*

Referensi

Badan siber dan sandi negara (2020), Profil risiko sektor perbankan, 2020

https://sikapiuangmu.ojk.go.id/FrontEnd/CMS/Article/185 diakses pada 10 mei 2023

https://sikapiuangmu.ojk.go.id/FrontEnd/CMS/Article/346 diakses pada 11 mei 2023

Laksana, G. B., Astuti, E. S., & Dewantara, R. Y. (2015). Pengaruh Persepsi Kemanfaatan, Persepsi Kemudahan Penggunaan, Persepsi Resiko Dan Persepsi Kesesuaian Terhadap Minat Menggunakan Mobile Banking (Studi Pada Nasabah Bank Rakyat Indonesia (BRI) Kantor Cabang Rembang,Jawa Tengah). *Administrasi Bisnis (JAB)*, 1-8.

Muftiadi, A., Agustina, T. P., & Evi, M. (2022). Studi kasus keamanan jaringan komputer: analisis ancaman phising terhadap layanan online banking. *Jurnal Ilmiah Teknik*, 60 - 65.

Peraturan Bank Indonesia No. 22/20/PBI/2020 tentang Perlindungan Konsumen Bank Indonesia;

Peraturan Otoritas jasa keuangan Nomor 12 Tahun 2018 Tentang Penyelenggaran Layanan Perbankan Digital Oleh Bank Umum

Radiansyah, I., Candiwan, & Priyadi, Y. (2016). Analisis Ancaman Phishing Dalam Layanan Online Banking. *Ekonomika-Bisnis*, 1-14.

Rumlus, M. H., & Hartadi, H. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik (Policy the Discontinuation of Personal Data Storage in Electronic Media). *JURNAL HAM*, 285 - 299. vol 11 no 2

Simatupang, B. M. (2021). *Perbankan Digital : Menuju Bank 4.0.* Jakarta: PT Gramedia Pustaka Utama.

Situmeang, S. M. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. *S A S I*, 38 - 52.

Wardhana, Aditya. 2015. "Kualitas Layanan Mobile Banking (M-Banking) Terhadap Kepuasan Nasabah Di Indonesia". *Jurnal Ekonomi*, Vol. 10 No. 2

Widayanti, W. P. (2022). Tindak Pidana Pencurian Data Nasabah Dalam Bidang Perbankan Sebagai Cyber Crime. *Jurnal Hukum dan Perundang-undangan*, Vol 2 No 2, 1-21.

Zed, M. 2004. *Metodologi Penelitian Kepustakaan.* Jakarta: Yayasan Obor Indonesia.