BAB III

HAMBATAN-HAMBATAN DAN BENTUK CRIME DALAM ELEKTRONIK BANKING

A. Bentuk Hambatan

Elektronik banking dalam perbankan mencakup wilayah yang luas dari teknologi yang berkembang pesat akhir-akhir ini. Elektronik banking merupakan salah satu sector yang terpengaruh oleh perkembangan teknologi informasi dan komunikasi dalam perbankan, penggunaan teknologi informasi dan komunikasi di sektor perbankan nasional relative lebih maju dibandingkan sektor lainnya.

Selain melihat pekembangan dan kemajuan dari perbankan dengan pemanfaatan teknologi, hadirnya elektronik banking menjadi salah satu gambaran dari tehnologi. Melihat perkembangan dari perbankan nasional, bank juga mengedepankan keyamanan dari nasabahnya. Beberapa fitur-fitur yang di desain secara ringkas dalam pelaksanaannya, bank juga memperhatikan kemudahan nasabah dalam mengakses web atau aplikasi dari bank masing-masing yang di gunakan oleh nasabahnya.

Bank telah mendesain sedemikian rupa dari elektronik banking untuk memudahkan dalam penggunaaanya tetapi dalam kemudahan tersebut terdapat pula beberapa hambatan-hambatan dalam penggunaan dari elektronik banking tersebut. Adapaun hambatan-hambatan dalam penggunaan elektronik banking sebagai berikut:[1]

1. Transaksi E-banking bukan hanya mempermudah tetapi dapat menimbulkan resiko seperti strategi operasional dan reputasi serta adanya berbagai macam ancaman terhadap aliran data *realible* dan ancaman kerusakan/kegagalan

[1] Dosen pendidikan, elektronik banking,"situs resmi dosen pendidikan. https://www.dosenpendidikan.co.id/e-banking/ (diakses 30 november 2020).

terhadap sistem Elektronik Banking kemudian semakin kompleksnya teknologi yang menjadi dasar E-Banking.

2. Kerusakan/kerugian/kehilangan yang diderita baik dari bank maupun dari nasabah diakibatkan juga oleh putugas internal atau manajemen bank.
3. E-banking menjadi salah satu target dari para cybercrime yang memiliki kendala dalam hal pembuktian baik secara teknis maupun non-teknis.
4. Pemerintah maupun manajemen yang bertanggung jawab terhadap kendala-kendala yang di hadapi sampai saat ini masih terkesan sangat lambat dalam melakukan antisipasi terhadap maraknya kejahatan yang terjadi melalui E-banking.
5. Kegiatan E-Banking masih belum memiliki payung hukum yang akurat dan tegas yang disebabkan oleh RUU informasi dan transaksi elektronik.
6. Para pelaku usaha perbankan dan masyarakat pada umumnya masih kurang peduli terhadap proses penangan kasus-kasus tindak pidana E-banking.

Meskipun terdapat landasan hukum sebagai penanganan dari hambatan tersebut, masih membutuhkan perhatian dari sistem informasi dari perbankan nasional dalam penanganannya. Bukan hanya hambatan yang ada di atas hambatan secara fisik ialah kemampuan nasabah tentang penggunaan teknologi dikarenakan kurangnya ilmu pengetahuan masyarakat tentang fasilitas e-banking sehingga masih banyak yang tidak mengerti dalam penggunaan teknologi (gaptek) yang menyebabkan para nasabah masih saja memilih transaksi dengan datang ke kantor.

B. Crime (kejahatan) dalam elektronik banking

Electronic banking menawarkan berbagai kemudahan bagi nasabah, namun di sisi lain memiliki resiko yang harus diwaspadai. Berikut ini adalah beberapa contoh

penyalahgunaan e-banking pada industry perbankan di Indonesia, termaksu diluar negri yang Sering terjadi melalui media (*delivery channel*) ATM, EDC, internet banking, sms banking, mobile Banking, e-commerce, phone banking dan video banking yang dilakukan oleh pihak eksternal, internal bank maupun kerjasama pihak eksternal dan internal bank, sebagai berikut:

1. ATM (Automated teller machine)

a. *Card Skimming* adalah tinfakan pencurian data kartu ATM dengan cara menyalin (membaca dan menyimpan) informasi yang terdapat pada strip magnetis secara illegal. Strip megnetis adalah garis lebar hitam yang berada dibagian belakang kartu ATM. Fungsinya pita kaset untuk menyimpan data nomor kartu, masa berlaku kartu dana nama nasabah. *Card skimming* dilakukan menggunakan alat pembaca kartu yang ditempatkan slot kartu di mesin ATM.[2]

Hal-hal yang dapat dilakukan untuk meminimalisir bahaya *card skimming*, antara lain:

1) Memperhatikan kondisi mesin ATM sebelum digunakan. *Card skimmer* seringkali tidak terlihat secara kasat mata karena warna dan bentuknya telah disesuaikan dengan mesin ATM,
2) Hati-hati sebelum menekan tombol PIN. Usahakan agar tombol yang di tekan tidak terlihat oleh orang lain. Nasabah juga perlu mencermati adanya kamera yang dapat merekam tombol PIN yang ditekan oleh nasabah,

[2] Otoritas Jasa Keuangan, *Bijak Ber-Eletronic Banking*, h. 43.

3) Hindari menggunakan PIN yang mudah di tebak oleh orang lain, seperti tanggal lahir, nomor telepon, dan nomor kartu,
4) Menggangi nomor PIN secara periodic, terutama jika ada indikasi bahwa PIN telah di ketahui oleh orang lain.

b. Call senter palsu

Bank memiliki call center untuk melayani nasabah, seperti permintaan informasi, laporan keluhan, dan blokir kartu ATM. Nomor telepon call center dapat diketahui melalui website resmi, spanduk, poster, kartu ATM, dan sticker pada mesin ATM. Layanan call center dapat disalahgunakan oleh pelaku kejahatan dengan membuat call center palsu untuk mendapatkan data rahasia nasabah (misalnya PIN) atau memandu nasabah bertransaksi (misalnya transfer atau beli pulsa) di mesin ATM untuk keuntungan pelaku.

Dalam menjalankan call center palsu, pelaku berusaha mengarahkan nasabah agar menghubungi nomor telepon call center palsu dengan beberapa cara, antara lain:

1) Memasang sticker yang berisi nomor call center palsu pada mesin ATM atau ruang ATM. Nomor call center palsu tersebut adalah nomor telepon milik pelaku.
2) Jika ada nasabah yang menghubungi nomor tersebut, pelaku meminta nasabah untuk menyebutkan data rahasia nasabah, seperti seperti PIN, nomor kartu kredit, masa berlaku kartu kredit, dan kode pengaman kartu kredit atau Card VerificationValue (CVV). Dan melakukan transaksi di ATM, seperti transfer, pembelian, atau pembayaran yang menguntungkan pelaku tanpa disadari oleh nasabah.

3) Memanfaatkan data rahasia nasabah untuk mengakses dan bertransaksi menggunakan rekening nasabah. Modus ini biasanya dikombinasikan dengan teknik lain, seperti card trapping dan belanja on-line.

Hal-hal yang dapat dilakukan untuk meminimalisir call center palsu, antara lain: 1) Mencermati nomor call center yang tertera pada sticker di mesin atau ruang ATM. Call center resmi biasanya menggunakan nomor khusus yang relatif mudah untuk diingat dan tertera pada bagian belakang kartu ATM nasabah;

2) Mencatat nomor telepon call center pada media lain, misalnya di ponsel atau catatan lainnya sehingga nasabah dapat menghubungi call center bank pada saat dibutuhkan

3) Tidak menginformasikan nomor PIN. Nasabah harus selalu merahasiakan nomor PIN, tidak memberitahukan kepada orang lain termasuk kerabat dekat dan pegawai bank atau call center.[3]

Card skimming dan call senter palsu merupakan bentuk tindak kejahatan yang gunakan oleh pelaku, bukan hanya *card skimming* dan call senter palsu tetapi *card trapping*, pencurian data pribadi dan meminjamkan kartu kepada orang lain serta *social engineering* menjadi tindak kenjahatan dalam elektroik banking khususnya dalam transaksi ATM.

2. EDC (Electronic Data Capture)

EDC merupakan suatu perangkat terminal yang dapat digunakan untuk bertransaksi menggunakan kartu debit/kredit/prabayar di *merchant*. Terminal tersebut

[3] Otoritas Jasa Keuangan, *Bijak Ber-Eletronic Banking*, h. 47.

terhubung ke jaringan computer bank. Adapun bentuk *crime*(kejahatan) dalam EDC yaitu:

a. *Card intercept*

Seperti halnya pada ATM, card intercept juga bisa terjadi pada EDC. Card intercept di EDC meliputi kartu debit dan kartu kredit. Card intercept pada saat bertransaksi di mesin EDC biasanya menimpa kartu ATM instan (tanpa nama) dimana kartu nasabah yang asli ditukar dengan kartu lain oleh petugas kasir tanpa disadari oleh nasabah.[4]

Adapun yang dapat dilakukan untuk meminimalisir bahaya card intercept, Jangan serahkan kartu kepada pelayan tanpa diawasi, Sebaiknya nasabah datang langsung ke meja kasir dan memastikan kartu yang digunakan untuk bertransaksi aman dan tidak tertukar/ditukar dan Pastikan kartu yang dikembalikan oleh kasir setelah transaksi.

b. Gesek Tunai

Gesek tunai atau sering disebut dengan "gestun", adalah transaksi yang dilakukan nasabah menggunakan kartu kerdit pada merchant tertentu dengan seolah-olah melakukan transaksi pembelian dengan merchant tersebut, namun nasabah tidak menerima barang atau jasa melainkan memperoleh uang tunai dari merchant dengan fee tertentu yang dibebankan oleh merchant kepada nasabah.

Adanya merchant seperti ini akan dijadikan pelaku kejahatan carding (pemalsu kartu) untuk melakukan transaksi kartu hasil kejahatannya, karena autentikasi transaksi gestun ini cukup dengan tanda tangan tanpa perlu PIN nasabah. Yang dapat dilakukan untuk meminimalisir bahaya gesek tunai, yaitu nasabah harus

[4] Otoritas Jasa Keuangan, *Bijak Ber-Eletronic Banking*, h. 55.

memahami bahwa gesek tunai bukan merupakan produk bank, sehingga segala bentuk kerugian atas transaksi ini bukan merupakan tanggung jawab bank. Nasabah dianjurkan untuk tidak melakukan transaksi gesek tunai menggunakan kartu kredit.

Card intercept dan gesek tunai dapat menjadi bentuk kejahatan dari pihak lain, bukan hanya dari keduanya tetapi *card skimming*, *Card Reader Ilegal*, penukaran kartu serta kartu hilang menjadi bentuk kejahatan lainnya. Hal ini perlu di perketat dari segi keamanan dari perbankan nasional demi menjaga kenyamanan dan kepercayaan nasabah.

3. Internet Banking

Internet Banking termaksud saluran yang memungkinkan nasabah melakukan transaksi via internet dengan menggunakan komputer/PC.

a. Phising

Phishing adalah tindakan meminta (memancing) pengguna komputer untuk mengungkapkan informasi rahasia dengan cara mengirimkan pesan penting palsu, dapat berupa e-mail, website, atau komunikasi elektronik lainnya. Pesan palsu tersebut tampak seperti sungguhan dan meminta korban untuk segera mengirimkan informasi tertentu, biasanya diikuti dengan ancaman jika tidak mengirimkan informasi tersebut maka akan mengalami konsekuensi buruk.

Dalam melakukan phishing, pelaku biasanya melakukan hal-hal antara lain:

1) Mengirimkan pesan melalui e-mail, SMS, halaman web, atau media komunikasi elektronik lainnya kepada calon korban yang menjadi targetnya.

2) Meminta informasi personal yang sensitif, seperti user ID, password/PIN, nomor kartu kredit, masa berlaku kartu kredit, dan CVV.

3) Memberikan batasan waktu yang singkat (urgent). Penjahat mengarahkan korban melakukan tindakan sebelum memikirkannya secara mendalam, sehingga mereka menciptakan suasana kegentingan dan menginformasikan konsekuensi buruk jika tidak ditindaklanjuti.[5]

Namun demikian, sangat dimungkinkan bahwa pesan phishing menggunakan gaya bahasa yang baik untuk membuat nasabah merasa lebih yakin dan percaya bahwa pesan tersebut seolah-oleh merupakan pesan resmi dari bank.

Hal-hal yang dapat dilakukan untuk meminimalisir bahaya phishing, antara lain:

1) Jangan pernah mengirimkan informasi sensitif melalui e-mail. Perlu diketahui bahwa suatu perusahaan tidak akan meminta informasi sensitif melalui e-mail atau sarana elektronis lainnya yang tidak aman.

2) Menggunakan anti virus yang terkini.

3) Jangan mengklik link apapun pada pesan (e-mail) yang terindikasi phishing.

4) Mengkonfirmasikan kepada pihak bank melalui call center yang resmi jika ada permintaan yang mencurigakan.

[5] Otoritas Jasa Keuangan, *Bijak Ber-Eletronic Banking*, h. 60.

5) Jangan pernah memasukkan user ID dan password pada suatu halaman web yang terbuka otomatis (pop up) atau dari link. Ketiklah alamat halaman web yang akan dibuka.

6) Hati-hati mengunduh attachment e-mail karena dapat berisi virus/malware yang dapat mencuri data sensitif.

b. Typosite

Typosite pada layanan internet banking adalah membuat halaman web yang alamatnya mirip dengan halaman web internet banking suatu bank. Tujuannya untuk menjebak nasabah agar memasukkan user ID, password, dan informasi rahasia lainnya pada halaman web palsu tersebut. Selanjutnya, informasi rahasia yang telah diperoleh, digunakan oleh pelaku untuk mengakses halaman web yang sebenarnya. Halaman web yang dibuat oleh pelaku sangat mirip dengan halaman web internet banking bank sehingga nasabah sulit mengenali kejahatan ini, biasanya halaman web palsu tidak dapat menampilkan nama lengkap nasabah karena pelaku tidak memiliki informasinya.[6]

Hal-hal yang dapat dilakukan untuk meminimalisir bahaya typosite, antara lain:

1) Selalu memeriksa kembali ejaan nama situs, jangan sampai ada kesalahan ketik, termasuk penggunaan simbol.
2) Mengklik View Certificate untuk melihat rincian sertifikat dan memastikan apakah alamat web dapat dipercayai. Jika keluar pesan warning mengenai sertifikat saat mengakses server internet banking, lebih

[6] Otoritas Jasa Keuangan, *Bijak Ber-Eletronic Banking*, h. 63.

baik tidak jadi mengakses situs tersebut atau mengecek ulang nama situs yang telah ketikkan.

3) Menghentikan aktivitas transaksi jika merasa ada yang ganjil pada halaman web yang sedang diakses. Selanjutnya, tanyakan hal tersebut ke call center bank yang resmi.

4) Membuat short cut atau menyimpan alamat situs resmi internet banking pada browser (bookmark) sehingga nasabah dapat menggunakan short cut dan bookmark tersebut untuk meminimalkan kesalahan pengitikan alamat situs internet banking.

Man/Malware In The Browser (Mib) dan Keylogging (Keylogger) merupakan bentuk kejahatan lainnya yang dapat di bobol melalui perangkat keras. Dengan canggihnya teknologi sampai saat ini pelaku kejahatan juga mendapatkan backup dari software yang di buat untuk membobol dari sistem perbankan tersebut.

4. SMS Banking

a. Pencurian Ponsel

SMS Banking adalah transaksi perbankan elektronik yang menggunakan media ponsel. Pencurian ponsel dapat terjadi apabila nasabah lengah dalam menyimpan ponsel. Selain itu, ponsel mudah untuk disalahgunakan apabila setting pengaman dalam ponsel tidak diaktifkan, seperti password/passcode, autolock, screen-lock, pattern-lock. Nasabah biasanya menyimpan informasi penting seperti PIN, user id, password, dll dalam ponsel agar tidak lupa dan memudahkan bertransaksi.[7]

[7] Otoritas Jasa Keuangan, *Bijak Ber-Eletronic Banking*, h. 70.

Dalam SMS banking, pelaku memanfaatkan kelengahan nasabah antara lain dengan cara:

1) Ponsel hilang atau dipinjamkan, sementara informasi penting seperti PIN tersimpan di daftar contact atau catatan lainnya
2) Penduplikasian/penggandaan nomor ponsel dengan alat tertentu sehinggga informasi penting dikuasai oleh si pelaku.
3) Pendaftaran layanan SMS banking oleh orang lain (bukan pemilik rekening). Pelaku biasanya sudah menguasai ponsel Bijak Ber-Electronic Banking 57 dan sekaligus mengetahui semua informasi penting dari data pemilik ponsel sebenarnya.

Hal-hal yang dapat dilakukan untuk meminimalisir risiko SMS banking akibat pencurian ponsel, antara lain:

1) Mengaktifkan setting pengamanan pada ponsel seperti password/passcode, auto-lock, screen-lock, pattern-lock dll.
2) Tidak menulis PIN atau informasi lainnya di dalam ponsel.
3) Tidak meminjamkan ponsel kepada pihak lain tanpa pengawasan sementara ponsel tersebut sudah sudah terdapat layanan untuk SMS Banking.
4) Segera melapor ke bank atau ke pihak operator telekomunikasi apabila ponsel hilang atau dicuri untuk segera dapat diblokir, baik nomor ponselnya maupun transaksi SMS banking-nya di bank.

SMS banking termaksud dalam tehnologi yang telah di desain oleh perbankan. dalam tindak kejahatan sms banking sangat sulit di hacker karena tidak menggunkan

software atau web lainnya, melainkan langsung dengan nomor telephone untuk dapat mengakses ke rekening nasabah.

5. Mobile Banking

Pembajakan nomor ponsel adalah pengambilalihan nomor ponsel oleh orang lain dengan cara melaporkan kehilangan kepada perusahan operator telpon dan menerbitkan SIM card yang baru. Pembajakan nomor ponsel terjadi biasanya pada saat ponsel nasabah tidak aktif atau tidak mendapatkan sinyal. Hal ini dimaksudkan untuk menghindari kecurigaan nasabah.

Hal-hal yang dapat dilakukan untuk meminimalisir bahaya penyalahgunaan mobile banking, antara lain:

a. Merahasiakan PIN dan tidak menyimpan pada ponsel.
b. Menggunakan PIN yang tidak mudah ditebak.
c. Mengganti PIN secara berkala.
d. Senantiasa memperhatikan notifikasi e-mail dari bank.

Mobile banking dan SMS banking adalah produk dari elektronik banking yang diluncurkan oleh pihak bank untuk memeberikan pelayanan kepada nasabahnya. Kedua produk ini sama dalam bentuk kejahatan yang dapat dilakukan oleh pelaku. Salah satunya dengan pencurian nomor ponsel dan ponsel telah digunakan oleh orang lain.

6. E-Commerce

Carding pada e-commerce adalah suatu aktivitas belanja secara on-line (maya), dengan menggunakan data kartu debet atau kartu kredit yang diperoleh secara illegal. Kejahatan carding pada e-commerce sangat mudah dilakukan oleh pelaku kejahatan karena tanpa harus memegang fisik kartu, namun cukup dengan

mengetahui informasi tertentu pada kartu debet atau kartu kredit, antara lain berupa nomor kartu, tanggal expired kartu, masa berlaku kartu, CCV (berupa 3 angka pada bagian belakang kartu kredit), limit kartu dan informasi lainnya si pelaku sudah dapat melakukan transaksi pada e-commerce.[8]

Dalam kejadian carding, pelaku akan menggunakan data-data kartu debet dan/atau kartu kredit, antara lain dengan cara:

a. Pelaku mencari dan mendapatkan data-data kartu debet dan/ atau kartu kredit. Untuk mendapatkan data-data tersebut, pelaku dapat melakukan dengan cara-cara tertentu dan beberapa dijelaskan juga dalam buku ini, misalnya marketing palsu, merchant palsu, pencatatan data-data sensitif oleh oknum pada merchant, ataupun dari kartu yang hilang.
b. Pelaku menggunakan data-data tesebut untuk berbelanja secara on-line.
c. Transaksi terjadi dan tagihan akan dibebankan kepada nasabah yang memiliki kartu dengan data yang telah di gunakan.

Hal-hal yang dapat dilakukan untuk meminimalisir risiko carding melalui e-commerce, antara lain :

a. Simpan dan perlakukan kartu debet dan/atau kartu kredit dengan baik.
b. Tidak memberikan informasi penting pada kartu seperti nomor kartu, tanggal expired kartu dan CVV kepada siapapun baik secara langsung maupun media e-mail, website, SMS dan sarana lain.
c. Berhati-hati dalam menggunakan kartu kredit pada saat bertransaksi, untuk menghindarkan pencatatan data-data penting oleh merchant.

[8] Otoritas Jasa Keuangan, *Bijak Ber-Eletronic Banking*, h. 80.

d. Saat ini sebagian Bank telah meningkatkan pengamanan melalui 3D Secure yaitu OTP (One Time Password) yang dikirim melalui SMS kepada nasabah pemegang kartu. Upayakan nasabah mencari info mengenai fitur 3D Secure tersebut kepada bank penerbit kartu untuk meningkatkan keamanan penggunaan kartu tersebut.

7. Phone Banking

Modus nomor call center palsu merupakan salah satu modus yang masuk dalam kategori modus berbasis social engineering yang dilakukan dengan cara mengelabui nasabah yang bertransaksi melalui telepon. Modus ini dilakukan pelaku dengan memasang nomor call center palsu di lokasi yang dianggap strategis dengan harapan agar nasabah phone banking mencatat dan menghubungi call center palsu tersebut untuk bertransaksi keuangan. Dalam melakukan aksinya, cara yang digunakan oleh pelaku antara lain:

a. Menyebar dan menginformasikan nomor call center palsu atau nomor phone banking palsu. Nomor call center palsu atau nomor phone banking palsu tersebut adalah nomor telepon milik pelaku.
b. Jika ada nasabah yang menghubungi nomor tersebut, pelaku akan berpura-pura bertindak sebagai petugas bank.
c. Pelaku meminta nasabah menyebutkan data rahasia nasabah, seperti PIN, nomor kartu kredit, masa berlaku kartu kredit, dan kode pengaman kartu kredit (CVV).
d. Setelah mendapatkan data-data rahasia dari nasabah melalui nomor call center palsu atau nomor phone banking palsu, pelaku melakukan transaksi

e. illegal baik, yang biasanya dilakukan melalui e-commerce (belanja on-line) sehingga tidak diperlukan kartu debet dan/atau kartu kredit.

f. Modus ini dapat juga melibatkan teknik lain, seperti card trapping dan pencurian kartu.

8. Video banking

Booth video banking palsu, adalah booth (bilik atau gerai) yang dibuat oleh pelaku kejahatan yang menyerupai booth video banking asli yang dibuat oleh bank dengan tujuan untuk mendapatkan data-data nasabah baik informasi data identitas maupun informasi yang terdapat pada kartu nasabah. Semua Informasi tersebut biasanya diperoleh melalui mesin EDC yang sudah disiapkan oleh si pelaku maupun EDC asli namun telah ditambahkan dengan alat skimmer.[9]

Dalam melakukan aksinya, pelaku melakukan hal-hal antara lain:

a. Membuka booth video banking yang menyerupai dengan booth asli yang dimiliki bank.

b. Melengkapi booth tersebut dengan nomor call center palsu untuk mengelabui nasabah yang memerlukan bantuan langsung petugas.

c. Meminta nasabah untuk menyebutkan data identitas ataupun data kartu nasabah ataupun meminta nasabah melakukan transaksi dengan EDC baik yang asli ataupun yang telah dilengkapi dengan skimmer.

d. Mempergunakan informasi identitas dan kartu nasabah untuk bertransaksi.

Hal-hal yang dapat dilakukan untuk meminimalisir bahaya booth video banking palsu, antara lain:

[9] Otoritas Jasa Keuangan, *Bijak Ber-Eletronic Banking*, h. 85.

a. Memperhatikan kondisi booth apabila terdapat hal-hal yang mencurigakan seperti nomor call center, sebaiknya mengurungkan niat untuk menggunakan fasilitas yang ada di dalam booth tersebut.
b. Mencari nomor telepon bank yang sebenarnya dan kemudian menghubungi bank tersebut untuk melaporkan atau menanyakan kebenaran keberadaan booth tersebut.
c. Tidak menyampaikan data identitas ataupun data kartu.

Perkembangan operasional perbankan yang menggunakan tehnologi informasi secara modern dalam rangka memenuhi kebutuhan masyarakat terhadap pelayanan perbankan yang cepat dan efesien. Di sisi lain produk bank ini dapat menimbulkan sebuah resiko apabila tidak didukung kemanan yang kuat, prosedur dan manajemen resiko yang memadai dari bank yang menyediakan produk tersebut.