OTORITAS
JASA
KEUANGAN

BIJAK BER-eBANKING

TIDAK UNTUK DIPERJUAL BELIKAN

BIJAK BER-ELECTRONIC BANKING

Jakarta, Mei 2015

DISCLAIMER

Buku ini diharapkan dapat menjawab sebagian dari kebutuhan dan tantangan penyelenggaraan dan penggunaan e-banking. Meskipun demikian, isi buku ini tidak menjamin dan memastikan bahwa penyelenggara dan pengguna produk e-banking menjadi terbebas dari segala risiko baik *financial maupun non-financial* dalam menyelenggarakan dan bertransaksi dengan e-banking.

TIM PENYUSUN

A. Pengarah

Nelson Tampubolon	:	Dewan Komisioner OJK
Irwan Lubis	:	Deputi Komisioner Pengawas Perbankan III - OJK
Agus E. Siregar	:	Kepala Departemen Pengawasan Bank3 (DPB3) - OJK

B. Tim Perumus

Jasmi	:	Direktur - DPB3
Yusup Ansori	:	Direktur - DPB3
Irnal Fiscallutfi	:	Direktur - DPB2
Nahor P. Hutauruk	:	Direktur - DPB1
Ali Yusuf Asbi	:	Deputi Direktur - DPB3
Ridwan I. Situmorang	:	Deputi Direktur - DPB2
Guntar Kumala	:	Deputi Direktur - DPB1
Ahmad Nurdin	:	Kepala Bagian - DPB3
Pardiyono	:	Kepala Bagian - DPB3
Anton Sudharma	:	Kepala Bagian - DPB3
Budi Santoso	:	Kepala Bagian - DPB3
Iwan Irawan	:	Kepala Bagian - DPB1
Dayu Nawang M.	:	Kasubbag - DPB3

Rendra W. Prasetyo	:	Staf - DPB3
Rahayu Rianti	:	Staf - DPB3
Riris Grace Karolina	:	Staf - DPB2
Gozali Mulyono	:	Staf - DPB2

C. Kontributor/
Nara sumber : Bank Mandiri, BRI, BNI, BTN, BCA, Bank CIMB Niaga, Bank Danamon, Bank BII, Bank Panin, Bank Permata, Bank OCBC NISP, Bank UOB Indonesia, Bank Bukopin

DAFTAR ISI

KATA SAMBUTAN

Pertama-tama marilah kita mengucapkan puji syukur kehadirat Tuhan Yang Maha Kuasa, karena dengan kuasa dan kehendak-NYA-lah kita semua diberikan kesehatan dan kesempatan untuk menghadirkan buku ini. Selanjutnya saya juga ingin menyampaikan apresiasi kepada semua pihak yang telah menginisiasi, mengarahkan, menyumbangkan ide, tulisan, dan lain-lain hingga penerbitan buku ini dapat terealisir, sebagai bagian dari wujud tanggung jawab insan OJK terhadap pemangku kepentingan, terutama masyarakat luas pengguna maupun calon pengguna industri jasa keuangan, khususnya sektor perbankan.

Suatu keniscayaan bahwa seiring dengan perkembangan teknologi yang semakin maju, peningkatan kebutuhan dan tuntutan masyarakat yang semakin tinggi terhadap produk dan aktivitas perbankan baik dari sisi keberagaman, kecepatan, maupun fleksibilitas waktu bertransaksi, termasuk keamanan dan kenyamanan dalam bertransaksi serta disisi lain sejalan pula dengan upaya industri perbankan untuk beroperasi secara lebih efisien, maka berbagai kebutuhan tersebut dijawab oleh industri perbankan, antara lain dengan menghadirkan produk dan aktivitas *electronic banking* dengan *delivery channel* yang semakin beragam.

Sejalan dengan itu, otoritas pengawas telah, sedang dan akan terus mengawal perkembangan dan menjaga keseimbangan

kebutuhan dan tuntutan masyarakat terhadap produk dan aktivitas perbankan yang semakin kompleks dan efisien dimaksud dengan mengacu pada prinsip kehati-hatian dalam kerangka pengawasan secara mikro terhadap masing-masing individu perbankan sekaligus guna melindungi kepentingan nasabah industri perbankan khususnya dan masyarakat dan pada umumnya.

Penerbitan buku "Bijak Ber-eBanking" ini dinilai tepat dan diharapkan menjadi salah satu alternatif untuk ikut menjawab berbagai kebutuhan tersebut di atas. Buku ini dikemas dalam bentuk yang mudah dipahami mengenai apa dan bagaimana sebuah *electronic banking* dan beberapa contoh kejadian seputar transaksi *electronic banking* berikut ilustrasinya, baik yang terjadi di Indonesia maupun di luar negeri. Saya mengharapkan semoga buku ini dapat lebih meningkatkan pemahaman masyarakat pengguna/calon pengguna produk dan aktivitas *electronic banking*, termasuk bagi industri perbankan dalam kaitannya dengan potensi risiko yang mungkin timbul dari produk dan aktivitas dimaksud.

Semoga upaya ini mendapat berkah Tuhan Yang Maha Esa.

Selamat membaca.

Jakarta, Mei 2015

Nelson Tampubolon
Dewan Komisioner OJK

OTORITAS
JASA
KEUANGAN

Mengatur
Mengawasi
Melindungi

Untuk Industri Keuangan yang Sehat

OTORITAS JASA KEUANGAN

MENGATUR - MENGAWASI - MELINDUNGI

UNTUK INDUSTRI KEUANGAN YANG SEHAT

BAB I - PENDAHULUAN

A. Latar Belakang

Perkembangan perbankan saat ini memberikan dan menawarkan kemudahan bagi nasabah melalui layanan operasional yang sangat beragam, termasuk layanan e-banking *(electronic banking)*. Layanan e-banking saat ini dimiliki oleh hampir semua Bank Umum yang ada, baik dengan jenis *delivery channel* yang sangat umum (seperti ATM) maupun dengan jenis *delivery channel* lainnya seperti SMS, telephone, EDC (*Electronic Data Capture*) dan internet. Hal tersebut juga sejalan dengan kecenderungan perkembangan media sosial maupun kebijakan yang ada untuk mewujudkan atau mengarahkan transaksi pada masyarakat dilakukan tidak melulu dengan uang tunai *(less cash society),* sehingga telah banyak pelaku ekonomi atau masyarakat yang memanfaatkan layanan perbankan modern yang lebih efisien dan efektif melalui e-banking.

Transaksi yang dilakukan melalui e-banking setiap tahun mengalami pertumbuhan yang cukup besar pada beberapa bank. Berdasarkan data13 bank besar di Indonesia, frekuensi transaksi melalui e-banking pada tahun 2012 sebanyak 3,79 Milyar transaksi dan dengan nilai nominal Rp. 4.441 Trilyun, bertambah menjadi sebanyak 4,73 Milyar transaksi dengan nilai nilai nominal Rp. 5.495 Trilyun pada tahun 2013, pada tahun 2014 meningkat

masing-masing menjadi 5,69 Milyar transaksi dengan nilai nominal Rp. 6.447 Trilyun.

Pertumbuhan tersebut berpotensi meningkat sejalan dengan kecenderungan layanan bank mengarah pada *digital banking*. Hal ini dikarenakan antara lain layanan e-banking memiliki fitur yang menarik dan nyaman digunakan serta memberi kemudahan bagi nasabah untuk melakukan transaksi keuangan seperti transfer antar-bank, pembayaran kartu kredit, pembayaran listrik, pembayaran telepon, pembayaran tagihan ponsel, pembayaran asuransi, pembayaran internet, pembayaran tiket penerbangan, dan *virtual account*. Selain itu semakin marak bisnis daring *(online shop)* serta pertumbuhan jenis dan jumlah *smartphone* yang semakin meningkat telah memberikan andil dalam pertumbuhan transaksi melalui e-banking.

Pertumbuhan e-banking yang didukung dengan perkembangan teknologi, media sosial dan pola hidup masyarakat memberikan manfaat bagi industri perbankan antara lain menghasilkan pendapatan dari *fee-based income,* mengurangi biaya transaksi, pengembangan bisnis, dan meningkatkan kepercayaan/loyalitas nasabah. Penggunaan e-banking juga memberikan kenyamanan dan kemudahan bertransaksi secara bebas, tidak terbatas oleh waktu dan lokasi , khusus untuk *internet banking*, layanannya dapat dinikmati oleh nasabah *anytime, anywhere, dan by any*

device. faktor keamanan perlu mendapatkan perhatian yang cukup untuk meminimalkan potensi penyalahgunaan atau fraud melalui e-banking. Sebagai contoh, meskipun layanan *internet banking* dapat dinikmati oleh nasabah *anytime*, anywhere, dan by *any device*, tetapi dilengkapi dengan OTP (*One Time Password*), yaitu kode yang hanya dapat diperoleh melalui perangkat tertentu yang dimiliki oleh nasabah dan *password*, yaitu sesuatu yang hanya diketahui oleh nasabah.

B. Tujuan

Buku ini menjelaskan dan menguraikan gambaran umum mengenai jenis-jenis dan manfaat layanan serta modus kejadian penyalahgunaan e-banking, sehingga buku ini diharapkan dapat digunakan oleh nasabah, bank maupun pengawas bank terkait dengan tujuan antara lain:

- Memberikan pemahaman yang memadai kepada nasabah dalam melakukan transaksi melalui e-banking sehingga dapat meningkatkan rasa aman dan nyaman bertransaksi di e-banking.
- Menyusun langkah-langkah pengamanan maupun memberikan edukasi yang memadai oleh bank untuk mendukung penggunaan e-banking sebagai sarana transaksi oleh nasabah.
- Memberikan pemahaman kepada pengawas bankatas permasalahan pada e-banking, serta sebagai referensi

untuk melakukan langkah pembinaan atas kelemahan dan permasalahan pada e-banking sehingga bank diharapkan dapat menentukan langkah pencegahannya (mitigasi).

Selain itu,materi buku ini juga tersedia di website resmi OJK sehingga *stakeholder* lainnya dapat memperoleh informasi dan manfaatnya.

Uraian dalam buku ini lebih dititikberatkan sebagai salah satu wujud dari proses mengedukasi dan melindungi konsumen pengguna jasa produk/aktivitas perbankan terkait dengan e-banking, serta sekaligus dapat pula dimanfaatkan sebagai salah satu referensi pelaksanaan prinsip kehati-hatian bagi industri perbankan dalam menyelenggarakan e-banking.

C. Cakupan

Cakupan penyusunan buku ini meliputi layanan e-banking dan permasalahannya yang terjadi pada industri perbankan di Indonesia maupun di luar Indonesia. Adapun layanan e-banking yang ada pada industri perbankan tersebut antara lain meliputi ATM (*Automated Teller Machine*), *internet banking*, *mobile banking*, *SMS banking*, kartu kredit, kartu debet, *phone banking*, EDC (*Electronic Data Capture*) dan *video banking*.

Mengatur
Mengawasi
Melindungi

Untuk Industri Keuangan yang Sehat

OTORITAS JASA KEUANGAN

MENGATUR - MENGAWASI - MELINDUNGI

UNTUK INDUSTRI KEUANGAN YANG SEHAT

BAB II - GAMBARAN UMUM

A. Gambaran Umum *Electronic Banking* (e-Banking)

Perkembangan pesat Teknologi Informasi (TI) dan globalisasi mendukung Bank untuk meningkatkan pelayanan kepada nasabah secara aman, nyaman, dan efektif, diantaranya melalui media elektronik atau dikenal dengan *Electronic Banking* (e-banking). E-banking merupakan layanan yang memungkinkan nasabah Bank untuk memperoleh informasi, melakukan komunikasi, dan melakukan transaksi perbankan melalui media elektronik seperti *Automatic Teller Machine* (ATM), *Electronic Data Capture* (EDC)/ *Point Of Sales* (POS), *internet banking, SMS banking, mobile banking, e-commerce, phone banking*, dan *video banking*.

E-Banking memberikan banyak manfaat baik bagi nasabah, bank, dan otoritas. Bagi nasabah, e-banking memberikan kemudahan bertransaksi dalam hal waktu, tempat, dan biaya. Nasabah tidak perlu mendatangi kantor bank untuk memperoleh informasi atau melakukan transaksi perbankan. Bahkan untuk beberapa produk e-banking nasabah dapat bertransaksi selama 24 jam dengan menggunakan *laptop* atau perangkat *mobile* seperti telepon seluler yang dapat dibawa kemana saja selama terhubung dengan jaringan internet dan/atau SMS.

Bagi bank, e-banking meningkatkan pendapatan berbasis komisi *(fee based income)* dan mengurangi biaya operasional apabila dibandingkan dengan pelayanan transaksi melalui kantor cabang yang relatif besar untuk membayar karyawan, sewa gedung, pengamanan, listrik, dan lainnya.

Bagi otoritas, perkembangan teknologi e-banking mendorong mewujudkan masyarakat *less cash society. Less cash* society adalah gaya hidup dengan menggunakan media transaksi atau uang elektronik dalam bertransaksi sehingga tidak perlu membawa uang fisik. *Less cash society* selain dapat meningkatkan sistem pembayaran yang cepat, aman, dan efisien, untuk mempercepat perputaran aktivitas ekonomi dan stabilitas sistem keuangan, juga dapat mencegah tindak pidana kriminal maupun tindak pidana pencucian uang.

Di bawah ini merupakan beberapa produk yang termasuk dalam layanan e-banking.

Automated Teller Machine (ATM)

Definisi

ATM atau yang lebih dikenal dengan nama Anjungan Tunai Mandiri merupakan suatu terminal/mesin komputer yang terhubung dengan jaringan komunikasi bank, yang memungkinkan nasabah

melakukan transaksi keuangan secara mandiri tanpa bantuan dari *teller* ataupun petugas bank lainnya.

Sesuai dengan perkembangan teknologi, saat ini bank juga telah menyediakan 3 tipe mesin ATM lainnya, yaitu: mesin ATM yang hanya melayani transaksi non tunai, mesin ATM yang melayani transaksi penyetoran uang tunai *Cash Deposit Machine* atau CDM, dan mesin ATM yang dapat melayani semua transaksi yang telah disebutkan di atas.

Selain di kantor bank, saat ini nasabah dapat dengan mudah menemukan mesin ATM di berbagai tempat, seperti restoran, pusat perbelanjaan, bandar udara, pasar, dan lokasi-lokasi strategis lainnya.

Fitur

Melalui ATM, nasabah bank dapat mengakses rekeningnya untuk melakukan berbagai transaksi keuangan, yaitu transaksi penarikan tunai dan transaksi non tunai, seperti pengecekan saldo, pembayaran tagihan kartu kredit, pembayaran tagihan listrik, pembelian pulsa, dan sebagainya.

Cara Kerja

Untuk menggunakan ATM, nasabah harus memiliki kartu ATM/ debit/kredit dan PIN. PIN adalah kode (4-6 digit) angka yang dibuat oleh nasabah saat pertama kali menerima kartu ATM di bank. Kode tersebut harus dijaga kerahasiannya oleh nasabah supaya kartu ATM tidak dapat disalahgunakan oleh orang lain.

Nasabah memasukkan kartu pada slot kartu di mesin ATM dengan memperhatikan sisi kartu yang harus dimasukkan terlebih dahulu, kemudian nasabah akan diminta untuk memasukkan PIN. Setelah itu nasabah dapat melakukan transaksi dengan memilih menu yang tertera pada layar monitor ATM.

Electronic Data Capture (EDC)

Definisi

EDC merupakan suatu perangkat/ terminal yang dapat digunakan untuk bertransaksi menggunakan kartu debit/kredit/prabayar di *merchant* atau toko. Terminal tersebut terhubung ke jaringan komputer bank. EDC terdiri dari alat pembaca informasi pada pita

magnetis kartu *(card's magnetic stripe)* atau *chip*, tombol menu dan angka untuk memasukkan jenis transaksi, nilai transaksi, dan PIN, layar untuk melihat jenis dan nilai transaksi, dan printer untuk mencetak bukti transaksi.

Fitur

Saat ini, EDC digunakan di banyak toko untuk memudahkan nasabah melakukan transaksi, bahkan EDC dapat digunakan untuk pembayaran telepon, listrik, pulsa, tiket pesawat, dan transaksi lainnya. Pada umumnya EDC terhubung ke sistem bank menggunakan jaringan telepon *fixed line*, namun untuk beberapa pusat perbelanjaan yang memiliki banyak mesin EDC, ada juga yang menggunakan jaringan *leased line*. Seiring dengan perkembangan teknologi selular, EDC juga dapat menggunakan jaringan dengan sistem GPRS *(wireless)*.

Selain ditransaksikan dengan cara digesek, ada juga EDC yang yang digunakan dengan cara menempelkan kartu pada mesin (*card tapping*) seperti yang digunakan untuk membayar parkir, tol, alat transportasi, dan lainnya.

Cara Kerja

Untuk menggunakan EDC, nasabah harus memiliki kartu debit, kartu kredit, atau kartu elektronik. Cara menggunakannya yaitu dengan menggesekkan/memasukkan kartu pada mesin

kemudian pegawai *merchant* menginputkan jumlah uang yang akan dibayarkan, setelahnya nasabah akan diminta untuk menginputkan PIN pada mesin atau menyertakan tandatangan sebagai pembuktian keaslian nasabah *(authentication)* pada struk yang dikeluarkan oleh EDC. Namun pada EDC yang berjenis *card tapping,* nasabah cukup menempelkan kartu pada EDC saat melakukan pembayaran dan tidak perlu menginputkan PIN atau tanda tangan.

Internet Banking

Definisi

Internet banking adalah layanan untuk melakukan transaksi perbankan melalui jaringan internet. Merupakan kegiatan perbankan yang memanfaatkan teknologi internet sebagai media untuk melakukan transaksi dan mendapatkan informasi lainnya

melalui *website* milik bank. Kegiatan ini menggunakan jaringan internet sebagai perantara atau penghubung antara nasabah dengan bank tanpa harus mendatangi kantor bank. Nasabah dapat menggunakan perangkat komputer *desktop, laptop, tablet*, atau *smartphone* yang terhubung ke jaringan internet sebagai penghubung antara perangkat nasabah dengan sistem bank.

Fitur

Fitur layanan *internet banking* antara lain informasi umum rekening tabungan/giro, rekening deposito, kartu kredit, informasi mutasi rekening, transfer dana, baik transfer antar rekening maupun antar bank, pembelian pulsa, pembelian tiket, penempatan deposito, layanan informasi seperti suku bunga dan kurs, dan pembayaran, misalnya pembayaran telepon, internet, kabel TV, asuransi, listrik dan berbagai jenis pembayaran lainnya.

Cara Kerja

Untuk menggunakan *internet banking*, nasabah harus memiliki *user id, password*, media token atau *One Time Password* (OTP), dan jaringan internet. *User id, password,* dan media token dapat diperoleh dengan mendaftarkan diri ke bank. Saat menggunakan *internet banking*, nasabah harus memastikan *website* yang diakses adalah *website internet banking* milik bank, kemudian nasabah akan diminta untuk memasukkan *user id* dan *password* pada halaman muka atau *login*. Pada saat melakukan transaksi

finansial, nasabah akan diminta untuk memasukkan sandi OTP yang diperoleh dari media token atau SMS. Setelah transaksi selesai, nasabah harus memastikan telah keluar/*log out* dari halaman *internet banking*. Bank mengirimkan notifikasi melalui *e-mail* sebagai bukti bahwa transaksi telah berhasil. Notifikasi *e-mail* ini juga sebagai pengendalian agar nasabah mengetahui jika akun *internet banking*-nya digunakan oleh orang lain.

SMS Banking

Definisi

SMS banking adalah layanan perbankan yang dapat diakses langsung melalui telepon selular/*handphone* dengan menggunakan media SMS *(Short Message Service)*.

Fitur

Fitur *SMS Banking* antara lain layanan informasi (saldo, mutasi rekening, tagihan kartu kredit, dan suku bunga); dan layanan transaksi, seperti transfer, pembayaran tagihan (listrik, air, pajak, kartu kredit, asuransi, internet), pembelian (pulsa, tiket), dan berbagai fitur lainnya.

Cara Kerja

Untuk dapat menggunakan *SMS Banking*, nasabah harus mendaftarkan diri dan mendaftarkan nomor ponsel terlebih dahulu ke bank serta mendapatkan *password*, kemudian nasabah dapat bertransaksi dengan cara mengetik SMS sesuai dengan format SMS yang telah ditentukan. Format SMS berbeda-beda berdasarkan format yang telah ditentukan oleh masing-masing bank, contohnya: untuk melakukan transfer, nasabah dapat mengetik : Transfer <rek_sumber><rek_tujuan><nominal><password>. Pesan ini kemudian dikirim ke nomor tujuan yang telah ditentukan bank. Untuk menggunakan fasilitas ini nasabah sebaiknya mempelajari petunjuk format SMS yang tertera pada buku petunjuk *SMS banking* atau *website* bank.

Mobile Banking

Definisi

Mobile banking merupakan layanan yang memungkinkan nasabah bank melakukan transaksi perbankan melalui ponsel atau *smartphone*. Layanan

mobile banking dapat digunakan dengan menggunakan menu yang sudah tersedia pada SIM *(Subscriber Identity Module)* Card, USSD *(Unstructured Suplementary Service Data),* atau melalui aplikasi yang dapat diunduh dan diinstal oleh nasabah. Mobile banking menawarkan kemudahan jika dibandingkan dengan SMS banking karena nasabah tidak perlu mengingat format pesan SMS yang akan dikirimkan ke bank dan juga nomor tujuan SMS banking.

Fitur

Fitur-fitur layanan *mobile banking* antara lain layanan informasi (saldo, mutasi rekening, tagihan kartu kredit, suku bunga, dan lokasi cabang/ATM terdekat); dan layanan transaksi, seperti transfer, pembayaran tagihan (listrik, air, pajak, kartu kredit, asuransi, internet), pembelian (pulsa, tiket), dan berbagai fitur lainnya.

Cara Kerja

Untuk menggunakan *mobile banking*, nasabah harus mendaftarkan diri terlebih dahulu ke bank untuk mendapatkan *password*. Nasabah dapat memanfaatkan layanan mobile banking dengan cara mengakses menu yang telah tersedia pada *SIM Card* atau aplikasi yang terinstal di ponsel. Apabila nasabah menggunakan *mobile banking* melalui menu yang telah tersedia pada *SIM Card*, nasabah dapat memilih menu sesuai kebutuhan

kemudian nasabah akan diminta untuk menginputkan *PIN SMS Banking* saat menjalankan transaksi. Sedangkan apabila nasabah menggunakan *mobile banking* melalui aplikasi yang terinstal di ponsel, nasabah harus mengunduh dan menginstal aplikasi pada telepon seluler terlebih dahulu. Pada saat membuka aplikasi tersebut, nasabah harus memasukkan *password* untuk *login*, kemudian nasabah dapat memilih menu transaksi yang tersedia dan diminta memasukkan PIN saat menjalankan transaksi.

Electronic Commerce (e-Commerce)

Definisi

E-commerce atau perdagangan elektronik merupakan penyebaran, pembelian, penjualan, pemasaran barang dan jasa melalui sistem elektronik seperti internet atau televisi. Melalui *e-commerce*, pembeli dan penjual dapat melakukan transaksi secara *online.*

Jenis-jenis *e-commerce* antara lain:

a. *E-commerce* yang menggunakan sosial media atau forum untuk berjualan, namun transaksi tidak diselesaikan melalui *website* tersebut namun biasanya akan berkomunikasi secara langsung untuk bertransaksi.
b. *E-commerce* yang proses jual belinya dilakukan melalui *website* si penjual.

c. *E-commerce* yang proses jual belinya dilakukan di "lapak" *online*. Penjual bukanlah penyedia *website*, melainkan anggota-anggota yang mendaftar untuk berjualan di lapak *online* yang telah tersedia. Setiap transaksi yang terjadi pada lapak *online* tersebut, pengelola lapak akan menjadi pihak ketiga yang menerima pembayaran dan menjamin barang diterima oleh pembeli, lalu uang pembayaran akan diteruskan ke pihak penjual.

Fitur

Melalui *e-commerce*, masyarakat dapat melakukan jual beli, contohnya pembelian buku, alat elektronik, pakaian, kendaraan, bahkan rumah secara *online*. Pembayaran yang dilakukan pada saat bertransaksi secara *online* dapat menggunakan kartu kredit, debit, atau dengan menggunakan alat pembayaran *virtual* seperti *paypal.*

Cara Kerja

Untuk bertransaksi secara *online*, pembeli harus memiliki jaringan internet, alat pembayaran seperti kartu kredit, kartu debit, atau akun pembayaran *virtual*. Alur proses *e-commerce* pada umumnya

adalah sebagai berikut, pengguna mengakses *website* penjualan produk, melakukan pemesanan, menerima tagihan elektronik, kemudian pembeli dapat melakukan pembayaran secara elektronik. Beberapa perusahaan kartu kredit saat ini bekerjasama dengan perusahaan *internet security* untuk membuat standar enkripsi khusus demi keamanan bertransaksi, walaupun demikian nasabah diharapkan tetap menjaga keamanan bertransaksi misalnya dengan memperhatikan keamanan jaringan saat akan melakukan transaksi, memastikan perangkat dilengkapi dengan *antivirus, anti malware, firewall*, dan me-*review rating* si penjual sebelum melakukan transaksi *online.*

Phone Banking

Definisi

Phone Banking adalah layanan untuk bertransaksi perbankan atau mendapatkan informasi perbankan lewat telepon dengan menghubungi nomor layanan pada bank. Layanan tersebut antara lain bertujuan memberikan kemudahan kepada nasabah dalam melakukan berbagai transaksi perbankan melalui telepon. Nasabah tidak perlu lagi datang

ke bank atau mesin ATM untuk melakukan berbagai transaksi tersebut. Layanan *phone banking* ini merupakan salah satu dari perkembangan teknologi *call center.* Pada umumnya layanan *phone banking* dapat diakses selama 24 jam sehingga nasabah dapat menggunakannya dimana saja dan kapan saja.

Fitur

Fitur *phone banking* antara lain informasi perbankan misalnya informasi suku bunga, kurs, info produk bank, lokasi ATM dan kantor cabang, transaksi perbankan misalnya informasi saldo, pembayaran tagihan listrik, telepon pasca bayar, kartu kredit, pemindahbukuan, transfer antar bank, pembelian isi ulang pulsa, mutasi rekening, perubahan PIN dan data nasabah.

Cara Kerja

Phone banking dapat diakses oleh nasabah maupun non-nasabah bank untuk informasi umum bank. Bagi nasabah yang ingin menggunakan layanan *phone banking* dapat mendaftarkan diri terlebih dahulu ke bank untuk mendapatkan PIN *phone banking*. Setelah itu nasabah dapat menghubungi nomor *phone banking* bank dan nasabah akan dilayani oleh pegawai bank maupun IVR (*Interactive Voice Response*). IVR adalah teknologi yang dapat mendeteksi suara dan penekanan tombol telepon kemudian meresponnya kembali dalam bentuk suara atau media lain.

Video Banking

Definisi

Video Banking merupakan teknologi yang memungkinkan nasabah melakukan aktivitas perbankan jarak jauh menggunakan suatu perangkat khusus yang disediakan oleh bank yang memungkinkan nasabah berkomunikasi *audio visual* dengan petugas bank, menginput data, mencetak *statement*, dan mengeluarkan kartu baru. Pada umumnya bank menyediakan layanan *video banking* di lokasi-lokasi strategis seperti pusat perbelanjaan pada hari kerja maupun Sabtu dan Minggu. Jam operasionalnya pun lebih lama daripada jam operasional pelayanan melalui kantor bank.

Fitur

Fitur *video banking* di Indonesia pada saat ini antara lain pembukaan rekening, informasi produk, tarik dan setor tunai, transfer dana, pembelian pulsa, dan pembayaran tagihan seperti kartu kredit, listrik, dan telepon.

Cara Kerja

Untuk menggunakan layanan *video banking*, nasabah dapat mendatangi gerai perbankan digital yang menyediakan layanan ini. Selama bertransaksi nasabah akan dipandu oleh petugas bank, misalnya untuk melakukan pembukaan rekening baru melalui *video banking*, nasabah akan diminta untuk *memasukkan* data, *scan* kartu identitas, setoran awal, hingga cetak kartu sambil bertatap muka dan berkomunikasi dengan *customer service* bank melalui layar *video*.

B. Regulasi oleh Otoritas

Perbankan di Indonesia saat ini telah mengikuti perkembangan teknologi informasi dan komunikasi. Perkembangan ini ditandai dengan pesatnya penggunaan *electronic banking* (e-banking) untuk mendukung operasional kegiatan perbankan dan memudahkan nasabah melakukan transaksi.Walaupun demikian, penggunaan teknologi informasi tersebut perlu memperhatikan risiko yang dihadapi bank dan nasabah sehingga bank harus selalu menerapkan manajemen risiko teknologi informasi (TI) secara efektif.

Pengaturan dan pengawasan bank, khususnya manajemen risiko TI saat ini dilaksanakan oleh Otoritas Jasa Keuangan (OJK) sebagai lembaga pengawas industri jasa keuangan terpercaya, melindungi kepentingan konsumen dan masyarakat. Penerapan manajemen risiko TI bank diatur dalam PBI No.9/15/PBI/2007 tentang Penerapan Manajemen Risiko dalam Penggunaan

Teknologi Informasi dan SE No.9/30/DPNP perihal Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi Bank Umum. Beberapa hal yang diatur misalnya dalam kegiatan e-banking, bank wajib melaporkan rencana dan realisasi penerbitan produk e-banking yang bersifat transaksional dan harus memberikan edukasi kepada nasabah mengenai produk e-banking dan pengamanannya secara berkesinambungan. Pengaturan dan pengawasan terkait produk e-banking juga meliputi manajemen bank, kebijakan dan prosedur, penilaian risiko, mitigasi risiko, dan pengendalian pengamanan terkait e-banking.

C. Perkembangan Aktivitas E-banking Beberapa Bank di Indonesia

Penggunaan e-banking di Indonesia, baik dari jumlah nasabah pengguna transaksional, jumlah frekuensi e-banking dari tahun 2012 s/d 2014 secara umum meningkat. Peningkatan ini terjadi pada beberapa produk, misalnya *internet banking, mobile banking, SMS banking*, dan *phone banking*.

Jumlah Pengguna e-Banking Posisi 31 Desember 2014

Kartu Debit/ATM	82,006,699
Kartu Kredit	5,771,002
Kartu e-Money	9,788,145
Pengguna e-Money Berbasis Server	44,691
Pengguna *Internet Banking*	8,507,458
Pengguna *Mobile Banking*	14,738,817

Tabel 2.1 Perkembangan Frekuensi Transaksi e-banking di Beberapa Bank di Indonesia

Jenis Delivery Channel	*Frekuensi*				
	2012	*2013*	*2014*	*Perkembangan 2012 - 2013*	*Perkembangan 2013 - 2014*
ATM	*2,933,467,577*	*3,609,206,816*	*4,179,631,965*	*23.04%*	*15.80%*
EDC	*366,350,819*	*446,148,695*	*542,400,709*	*21.78%*	*21.57%*
Internet Banking	*235,957,566*	*311,880,376*	*437,798,960*	*32.18%*	*40.37%*
SMS /Mobile Banking	*224,876,666*	*325,550,038*	*473,196,941*	*44.77%*	*45.35%*
E-Commerce/ Merchant On-line	*2,790,843*	*3,707,515*	*7,778,488*	*32.85%*	*109.80%*
Phone Banking	*1,375,460*	*1,401,841*	*1,393,737*	*32.85%*	*-0.58%*
Video Banking	*7.684*	*16.418*	*28,097*		
Total Frekuensi Transaksi	*3,790,718,984*	*4,732,508,750*	*5,686,467,993*	*24,84%*	*20.16%*

Tabel 2.2 Perkembangan Nilai Transaksi e-banking di Beberapa Bank di Indonesia

Jenis *Delivery Channel*	Nilai Transaksi (dalam Milyar Rupiah)				
	2012	2013	2014	Perkembangan 2012 – 2013	Perkembangan 2013 – 2014
ATM	3,141,654	3,830,457	4,392,238	21.92%	14.67%
EDC	266,242	337,698	406,401	26.84%	20.34%
Internet Banking	669,607	860,546	1,062,820	28.52%	23.51%
SMS / Mobile Banking	343,441	437,853	544,371	27.49%	24.33%
E-Commerce/ Merchant On-line	5,514	10,849	16,134	96.76%	48.71%
Phone Banking	2,430	2,307	3,281	-5.05%	42.23%
Video Banking			104		
Total Nilai Transaksi	4,441,438	5,495,048	6,446,594	23.72%	17.32%

Mengatur
Mengawasi
Melindungi

Untuk Industri Keuangan yang Sehat

OTORITAS JASA KEUANGAN

MENGATUR - MENGAWASI - MELINDUNGI

UNTUK INDUSTRI KEUANGAN YANG SEHAT

BAB III –BIJAK DALAM MENGGUNAKAN LAYANAN E-BANKING

Electronic banking menawarkan berbagai kemudahan bagi nasabah, namun di sisi lain memiliki risiko yang harus diwaspadai. Berikut ini adalah beberapa contoh penyalahgunaan e-banking pada industri perbankan di Indonesia, termasuk di luar negeri 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:

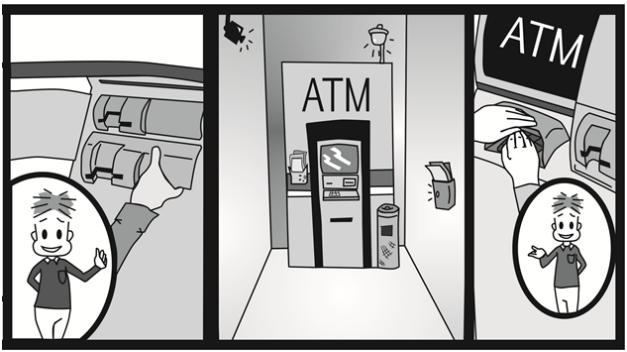
Delivery Channel	Media	Modus
ATM	Kartu, PIN, Mesin ATM.	- *Skimming* (menggunakan *skimmer*) - *Card Trapping* - *Card And PIN Sharing* - *Social Engineering* - *Call Center* palsu - Pencurian Data Kartu
EDC	Kartu, PIN, EDC, *Card Reader*.	- *Skimming* (menggunakan *skimmer*) - *Card Intercept* - Penggunaan *Card Reader Ilegal* - Pencurian Kartu/Data kartu - Gesek Tunai

Delivery Channel	Media	Modus
Internet Banking	User ID, Password, Token, Akun Medsos.	- P*hishing,* - *Man/Malware In The Browser (MIB)/* Sinkronisasi *Token* - *Typosite* - *Keylogger*
SMS Banking	PIN, Nomor Ponsel.	- Pencurian Ponsel, - Pembajakan Nomor Ponsel, - Ponsel digunakan oleh orang lain
Mobile Banking	PIN, Nomor Ponsel.	- Pencurian Ponsel - Pembajakan Nomor Ponsel - Clonning Nomor Ponsel
E-commerce	Data Kartu (Nomor Kartu, Masa Berlaku , Nama pada Kartu, CVV)	- *Carding*
Phone Banking	Nomor Rekening, PIN.	- *Call Center* palsu, - Menebak PIN Berulang-ulang.
Video Banking	Kartu Identitas, Penampakan Fisik.	- *Booth Video Banking* palsu.

A. ATM (*AUTOMATED TELLER MACHINE*)

CARD SKIMMING

Card Skimming adalah tindakan pencurian data kartu ATM dengan cara menyalin (membaca dan menyimpan) informasi yang terdapat pada strip magnetis secara ilegal. Strip magnetis adalah garis lebar hitam yang berada dibagian belakang kartu ATM. Fungsinya seperti pita kaset untuk menyimpan data nomor kartu, masa berlaku, dan nama nasabah. *Card skimming* dilakukan menggunakan alat pembaca kartu (*card skimmer*) yang ditempatkan pada slot kartu di mesin ATM.



Dalam *card skimming,* pelaku berusaha mendapatkan **data kartu** dan **PIN,** antara lain dengan cara:

1. Pelaku memasang alat *skimmer* pada mesin ATM;
2. Nasabah memasukkan kartu ke mesin ATM yang dipasangi alat *skimmer*, sehingga data kartu nasabah terbaca dan tersimpan pada alat tersebut;
3. Pelaku berusaha mendapatkan PIN ATM dengan cara mengintip tombol yang ditekan oleh nasabah atau dapat juga menggunakan kamera kecil yang dipasang oleh pelaku di mesin ATM;
4. Pelaku membuat kartu palsu menggunakan data yang telah diperoleh dan bertransaksi menggunakannya PIN yang telah diketahui (terekam).

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

- Memperhatikan kondisi mesin ATM sebelum digunakan. *Card Skimmer* seringkali tidak terlihat secara kasat mata karena warna dan bentuknya telah disesuaikan dengan mesin ATM;
- Hati-hati sebelum menekan tombol PIN. Usahakan agar tombol yang ditekan tidak terlihat oleh orang lain. Nasabah juga perlu mencermati adanya kamera yang dapat merekam tombol PIN yang ditekan oleh nasabah;
- Hindari menggunakan PIN yang mudah ditebak oleh orang lain, seperti tanggal lahir, nomor telepon, dan nomor kartu;

- Mengganti nomor PIN secara periodik, terutama jika ada indikasi bahwa PIN telah diketahui oleh orang lain.

CARD TRAPPING

Gbr. Contoh nomor call center palsu

Card trapping adalah mengambil fisik kartu dengan menggunakan suatu benda asing, seperti korek api, lidi, plastik, karet, benang, atau lem yang dipasang pada slot kartu di mesin ATM.

Dalam *card trapping*, pelaku berusaha mendapat fisik kartu dan PIN, antara lain dengan cara:

1. Pelaku memasang benda asing ke dalam slot kartu di mesin ATM.
2. Saat nasabah menggunakan mesin ATM tersebut, maka kartu ATM akan tersangkut oleh benda asing yang dipasang oleh pelaku, tidak dapat masuk maupun keluar.
3. Pelaku berusaha mendapatkan PIN nasabah dengan beberapa cara, misalnya:

- berpura-pura menawarkan bantuan dan meminta nasabah memasukkan PIN ke dalam mesin ATM. Pelaku memperhatikan dan mengingat nomor PIN nasabah;
- meminta nasabah untuk menghubungi *call center* palsu, lalu nasabah akan diminta menyebutkan PIN oleh petugas *call center* palsu tersebut; atau
- menggunakan kamera kecil yang dipasang oleh pelaku di mesin ATM.

4. Pelaku mengambil kartu ATM nasabah yang tersangkut di mesin ATM setelah nasabah meninggalkan mesin ATM. Modus lainnya untuk mendapatkan kartu nasabah, biasanya pelaku mendatangi nasabah di mesin ATM dan menawarkan bantuan, sementara pelaku lainnya akan mengalihkan perhatian nasabah, misalnya dengan menjatuhkan koin dan lain-lain. Selanjutnya, pelaku dengan cepat akan menukar kartu ATM nasabah dengan kartu ATM palsu yang sudah disediakan pelaku. Pelaku mendapatkan PIN nasabah dengan cara yang sama pada langkah sebelumnya.
5. Pelaku menggunakan kartu ATM dan PIN nasabah untuk mengambil tunai di mesin ATM atau transfer ke rekening lain.

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

- Memperhatikan kondisi mesin ATM sebelum digunakan. Nasabah perlu memperhatikan kondisi mesin ATM, sebelum

bertransaksi. Apabila terdapat hal yang tidak biasa seperti terdapat benda asing pada slot kartu ATM, nasabah hendaknya tidak melanjutkan bertransaksi, dan melaporkan hal tersebut melalui *call center* bank;

- Tidak panik. Nasabah tidak perlu panik saat kartu ATM tidak dapat masuk kedalam mesin ATM. Apabila terdapat seseorang yang menawarkan bantuan, sebaiknya nasabah tidak perlu melanjutkan transaksi;
- Mencari alternatif mesin ATM di lokasi lain;
- Tidak menginformasikan nomor PIN kepada orang lain, termasuk kepada petugas bank; dan
- Mewaspadai orang sekitar, jangan mudah percaya kepada orang yang tidak dikenal.

CALL CENTER 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:
   - Menyebutkan data rahasia nasabah, seperti seperti PIN, nomor kartu kredit, masa berlaku kartu kredit, dan kode pengaman kartu kredit atau *Card VerificationValue* (CVV).
   - 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:

- 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;

- Mencatat nomor telepon *call center* pada media lain, misalnya di ponsel atau catatan lainnya sehingga nasabah dapat menghubungi *call center* bank pada saat dibutuhkan; dan
- Tidak menginformasikan nomor PIN. Nasabah harus selalu merahasiakan nomor PIN, tidak memberitahukan kepada orang lain termasuk kerabat dekat dan pegawai bank atau *call center*.

PENCURIAN DATA KARTU

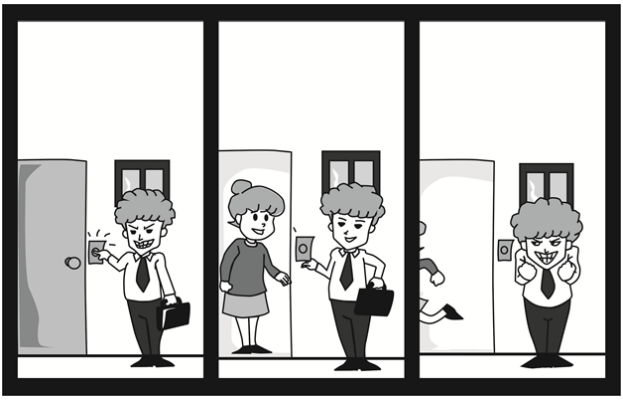
Pencurian data kartu (ATM/debit/kredit) dapat terjadi ketika nasabah berhadapan dengan petugas *marketing* palsu, menggunakan mesin EDC palsu (*dummy* EDC), atau menggunakan mesin ATM palsu (*dummy* ATM). Pelaku pencurian data kartu berusaha mendapatkan data nomor kartu kredit (atau data kartu debit yang menjadi *member principal* kartu kredit), masa berlaku kartu debit/kredit, dan kode pengaman kartu debit/kredit (CVV).

Dalam melakukan pencurian data kartu, pelaku melakukan hal-hal antara lain:

A. Petugas *marketing* palsu

1. Pelaku membuka kios sementara *(booth)* yang dilengkapi dengan spanduk *(banner)*, tanda pengenal, dan seragam yang mirip dengan bank tertentu.

2. Menawarkan produk bank, misalnya kartu kredit dan meminta nasabah:
   - menyerahkan kartu identitas dan/atau kartu kredit untuk difotokopi atau diambil oleh petugas dan menjanjikan penggantian dengan kartu kredit yang baru.
   - Mengisi formulir yang berisi data-data pribadi nasabah.
3. Pelaku dapat juga mendatangi nasabah ke rumah/kantor/ tempat usaha, menawarkan produk bank dengan modus seperti disebutkan pada nomor 2.



Hal-hal yang dapat dilakukan untuk meminimalisir pencurian data kartu, antara lain:

- Memastikan keaslian kios sementara (*booth*), spanduk (*banner*), tanda pengenal, dan seragam yang dikenakan oleh petugas *marketing*. Jika meragukan keasliannya, jangan lakukan transaksi, membuka rekening, atau memberikan data kartu kepada petugas kios sementara tersebut;
- Menghubungi layanan resmi atau kantor bank jika ingin mendaftar produk/layanan bank; dan
- Tidak memberikan fisik kartu atau fotokopi kartu kredit kepada pihak manapun, termasuk petugas bank.

B. Mesin EDC/ATM palsu

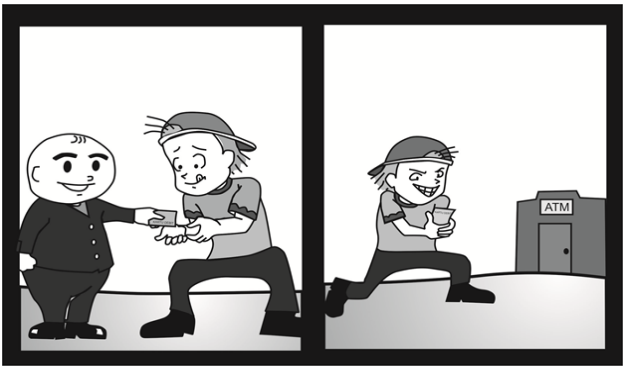
Pelaku memasang mesin EDC dan/atau ATM palsu di tempat umum. Pada saat nasabah menggunakan mesin tersebut, data kartu dan PIN nasabah akan terekam. Selanjutnya pelaku membuat kartu palsu menggunakan data yang telah diperoleh dan bertransaksi menggunakannya PIN yang telah diketahui (terekam).

Hal-hal yang dapat dilakukan untuk meminimalisir pencurian data kartu, antara lain:

- Mengamati mesin EDC/ATM sebelum digunakan. Jika ada kejanggalan (misalnya logo tidak sesuai atau tampilan layar tidak lazim) sebaiknya tidak menggunakan mesin tersebut;

- Segera mengganti PIN pada mesin lain yang resmi jika nasabah sudah terlanjur menggunakan mesin EDC/ATM palsu tersebut; dan
- Menginformasikan kepada bank jika menemukan adanya kejanggalan pada mesin EDC/ATM.

MEMINJAMKAN KARTU DAN PIN KEPADA ORANG LAIN



Nasabah harus memperlakukan kartu dan PIN sebagai sesuatu yang bersifat pribadi dan rahasia. Kartu dan PIN yang diberikan kepada orang lain, dapat disalahgunakan untuk bertransaksi di luar pengetahuan nasabah. Banyak kejadian pembobolan rekening nasabah oleh orang dekat seperti keluarga atau orang lain yang dipercaya oleh nasabah.

Hal-hal yang dapat dilakukan untuk meminimalisir risiko ini, antara lain:

- Nasabah hendaknya tidak meminjamkan kartu ATM dan/atau memberitahukan PIN kepada orang lain, sekalipun kepada keluarga, teman dekat, atau petugas bank; dan
- Hindari mencatat PIN dimanapun, termasuk di ponsel, dompet, buku, tempelan dinding, dll.

SOCIAL ENGINEERING

Social engineering adalah upaya yang memanfaatkan pendekatan sosial untuk mendapatkan data rahasia nasabah atau meminta nasabah melakukan sesuatu yang menguntungkan pelaku, seperti transfer uang, pembayaran tagihan, dan pembelian pulsa.

Dalam *social engineering,* pelaku menggunakan beberapa cara, antara lain:

1. Pelaku mengirimkan pesan melalui SMS, *e-mail*, atau media lain yang berisi pengumuman pemenang hadiah dan meminta nasabah untuk menghubungi nomor telepon atau membuka *website* tertentu;
2. Pelaku memandu nasabah untuk:
   - memberikan informasi rahasia seperti PIN, nomor kartu kredit, masa berlaku kartu kredit, dan kode pengaman kartu kredit (CVV, yaitu 3 angka yang tertera di belakang kartu); atau

- datang ke mesin ATM, menggunakan *internet banking*, atau menggunakan e-banking lainnya, dan melakukan transaksi transfer, pembelian, atau pembayaran yang menguntungkan pelaku tanpa disadari oleh nasabah.

Hal-hal yang dapat dilakukan untuk meminimalisir risiko *social engineering*, antara lain:

- Nasabah hendaknya tidak mudah tergoda dengan tawaran hadiah yang disampaikan melalui telepon, SMS, *e-mail*, atau media sosial;
- Mencari informasi ke sumber lain yang terpercaya untuk memastikan kebenaran informasi yang diterima;
- Tidak memberikan informasi rahasia seperti PIN, nomor kartu kredit, masa berlaku kartu kredit, dan kode CVV kepada orang lain.

B. EDC (*ELECTRONIC DATA CAPTURE*)

CARD SKIMMING

Seperti pada ATM, *card skimming* juga dapat terjadi pada transaksi melalui mesin EDC. Modus *card skimming* pada ATM dan EDC sedikit berbeda, pada ATM alat *skimmer* akan dilekatkan pada mesin ATM yang resmi, sedangkan pada EDC alat *skimmer*

terpisah dari mesin EDC yang resmi. Pelaku akan melakukan *double swipe* yaitu menggesek kartu nasabah pada mesin EDC Bank dan alat *skimmer* yang sudah disiapkan, seringkali alat *skimmer* tersebut dilekatkan pada mesin kasir milik *merchant.*

Hal-hal yang dapat dilakukan untuk meminimalisir bahaya *skimming* pada saat transaksi menggunakan mesin EDC, antara lain :

- Jangan serahkan kartu kepada pelayan tanpa didampingi. Seringkali nasabah lengah dengan memberikan kartu kepada pelayan untuk bertransaksi menggunakan mesin EDC, hal ini memungkinkan pelayan atau kasir menggesek kartu nasabah di mesin *skimmer* tanpa disadari oleh nasabah;
- Awasi pada saat kasir menggesek kartu. Nasabah harus mengawasi aktifitas kasir, pastikan bahwa kartu hanya digesekkan di mesin EDC resmi milik bank. Penggesekan kartu untuk transaksi perbankan hanya dilakukan sekali yaitu pada mesin EDC milik bank. Hal yang umum saat ini, kartu nasabah digesekkan dua kali yaitu pada mesin EDC dan mesin kasir untuk mencetak nama pembeli pada struk pembelian pada mesin *cash register* milik *merchant,* nasabah

harus berhati-hati dan berhak menolak untuk menggesekkan kartu di mesin kasir dengan alasan keamanan data; dan

- Hati-hati sebelum menekan nomor PIN di mesin EDC. Meskipun tidak seorangpun memperhatikan ketika nasabah memasukkan PIN, nasabah harus tetap berhati-hati kemungkinan adanya kamera tersembunyi. Akan lebih baik apabila dalam setiap menekan PIN, nasabah menutup dengan tangan.

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.

Hal-hal 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;
- Pastikan kartu yang dikembalikan oleh kasir setelah transaksi

adalah kartu yang benar. Nasabah harus mengecek kartu yang dikembalikan oleh kasir setelah bertransaksi adalah kartu yang benar. Sebaiknya nasabah menghapal atau mencatat nomer kartu ATM (minimal 4 digit terakhir) untuk memastikan kartu tidak tertukar atau ditukar dengan sengaja pada saat transaksi.

PENGGUNAAN *CARD READER ILEGAL*

Modus penggunaan *card reader ilegal* adalah tindakan pencurian saldo yang ada pada kartu *e-money* melalui proses *tapping* secara diam-diam oleh oknum *merchant* dengan menggunakan *card reader* atau mesin EDC yang bekerja dalam kondisi *online* maupun *offline*. Pelaku yang sudah dilengkapi dengan peralatan tersebut secara diam-diam (pada jarak tertentu yang memungkinkan terjadinya transaksi) melakukan *tapping* kepada calon korban, atau dilakukan secara acak tanpa disadari oleh korban dengan tujuan mengurangi saldo yang ada di dalam kartu *e-money* dalam jumlah tertentu sesuai keinginan pelaku. Saldo yang telah diambil tersebut baik secara otomatis ataupun tidak (bergantung kondisi *on-line/off-line* pada EDC), akan masuk ke dalam rekening pelaku.

Hal-hal yang dapat dilakukan untuk meminimalisir bahaya penggunaan *card reader ilegal*:

- Menyimpan kartu *e-money* dengan aman. Menjaga dan menempatkan kartu *e-money* di tempat yang memiliki penghalang memadai untuk menghindari *tapping;* dan
- Mengecek saldo kartu *e-money* setiap kali selesai melakukan suatu transaksi, untuk memastikan jumlah saldo berkurang secara wajar. Apabila nasabah menemukan saldo berkurang secara tidak wajar segera laporkan kepada bank penerbit untuk diketahui penyebabnya.

PENUKARAN (PENGAMBILAN) KARTU OLEH PETUGAS *MARKETING* PALSU

Penukaran atau pengambilan kartu dilakukan ketika nasabah pemilik kartu ditawari oleh petugas *marketing* palsu untuk melakukan penggantian kartu. Pelaku berusaha untuk mendapatkan kartu kredit nasabah, dengan cara sebagai berikut:

1. Pelaku membuka kios sementara *(booth)* dilengkapi dengan spanduk *(banner),* tanda pengenal, dan seragam yang mirip dengan bank tertentu atau dapat juga mendatangi nasabah ke rumah/kantor/tempat usaha.
2. Pelaku menjanjikan promo *upgrade* jenis kartu dari segi *limit*, jenis kartu, dan keuntungan lainnya.
3. Nasabah pemilik kartu menyerahkan kartu kredit yang dimiliki kepada *marketing* palsu.

4. Pelaku menggunakan kartu tersebut untuk bertransaksi atau penarikan tunai.

Hal-hal yang dapat dilakukan untuk menghindari penukaran kartu oleh petugas *marketing* palsu, antara lain :

- Memastikan keaslian kios sementara *(booth),* spanduk *(banner),* tanda pengenal dan seragam yang dikenakan oleh petugas *marketing*;
- Melakukan konfirmasi ke bank penerbit apabila menerima tawaran promo dari *marketing*;
- Menghubungi layanan/konter resmi jika ingin melakukan *upgrade* kartu; dan
- Tidak memberikan fisik kartu dan PIN kepada pihak manapun, termasuk petugas bank.

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 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.

KARTU HILANG

Nasabah pemegang kartu debit dan/atau kartu kredit dapat mengalami kehilangan kartu debit dan/atau kartu kredit. Kejadian kehilangan kartu tersebut dapat disebabkan kelalaian nasabah maupun disebabkan suatu tidak kejahatan yang dilakukan kepada nasabah, misalnya penjambretan, pencurian, dan penipuan.

Saat ini, penggunaan kartu debit dan/atau kartu kredit untuk berbelanja pada *merchant* memungkinkan dilakukan tanpa PIN, cukup dengan menandatangani struk transaksi. Kartu yang memungkinkan bertransaksi menggunakan tanda tangan adalah kartu debit dan kartu kredit yang tergabung dalam jaringan Visa

dan Mastercard. Oleh karena itu, meskipun nasabah tidak pernah mengungkapkan PIN kepada siapapun, tidak pernah menuliskan PIN pada kartu, ataupun merasa hanya nasabah tersebut saja yang mengetahui PIN kartu tersebut, risiko terhadap penggunaan kartu debit dan/atau kartu kredit tersebut oleh pihak yang tidak berwenang masih tetap ada.

Dalam kejadian nasabah kehilangan kartu, pelaku akan mencoba menggunakan kartu nasabah yang hilang, antara lain dengan cara:

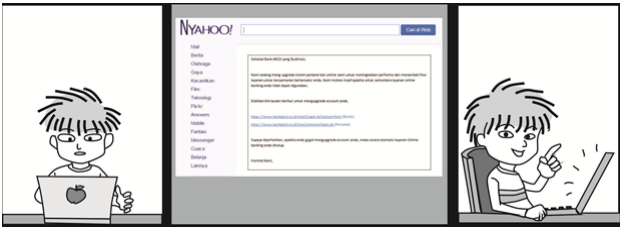
1. Pelaku mendapatkan kartu nasabah yang hilang. Apabila pada bagian belakang kartu terdapat tanda tangan nasabah, pelaku akan mencoba untuk menirukan tanda tangan tersebut untuk bertransaksi. Apabila pada bagian belakang kartu tidak terdapat tanda tangan nasabah, pelaku akan membiarkan tetap kosong atau dapat saja pelaku menandatangani bagian belakang kartu dengan tanda tangan palsu.
2. Pelaku akan bertransaksi (baik untuk membeli barang atau melakukan gesek tunai) melalui *merchant* yang tidak terlalu ketat dalam melakukan verifikasi tanda tangan pada kartu debet dan/kartu kredit. Selain itu, pelaku biasa mencari *merchant* yang tidak diawasi CCTV.

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

- Segera melaporkan kehilangan kartu dan melakukan blokir rekening untuk kartu-kartu yang hilang melalui kantor atau *call center* bank.
- Nasabah menjaga kartu dengan baik, dan jangan letakkan kartu pada sembarang tempat khususnya di tempat umum;
- Mengecek transaksi terakhir yang dilakukan melalui kartu yang hilang tersebut, pengecekan dapat dilakukan menggunakan fasilitas *internet banking, mobile banking, phone banking,* atau datang ke kantor bank; dan
- Melaporkan kejadian kehilangan kartu dan meminta surat keterangan kehilangan kartu kepada kepolisian.

C. INTERNET BANKING

PHISHING



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.

Selain ketiga hal di atas, suatu *phishing* dapat juga ditandai dengan adanya kesalahan ketik dan gaya bahasa yang kurang baik. Pesan *phishing* biasanya tidak melalui proses *review* dan *editing* yang baik, bahkan tidak jarang berupa terjemahan kasar dari bahasa asing. 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. Sebagai contoh, pelaku akan mengirimkan pesan bahwa saat ini sedang terjadi pemeliharaan *server* untuk transaksi *internet banking* sehingga nasabah diminta untuk memasukkan data-data sensitif dan penting. Apabila nasabah tidak memasukkan, maka rekening nasabah tersebut akan menjadi tidak aktif dan tidak dapat digunakan.

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

- 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.
- Menggunakan *anti virus* yang terkini.
- Jangan mengklik *link* apapun pada pesan (*e-mail*) yang terindikasi *phishing*.
- Mengkonfirmasikan kepada pihak bank melalui *call center* yang resmi jika ada permintaan yang mencurigakan.
- 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.
- Hati-hati mengunduh *attachment e-mail* karena dapat berisi *virus/malware* yang dapat mencuri data sensitif.

MAN/MALWARE IN THE BROWSER (MIB)

MIB adalah teknik pembobolan rekening *internet banking* dengan memanfaatkan *software* jahat (*malware*) yang telah menginfeksi *browser internet* nasabah. *Malware* tersebut dapat melakukan beberapa hal sesuai keingingan pembuatnya, misalnya:

- Mencuri data *user ID* dan *password* nasabah,
- Mengambil alih koneksi nasabah ke bank lalu memasukkan transaksi pemindahbukuan/transfer dari rekening nasabah ke rekening pelaku, dan
- Mengganti halaman *web* di *browser* nasabah sesuai keinginan pelaku.

Dalam melakukan MIB, pelaku menggunakan beberapa langkah, antara lain:

- Menyediakan program *malware* pada alamat *web* tertentu. Jika nasabah membuka *web* atau mengunduh sesuatu (*software*, gambar, *video*, dll) dari *web* tersebut, maka *malware* akan masuk ke komputer nasabah.
- Setelah *malware* terinstal di komputer nasabah, *malware* tersebut merekam apa saja yang diketik oleh nasabah sehingga pelaku bisa mendapatkan data *user ID* dan *password internet banking* nasabah.
- *Malware* mengambil alih koneksi *internet banking* milik nasabah lalu memasukkan transaksi sesuai keinginan pelaku, misalnya transfer dari rekening nasabah ke rekening pelaku.
- Jika *internet banking* dilengkapi dengan otentikasi token, *malware* mengirimkan pesan palsu kepada nasabah, meminta kode token kepada nasabah dengan alasan, misalnya: sinkronisasi token.

Hampir seluruh proses MIB bersifat transparan, berjalan di belakang layar, dan tidak dapat dilihat atau dirasakan oleh nasabah. Satu-satunya proses yang dapat dirasakan oleh nasabah adalah pada saat pelaku (*malware*) melakukan *phishing*, antara lain:

- Menampilkan layar *pop up* yang menginformasikan antara lain bank penyelenggara *internet banking* sedang melakukan pemeliharaan sistem atau data nasabah (misalnya sinkronisasi token).
- Meminta nasabah memasukkan kode token (*one time password* / OTP). Kode token tersebut digunakan oleh pelaku untuk menjalankan transaksi di *internet banking* nasabah.

Salah satu cara yang dapat digunakan nasabah sebagai tanda untuk lebih waspada yaitu adanya notifikasi melalui *e-mail* dari bank yang menginformasikan transaksi tertentu meskipun nasabah tidak melakukannya, misalnya informasi pendaftaran rekening tujuan transfer, informasi pendaftaran transaksi tunda, dan informasi transaksi berhasil dijalankan.

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

- Menggunakan komputer pribadi dan jaringan yang terpercaya untuk mengakses layanan *internet banking*. Sebaiknya menghindari penggunaan komputer publik, misalnya di

warnet, dan/atau jaringan yang tidak terpercaya, misalnya *wifi access point* yang disediakan oleh kafe atau toko di pusat perbelanjaan.

- Melengkapi komputer pribadi dengan *anti virus* yang terkini.
- Menghindari akses ke dan/atau mengunduh *file* dari alamat *web* yang tidak terpercaya.
- Mewaspadai permintaan informasi yang tidak wajar, misalnya permintaan untuk memasukkan kode token melalui layar *pop up*.
- Segera menindaklanjuti dengan menghubungi *call center* resmi apabila terdapat notifikasi dari bank mengenai adanya aktivitas pada rekening sementara nasabah tidak pernah melakukan hal tersebut.

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, namun biasanya

halaman *web* tersebut tidak terkini dan tidak dapat merespon secara interaktif, misalnya menampilkan ucapan selamat datang dengan menyebut nama lengkap nasabah. Halaman *web* palsu tidak dapat menampilkan nama lengkap nasabah karena pelaku tidak memiliki informasinya.

Dalam *typosite*, cara yang digunakan oleh pelaku, antara lain:

1. Membuat situs yang namanya mirip dengan alamat *web* suatu bank. Setiap orang dapat menamai situsnya dengan nama apapun sepanjang belum ada yang menggunakannya. Misalnya, situs resminya adalah www.ibanking-bankABC.com, sementara situs palsunya adalah www.ibank-bankABC.com, www.ibanking-ACBbank.com, dan sebagainya.
2. Menunggu hingga ada nasabah yang salah ketik sehingga masuk ke halaman web tersebut.
3. Mencatat/merekam *user ID* dan *password* yang dimasukkan oleh nasabah.
4. Menggunakan *user ID* dan *password* untuk membobol akun *internet banking* nasabah di situs yang resmi.

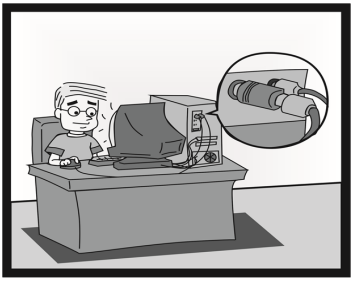
Jika *internet banking* dilengkapi dengan OTP, pelaku biasanya menggunakan teknik *phishing* untuk mendapatkan kode OTP, yaitu mengirimkan pesan disertai ancaman sehingga nasabah memberikan informasi OTP ke pelaku melalui halaman *web* palsu tersebut. Pelaku dapat juga menunggu hingga nasabah melakukan

transaksi tertentu, misalnya transfer keluar, lalu mengubah pesan (*challenge code*) sesuai kebutuhan pelaku, menangkap OTP yang dimasukkan oleh nasabah, dan menggunakan OTP tersebut untuk menjalankan transaksi pelaku di halaman *web* resmi.

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

- Selalu memeriksa kembali ejaan nama situs, jangan sampai ada kesalahan ketik, termasuk penggunaan sImbol.
- 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 baik tidak jadi mengakses situs tersebut atau mengecek ulang nama situs yang telah ketikkan.
- Menghentikan aktivitas transaksi jika merasa ada yang ganjil pada halaman *web* yang sedang diakses. Selanjutnya, tanyakan hal tersebut ke *call center* bank yang resmi.
- 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*.

KEYLOGGING (KEYLOGGER)



Keylogger adalah suatu perangkat yang dipasang di antara *keyboard* dan CPU, digunakan untuk merekam apapun yang diketikkan oleh nasabah di *keyboard*. Tujuannya adalah untuk mendapatkan *user ID* dan *password* nasabah. Meskipun saat mengetikkan *password* yang tampil di layar hanyalah '*****', namun isi *password* tersebut tetap dapat terekam dan terbaca oleh pelaku. Hasil rekamannya dapat dikirimkan melalui *e-mail* kepada pelaku atau dapat juga di-*copy* langsung dari perangkat *keylogger*.

Seiring dengan perkembangan teknologi, *keylogger* dapat berupa *software* yang terinstal di komputer nasabah.

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

- Memastikan bahwa komputer yang digunakan aman dari perangkat *keylogger*
- Menghindari penggunaan komputer publik, seperti di warnet, bandara, dan kafe.

- Menghentikan aktivitas transaksi jika merasa ada yang ganjil pada komputer yang sedang diakses.
- Berhati-hati dalam mengunduh dan/atau menginstal *software*.

D. SMS BANKING

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, auto-lock, screen-lock, pattern-lock*. Nasabah biasanya menyimpan informasi penting seperti PIN, *user id, password*, dll dalam ponsel agar tidak lupa dan memudahkan bertransaksi.

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

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:

- Mengaktifkan setting pengamanan pada ponsel seperti *password/passcode, auto-lock, screen-lock, pattern-lock* dll.
- Tidak menulis PIN atau informasi lainnya di dalam ponsel atau
- Tidak meminjamkan ponsel kepada pihak lain tanpa pengawasan sementara ponsel tersebut sudah sudah terdapat layanan untuk *SMS Banking*.
- 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.

PEMBAJAKAN NOMOR PONSEL DAN PENCURIAN PIN *SMS BANKING*

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

Dalam pembajakan nomor ponsel, pelaku menggunakan cara antara lain:

- Pelaku menggunakan surat kuasa palsu yang dilampiri fotocopy KTP nasabah.
- Jika berhasil mendapatkan SIM card pengganti, maka pelaku bisa mengirimkan dan menerima SMS ke bank seakan-akan ia adalah nasabah yang sebenarnya.
- Pelaku menghubungi *call center* bank, dan meminta untuk dilakukan reset PIN. Notifikasi perubahan PIN akan disampaikan ke *e-mail* / SMS nasabah, dimana ponsel nasabah sudah dikuasai pelaku.

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

- Merahasiakan PIN dan tidak menyimpan pada ponsel
- Menggunakan PIN yang tidak mudah ditebak
- Mengganti PIN secara berkala
- Senantiasa memperhatikan notifikasi *e-mail* dari Bank.

PONSEL DIGUNAKAN OLEH ORANG LAIN

SMS banking dapat disalahgunakan jika ponsel nasabah digunakan oleh orang lain, baik itu karena dipinjamkan, dicuri, atau hilang. Selain itu, ponsel mudah untuk disalahgunakan apabila *setting* pengaman dalam ponsel tidak diaktifkan, seperti

password/passcode, auto-lock, screen-lock, pattern-lock. Nasabah umumnya menyimpan informasi penting seperti PIN, *user id, password*, dll dalam ponsel agar tidak lupa dan memudahkan bertransaksi. Sebagai contoh, PIN *SMS banking* akan tersimpan pada *"sent items"* sehingga dapat diketahui dan disalahgunakan oleh orang lain.

Pelaku berusaha mendapatkan ponsel dan PIN antara lain dengan cara:

1. Pelaku memanfaatkan kelengahan nasabah dengan mengambil ponsel nasabah.
2. Pelaku mencari PIN yang tersimpan pada ponsel atau pelaku menghubungi *call center* bank meminta untuk dilakukan *reset* PIN.
3. Pelaku mendapatkan PIN dari notifikasi *e-mail* yang dikirimkan bank.

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

- Mengaktifkan *setting* pengamanan pada ponsel seperti *password/passcode, auto-lock, screen-lock, pattern-lock* dll
- Menghapus SMS yang berisi PIN dari *sent item* maupun dari *folder* lainnya.
- Menggunakan PIN yang tidak mudah ditebak.
- Mengganti PIN secara berkala

- Segera melakukan pemblokiran akun *SMS banking* dan/atau nomor ponsel jika kehilangan ponsel.
- Senantiasa memperhatikan notifikasi *e-mail* dari Bank.

E. MOBILE BANKING

PEMBAJAKAN NOMOR PONSEL DAN PENCURIAN PIN *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.

Dalam pembajakan nomor ponsel, pelaku menggunakan cara antara lain:

- Pelaku menggunakan surat kuasa palsu yang dilampiri fotocopy KTP nasabah.
- Jika berhasil mendapatkan *SIM card* pengganti, maka pelaku bisa mengirimkan dan menerima SMS ke bank seakan-akan ia adalah nasabah yang sebenarnya.
- Pelaku menghubungi *call center* bank, dan meminta untuk dilakukan *reset* PIN. Notifikasi perubahan PIN akan

disampaikan ke *e-mail* / SMS nasabah, dimana ponsel nasabah sudah dikuasai pelaku.

- Jika pelaku telah mengetahui PIN *SMS banking* nasabah, maka dapat digunakan untuk membobol rekening nasabah di bank.

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

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

PONSEL DIGUNAKAN OLEH ORANG LAIN

Mobile Banking dapat disalahgunakan jika ponsel nasabah digunakan oleh orang lain, baik itu karena dipinjamkan, dicuri, atau hilang. Selain itu, ponsel mudah untuk disalahgunakan apabila *setting* pengaman dalam ponsel tidak diaktifkan, seperti *password/passcode, auto-lock, screen-lock, pattern-lock*. Nasabah umumnya menyimpan informasi penting seperti PIN, *user id, password*, dll dalam ponsel agar tidak lupa dan memudahkan bertransaksi. Sebagai contoh, PIN *SMS banking* akan tersimpan pada *sent items* sehingga dapat diketahui dan disalahgunakan oleh orang lain.

Pelaku berusaha mendapatkan ponsel dan PIN antara lain dengan cara:

1. Pelaku memanfaatkan kelengahan nasabah dengan mengambil ponsel nasabah.
2. Pelaku mencari PIN yang tersimpan pada ponsel atau pelaku menghubungi *call center* bank meminta untuk dilakukan *reset* PIN.
3. Pelaku mendapatkan PIN dari notifikasi *e-mail* yang dikirimkan bank.

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

- Mengaktifkan *setting* pengamanan pada ponsel seperti *password/passcode, auto-lock, screen-lock, pattern-lock* dll
- Menghapus SMS yang berisi PIN dari *sent item* maupun dari *folder* lainnya.
- Menggunakan PIN yang tidak mudah ditebak.
- Mengganti PIN secara berkala
- Segera melakukan pemblokiran akun *SMS banking* dan/atau nomor ponsel jika kehilangan ponsel.
- Senantiasa memperhatikan notifikasi *e-mail* dari bank.

F. E-COMMERCE

CARDING

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*.

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

1. 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.
2. Pelaku menggunakan data-data tesebut untuk berbelanja secara *on-line*.

3. Transaksi terjadi dan tagihan akan dibebankan kepada nasabah yang memiliki kartu dengan data-data yang telah digunakan secara *illegal* oleh pelaku.

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

- Simpan dan perlakukan kartu debet dan/atau kartu kredit dengan baik.
- 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.
- Berhati-hati dalam menggunakan kartu kredit pada saat bertransaksi, untuk menghindarkan pencatatan data-data penting oleh *merchant*.
- 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.

G. PHONE BANKING

NOMOR *CALL CENTER* PALSU DAN/ATAU NOMOR *PHONE BANKING* PALSU

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:

1. 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.
2. Jika ada nasabah yang menghubungi nomor tersebut, pelaku akan berpura-pura bertindak sebagai petugas bank.
3. Pelaku meminta nasabah menyebutkan data rahasia nasabah, seperti PIN, nomor kartu kredit, masa berlaku kartu kredit, dan kode pengaman kartu kredit (CVV).
4. Setelah mendapatkan data-data rahasia dari nasabah melalui nomor *call center* palsu atau nomor *phone banking* palsu,

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

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

Hal-hal yang dapat dilakukan untuk meminimalisir bahaya nomor *call center* palsu :

- Meminta nomor *call center* atau nomor *phone banking* secara langsung dari kantor cabang, *website* resmi dan atau publikasi resmi dari bank.
- Simpan dan catat nomor *call center* dan/atau nomor *phone banking* pada daftar nomor telepon di ponsel.
- Batalkan transaksi jika nasabah curiga dengan nomor telpon tersebut ataupun curiga dengan respon dari nomor telpon tersebut.

MENEBAK PIN SECARA BERULANG-ULANG

Modus kejahatan dengan cara menebak nomor PIN *phone banking* nasabah secara berulang-ulang dapat dilakukan dengan memanfaatkan kelemahan sistem bank yang setiap hari melakukan *reset counter number* yang menampung jumlah kesalahan nomor PIN sehingga PIN tersebut tidak akan pernah terblokir. Pelaku yang telah memiliki kartu debit dapat mencoba memasukkan

nomor PIN berulang kali namun untuk menghindari terblokirnya kartu tersebut, sebelum mencapai frekuensi maksimum kesalahan PIN, pelaku berhenti mencoba memasukkan PIN dan mencobanya kembali pada keesokan harinya dengan metode yang sama hingga didapatkan nomor PIN yang benar.

Dalam melakukan aksinya, cara yang digunakan oleh pelaku antara lain:

1. Pelaku mencari beberapa data sensitif dan penting dari nasabah, antara lain nomor rekening, nomor kartu debet dan/ atau kartu kredit, tanggal *expired* atau masa berlaku kartu, limit kartu, dan beberapa data lainnya yang dapat digunakan untuk verifikasi transaksi *phone banking*.
2. Pelaku menghubungi nomor *phone banking*, dan mencoba melakukan verifikasi dengan memasukkan PIN. PIN yang dimasukkan tersebut merupakan tebakan dari pelaku.
3. Apabila kesalahan PIN sudah mendekati batas kesalahan yang diperkenankan, maka pelakukan akan menghentikan upayanya dan mencobanya di lain waktu.
4. Apabila tebakan PIN benar, maka pelaku dapat melakukan transaksi melalui fasilitas *phone banking* tersebut.

Hal-hal yang dapat dilakukan untuk meminimalisir bahaya menebak PIN secara berulang-ulang :

- Menjaga data-data rahasia dan sensitif seperti nomor rekening, nomor kartu debet dan/atau kartu kredit, tanggal *expired* atau masa berlaku kartu, limit kartu, dan beberapa data lainnya yang dapat digunakan untuk verifikasi transaksi *phone banking*.
- Secara periodik melakukan pengecekan transaksi pada rekening.
- Memanfaatkan fasilitas notifikasi transaksi *phone banking* melalui SMS apabila bank menyediakan layanan tersebut.

H. VIDEO BANKING

BOOTH VIDEO BANKING PALSU

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* yang cara kerjanya telah dijelaskan pada pembahasan sebelumnya.

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

1. Membuka *booth video banking* yang menyerupai dengan *booth* asli yang dimiliki bank.
2. Melengkapi *booth* tersebut dengan nomor *call center* palsu untuk mengelabui nasabah yang memerlukan bantuan langsung petugas.
3. 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*.
4. Mempergunakan informasi identitas dan kartu nasabah untuk bertransaksi.

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

- 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.
- Mencari nomor telepon bank yang sebenarnya dan kemudian menghubungi bank tersebut untuk melaporkan atau menanyakan kebenaran keberadaan *booth* tersebut.
- Tidak menyampaikan data identitas ataupun data kartu.

OTORITAS JASA KEUANGAN

Mengatur
Mengawasi
Melindungi

Untuk Industri Keuangan yang Sehat

OTORITAS JASA KEUANGAN

MENGATUR - MENGAWASI - MELINDUNGI

UNTUK INDUSTRI KEUANGAN YANG SEHAT

BAB IV - PENUTUP

Perkembangan operasional perbankan yang menggunakan modernisasi teknologi informasi dalam rangka memenuhi kebutuhan masyarakat terhadap pelayanan perbankan yang cepat dan efisien serta kebijakan *less cash society* menjadi *trend* perkembangan produk perbankan kedepan melalui layanan produk e-banking. Di sisi lain produk bank ini dapat menimbulkan risiko apabila tidak didukung dengan *environment, security,* prosedur dan manajemen risiko yang memadai dari bank yang menyediakan produk tersebut termasuk pemahaman yang memadai dari nasabah pengguna maupun calon pengguna produk e-banking.

Transaksi e-banking baik frekuensi maupun *volume* transaksi dari beberapa bank di Indonesia selama kurun waktu tahun 2012, 2013 dan 2014 menunjukkan perkembangan yang pesat. Kedepannya, sejalan dengan perkembangan teknologi, kebutuhan masyarakat dan tuntutan terhadap perbankan yang semakin efisien, maka transaksi dan nasabah termasuk bank yang menyelenggarakan produk e-banking diperkirakan semakin meningkat. Hal tersebut menimbulkan pula tantangan terhadap penyelenggaraan e-banking, kebutuhan pengawasan terhadap perbankan dan di sisi lain perlunya edukasi kepada masyarakat luas.

Selanjutnya, Otoritas telah, sedang dan akan terus melakukan pengaturan dan pengawasan terhadap produk e-banking untuk lebih meyakini bahwa operasional bank tekait dengan produk e-banking senantiasa mengacu kepada prinsip kehati-hatian sehingga aman dan nyaman bagi nasabah perbankan untuk melakukan transaksi dan menggunakan produk e-banking.

Buku ini diharapkan dapat menjawab sebagian dari kebutuhan dan tantangan penyelenggaraan dan penggunaan e-banking. Meskipun demikian, isi buku ini tidak menjamin dan memastikan bahwa penyelenggara dan pengguna produk e-banking menjadi terbebas dari segala risiko baik *financial* maupun *non-financial* dalam menyelenggarakan dan bertransaksi dengan e-banking.

GLOSSARY

3-D Secure:

pengamanan tambahan berupa kode sekali pakai atau *One Time Password* (OTP) untuk bertransaksi kartu kredit secara *on-line*. Sistem bank mengirimkan kode acak melalui SMS ke nomor ponsel nasabah pada saat nasabah melakukan transaksi *on-line*.

Access - akses:

jalan masuk. Suatu usaha untuk membuka suatu saluran komunikasi dengan perangkat *hardware* atau *software* tertentu, seperti *modem* yang digunakan untuk membuka akses internet. Perangkat *hardware* atau *software* tersebut selain untuk memberikan data juga digunakan untuk menerima data untuk disimpan.

Account:

penampungan data tentang seseorang, sedikitnya terdiri dari nama pengguna dan *password*. Di dalam sistem perbankan, *account* adalah satu data kepemilikan atas suatu produk perbankan, dapat terdiri dari nama nasabah, kode produk, nilai nominal yang dimiliki.

Access point:

perangkat keras yang memungkinkan perangkat *wireless* lain (seperti *laptop*, ponsel) untuk terhubung ke jaringan kabel menggunakan *Wi-fi, bluetooth* atau perangkat standar lainnya.

Auto-lock:

penguncian otomatis terhadap suatu perangkat (misalnya ponsel) dengan parameter waktu atau tombol tertentu sehingga perangkat tersebut tidak dapat digunakan oleh orang lain yang tidak memiliki akses.

Bisnis Daring atau online shop:

suatu kegiatan atau pekerjaan untuk memasarkan produk yang dimilikinya dengan mempergunakan jaringan internet dengan tujuan untuk memperoleh keuntungan.

Browser:

perangkat lunak yang berfungsi untuk menerima dan menyajikan sumber informasi di Internet.

Card reader:

alat untuk membaca kartu elektronik.

Card Verification Value (CVV):

tiga digit angka terakhir yang terdapat pada bagian belakang kartu kredit, biasanya berada di tempat tanda tangan pada kartu kredit.

Cash Deposit Machine (CDM):

mesin ATM yang memungkinkan nasabah dapat melakukan penyetoran tunai melalui mesin ATM secara *real time on-line* dengan rekening dan secara otomatis mesin ATM tersebut akan mendeteksi denominasi dan kondisi fisik uang (asli atau palsu, baik atau rusak).

Clonning:

penggandaan atau duplikasi terhadap suatu barang.

Closed Circuit Television (CCTV):

suatu sistem yang digunakan sebagai pelengkap keamanan dan pemantauan yang banyak digunakan untuk di perkantoran, toko, industri, militer, perumahan, di sekitar aset milik perbankan.

Customer Service:

petugas bank yang melayani nasabah untuk keperluan pembukaan rekening, perubahan data nasabah, pengaduan nasabah, dan layanan *non-financial* lainnya.

Delivery Channel:

jalur atau media yang digunakan oleh bank untuk memberikan layanan kepada nasabahnya baik secara konvensional ataupun elektronik, yang meliputi : *teller, SMS Banking, Mobile Banking, Phone Banking, EDC, Internet Banking*, ATM*, Video Banking, E-commerce.*

Digital Banking:

satu cara akses ke sistem perbankan yang dapat dilakukan kapan saja dan dimana saja dengan menggunakan jaringan internet.

Unduh:

adalah meminta sebuah *file* dari komputer lain (*web site, server* atau yang lainnya) dan menerimanya.

Electronic Banking (E-Banking):

layanan yang memungkinkan nasabah bank untuk memperoleh informasi, melakukan komunikasi, dan melakukan transaksi perbankan melalui media elektronik seperti *Automatic Teller Machine* (ATM), *phone banking, Electronic Fund Transfer* (EFT), *Electronic Data Capture* (EDC) / *Point Of Sales* (POS), *internet banking* dan *mobile banking.*

E-mail/surat elektronik:

sarana kirim mengirim surat melalui jalur jaringan komputer (misalnya Internet).

E-money atau stored value atau prepaid card:

produk yang merupakan media yang dipakai dalam mekanisme sistem pembayaran melalui pembayaran di *point of sales (merchant),* transfer antar dua media elektronik atau jaringan komputer menggunakan nilai uang yang tersimpan pada kartu atau produk tersebut.

Enkripsi:

alat untuk mencapai keamanan data dengan menerjemahkannya dengan menggunakan sebuah *key (password).* Enkripsi mencegah *password* atau *key* supaya tidak mudah dibaca pada *file* konfigurasi.

Fee-based income:

komisi yang diterima bank dari pemasaran produk maupun transaksi jasa perbankan yang dibebankan kepada nasabah sehubungan dengan produk dan jasa bank yang dinikmatinya.

File:

kumpulan data yang berisi informasi, dapat berupa dokumen atau elektronik dan dapat tersimpan di dalam suatu tempat penyimpanan fisik atau digital. Untuk *file* elektronik memiliki berbagai format dengan kegunaan yang berbeda.

Firewall:

peralatan untuk menjaga keamanan jaringan yang melakukan pengawasan dan penyeleksian atas lalu lintas data/informasi melalui jaringan serta memisahkan jaringan privat dan publik. Peralatan ini dapat digunakan untuk melindungi komputer yang telah terhubung ke jaringan dari serangan yang dapat mengkompromikan suatu komputer.

Fraud:

segala macam yang dapat dipikirkan dan diupayakan oleh seseorang untuk mendapatkan keuntungan dari orang lain dengan cara yang tidak jujur yang menyebabkan orang lain tertipu.

General Packet Radio Service (GPRS):

teknologi yang memungkinkan pengiriman dan penerimaan data dalam bentuk paket data, seperti *e-mail*, gambar, dll.

Interactive Voice Response (IVR):

teknologi telepon dimana pelanggan menggunakan telepon untuk terhubung dengan *database* yang berisi informasi tanpa harus berbicara dengan petugasnya.

Kartu kredit:

kartu yang dikeluarkan oleh pihak bank dan sejenisnya untuk memungkinkan pembawanya membeli barang-barang yang dibutuhkannya secara hutang. Kartu kredit merupakan suatu jenis penyelesaian transaksi ritel, yang diterbitkan kepada pengguna sistem tersebut sebagai alat pembayaran yang dapat digunakan dalam membayar suatu transaksi.

Kartu debit:

sebuah kartu pembayaran secara elektronik yang diterbitkan oleh bank yang berfungsi sebagai pengganti pembayaran dengan uang tunai.

Keyboard:

perangkat keras pada komputer yang berbentuk papan dengan berbagai macam fungsi perintah yang selanjutnya dikirim ke perangkat CPU. *Keyboard* terdiri dari banyak tombol ketik dengan simbol masing-masing.

Keylogger:

ancaman berupa perangkat lunak atau perangkat keras/*hardware* yang digunakan untuk memperoleh informasi (PIN, *password*) yang diketikkan pengguna pada *keyboard* (biasanya di warung internet).

Leased Line:

saluran koneksi telepon permanen antara dua titik yang disediakan oleh perusahaan telekomunikasi publik. Umumnya, *leased line* digunakan ketika terdapat kebutuhan komunikasi data jarak jauh yang harus dilakukan secara terus-menerus. *Leased line* memiliki beberapa tingkatan tarif yang bergantung kepada lebar jalur data *(bandwidth)* yang mampu dikirimkan melalui jaringan *leased line* tersebut.

Less cash society:

gaya hidup dengan menggunakan uang elektronik dalam bertransaksi, sehingga tidak perlu membawa uang fisik.

Login:

proses untuk mengakses komputer atau sistem atau aplikasi atau suatu layanan di media elektronis dengan memasukkan informasi yang telah terdaftar seperti *user id* dan *password.*

Malware:

perangkat lunak yang diciptakan untuk menyusup dan merusak sistem komputer tanpa izin dari pemilik.

Marketing:

proses menawarkan barang dan jasa kepada calon pelanggan.

Merchant:

penjual barang/jasa yang memiliki *physical store* maupun *on-line store* yang bekerja sama dengan bank dalam penyediaan layanan penerimaan pembayaran.

Media Sosial:

media *on-line* yang memungkinkan manusia untuk saling berinteraksi satu sama lain tanpa dibatasi ruang dan waktu.

On-line:

sistem atau komputer yang terkoneksi/terhubung dengan jaringan internet.

Off-line:

sistem atau komputer yang tidak terdapat hubungan jaringan atau tidak dapat berkomunikasi dengan sistem atau komputer lain.

One Time Password (OTP) :

kode verifikasi yang dikirimkan melalui SMS atau email untuk memastikan kebenaran transaksi oleh pemilik rekening.

Password:

kode atau simbol khusus untuk mengamankan sistem komputer yaitu untuk mengidentifikasi pihak yang mengakses data, program atau aplikasi komputer dan digunakan.

Pattern-lock:

penguncian layar perangkat (misalnya ponsel) menggunakan metode penguncian dengan pola, berfungsi seperti *password.*

Personal Identification Number (PIN):

rangkaian digit unik terdiri dari huruf, angka atau kode ASCII yang digunakan untuk mengidentifikasi pengguna komputer, pengguna ATM, internet banking, mobile banking,dll.

Pita magnetis (Card's magnetic stripe):

suatu pita perekam yang digunakan untuk media penyimpan data. Setiap karakter ditulis melintasi lebar pita dalam bentuk bintik-bintik yang diberi muatan magnet, pembacaan dari dan penulisan ke pita dilakukan dengan menggerakkan permukaan pita melintasi suatu *read/write head sebuah tape drive.*

Pop Up:

jendela yang muncul ketika mengunjungi halaman suatu web atau aplikasi.

Screen-lock:

penguncian layar perangkat (misalnya ponsel) sehingga *user* yang tidak memiliki akses tidak dapat mempergunakannya. Metode *screen-lock* dapat berupa penguncian dengan *password* atau pola.

Server:

sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer.

Setting:

pengaturan baik terhadap perangkat keras atau perangkat lunak.

Subscriber Identity Module (SIM) Card:

sebuah kartu pintar dalam berbagai ukuran yang menyimpan kunci pengenal jasa telekomunikasi sehingga dapat saling berkomunikasi.

Smartphone:

ponsel pintar atau ponsel cerdas yaitu telepon genggam yang mempunyai kemampuan dan fungsi menyerupai komputer.

Social Engineering:

teknik pembohongan melalui perilaku sosial yang dilakukan oleh hacker untuk mengelabui orang agar memberikan informasi rahasia seperti PIN, *Password*, dll.

Software / perangkat lunak:

sekumpulan program elektronik yang dapat menjalankan suatu perintah.

Teller:

petugas bank yang melayani transaksi simpanan, penarikan, pencairan cek, dan pelayanan perbankan tunai /non tunai lainnya kepada nasabah.

Token:

alat pengaman tambahan untuk melakukan transaksi finansial di *internet banking*.

Unstructured Suplementary Service Data (USSD):

sebuah protokol berbasis GSM untuk berkomunikasi dari *handphone* pengguna ke penyedia layanan telekomunikasi (dan sebaliknya).

Upgrade:

penggantian produk dengan versi yang lebih baru atau lebih baik dengan produk yang dihasilkan oleh perusahaan yang sama.

User Identification/User ID:

serangkaian huruf, angka, simbol atau kombinasinya untuk mengidentifikasi pihak yang mengakses data, program atau aplikasi komputer dan digunakan dengan tujuan mengamankan suatu sistem atau aplikasi tersebut.

Virtual account:

nomor identifikasi pelanggan yang dibuka oleh bank atas permintaan perusahaan untuk diberikan oleh perusahaan kepada pelanggannya (perorangan maupun non perorangan) sebagai nomor rekening tujuan penerimaan *(collection)*.

Virus:

program yang bersifat merusak dan akan aktif dengan bantuan orang (dieksekusi), dan tidak dapat mereplikasi sendiri, penyebarannya karena dilakukan oleh orang, seperti *copy,* biasanya melalui *attachement e-mail, game,* program bajakan dll.

Website:

web page atau informasi yang disampaikan melalui suatu *web browser* atau sekumpulan *web page* yang dirancang, dipresentasikan dan saling terhubung untuk membentuk suatu sumber informasi dan atau melaksanakan fungsi transaksi.

Wireless :

jaringan komunikasi dimana perangkat-perangkat di dalamnya (PC, komputer, ataupun *handphone*) dapat berkomunikasi tanpa kabel.

OTORITAS
JASA
KEUANGAN

BIJAK BER-eBANKING

TIDAK UNTUK DIPERJUAL BELIKAN

BIJAK BER-ELECTRONIC BANKING

Jakarta, Mei 2015

DISCLAIMER

Buku ini diharapkan dapat menjawab sebagian dari kebutuhan dan tantangan penyelenggaraan dan penggunaan e-banking. Meskipun demikian, isi buku ini tidak menjamin dan memastikan bahwa penyelenggara dan pengguna produk e-banking menjadi terbebas dari segala risiko baik *financial maupun non-financial* dalam menyelenggarakan dan bertransaksi dengan e-banking.

TIM PENYUSUN

A. Pengarah

Nelson Tampubolon	:	Dewan Komisioner OJK
Irwan Lubis	:	Deputi Komisioner Pengawas Perbankan III - OJK
Agus E. Siregar	:	Kepala Departemen Pengawasan Bank3 (DPB3) - OJK

B. Tim Perumus

Jasmi	:	Direktur - DPB3
Yusup Ansori	:	Direktur - DPB3
Irnal Fiscallutfi	:	Direktur - DPB2
Nahor P. Hutauruk	:	Direktur - DPB1
Ali Yusuf Asbi	:	Deputi Direktur - DPB3
Ridwan I. Situmorang	:	Deputi Direktur - DPB2
Guntar Kumala	:	Deputi Direktur - DPB1
Ahmad Nurdin	:	Kepala Bagian - DPB3
Pardiyono	:	Kepala Bagian - DPB3
Anton Sudharma	:	Kepala Bagian - DPB3
Budi Santoso	:	Kepala Bagian - DPB3
Iwan Irawan	:	Kepala Bagian - DPB1
Dayu Nawang M.	:	Kasubbag - DPB3

Rendra W. Prasetyo	:	Staf - DPB3
Rahayu Rianti	:	Staf - DPB3
Riris Grace Karolina	:	Staf - DPB2
Gozali Mulyono	:	Staf - DPB2

C. Kontributor/
Nara sumber : Bank Mandiri, BRI, BNI, BTN, BCA, Bank CIMB Niaga, Bank Danamon, Bank BII, Bank Panin, Bank Permata, Bank OCBC NISP, Bank UOB Indonesia, Bank Bukopin

DAFTAR ISI

KATA SAMBUTAN

Pertama-tama marilah kita mengucapkan puji syukur kehadirat Tuhan Yang Maha Kuasa, karena dengan kuasa dan kehendak-NYA-lah kita semua diberikan kesehatan dan kesempatan untuk menghadirkan buku ini. Selanjutnya saya juga ingin menyampaikan apresiasi kepada semua pihak yang telah menginisiasi, mengarahkan, menyumbangkan ide, tulisan, dan lain-lain hingga penerbitan buku ini dapat terealisir, sebagai bagian dari wujud tanggung jawab insan OJK terhadap pemangku kepentingan, terutama masyarakat luas pengguna maupun calon pengguna industri jasa keuangan, khususnya sektor perbankan.

Suatu keniscayaan bahwa seiring dengan perkembangan teknologi yang semakin maju, peningkatan kebutuhan dan tuntutan masyarakat yang semakin tinggi terhadap produk dan aktivitas perbankan baik dari sisi keberagaman, kecepatan, maupun fleksibilitas waktu bertransaksi, termasuk keamanan dan kenyamanan dalam bertransaksi serta disisi lain sejalan pula dengan upaya industri perbankan untuk beroperasi secara lebih efisien, maka berbagai kebutuhan tersebut dijawab oleh industri perbankan, antara lain dengan menghadirkan produk dan aktivitas *electronic banking* dengan *delivery channel* yang semakin beragam.

Sejalan dengan itu, otoritas pengawas telah, sedang dan akan terus mengawal perkembangan dan menjaga keseimbangan

kebutuhan dan tuntutan masyarakat terhadap produk dan aktivitas perbankan yang semakin kompleks dan efisien dimaksud dengan mengacu pada prinsip kehati-hatian dalam kerangka pengawasan secara mikro terhadap masing-masing individu perbankan sekaligus guna melindungi kepentingan nasabah industri perbankan khususnya dan masyarakat dan pada umumnya.

Penerbitan buku "Bijak Ber-eBanking" ini dinilai tepat dan diharapkan menjadi salah satu alternatif untuk ikut menjawab berbagai kebutuhan tersebut di atas. Buku ini dikemas dalam bentuk yang mudah dipahami mengenai apa dan bagaimana sebuah *electronic banking* dan beberapa contoh kejadian seputar transaksi *electronic banking* berikut ilustrasinya, baik yang terjadi di Indonesia maupun di luar negeri. Saya mengharapkan semoga buku ini dapat lebih meningkatkan pemahaman masyarakat pengguna/calon pengguna produk dan aktivitas *electronic banking*, termasuk bagi industri perbankan dalam kaitannya dengan potensi risiko yang mungkin timbul dari produk dan aktivitas dimaksud.

Semoga upaya ini mendapat berkah Tuhan Yang Maha Esa.

Selamat membaca.

Jakarta, Mei 2015

Nelson Tampubolon
Dewan Komisioner OJK

OTORITAS
JASA
KEUANGAN

Mengatur
Mengawasi
Melindungi

Untuk Industri Keuangan yang Sehat

OTORITAS JASA KEUANGAN

MENGATUR - MENGAWASI - MELINDUNGI

UNTUK INDUSTRI KEUANGAN YANG SEHAT

BAB I - PENDAHULUAN

A. Latar Belakang

Perkembangan perbankan saat ini memberikan dan menawarkan kemudahan bagi nasabah melalui layanan operasional yang sangat beragam, termasuk layanan e-banking *(electronic banking)*. Layanan e-banking saat ini dimiliki oleh hampir semua Bank Umum yang ada, baik dengan jenis *delivery channel* yang sangat umum (seperti ATM) maupun dengan jenis *delivery channel* lainnya seperti SMS, telephone, EDC (*Electronic Data Capture*) dan internet. Hal tersebut juga sejalan dengan kecenderungan perkembangan media sosial maupun kebijakan yang ada untuk mewujudkan atau mengarahkan transaksi pada masyarakat dilakukan tidak melulu dengan uang tunai *(less cash society),* sehingga telah banyak pelaku ekonomi atau masyarakat yang memanfaatkan layanan perbankan modern yang lebih efisien dan efektif melalui e-banking.

Transaksi yang dilakukan melalui e-banking setiap tahun mengalami pertumbuhan yang cukup besar pada beberapa bank. Berdasarkan data13 bank besar di Indonesia, frekuensi transaksi melalui e-banking pada tahun 2012 sebanyak 3,79 Milyar transaksi dan dengan nilai nominal Rp. 4.441 Trilyun, bertambah menjadi sebanyak 4,73 Milyar transaksi dengan nilai nilai nominal Rp. 5.495 Trilyun pada tahun 2013, pada tahun 2014 meningkat

masing-masing menjadi 5,69 Milyar transaksi dengan nilai nominal Rp. 6.447 Trilyun.

Pertumbuhan tersebut berpotensi meningkat sejalan dengan kecenderungan layanan bank mengarah pada *digital banking*. Hal ini dikarenakan antara lain layanan e-banking memiliki fitur yang menarik dan nyaman digunakan serta memberi kemudahan bagi nasabah untuk melakukan transaksi keuangan seperti transfer antar-bank, pembayaran kartu kredit, pembayaran listrik, pembayaran telepon, pembayaran tagihan ponsel, pembayaran asuransi, pembayaran internet, pembayaran tiket penerbangan, dan *virtual account*. Selain itu semakin marak bisnis daring *(online shop)* serta pertumbuhan jenis dan jumlah *smartphone* yang semakin meningkat telah memberikan andil dalam pertumbuhan transaksi melalui e-banking.

Pertumbuhan e-banking yang didukung dengan perkembangan teknologi, media sosial dan pola hidup masyarakat memberikan manfaat bagi industri perbankan antara lain menghasilkan pendapatan dari *fee-based income,* mengurangi biaya transaksi, pengembangan bisnis, dan meningkatkan kepercayaan/loyalitas nasabah. Penggunaan e-banking juga memberikan kenyamanan dan kemudahan bertransaksi secara bebas, tidak terbatas oleh waktu dan lokasi , khusus untuk *internet banking*, layanannya dapat dinikmati oleh nasabah *anytime, anywhere, dan by any*

device. faktor keamanan perlu mendapatkan perhatian yang cukup untuk meminimalkan potensi penyalahgunaan atau fraud melalui e-banking. Sebagai contoh, meskipun layanan *internet banking* dapat dinikmati oleh nasabah *anytime*, anywhere, dan by *any device*, tetapi dilengkapi dengan OTP (*One Time Password*), yaitu kode yang hanya dapat diperoleh melalui perangkat tertentu yang dimiliki oleh nasabah dan *password*, yaitu sesuatu yang hanya diketahui oleh nasabah.

B. Tujuan

Buku ini menjelaskan dan menguraikan gambaran umum mengenai jenis-jenis dan manfaat layanan serta modus kejadian penyalahgunaan e-banking, sehingga buku ini diharapkan dapat digunakan oleh nasabah, bank maupun pengawas bank terkait dengan tujuan antara lain:

- Memberikan pemahaman yang memadai kepada nasabah dalam melakukan transaksi melalui e-banking sehingga dapat meningkatkan rasa aman dan nyaman bertransaksi di e-banking.
- Menyusun langkah-langkah pengamanan maupun memberikan edukasi yang memadai oleh bank untuk mendukung penggunaan e-banking sebagai sarana transaksi oleh nasabah.
- Memberikan pemahaman kepada pengawas bankatas permasalahan pada e-banking, serta sebagai referensi

untuk melakukan langkah pembinaan atas kelemahan dan permasalahan pada e-banking sehingga bank diharapkan dapat menentukan langkah pencegahannya (mitigasi).

Selain itu,materi buku ini juga tersedia di website resmi OJK sehingga *stakeholder* lainnya dapat memperoleh informasi dan manfaatnya.

Uraian dalam buku ini lebih dititikberatkan sebagai salah satu wujud dari proses mengedukasi dan melindungi konsumen pengguna jasa produk/aktivitas perbankan terkait dengan e-banking, serta sekaligus dapat pula dimanfaatkan sebagai salah satu referensi pelaksanaan prinsip kehati-hatian bagi industri perbankan dalam menyelenggarakan e-banking.

C. Cakupan

Cakupan penyusunan buku ini meliputi layanan e-banking dan permasalahannya yang terjadi pada industri perbankan di Indonesia maupun di luar Indonesia. Adapun layanan e-banking yang ada pada industri perbankan tersebut antara lain meliputi ATM (*Automated Teller Machine*), *internet banking*, *mobile banking*, *SMS banking*, kartu kredit, kartu debet, *phone banking*, EDC (*Electronic Data Capture*) dan *video banking*.

Mengatur
Mengawasi
Melindungi

Untuk Industri Keuangan yang Sehat

OTORITAS JASA KEUANGAN

MENGATUR - MENGAWASI - MELINDUNGI

UNTUK INDUSTRI KEUANGAN YANG SEHAT

BAB II - GAMBARAN UMUM

A. Gambaran Umum *Electronic Banking* (e-Banking)

Perkembangan pesat Teknologi Informasi (TI) dan globalisasi mendukung Bank untuk meningkatkan pelayanan kepada nasabah secara aman, nyaman, dan efektif, diantaranya melalui media elektronik atau dikenal dengan *Electronic Banking* (e-banking). E-banking merupakan layanan yang memungkinkan nasabah Bank untuk memperoleh informasi, melakukan komunikasi, dan melakukan transaksi perbankan melalui media elektronik seperti *Automatic Teller Machine* (ATM), *Electronic Data Capture* (EDC)/ *Point Of Sales* (POS), *internet banking, SMS banking, mobile banking, e-commerce, phone banking*, dan *video banking*.

E-Banking memberikan banyak manfaat baik bagi nasabah, bank, dan otoritas. Bagi nasabah, e-banking memberikan kemudahan bertransaksi dalam hal waktu, tempat, dan biaya. Nasabah tidak perlu mendatangi kantor bank untuk memperoleh informasi atau melakukan transaksi perbankan. Bahkan untuk beberapa produk e-banking nasabah dapat bertransaksi selama 24 jam dengan menggunakan *laptop* atau perangkat *mobile* seperti telepon seluler yang dapat dibawa kemana saja selama terhubung dengan jaringan internet dan/atau SMS.

Bagi bank, e-banking meningkatkan pendapatan berbasis komisi *(fee based income)* dan mengurangi biaya operasional apabila dibandingkan dengan pelayanan transaksi melalui kantor cabang yang relatif besar untuk membayar karyawan, sewa gedung, pengamanan, listrik, dan lainnya.

Bagi otoritas, perkembangan teknologi e-banking mendorong mewujudkan masyarakat *less cash society. Less cash* society adalah gaya hidup dengan menggunakan media transaksi atau uang elektronik dalam bertransaksi sehingga tidak perlu membawa uang fisik. *Less cash society* selain dapat meningkatkan sistem pembayaran yang cepat, aman, dan efisien, untuk mempercepat perputaran aktivitas ekonomi dan stabilitas sistem keuangan, juga dapat mencegah tindak pidana kriminal maupun tindak pidana pencucian uang.

Di bawah ini merupakan beberapa produk yang termasuk dalam layanan e-banking.

Automated Teller Machine (ATM)

Definisi

ATM atau yang lebih dikenal dengan nama Anjungan Tunai Mandiri merupakan suatu terminal/mesin komputer yang terhubung dengan jaringan komunikasi bank, yang memungkinkan nasabah

melakukan transaksi keuangan secara mandiri tanpa bantuan dari *teller* ataupun petugas bank lainnya.

Sesuai dengan perkembangan teknologi, saat ini bank juga telah menyediakan 3 tipe mesin ATM lainnya, yaitu: mesin ATM yang hanya melayani transaksi non tunai, mesin ATM yang melayani transaksi penyetoran uang tunai *Cash Deposit Machine* atau CDM, dan mesin ATM yang dapat melayani semua transaksi yang telah disebutkan di atas.

Selain di kantor bank, saat ini nasabah dapat dengan mudah menemukan mesin ATM di berbagai tempat, seperti restoran, pusat perbelanjaan, bandar udara, pasar, dan lokasi-lokasi strategis lainnya.

Fitur

Melalui ATM, nasabah bank dapat mengakses rekeningnya untuk melakukan berbagai transaksi keuangan, yaitu transaksi penarikan tunai dan transaksi non tunai, seperti pengecekan saldo, pembayaran tagihan kartu kredit, pembayaran tagihan listrik, pembelian pulsa, dan sebagainya.

Cara Kerja

Untuk menggunakan ATM, nasabah harus memiliki kartu ATM/ debit/kredit dan PIN. PIN adalah kode (4-6 digit) angka yang dibuat oleh nasabah saat pertama kali menerima kartu ATM di bank. Kode tersebut harus dijaga kerahasiannya oleh nasabah supaya kartu ATM tidak dapat disalahgunakan oleh orang lain.

Nasabah memasukkan kartu pada slot kartu di mesin ATM dengan memperhatikan sisi kartu yang harus dimasukkan terlebih dahulu, kemudian nasabah akan diminta untuk memasukkan PIN. Setelah itu nasabah dapat melakukan transaksi dengan memilih menu yang tertera pada layar monitor ATM.

Electronic Data Capture (EDC)

Definisi

EDC merupakan suatu perangkat/ terminal yang dapat digunakan untuk bertransaksi menggunakan kartu debit/kredit/prabayar di *merchant* atau toko. Terminal tersebut terhubung ke jaringan komputer bank. EDC terdiri dari alat pembaca informasi pada pita

magnetis kartu *(card's magnetic stripe)* atau *chip*, tombol menu dan angka untuk memasukkan jenis transaksi, nilai transaksi, dan PIN, layar untuk melihat jenis dan nilai transaksi, dan printer untuk mencetak bukti transaksi.

Fitur

Saat ini, EDC digunakan di banyak toko untuk memudahkan nasabah melakukan transaksi, bahkan EDC dapat digunakan untuk pembayaran telepon, listrik, pulsa, tiket pesawat, dan transaksi lainnya. Pada umumnya EDC terhubung ke sistem bank menggunakan jaringan telepon *fixed line*, namun untuk beberapa pusat perbelanjaan yang memiliki banyak mesin EDC, ada juga yang menggunakan jaringan *leased line*. Seiring dengan perkembangan teknologi selular, EDC juga dapat menggunakan jaringan dengan sistem GPRS *(wireless)*.

Selain ditransaksikan dengan cara digesek, ada juga EDC yang yang digunakan dengan cara menempelkan kartu pada mesin (*card tapping*) seperti yang digunakan untuk membayar parkir, tol, alat transportasi, dan lainnya.

Cara Kerja

Untuk menggunakan EDC, nasabah harus memiliki kartu debit, kartu kredit, atau kartu elektronik. Cara menggunakannya yaitu dengan menggesekkan/memasukkan kartu pada mesin

kemudian pegawai *merchant* menginputkan jumlah uang yang akan dibayarkan, setelahnya nasabah akan diminta untuk menginputkan PIN pada mesin atau menyertakan tandatangan sebagai pembuktian keaslian nasabah *(authentication)* pada struk yang dikeluarkan oleh EDC. Namun pada EDC yang berjenis *card tapping,* nasabah cukup menempelkan kartu pada EDC saat melakukan pembayaran dan tidak perlu menginputkan PIN atau tanda tangan.

Internet Banking

Definisi

Internet banking adalah layanan untuk melakukan transaksi perbankan melalui jaringan internet. Merupakan kegiatan perbankan yang memanfaatkan teknologi internet sebagai media untuk melakukan transaksi dan mendapatkan informasi lainnya

melalui *website* milik bank. Kegiatan ini menggunakan jaringan internet sebagai perantara atau penghubung antara nasabah dengan bank tanpa harus mendatangi kantor bank. Nasabah dapat menggunakan perangkat komputer *desktop, laptop, tablet*, atau *smartphone* yang terhubung ke jaringan internet sebagai penghubung antara perangkat nasabah dengan sistem bank.

Fitur

Fitur layanan *internet banking* antara lain informasi umum rekening tabungan/giro, rekening deposito, kartu kredit, informasi mutasi rekening, transfer dana, baik transfer antar rekening maupun antar bank, pembelian pulsa, pembelian tiket, penempatan deposito, layanan informasi seperti suku bunga dan kurs, dan pembayaran, misalnya pembayaran telepon, internet, kabel TV, asuransi, listrik dan berbagai jenis pembayaran lainnya.

Cara Kerja

Untuk menggunakan *internet banking*, nasabah harus memiliki *user id, password*, media token atau *One Time Password* (OTP), dan jaringan internet. *User id, password,* dan media token dapat diperoleh dengan mendaftarkan diri ke bank. Saat menggunakan *internet banking*, nasabah harus memastikan *website* yang diakses adalah *website internet banking* milik bank, kemudian nasabah akan diminta untuk memasukkan *user id* dan *password* pada halaman muka atau *login*. Pada saat melakukan transaksi

finansial, nasabah akan diminta untuk memasukkan sandi OTP yang diperoleh dari media token atau SMS. Setelah transaksi selesai, nasabah harus memastikan telah keluar/*log out* dari halaman *internet banking*. Bank mengirimkan notifikasi melalui *e-mail* sebagai bukti bahwa transaksi telah berhasil. Notifikasi *e-mail* ini juga sebagai pengendalian agar nasabah mengetahui jika akun *internet banking*-nya digunakan oleh orang lain.

SMS Banking

Definisi

SMS banking adalah layanan perbankan yang dapat diakses langsung melalui telepon selular/*handphone* dengan menggunakan media SMS *(Short Message Service)*.

Fitur

Fitur *SMS Banking* antara lain layanan informasi (saldo, mutasi rekening, tagihan kartu kredit, dan suku bunga); dan layanan transaksi, seperti transfer, pembayaran tagihan (listrik, air, pajak, kartu kredit, asuransi, internet), pembelian (pulsa, tiket), dan berbagai fitur lainnya.

Cara Kerja

Untuk dapat menggunakan *SMS Banking*, nasabah harus mendaftarkan diri dan mendaftarkan nomor ponsel terlebih dahulu ke bank serta mendapatkan *password*, kemudian nasabah dapat bertransaksi dengan cara mengetik SMS sesuai dengan format SMS yang telah ditentukan. Format SMS berbeda-beda berdasarkan format yang telah ditentukan oleh masing-masing bank, contohnya: untuk melakukan transfer, nasabah dapat mengetik : Transfer <rek_sumber><rek_tujuan><nominal><password>. Pesan ini kemudian dikirim ke nomor tujuan yang telah ditentukan bank. Untuk menggunakan fasilitas ini nasabah sebaiknya mempelajari petunjuk format SMS yang tertera pada buku petunjuk *SMS banking* atau *website* bank.

Mobile Banking

Definisi

Mobile banking merupakan layanan yang memungkinkan nasabah bank melakukan transaksi perbankan melalui ponsel atau *smartphone*. Layanan

mobile banking dapat digunakan dengan menggunakan menu yang sudah tersedia pada SIM *(Subscriber Identity Module)* Card, USSD *(Unstructured Suplementary Service Data),* atau melalui aplikasi yang dapat diunduh dan diinstal oleh nasabah. Mobile banking menawarkan kemudahan jika dibandingkan dengan SMS banking karena nasabah tidak perlu mengingat format pesan SMS yang akan dikirimkan ke bank dan juga nomor tujuan SMS banking.

Fitur

Fitur-fitur layanan *mobile banking* antara lain layanan informasi (saldo, mutasi rekening, tagihan kartu kredit, suku bunga, dan lokasi cabang/ATM terdekat); dan layanan transaksi, seperti transfer, pembayaran tagihan (listrik, air, pajak, kartu kredit, asuransi, internet), pembelian (pulsa, tiket), dan berbagai fitur lainnya.

Cara Kerja

Untuk menggunakan *mobile banking*, nasabah harus mendaftarkan diri terlebih dahulu ke bank untuk mendapatkan *password*. Nasabah dapat memanfaatkan layanan mobile banking dengan cara mengakses menu yang telah tersedia pada *SIM Card* atau aplikasi yang terinstal di ponsel. Apabila nasabah menggunakan *mobile banking* melalui menu yang telah tersedia pada *SIM Card*, nasabah dapat memilih menu sesuai kebutuhan

kemudian nasabah akan diminta untuk menginputkan *PIN SMS Banking* saat menjalankan transaksi. Sedangkan apabila nasabah menggunakan *mobile banking* melalui aplikasi yang terinstal di ponsel, nasabah harus mengunduh dan menginstal aplikasi pada telepon seluler terlebih dahulu. Pada saat membuka aplikasi tersebut, nasabah harus memasukkan *password* untuk *login*, kemudian nasabah dapat memilih menu transaksi yang tersedia dan diminta memasukkan PIN saat menjalankan transaksi.

Electronic Commerce (e-Commerce)

Definisi

E-commerce atau perdagangan elektronik merupakan penyebaran, pembelian, penjualan, pemasaran barang dan jasa melalui sistem elektronik seperti internet atau televisi. Melalui *e-commerce*, pembeli dan penjual dapat melakukan transaksi secara *online.*

Jenis-jenis *e-commerce* antara lain:

a. *E-commerce* yang menggunakan sosial media atau forum untuk berjualan, namun transaksi tidak diselesaikan melalui *website* tersebut namun biasanya akan berkomunikasi secara langsung untuk bertransaksi.
b. *E-commerce* yang proses jual belinya dilakukan melalui *website* si penjual.

c. *E-commerce* yang proses jual belinya dilakukan di "lapak" *online*. Penjual bukanlah penyedia *website*, melainkan anggota-anggota yang mendaftar untuk berjualan di lapak *online* yang telah tersedia. Setiap transaksi yang terjadi pada lapak *online* tersebut, pengelola lapak akan menjadi pihak ketiga yang menerima pembayaran dan menjamin barang diterima oleh pembeli, lalu uang pembayaran akan diteruskan ke pihak penjual.

Fitur

Melalui *e-commerce*, masyarakat dapat melakukan jual beli, contohnya pembelian buku, alat elektronik, pakaian, kendaraan, bahkan rumah secara *online*. Pembayaran yang dilakukan pada saat bertransaksi secara *online* dapat menggunakan kartu kredit, debit, atau dengan menggunakan alat pembayaran *virtual* seperti *paypal.*

Cara Kerja

Untuk bertransaksi secara *online*, pembeli harus memiliki jaringan internet, alat pembayaran seperti kartu kredit, kartu debit, atau akun pembayaran *virtual*. Alur proses *e-commerce* pada umumnya

adalah sebagai berikut, pengguna mengakses *website* penjualan produk, melakukan pemesanan, menerima tagihan elektronik, kemudian pembeli dapat melakukan pembayaran secara elektronik. Beberapa perusahaan kartu kredit saat ini bekerjasama dengan perusahaan *internet security* untuk membuat standar enkripsi khusus demi keamanan bertransaksi, walaupun demikian nasabah diharapkan tetap menjaga keamanan bertransaksi misalnya dengan memperhatikan keamanan jaringan saat akan melakukan transaksi, memastikan perangkat dilengkapi dengan *antivirus, anti malware, firewall*, dan me-*review rating* si penjual sebelum melakukan transaksi *online.*

Phone Banking

Definisi

Phone Banking adalah layanan untuk bertransaksi perbankan atau mendapatkan informasi perbankan lewat telepon dengan menghubungi nomor layanan pada bank. Layanan tersebut antara lain bertujuan memberikan kemudahan kepada nasabah dalam melakukan berbagai transaksi perbankan melalui telepon. Nasabah tidak perlu lagi datang

ke bank atau mesin ATM untuk melakukan berbagai transaksi tersebut. Layanan *phone banking* ini merupakan salah satu dari perkembangan teknologi *call center.* Pada umumnya layanan *phone banking* dapat diakses selama 24 jam sehingga nasabah dapat menggunakannya dimana saja dan kapan saja.

Fitur

Fitur *phone banking* antara lain informasi perbankan misalnya informasi suku bunga, kurs, info produk bank, lokasi ATM dan kantor cabang, transaksi perbankan misalnya informasi saldo, pembayaran tagihan listrik, telepon pasca bayar, kartu kredit, pemindahbukuan, transfer antar bank, pembelian isi ulang pulsa, mutasi rekening, perubahan PIN dan data nasabah.

Cara Kerja

Phone banking dapat diakses oleh nasabah maupun non-nasabah bank untuk informasi umum bank. Bagi nasabah yang ingin menggunakan layanan *phone banking* dapat mendaftarkan diri terlebih dahulu ke bank untuk mendapatkan PIN *phone banking*. Setelah itu nasabah dapat menghubungi nomor *phone banking* bank dan nasabah akan dilayani oleh pegawai bank maupun IVR (*Interactive Voice Response*). IVR adalah teknologi yang dapat mendeteksi suara dan penekanan tombol telepon kemudian meresponnya kembali dalam bentuk suara atau media lain.

Video Banking

Definisi

Video Banking merupakan teknologi yang memungkinkan nasabah melakukan aktivitas perbankan jarak jauh menggunakan suatu perangkat khusus yang disediakan oleh bank yang memungkinkan nasabah berkomunikasi *audio visual* dengan petugas bank, menginput data, mencetak *statement*, dan mengeluarkan kartu baru. Pada umumnya bank menyediakan layanan *video banking* di lokasi-lokasi strategis seperti pusat perbelanjaan pada hari kerja maupun Sabtu dan Minggu. Jam operasionalnya pun lebih lama daripada jam operasional pelayanan melalui kantor bank.

Fitur

Fitur *video banking* di Indonesia pada saat ini antara lain pembukaan rekening, informasi produk, tarik dan setor tunai, transfer dana, pembelian pulsa, dan pembayaran tagihan seperti kartu kredit, listrik, dan telepon.

Cara Kerja

Untuk menggunakan layanan *video banking*, nasabah dapat mendatangi gerai perbankan digital yang menyediakan layanan ini. Selama bertransaksi nasabah akan dipandu oleh petugas bank, misalnya untuk melakukan pembukaan rekening baru melalui *video banking*, nasabah akan diminta untuk *memasukkan* data, *scan* kartu identitas, setoran awal, hingga cetak kartu sambil bertatap muka dan berkomunikasi dengan *customer service* bank melalui layar *video*.

B. Regulasi oleh Otoritas

Perbankan di Indonesia saat ini telah mengikuti perkembangan teknologi informasi dan komunikasi. Perkembangan ini ditandai dengan pesatnya penggunaan *electronic banking* (e-banking) untuk mendukung operasional kegiatan perbankan dan memudahkan nasabah melakukan transaksi.Walaupun demikian, penggunaan teknologi informasi tersebut perlu memperhatikan risiko yang dihadapi bank dan nasabah sehingga bank harus selalu menerapkan manajemen risiko teknologi informasi (TI) secara efektif.

Pengaturan dan pengawasan bank, khususnya manajemen risiko TI saat ini dilaksanakan oleh Otoritas Jasa Keuangan (OJK) sebagai lembaga pengawas industri jasa keuangan terpercaya, melindungi kepentingan konsumen dan masyarakat. Penerapan manajemen risiko TI bank diatur dalam PBI No.9/15/PBI/2007 tentang Penerapan Manajemen Risiko dalam Penggunaan

Teknologi Informasi dan SE No.9/30/DPNP perihal Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi Bank Umum. Beberapa hal yang diatur misalnya dalam kegiatan e-banking, bank wajib melaporkan rencana dan realisasi penerbitan produk e-banking yang bersifat transaksional dan harus memberikan edukasi kepada nasabah mengenai produk e-banking dan pengamanannya secara berkesinambungan. Pengaturan dan pengawasan terkait produk e-banking juga meliputi manajemen bank, kebijakan dan prosedur, penilaian risiko, mitigasi risiko, dan pengendalian pengamanan terkait e-banking.

C. Perkembangan Aktivitas E-banking Beberapa Bank di Indonesia

Penggunaan e-banking di Indonesia, baik dari jumlah nasabah pengguna transaksional, jumlah frekuensi e-banking dari tahun 2012 s/d 2014 secara umum meningkat. Peningkatan ini terjadi pada beberapa produk, misalnya *internet banking, mobile banking, SMS banking*, dan *phone banking*.

Jumlah Pengguna e-Banking Posisi 31 Desember 2014

Kartu Debit/ATM	82,006,699
Kartu Kredit	5,771,002
Kartu e-Money	9,788,145
Pengguna e-Money Berbasis Server	44,691
Pengguna *Internet Banking*	8,507,458
Pengguna *Mobile Banking*	14,738,817

Tabel 2.1 Perkembangan Frekuensi Transaksi e-banking di Beberapa Bank di Indonesia

Jenis Delivery Channel	*Frekuensi*				
	2012	*2013*	*2014*	*Perkembangan 2012 - 2013*	*Perkembangan 2013 - 2014*
ATM	*2,933,467,577*	*3,609,206,816*	*4,179,631,965*	*23.04%*	*15.80%*
EDC	*366,350,819*	*446,148,695*	*542,400,709*	*21.78%*	*21.57%*
Internet Banking	*235,957,566*	*311,880,376*	*437,798,960*	*32.18%*	*40.37%*
SMS /Mobile Banking	*224,876,666*	*325,550,038*	*473,196,941*	*44.77%*	*45.35%*
E-Commerce/ Merchant On-line	*2,790,843*	*3,707,515*	*7,778,488*	*32.85%*	*109.80%*
Phone Banking	*1,375,460*	*1,401,841*	*1,393,737*	*32.85%*	*-0.58%*
Video Banking	*7.684*	*16.418*	*28,097*		
Total Frekuensi Transaksi	*3,790,718,984*	*4,732,508,750*	*5,686,467,993*	*24,84%*	*20.16%*

Tabel 2.2 Perkembangan Nilai Transaksi e-banking di Beberapa Bank di Indonesia

Jenis *Delivery Channel*	Nilai Transaksi (dalam Milyar Rupiah)				
	2012	2013	2014	Perkembangan 2012 – 2013	Perkembangan 2013 – 2014
ATM	3,141,654	3,830,457	4,392,238	21.92%	14.67%
EDC	266,242	337,698	406,401	26.84%	20.34%
Internet Banking	669,607	860,546	1,062,820	28.52%	23.51%
SMS / Mobile Banking	343,441	437,853	544,371	27.49%	24.33%
E-Commerce/ Merchant On-line	5,514	10,849	16,134	96.76%	48.71%
Phone Banking	2,430	2,307	3,281	-5.05%	42.23%
Video Banking			104		
Total Nilai Transaksi	4,441,438	5,495,048	6,446,594	23.72%	17.32%

Mengatur
Mengawasi
Melindungi

Untuk Industri Keuangan yang Sehat

OTORITAS JASA KEUANGAN

MENGATUR - MENGAWASI - MELINDUNGI

UNTUK INDUSTRI KEUANGAN YANG SEHAT

BAB III –BIJAK DALAM MENGGUNAKAN LAYANAN E-BANKING

Electronic banking menawarkan berbagai kemudahan bagi nasabah, namun di sisi lain memiliki risiko yang harus diwaspadai. Berikut ini adalah beberapa contoh penyalahgunaan e-banking pada industri perbankan di Indonesia, termasuk di luar negeri 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:

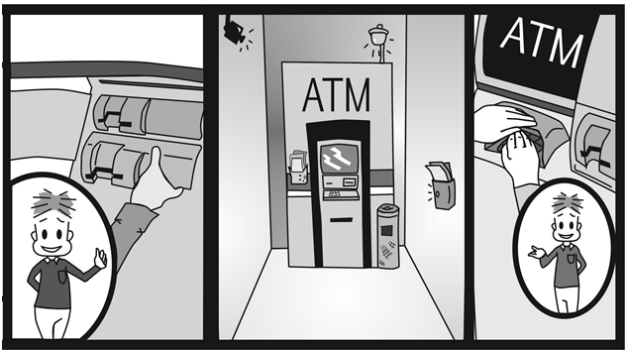
Delivery Channel	Media	Modus
ATM	Kartu, PIN, Mesin ATM.	- *Skimming* (menggunakan *skimmer*) - *Card Trapping* - *Card And PIN Sharing* - *Social Engineering* - *Call Center* palsu - Pencurian Data Kartu
EDC	Kartu, PIN, EDC, *Card Reader*.	- *Skimming* (menggunakan *skimmer*) - *Card Intercept* - Penggunaan *Card Reader Ilegal* - Pencurian Kartu/Data kartu - Gesek Tunai

Delivery Channel	Media	Modus
Internet Banking	User ID, Password, Token, Akun Medsos.	- P*hishing,* - *Man/Malware In The Browser (MIB)/* Sinkronisasi *Token* - *Typosite* - *Keylogger*
SMS Banking	PIN, Nomor Ponsel.	- Pencurian Ponsel, - Pembajakan Nomor Ponsel, - Ponsel digunakan oleh orang lain
Mobile Banking	PIN, Nomor Ponsel.	- Pencurian Ponsel - Pembajakan Nomor Ponsel - Clonning Nomor Ponsel
E-commerce	Data Kartu (Nomor Kartu, Masa Berlaku , Nama pada Kartu, CVV)	- *Carding*
Phone Banking	Nomor Rekening, PIN.	- *Call Center* palsu, - Menebak PIN Berulang-ulang.
Video Banking	Kartu Identitas, Penampakan Fisik.	- *Booth Video Banking* palsu.

A. ATM (*AUTOMATED TELLER MACHINE*)

CARD SKIMMING

Card Skimming adalah tindakan pencurian data kartu ATM dengan cara menyalin (membaca dan menyimpan) informasi yang terdapat pada strip magnetis secara ilegal. Strip magnetis adalah garis lebar hitam yang berada dibagian belakang kartu ATM. Fungsinya seperti pita kaset untuk menyimpan data nomor kartu, masa berlaku, dan nama nasabah. *Card skimming* dilakukan menggunakan alat pembaca kartu (*card skimmer*) yang ditempatkan pada slot kartu di mesin ATM.



Dalam *card skimming,* pelaku berusaha mendapatkan **data kartu** dan **PIN,** antara lain dengan cara:

1. Pelaku memasang alat *skimmer* pada mesin ATM;
2. Nasabah memasukkan kartu ke mesin ATM yang dipasangi alat *skimmer*, sehingga data kartu nasabah terbaca dan tersimpan pada alat tersebut;
3. Pelaku berusaha mendapatkan PIN ATM dengan cara mengintip tombol yang ditekan oleh nasabah atau dapat juga menggunakan kamera kecil yang dipasang oleh pelaku di mesin ATM;
4. Pelaku membuat kartu palsu menggunakan data yang telah diperoleh dan bertransaksi menggunakannya PIN yang telah diketahui (terekam).

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

- Memperhatikan kondisi mesin ATM sebelum digunakan. *Card Skimmer* seringkali tidak terlihat secara kasat mata karena warna dan bentuknya telah disesuaikan dengan mesin ATM;
- Hati-hati sebelum menekan tombol PIN. Usahakan agar tombol yang ditekan tidak terlihat oleh orang lain. Nasabah juga perlu mencermati adanya kamera yang dapat merekam tombol PIN yang ditekan oleh nasabah;
- Hindari menggunakan PIN yang mudah ditebak oleh orang lain, seperti tanggal lahir, nomor telepon, dan nomor kartu;

- Mengganti nomor PIN secara periodik, terutama jika ada indikasi bahwa PIN telah diketahui oleh orang lain.

CARD TRAPPING

Gbr. Contoh nomor call center palsu

Card trapping adalah mengambil fisik kartu dengan menggunakan suatu benda asing, seperti korek api, lidi, plastik, karet, benang, atau lem yang dipasang pada slot kartu di mesin ATM.

Dalam *card trapping*, pelaku berusaha mendapat fisik kartu dan PIN, antara lain dengan cara:

1. Pelaku memasang benda asing ke dalam slot kartu di mesin ATM.
2. Saat nasabah menggunakan mesin ATM tersebut, maka kartu ATM akan tersangkut oleh benda asing yang dipasang oleh pelaku, tidak dapat masuk maupun keluar.
3. Pelaku berusaha mendapatkan PIN nasabah dengan beberapa cara, misalnya:

- berpura-pura menawarkan bantuan dan meminta nasabah memasukkan PIN ke dalam mesin ATM. Pelaku memperhatikan dan mengingat nomor PIN nasabah;
- meminta nasabah untuk menghubungi *call center* palsu, lalu nasabah akan diminta menyebutkan PIN oleh petugas *call center* palsu tersebut; atau
- menggunakan kamera kecil yang dipasang oleh pelaku di mesin ATM.

4. Pelaku mengambil kartu ATM nasabah yang tersangkut di mesin ATM setelah nasabah meninggalkan mesin ATM. Modus lainnya untuk mendapatkan kartu nasabah, biasanya pelaku mendatangi nasabah di mesin ATM dan menawarkan bantuan, sementara pelaku lainnya akan mengalihkan perhatian nasabah, misalnya dengan menjatuhkan koin dan lain-lain. Selanjutnya, pelaku dengan cepat akan menukar kartu ATM nasabah dengan kartu ATM palsu yang sudah disediakan pelaku. Pelaku mendapatkan PIN nasabah dengan cara yang sama pada langkah sebelumnya.
5. Pelaku menggunakan kartu ATM dan PIN nasabah untuk mengambil tunai di mesin ATM atau transfer ke rekening lain.

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

- Memperhatikan kondisi mesin ATM sebelum digunakan. Nasabah perlu memperhatikan kondisi mesin ATM, sebelum

bertransaksi. Apabila terdapat hal yang tidak biasa seperti terdapat benda asing pada slot kartu ATM, nasabah hendaknya tidak melanjutkan bertransaksi, dan melaporkan hal tersebut melalui *call center* bank;

- Tidak panik. Nasabah tidak perlu panik saat kartu ATM tidak dapat masuk kedalam mesin ATM. Apabila terdapat seseorang yang menawarkan bantuan, sebaiknya nasabah tidak perlu melanjutkan transaksi;
- Mencari alternatif mesin ATM di lokasi lain;
- Tidak menginformasikan nomor PIN kepada orang lain, termasuk kepada petugas bank; dan
- Mewaspadai orang sekitar, jangan mudah percaya kepada orang yang tidak dikenal.

CALL CENTER 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:
   - Menyebutkan data rahasia nasabah, seperti seperti PIN, nomor kartu kredit, masa berlaku kartu kredit, dan kode pengaman kartu kredit atau *Card VerificationValue* (CVV).
   - 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:

- 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;

- Mencatat nomor telepon *call center* pada media lain, misalnya di ponsel atau catatan lainnya sehingga nasabah dapat menghubungi *call center* bank pada saat dibutuhkan; dan
- Tidak menginformasikan nomor PIN. Nasabah harus selalu merahasiakan nomor PIN, tidak memberitahukan kepada orang lain termasuk kerabat dekat dan pegawai bank atau *call center*.

PENCURIAN DATA KARTU

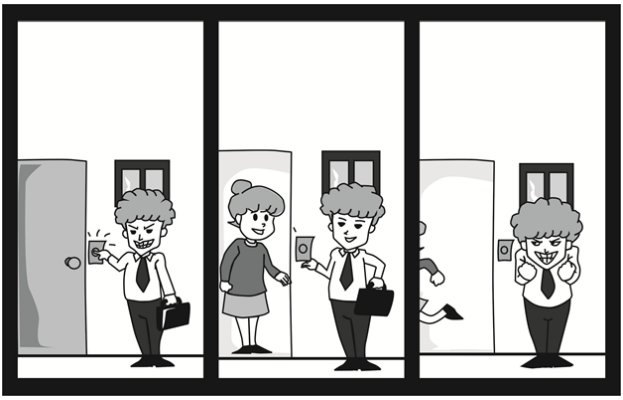
Pencurian data kartu (ATM/debit/kredit) dapat terjadi ketika nasabah berhadapan dengan petugas *marketing* palsu, menggunakan mesin EDC palsu (*dummy* EDC), atau menggunakan mesin ATM palsu (*dummy* ATM). Pelaku pencurian data kartu berusaha mendapatkan data nomor kartu kredit (atau data kartu debit yang menjadi *member principal* kartu kredit), masa berlaku kartu debit/kredit, dan kode pengaman kartu debit/kredit (CVV).

Dalam melakukan pencurian data kartu, pelaku melakukan hal-hal antara lain:

A. Petugas *marketing* palsu

1. Pelaku membuka kios sementara *(booth)* yang dilengkapi dengan spanduk *(banner)*, tanda pengenal, dan seragam yang mirip dengan bank tertentu.

2. Menawarkan produk bank, misalnya kartu kredit dan meminta nasabah:
   - menyerahkan kartu identitas dan/atau kartu kredit untuk difotokopi atau diambil oleh petugas dan menjanjikan penggantian dengan kartu kredit yang baru.
   - Mengisi formulir yang berisi data-data pribadi nasabah.
3. Pelaku dapat juga mendatangi nasabah ke rumah/kantor/ tempat usaha, menawarkan produk bank dengan modus seperti disebutkan pada nomor 2.



Hal-hal yang dapat dilakukan untuk meminimalisir pencurian data kartu, antara lain:

- Memastikan keaslian kios sementara (*booth*), spanduk (*banner*), tanda pengenal, dan seragam yang dikenakan oleh petugas *marketing*. Jika meragukan keasliannya, jangan lakukan transaksi, membuka rekening, atau memberikan data kartu kepada petugas kios sementara tersebut;
- Menghubungi layanan resmi atau kantor bank jika ingin mendaftar produk/layanan bank; dan
- Tidak memberikan fisik kartu atau fotokopi kartu kredit kepada pihak manapun, termasuk petugas bank.

B. Mesin EDC/ATM palsu

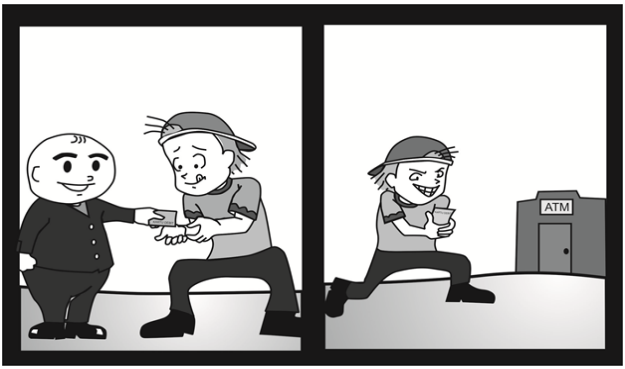
Pelaku memasang mesin EDC dan/atau ATM palsu di tempat umum. Pada saat nasabah menggunakan mesin tersebut, data kartu dan PIN nasabah akan terekam. Selanjutnya pelaku membuat kartu palsu menggunakan data yang telah diperoleh dan bertransaksi menggunakannya PIN yang telah diketahui (terekam).

Hal-hal yang dapat dilakukan untuk meminimalisir pencurian data kartu, antara lain:

- Mengamati mesin EDC/ATM sebelum digunakan. Jika ada kejanggalan (misalnya logo tidak sesuai atau tampilan layar tidak lazim) sebaiknya tidak menggunakan mesin tersebut;

- Segera mengganti PIN pada mesin lain yang resmi jika nasabah sudah terlanjur menggunakan mesin EDC/ATM palsu tersebut; dan
- Menginformasikan kepada bank jika menemukan adanya kejanggalan pada mesin EDC/ATM.

MEMINJAMKAN KARTU DAN PIN KEPADA ORANG LAIN



Nasabah harus memperlakukan kartu dan PIN sebagai sesuatu yang bersifat pribadi dan rahasia. Kartu dan PIN yang diberikan kepada orang lain, dapat disalahgunakan untuk bertransaksi di luar pengetahuan nasabah. Banyak kejadian pembobolan rekening nasabah oleh orang dekat seperti keluarga atau orang lain yang dipercaya oleh nasabah.

Hal-hal yang dapat dilakukan untuk meminimalisir risiko ini, antara lain:

- Nasabah hendaknya tidak meminjamkan kartu ATM dan/atau memberitahukan PIN kepada orang lain, sekalipun kepada keluarga, teman dekat, atau petugas bank; dan
- Hindari mencatat PIN dimanapun, termasuk di ponsel, dompet, buku, tempelan dinding, dll.

SOCIAL ENGINEERING

Social engineering adalah upaya yang memanfaatkan pendekatan sosial untuk mendapatkan data rahasia nasabah atau meminta nasabah melakukan sesuatu yang menguntungkan pelaku, seperti transfer uang, pembayaran tagihan, dan pembelian pulsa.

Dalam *social engineering,* pelaku menggunakan beberapa cara, antara lain:

1. Pelaku mengirimkan pesan melalui SMS, *e-mail*, atau media lain yang berisi pengumuman pemenang hadiah dan meminta nasabah untuk menghubungi nomor telepon atau membuka *website* tertentu;
2. Pelaku memandu nasabah untuk:
   - memberikan informasi rahasia seperti PIN, nomor kartu kredit, masa berlaku kartu kredit, dan kode pengaman kartu kredit (CVV, yaitu 3 angka yang tertera di belakang kartu); atau

- datang ke mesin ATM, menggunakan *internet banking*, atau menggunakan e-banking lainnya, dan melakukan transaksi transfer, pembelian, atau pembayaran yang menguntungkan pelaku tanpa disadari oleh nasabah.

Hal-hal yang dapat dilakukan untuk meminimalisir risiko *social engineering*, antara lain:

- Nasabah hendaknya tidak mudah tergoda dengan tawaran hadiah yang disampaikan melalui telepon, SMS, *e-mail*, atau media sosial;
- Mencari informasi ke sumber lain yang terpercaya untuk memastikan kebenaran informasi yang diterima;
- Tidak memberikan informasi rahasia seperti PIN, nomor kartu kredit, masa berlaku kartu kredit, dan kode CVV kepada orang lain.

B. EDC (*ELECTRONIC DATA CAPTURE*)

CARD SKIMMING

Seperti pada ATM, *card skimming* juga dapat terjadi pada transaksi melalui mesin EDC. Modus *card skimming* pada ATM dan EDC sedikit berbeda, pada ATM alat *skimmer* akan dilekatkan pada mesin ATM yang resmi, sedangkan pada EDC alat *skimmer*

terpisah dari mesin EDC yang resmi. Pelaku akan melakukan *double swipe* yaitu menggesek kartu nasabah pada mesin EDC Bank dan alat *skimmer* yang sudah disiapkan, seringkali alat *skimmer* tersebut dilekatkan pada mesin kasir milik *merchant.*

Hal-hal yang dapat dilakukan untuk meminimalisir bahaya *skimming* pada saat transaksi menggunakan mesin EDC, antara lain :

- Jangan serahkan kartu kepada pelayan tanpa didampingi. Seringkali nasabah lengah dengan memberikan kartu kepada pelayan untuk bertransaksi menggunakan mesin EDC, hal ini memungkinkan pelayan atau kasir menggesek kartu nasabah di mesin *skimmer* tanpa disadari oleh nasabah;
- Awasi pada saat kasir menggesek kartu. Nasabah harus mengawasi aktifitas kasir, pastikan bahwa kartu hanya digesekkan di mesin EDC resmi milik bank. Penggesekan kartu untuk transaksi perbankan hanya dilakukan sekali yaitu pada mesin EDC milik bank. Hal yang umum saat ini, kartu nasabah digesekkan dua kali yaitu pada mesin EDC dan mesin kasir untuk mencetak nama pembeli pada struk pembelian pada mesin *cash register* milik *merchant,* nasabah

harus berhati-hati dan berhak menolak untuk menggesekkan kartu di mesin kasir dengan alasan keamanan data; dan

- Hati-hati sebelum menekan nomor PIN di mesin EDC. Meskipun tidak seorangpun memperhatikan ketika nasabah memasukkan PIN, nasabah harus tetap berhati-hati kemungkinan adanya kamera tersembunyi. Akan lebih baik apabila dalam setiap menekan PIN, nasabah menutup dengan tangan.

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.

Hal-hal 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;
- Pastikan kartu yang dikembalikan oleh kasir setelah transaksi

adalah kartu yang benar. Nasabah harus mengecek kartu yang dikembalikan oleh kasir setelah bertransaksi adalah kartu yang benar. Sebaiknya nasabah menghapal atau mencatat nomer kartu ATM (minimal 4 digit terakhir) untuk memastikan kartu tidak tertukar atau ditukar dengan sengaja pada saat transaksi.

PENGGUNAAN *CARD READER ILEGAL*

Modus penggunaan *card reader ilegal* adalah tindakan pencurian saldo yang ada pada kartu *e-money* melalui proses *tapping* secara diam-diam oleh oknum *merchant* dengan menggunakan *card reader* atau mesin EDC yang bekerja dalam kondisi *online* maupun *offline*. Pelaku yang sudah dilengkapi dengan peralatan tersebut secara diam-diam (pada jarak tertentu yang memungkinkan terjadinya transaksi) melakukan *tapping* kepada calon korban, atau dilakukan secara acak tanpa disadari oleh korban dengan tujuan mengurangi saldo yang ada di dalam kartu *e-money* dalam jumlah tertentu sesuai keinginan pelaku. Saldo yang telah diambil tersebut baik secara otomatis ataupun tidak (bergantung kondisi *on-line/off-line* pada EDC), akan masuk ke dalam rekening pelaku.

Hal-hal yang dapat dilakukan untuk meminimalisir bahaya penggunaan *card reader ilegal*:

- Menyimpan kartu *e-money* dengan aman. Menjaga dan menempatkan kartu *e-money* di tempat yang memiliki penghalang memadai untuk menghindari *tapping;* dan
- Mengecek saldo kartu *e-money* setiap kali selesai melakukan suatu transaksi, untuk memastikan jumlah saldo berkurang secara wajar. Apabila nasabah menemukan saldo berkurang secara tidak wajar segera laporkan kepada bank penerbit untuk diketahui penyebabnya.

PENUKARAN (PENGAMBILAN) KARTU OLEH PETUGAS *MARKETING* PALSU

Penukaran atau pengambilan kartu dilakukan ketika nasabah pemilik kartu ditawari oleh petugas *marketing* palsu untuk melakukan penggantian kartu. Pelaku berusaha untuk mendapatkan kartu kredit nasabah, dengan cara sebagai berikut:

1. Pelaku membuka kios sementara *(booth)* dilengkapi dengan spanduk *(banner),* tanda pengenal, dan seragam yang mirip dengan bank tertentu atau dapat juga mendatangi nasabah ke rumah/kantor/tempat usaha.
2. Pelaku menjanjikan promo *upgrade* jenis kartu dari segi *limit*, jenis kartu, dan keuntungan lainnya.
3. Nasabah pemilik kartu menyerahkan kartu kredit yang dimiliki kepada *marketing* palsu.

4. Pelaku menggunakan kartu tersebut untuk bertransaksi atau penarikan tunai.

Hal-hal yang dapat dilakukan untuk menghindari penukaran kartu oleh petugas *marketing* palsu, antara lain :

- Memastikan keaslian kios sementara *(booth),* spanduk *(banner),* tanda pengenal dan seragam yang dikenakan oleh petugas *marketing*;
- Melakukan konfirmasi ke bank penerbit apabila menerima tawaran promo dari *marketing*;
- Menghubungi layanan/konter resmi jika ingin melakukan *upgrade* kartu; dan
- Tidak memberikan fisik kartu dan PIN kepada pihak manapun, termasuk petugas bank.

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 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.

KARTU HILANG

Nasabah pemegang kartu debit dan/atau kartu kredit dapat mengalami kehilangan kartu debit dan/atau kartu kredit. Kejadian kehilangan kartu tersebut dapat disebabkan kelalaian nasabah maupun disebabkan suatu tidak kejahatan yang dilakukan kepada nasabah, misalnya penjambretan, pencurian, dan penipuan.

Saat ini, penggunaan kartu debit dan/atau kartu kredit untuk berbelanja pada *merchant* memungkinkan dilakukan tanpa PIN, cukup dengan menandatangani struk transaksi. Kartu yang memungkinkan bertransaksi menggunakan tanda tangan adalah kartu debit dan kartu kredit yang tergabung dalam jaringan Visa

dan Mastercard. Oleh karena itu, meskipun nasabah tidak pernah mengungkapkan PIN kepada siapapun, tidak pernah menuliskan PIN pada kartu, ataupun merasa hanya nasabah tersebut saja yang mengetahui PIN kartu tersebut, risiko terhadap penggunaan kartu debit dan/atau kartu kredit tersebut oleh pihak yang tidak berwenang masih tetap ada.

Dalam kejadian nasabah kehilangan kartu, pelaku akan mencoba menggunakan kartu nasabah yang hilang, antara lain dengan cara:

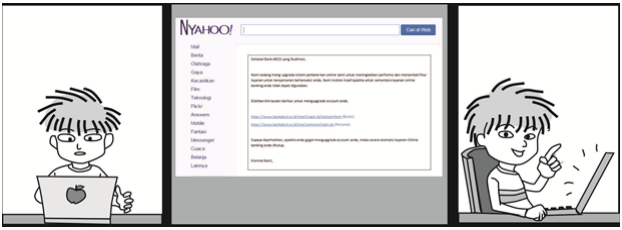
1. Pelaku mendapatkan kartu nasabah yang hilang. Apabila pada bagian belakang kartu terdapat tanda tangan nasabah, pelaku akan mencoba untuk menirukan tanda tangan tersebut untuk bertransaksi. Apabila pada bagian belakang kartu tidak terdapat tanda tangan nasabah, pelaku akan membiarkan tetap kosong atau dapat saja pelaku menandatangani bagian belakang kartu dengan tanda tangan palsu.
2. Pelaku akan bertransaksi (baik untuk membeli barang atau melakukan gesek tunai) melalui *merchant* yang tidak terlalu ketat dalam melakukan verifikasi tanda tangan pada kartu debet dan/kartu kredit. Selain itu, pelaku biasa mencari *merchant* yang tidak diawasi CCTV.

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

- Segera melaporkan kehilangan kartu dan melakukan blokir rekening untuk kartu-kartu yang hilang melalui kantor atau *call center* bank.
- Nasabah menjaga kartu dengan baik, dan jangan letakkan kartu pada sembarang tempat khususnya di tempat umum;
- Mengecek transaksi terakhir yang dilakukan melalui kartu yang hilang tersebut, pengecekan dapat dilakukan menggunakan fasilitas *internet banking, mobile banking, phone banking,* atau datang ke kantor bank; dan
- Melaporkan kejadian kehilangan kartu dan meminta surat keterangan kehilangan kartu kepada kepolisian.

C. INTERNET BANKING

PHISHING



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.

Selain ketiga hal di atas, suatu *phishing* dapat juga ditandai dengan adanya kesalahan ketik dan gaya bahasa yang kurang baik. Pesan *phishing* biasanya tidak melalui proses *review* dan *editing* yang baik, bahkan tidak jarang berupa terjemahan kasar dari bahasa asing. 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. Sebagai contoh, pelaku akan mengirimkan pesan bahwa saat ini sedang terjadi pemeliharaan *server* untuk transaksi *internet banking* sehingga nasabah diminta untuk memasukkan data-data sensitif dan penting. Apabila nasabah tidak memasukkan, maka rekening nasabah tersebut akan menjadi tidak aktif dan tidak dapat digunakan.

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

- 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.
- Menggunakan *anti virus* yang terkini.
- Jangan mengklik *link* apapun pada pesan (*e-mail*) yang terindikasi *phishing*.
- Mengkonfirmasikan kepada pihak bank melalui *call center* yang resmi jika ada permintaan yang mencurigakan.
- 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.
- Hati-hati mengunduh *attachment e-mail* karena dapat berisi *virus/malware* yang dapat mencuri data sensitif.

MAN/MALWARE IN THE BROWSER (MIB)

MIB adalah teknik pembobolan rekening *internet banking* dengan memanfaatkan *software* jahat (*malware*) yang telah menginfeksi *browser internet* nasabah. *Malware* tersebut dapat melakukan beberapa hal sesuai keingingan pembuatnya, misalnya:

- Mencuri data *user ID* dan *password* nasabah,
- Mengambil alih koneksi nasabah ke bank lalu memasukkan transaksi pemindahbukuan/transfer dari rekening nasabah ke rekening pelaku, dan
- Mengganti halaman *web* di *browser* nasabah sesuai keinginan pelaku.

Dalam melakukan MIB, pelaku menggunakan beberapa langkah, antara lain:

- Menyediakan program *malware* pada alamat *web* tertentu. Jika nasabah membuka *web* atau mengunduh sesuatu (*software*, gambar, *video*, dll) dari *web* tersebut, maka *malware* akan masuk ke komputer nasabah.
- Setelah *malware* terinstal di komputer nasabah, *malware* tersebut merekam apa saja yang diketik oleh nasabah sehingga pelaku bisa mendapatkan data *user ID* dan *password internet banking* nasabah.
- *Malware* mengambil alih koneksi *internet banking* milik nasabah lalu memasukkan transaksi sesuai keinginan pelaku, misalnya transfer dari rekening nasabah ke rekening pelaku.
- Jika *internet banking* dilengkapi dengan otentikasi token, *malware* mengirimkan pesan palsu kepada nasabah, meminta kode token kepada nasabah dengan alasan, misalnya: sinkronisasi token.

Hampir seluruh proses MIB bersifat transparan, berjalan di belakang layar, dan tidak dapat dilihat atau dirasakan oleh nasabah. Satu-satunya proses yang dapat dirasakan oleh nasabah adalah pada saat pelaku (*malware*) melakukan *phishing*, antara lain:

- Menampilkan layar *pop up* yang menginformasikan antara lain bank penyelenggara *internet banking* sedang melakukan pemeliharaan sistem atau data nasabah (misalnya sinkronisasi token).
- Meminta nasabah memasukkan kode token (*one time password* / OTP). Kode token tersebut digunakan oleh pelaku untuk menjalankan transaksi di *internet banking* nasabah.

Salah satu cara yang dapat digunakan nasabah sebagai tanda untuk lebih waspada yaitu adanya notifikasi melalui *e-mail* dari bank yang menginformasikan transaksi tertentu meskipun nasabah tidak melakukannya, misalnya informasi pendaftaran rekening tujuan transfer, informasi pendaftaran transaksi tunda, dan informasi transaksi berhasil dijalankan.

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

- Menggunakan komputer pribadi dan jaringan yang terpercaya untuk mengakses layanan *internet banking*. Sebaiknya menghindari penggunaan komputer publik, misalnya di

warnet, dan/atau jaringan yang tidak terpercaya, misalnya *wifi access point* yang disediakan oleh kafe atau toko di pusat perbelanjaan.

- Melengkapi komputer pribadi dengan *anti virus* yang terkini.
- Menghindari akses ke dan/atau mengunduh *file* dari alamat *web* yang tidak terpercaya.
- Mewaspadai permintaan informasi yang tidak wajar, misalnya permintaan untuk memasukkan kode token melalui layar *pop up*.
- Segera menindaklanjuti dengan menghubungi *call center* resmi apabila terdapat notifikasi dari bank mengenai adanya aktivitas pada rekening sementara nasabah tidak pernah melakukan hal tersebut.

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, namun biasanya

halaman *web* tersebut tidak terkini dan tidak dapat merespon secara interaktif, misalnya menampilkan ucapan selamat datang dengan menyebut nama lengkap nasabah. Halaman *web* palsu tidak dapat menampilkan nama lengkap nasabah karena pelaku tidak memiliki informasinya.

Dalam *typosite*, cara yang digunakan oleh pelaku, antara lain:

1. Membuat situs yang namanya mirip dengan alamat *web* suatu bank. Setiap orang dapat menamai situsnya dengan nama apapun sepanjang belum ada yang menggunakannya. Misalnya, situs resminya adalah www.ibanking-bankABC.com, sementara situs palsunya adalah www.ibank-bankABC.com, www.ibanking-ACBbank.com, dan sebagainya.
2. Menunggu hingga ada nasabah yang salah ketik sehingga masuk ke halaman web tersebut.
3. Mencatat/merekam *user ID* dan *password* yang dimasukkan oleh nasabah.
4. Menggunakan *user ID* dan *password* untuk membobol akun *internet banking* nasabah di situs yang resmi.

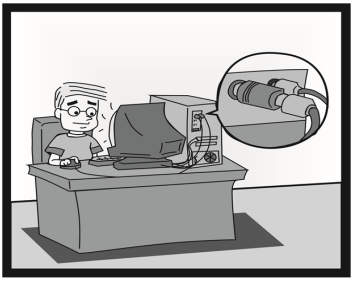
Jika *internet banking* dilengkapi dengan OTP, pelaku biasanya menggunakan teknik *phishing* untuk mendapatkan kode OTP, yaitu mengirimkan pesan disertai ancaman sehingga nasabah memberikan informasi OTP ke pelaku melalui halaman *web* palsu tersebut. Pelaku dapat juga menunggu hingga nasabah melakukan

transaksi tertentu, misalnya transfer keluar, lalu mengubah pesan (*challenge code*) sesuai kebutuhan pelaku, menangkap OTP yang dimasukkan oleh nasabah, dan menggunakan OTP tersebut untuk menjalankan transaksi pelaku di halaman *web* resmi.

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

- Selalu memeriksa kembali ejaan nama situs, jangan sampai ada kesalahan ketik, termasuk penggunaan sImbol.
- 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 baik tidak jadi mengakses situs tersebut atau mengecek ulang nama situs yang telah ketikkan.
- Menghentikan aktivitas transaksi jika merasa ada yang ganjil pada halaman *web* yang sedang diakses. Selanjutnya, tanyakan hal tersebut ke *call center* bank yang resmi.
- 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*.

KEYLOGGING (KEYLOGGER)



Keylogger adalah suatu perangkat yang dipasang di antara *keyboard* dan CPU, digunakan untuk merekam apapun yang diketikkan oleh nasabah di *keyboard*. Tujuannya adalah untuk mendapatkan *user ID* dan *password* nasabah. Meskipun saat mengetikkan *password* yang tampil di layar hanyalah '*****', namun isi *password* tersebut tetap dapat terekam dan terbaca oleh pelaku. Hasil rekamannya dapat dikirimkan melalui *e-mail* kepada pelaku atau dapat juga di-*copy* langsung dari perangkat *keylogger*.

Seiring dengan perkembangan teknologi, *keylogger* dapat berupa *software* yang terinstal di komputer nasabah.

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

- Memastikan bahwa komputer yang digunakan aman dari perangkat *keylogger*
- Menghindari penggunaan komputer publik, seperti di warnet, bandara, dan kafe.

- Menghentikan aktivitas transaksi jika merasa ada yang ganjil pada komputer yang sedang diakses.
- Berhati-hati dalam mengunduh dan/atau menginstal *software*.

D. SMS BANKING

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, auto-lock, screen-lock, pattern-lock*. Nasabah biasanya menyimpan informasi penting seperti PIN, *user id, password*, dll dalam ponsel agar tidak lupa dan memudahkan bertransaksi.

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

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:

- Mengaktifkan setting pengamanan pada ponsel seperti *password/passcode, auto-lock, screen-lock, pattern-lock* dll.
- Tidak menulis PIN atau informasi lainnya di dalam ponsel atau
- Tidak meminjamkan ponsel kepada pihak lain tanpa pengawasan sementara ponsel tersebut sudah sudah terdapat layanan untuk *SMS Banking*.
- 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.

PEMBAJAKAN NOMOR PONSEL DAN PENCURIAN PIN *SMS BANKING*

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

Dalam pembajakan nomor ponsel, pelaku menggunakan cara antara lain:

- Pelaku menggunakan surat kuasa palsu yang dilampiri fotocopy KTP nasabah.
- Jika berhasil mendapatkan SIM card pengganti, maka pelaku bisa mengirimkan dan menerima SMS ke bank seakan-akan ia adalah nasabah yang sebenarnya.
- Pelaku menghubungi *call center* bank, dan meminta untuk dilakukan reset PIN. Notifikasi perubahan PIN akan disampaikan ke *e-mail* / SMS nasabah, dimana ponsel nasabah sudah dikuasai pelaku.

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

- Merahasiakan PIN dan tidak menyimpan pada ponsel
- Menggunakan PIN yang tidak mudah ditebak
- Mengganti PIN secara berkala
- Senantiasa memperhatikan notifikasi *e-mail* dari Bank.

PONSEL DIGUNAKAN OLEH ORANG LAIN

SMS banking dapat disalahgunakan jika ponsel nasabah digunakan oleh orang lain, baik itu karena dipinjamkan, dicuri, atau hilang. Selain itu, ponsel mudah untuk disalahgunakan apabila *setting* pengaman dalam ponsel tidak diaktifkan, seperti

password/passcode, auto-lock, screen-lock, pattern-lock. Nasabah umumnya menyimpan informasi penting seperti PIN, *user id, password*, dll dalam ponsel agar tidak lupa dan memudahkan bertransaksi. Sebagai contoh, PIN *SMS banking* akan tersimpan pada *"sent items"* sehingga dapat diketahui dan disalahgunakan oleh orang lain.

Pelaku berusaha mendapatkan ponsel dan PIN antara lain dengan cara:

1. Pelaku memanfaatkan kelengahan nasabah dengan mengambil ponsel nasabah.
2. Pelaku mencari PIN yang tersimpan pada ponsel atau pelaku menghubungi *call center* bank meminta untuk dilakukan *reset* PIN.
3. Pelaku mendapatkan PIN dari notifikasi *e-mail* yang dikirimkan bank.

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

- Mengaktifkan *setting* pengamanan pada ponsel seperti *password/passcode, auto-lock, screen-lock, pattern-lock* dll
- Menghapus SMS yang berisi PIN dari *sent item* maupun dari *folder* lainnya.
- Menggunakan PIN yang tidak mudah ditebak.
- Mengganti PIN secara berkala

- Segera melakukan pemblokiran akun *SMS banking* dan/atau nomor ponsel jika kehilangan ponsel.
- Senantiasa memperhatikan notifikasi *e-mail* dari Bank.

E. MOBILE BANKING

PEMBAJAKAN NOMOR PONSEL DAN PENCURIAN PIN *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.

Dalam pembajakan nomor ponsel, pelaku menggunakan cara antara lain:

- Pelaku menggunakan surat kuasa palsu yang dilampiri fotocopy KTP nasabah.
- Jika berhasil mendapatkan *SIM card* pengganti, maka pelaku bisa mengirimkan dan menerima SMS ke bank seakan-akan ia adalah nasabah yang sebenarnya.
- Pelaku menghubungi *call center* bank, dan meminta untuk dilakukan *reset* PIN. Notifikasi perubahan PIN akan

disampaikan ke *e-mail* / SMS nasabah, dimana ponsel nasabah sudah dikuasai pelaku.

- Jika pelaku telah mengetahui PIN *SMS banking* nasabah, maka dapat digunakan untuk membobol rekening nasabah di bank.

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

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

PONSEL DIGUNAKAN OLEH ORANG LAIN

Mobile Banking dapat disalahgunakan jika ponsel nasabah digunakan oleh orang lain, baik itu karena dipinjamkan, dicuri, atau hilang. Selain itu, ponsel mudah untuk disalahgunakan apabila *setting* pengaman dalam ponsel tidak diaktifkan, seperti *password/passcode, auto-lock, screen-lock, pattern-lock*. Nasabah umumnya menyimpan informasi penting seperti PIN, *user id, password*, dll dalam ponsel agar tidak lupa dan memudahkan bertransaksi. Sebagai contoh, PIN *SMS banking* akan tersimpan pada *sent items* sehingga dapat diketahui dan disalahgunakan oleh orang lain.

Pelaku berusaha mendapatkan ponsel dan PIN antara lain dengan cara:

1. Pelaku memanfaatkan kelengahan nasabah dengan mengambil ponsel nasabah.
2. Pelaku mencari PIN yang tersimpan pada ponsel atau pelaku menghubungi *call center* bank meminta untuk dilakukan *reset* PIN.
3. Pelaku mendapatkan PIN dari notifikasi *e-mail* yang dikirimkan bank.

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

- Mengaktifkan *setting* pengamanan pada ponsel seperti *password/passcode, auto-lock, screen-lock, pattern-lock* dll
- Menghapus SMS yang berisi PIN dari *sent item* maupun dari *folder* lainnya.
- Menggunakan PIN yang tidak mudah ditebak.
- Mengganti PIN secara berkala
- Segera melakukan pemblokiran akun *SMS banking* dan/atau nomor ponsel jika kehilangan ponsel.
- Senantiasa memperhatikan notifikasi *e-mail* dari bank.

F. E-COMMERCE

CARDING

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*.

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

1. 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.
2. Pelaku menggunakan data-data tesebut untuk berbelanja secara *on-line*.

3. Transaksi terjadi dan tagihan akan dibebankan kepada nasabah yang memiliki kartu dengan data-data yang telah digunakan secara *illegal* oleh pelaku.

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

- Simpan dan perlakukan kartu debet dan/atau kartu kredit dengan baik.
- 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.
- Berhati-hati dalam menggunakan kartu kredit pada saat bertransaksi, untuk menghindarkan pencatatan data-data penting oleh *merchant*.
- 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.

G. PHONE BANKING

NOMOR *CALL CENTER* PALSU DAN/ATAU NOMOR *PHONE BANKING* PALSU

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:

1. 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.
2. Jika ada nasabah yang menghubungi nomor tersebut, pelaku akan berpura-pura bertindak sebagai petugas bank.
3. Pelaku meminta nasabah menyebutkan data rahasia nasabah, seperti PIN, nomor kartu kredit, masa berlaku kartu kredit, dan kode pengaman kartu kredit (CVV).
4. Setelah mendapatkan data-data rahasia dari nasabah melalui nomor *call center* palsu atau nomor *phone banking* palsu,

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

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

Hal-hal yang dapat dilakukan untuk meminimalisir bahaya nomor *call center* palsu :

- Meminta nomor *call center* atau nomor *phone banking* secara langsung dari kantor cabang, *website* resmi dan atau publikasi resmi dari bank.
- Simpan dan catat nomor *call center* dan/atau nomor *phone banking* pada daftar nomor telepon di ponsel.
- Batalkan transaksi jika nasabah curiga dengan nomor telpon tersebut ataupun curiga dengan respon dari nomor telpon tersebut.

MENEBAK PIN SECARA BERULANG-ULANG

Modus kejahatan dengan cara menebak nomor PIN *phone banking* nasabah secara berulang-ulang dapat dilakukan dengan memanfaatkan kelemahan sistem bank yang setiap hari melakukan *reset counter number* yang menampung jumlah kesalahan nomor PIN sehingga PIN tersebut tidak akan pernah terblokir. Pelaku yang telah memiliki kartu debit dapat mencoba memasukkan

nomor PIN berulang kali namun untuk menghindari terblokirnya kartu tersebut, sebelum mencapai frekuensi maksimum kesalahan PIN, pelaku berhenti mencoba memasukkan PIN dan mencobanya kembali pada keesokan harinya dengan metode yang sama hingga didapatkan nomor PIN yang benar.

Dalam melakukan aksinya, cara yang digunakan oleh pelaku antara lain:

1. Pelaku mencari beberapa data sensitif dan penting dari nasabah, antara lain nomor rekening, nomor kartu debet dan/ atau kartu kredit, tanggal *expired* atau masa berlaku kartu, limit kartu, dan beberapa data lainnya yang dapat digunakan untuk verifikasi transaksi *phone banking*.
2. Pelaku menghubungi nomor *phone banking*, dan mencoba melakukan verifikasi dengan memasukkan PIN. PIN yang dimasukkan tersebut merupakan tebakan dari pelaku.
3. Apabila kesalahan PIN sudah mendekati batas kesalahan yang diperkenankan, maka pelakukan akan menghentikan upayanya dan mencobanya di lain waktu.
4. Apabila tebakan PIN benar, maka pelaku dapat melakukan transaksi melalui fasilitas *phone banking* tersebut.

Hal-hal yang dapat dilakukan untuk meminimalisir bahaya menebak PIN secara berulang-ulang :

- Menjaga data-data rahasia dan sensitif seperti nomor rekening, nomor kartu debet dan/atau kartu kredit, tanggal *expired* atau masa berlaku kartu, limit kartu, dan beberapa data lainnya yang dapat digunakan untuk verifikasi transaksi *phone banking*.
- Secara periodik melakukan pengecekan transaksi pada rekening.
- Memanfaatkan fasilitas notifikasi transaksi *phone banking* melalui SMS apabila bank menyediakan layanan tersebut.

H. VIDEO BANKING

BOOTH VIDEO BANKING PALSU

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* yang cara kerjanya telah dijelaskan pada pembahasan sebelumnya.

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

1. Membuka *booth video banking* yang menyerupai dengan *booth* asli yang dimiliki bank.
2. Melengkapi *booth* tersebut dengan nomor *call center* palsu untuk mengelabui nasabah yang memerlukan bantuan langsung petugas.
3. 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*.
4. Mempergunakan informasi identitas dan kartu nasabah untuk bertransaksi.

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

- 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.
- Mencari nomor telepon bank yang sebenarnya dan kemudian menghubungi bank tersebut untuk melaporkan atau menanyakan kebenaran keberadaan *booth* tersebut.
- Tidak menyampaikan data identitas ataupun data kartu.

OTORITAS JASA KEUANGAN

Mengatur
Mengawasi
Melindungi

Untuk Industri Keuangan yang Sehat

OTORITAS JASA KEUANGAN

MENGATUR - MENGAWASI - MELINDUNGI

UNTUK INDUSTRI KEUANGAN YANG SEHAT

BAB IV - PENUTUP

Perkembangan operasional perbankan yang menggunakan modernisasi teknologi informasi dalam rangka memenuhi kebutuhan masyarakat terhadap pelayanan perbankan yang cepat dan efisien serta kebijakan *less cash society* menjadi *trend* perkembangan produk perbankan kedepan melalui layanan produk e-banking. Di sisi lain produk bank ini dapat menimbulkan risiko apabila tidak didukung dengan *environment, security,* prosedur dan manajemen risiko yang memadai dari bank yang menyediakan produk tersebut termasuk pemahaman yang memadai dari nasabah pengguna maupun calon pengguna produk e-banking.

Transaksi e-banking baik frekuensi maupun *volume* transaksi dari beberapa bank di Indonesia selama kurun waktu tahun 2012, 2013 dan 2014 menunjukkan perkembangan yang pesat. Kedepannya, sejalan dengan perkembangan teknologi, kebutuhan masyarakat dan tuntutan terhadap perbankan yang semakin efisien, maka transaksi dan nasabah termasuk bank yang menyelenggarakan produk e-banking diperkirakan semakin meningkat. Hal tersebut menimbulkan pula tantangan terhadap penyelenggaraan e-banking, kebutuhan pengawasan terhadap perbankan dan di sisi lain perlunya edukasi kepada masyarakat luas.

Selanjutnya, Otoritas telah, sedang dan akan terus melakukan pengaturan dan pengawasan terhadap produk e-banking untuk lebih meyakini bahwa operasional bank tekait dengan produk e-banking senantiasa mengacu kepada prinsip kehati-hatian sehingga aman dan nyaman bagi nasabah perbankan untuk melakukan transaksi dan menggunakan produk e-banking.

Buku ini diharapkan dapat menjawab sebagian dari kebutuhan dan tantangan penyelenggaraan dan penggunaan e-banking. Meskipun demikian, isi buku ini tidak menjamin dan memastikan bahwa penyelenggara dan pengguna produk e-banking menjadi terbebas dari segala risiko baik *financial* maupun *non-financial* dalam menyelenggarakan dan bertransaksi dengan e-banking.

GLOSSARY

3-D Secure:

pengamanan tambahan berupa kode sekali pakai atau *One Time Password* (OTP) untuk bertransaksi kartu kredit secara *on-line*. Sistem bank mengirimkan kode acak melalui SMS ke nomor ponsel nasabah pada saat nasabah melakukan transaksi *on-line*.

Access - akses:

jalan masuk. Suatu usaha untuk membuka suatu saluran komunikasi dengan perangkat *hardware* atau *software* tertentu, seperti *modem* yang digunakan untuk membuka akses internet. Perangkat *hardware* atau *software* tersebut selain untuk memberikan data juga digunakan untuk menerima data untuk disimpan.

Account:

penampungan data tentang seseorang, sedikitnya terdiri dari nama pengguna dan *password*. Di dalam sistem perbankan, *account* adalah satu data kepemilikan atas suatu produk perbankan, dapat terdiri dari nama nasabah, kode produk, nilai nominal yang dimiliki.

Access point:

perangkat keras yang memungkinkan perangkat *wireless* lain (seperti *laptop*, ponsel) untuk terhubung ke jaringan kabel menggunakan *Wi-fi, bluetooth* atau perangkat standar lainnya.

Auto-lock:

penguncian otomatis terhadap suatu perangkat (misalnya ponsel) dengan parameter waktu atau tombol tertentu sehingga perangkat tersebut tidak dapat digunakan oleh orang lain yang tidak memiliki akses.

Bisnis Daring atau online shop:

suatu kegiatan atau pekerjaan untuk memasarkan produk yang dimilikinya dengan mempergunakan jaringan internet dengan tujuan untuk memperoleh keuntungan.

Browser:

perangkat lunak yang berfungsi untuk menerima dan menyajikan sumber informasi di Internet.

Card reader:

alat untuk membaca kartu elektronik.

Card Verification Value (CVV):

tiga digit angka terakhir yang terdapat pada bagian belakang kartu kredit, biasanya berada di tempat tanda tangan pada kartu kredit.

Cash Deposit Machine (CDM):

mesin ATM yang memungkinkan nasabah dapat melakukan penyetoran tunai melalui mesin ATM secara *real time on-line* dengan rekening dan secara otomatis mesin ATM tersebut akan mendeteksi denominasi dan kondisi fisik uang (asli atau palsu, baik atau rusak).

Clonning:

penggandaan atau duplikasi terhadap suatu barang.

Closed Circuit Television (CCTV):

suatu sistem yang digunakan sebagai pelengkap keamanan dan pemantauan yang banyak digunakan untuk di perkantoran, toko, industri, militer, perumahan, di sekitar aset milik perbankan.

Customer Service:

petugas bank yang melayani nasabah untuk keperluan pembukaan rekening, perubahan data nasabah, pengaduan nasabah, dan layanan *non-financial* lainnya.

Delivery Channel:

jalur atau media yang digunakan oleh bank untuk memberikan layanan kepada nasabahnya baik secara konvensional ataupun elektronik, yang meliputi : *teller, SMS Banking, Mobile Banking, Phone Banking, EDC, Internet Banking*, ATM*, Video Banking, E-commerce.*

Digital Banking:

satu cara akses ke sistem perbankan yang dapat dilakukan kapan saja dan dimana saja dengan menggunakan jaringan internet.

Unduh:

adalah meminta sebuah *file* dari komputer lain (*web site, server* atau yang lainnya) dan menerimanya.

Electronic Banking (E-Banking):

layanan yang memungkinkan nasabah bank untuk memperoleh informasi, melakukan komunikasi, dan melakukan transaksi perbankan melalui media elektronik seperti *Automatic Teller Machine* (ATM), *phone banking, Electronic Fund Transfer* (EFT), *Electronic Data Capture* (EDC) / *Point Of Sales* (POS), *internet banking* dan *mobile banking.*

E-mail/surat elektronik:

sarana kirim mengirim surat melalui jalur jaringan komputer (misalnya Internet).

E-money atau stored value atau prepaid card:

produk yang merupakan media yang dipakai dalam mekanisme sistem pembayaran melalui pembayaran di *point of sales (merchant),* transfer antar dua media elektronik atau jaringan komputer menggunakan nilai uang yang tersimpan pada kartu atau produk tersebut.

Enkripsi:

alat untuk mencapai keamanan data dengan menerjemahkannya dengan menggunakan sebuah *key (password).* Enkripsi mencegah *password* atau *key* supaya tidak mudah dibaca pada *file* konfigurasi.

Fee-based income:

komisi yang diterima bank dari pemasaran produk maupun transaksi jasa perbankan yang dibebankan kepada nasabah sehubungan dengan produk dan jasa bank yang dinikmatinya.

File:

kumpulan data yang berisi informasi, dapat berupa dokumen atau elektronik dan dapat tersimpan di dalam suatu tempat penyimpanan fisik atau digital. Untuk *file* elektronik memiliki berbagai format dengan kegunaan yang berbeda.

Firewall:

peralatan untuk menjaga keamanan jaringan yang melakukan pengawasan dan penyeleksian atas lalu lintas data/informasi melalui jaringan serta memisahkan jaringan privat dan publik. Peralatan ini dapat digunakan untuk melindungi komputer yang telah terhubung ke jaringan dari serangan yang dapat mengkompromikan suatu komputer.

Fraud:

segala macam yang dapat dipikirkan dan diupayakan oleh seseorang untuk mendapatkan keuntungan dari orang lain dengan cara yang tidak jujur yang menyebabkan orang lain tertipu.

General Packet Radio Service (GPRS):

teknologi yang memungkinkan pengiriman dan penerimaan data dalam bentuk paket data, seperti *e-mail*, gambar, dll.

Interactive Voice Response (IVR):

teknologi telepon dimana pelanggan menggunakan telepon untuk terhubung dengan *database* yang berisi informasi tanpa harus berbicara dengan petugasnya.

Kartu kredit:

kartu yang dikeluarkan oleh pihak bank dan sejenisnya untuk memungkinkan pembawanya membeli barang-barang yang dibutuhkannya secara hutang. Kartu kredit merupakan suatu jenis penyelesaian transaksi ritel, yang diterbitkan kepada pengguna sistem tersebut sebagai alat pembayaran yang dapat digunakan dalam membayar suatu transaksi.

Kartu debit:

sebuah kartu pembayaran secara elektronik yang diterbitkan oleh bank yang berfungsi sebagai pengganti pembayaran dengan uang tunai.

Keyboard:

perangkat keras pada komputer yang berbentuk papan dengan berbagai macam fungsi perintah yang selanjutnya dikirim ke perangkat CPU. *Keyboard* terdiri dari banyak tombol ketik dengan simbol masing-masing.

Keylogger:

ancaman berupa perangkat lunak atau perangkat keras/*hardware* yang digunakan untuk memperoleh informasi (PIN, *password*) yang diketikkan pengguna pada *keyboard* (biasanya di warung internet).

Leased Line:

saluran koneksi telepon permanen antara dua titik yang disediakan oleh perusahaan telekomunikasi publik. Umumnya, *leased line* digunakan ketika terdapat kebutuhan komunikasi data jarak jauh yang harus dilakukan secara terus-menerus. *Leased line* memiliki beberapa tingkatan tarif yang bergantung kepada lebar jalur data *(bandwidth)* yang mampu dikirimkan melalui jaringan *leased line* tersebut.

Less cash society:

gaya hidup dengan menggunakan uang elektronik dalam bertransaksi, sehingga tidak perlu membawa uang fisik.

Login:

proses untuk mengakses komputer atau sistem atau aplikasi atau suatu layanan di media elektronis dengan memasukkan informasi yang telah terdaftar seperti *user id* dan *password.*

Malware:

perangkat lunak yang diciptakan untuk menyusup dan merusak sistem komputer tanpa izin dari pemilik.

Marketing:

proses menawarkan barang dan jasa kepada calon pelanggan.

Merchant:

penjual barang/jasa yang memiliki *physical store* maupun *on-line store* yang bekerja sama dengan bank dalam penyediaan layanan penerimaan pembayaran.

Media Sosial:

media *on-line* yang memungkinkan manusia untuk saling berinteraksi satu sama lain tanpa dibatasi ruang dan waktu.

On-line:

sistem atau komputer yang terkoneksi/terhubung dengan jaringan internet.

Off-line:

sistem atau komputer yang tidak terdapat hubungan jaringan atau tidak dapat berkomunikasi dengan sistem atau komputer lain.

One Time Password (OTP) :

kode verifikasi yang dikirimkan melalui SMS atau email untuk memastikan kebenaran transaksi oleh pemilik rekening.

Password:

kode atau simbol khusus untuk mengamankan sistem komputer yaitu untuk mengidentifikasi pihak yang mengakses data, program atau aplikasi komputer dan digunakan.

Pattern-lock:

penguncian layar perangkat (misalnya ponsel) menggunakan metode penguncian dengan pola, berfungsi seperti *password.*

Personal Identification Number (PIN):

rangkaian digit unik terdiri dari huruf, angka atau kode ASCII yang digunakan untuk mengidentifikasi pengguna komputer, pengguna ATM, internet banking, mobile banking,dll.

Pita magnetis (Card's magnetic stripe):

suatu pita perekam yang digunakan untuk media penyimpan data. Setiap karakter ditulis melintasi lebar pita dalam bentuk bintik-bintik yang diberi muatan magnet, pembacaan dari dan penulisan ke pita dilakukan dengan menggerakkan permukaan pita melintasi suatu *read/write head sebuah tape drive.*

Pop Up:

jendela yang muncul ketika mengunjungi halaman suatu web atau aplikasi.

Screen-lock:

penguncian layar perangkat (misalnya ponsel) sehingga *user* yang tidak memiliki akses tidak dapat mempergunakannya. Metode *screen-lock* dapat berupa penguncian dengan *password* atau pola.

Server:

sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer.

Setting:

pengaturan baik terhadap perangkat keras atau perangkat lunak.

Subscriber Identity Module (SIM) Card:

sebuah kartu pintar dalam berbagai ukuran yang menyimpan kunci pengenal jasa telekomunikasi sehingga dapat saling berkomunikasi.

Smartphone:

ponsel pintar atau ponsel cerdas yaitu telepon genggam yang mempunyai kemampuan dan fungsi menyerupai komputer.

Social Engineering:

teknik pembohongan melalui perilaku sosial yang dilakukan oleh hacker untuk mengelabui orang agar memberikan informasi rahasia seperti PIN, *Password*, dll.

Software / perangkat lunak:

sekumpulan program elektronik yang dapat menjalankan suatu perintah.

Teller:

petugas bank yang melayani transaksi simpanan, penarikan, pencairan cek, dan pelayanan perbankan tunai /non tunai lainnya kepada nasabah.

Token:

alat pengaman tambahan untuk melakukan transaksi finansial di *internet banking*.

Unstructured Suplementary Service Data (USSD):

sebuah protokol berbasis GSM untuk berkomunikasi dari *handphone* pengguna ke penyedia layanan telekomunikasi (dan sebaliknya).

Upgrade:

penggantian produk dengan versi yang lebih baru atau lebih baik dengan produk yang dihasilkan oleh perusahaan yang sama.

User Identification/User ID:

serangkaian huruf, angka, simbol atau kombinasinya untuk mengidentifikasi pihak yang mengakses data, program atau aplikasi komputer dan digunakan dengan tujuan mengamankan suatu sistem atau aplikasi tersebut.

Virtual account:

nomor identifikasi pelanggan yang dibuka oleh bank atas permintaan perusahaan untuk diberikan oleh perusahaan kepada pelanggannya (perorangan maupun non perorangan) sebagai nomor rekening tujuan penerimaan *(collection)*.

Virus:

program yang bersifat merusak dan akan aktif dengan bantuan orang (dieksekusi), dan tidak dapat mereplikasi sendiri, penyebarannya karena dilakukan oleh orang, seperti *copy,* biasanya melalui *attachement e-mail, game,* program bajakan dll.

Website:

web page atau informasi yang disampaikan melalui suatu *web browser* atau sekumpulan *web page* yang dirancang, dipresentasikan dan saling terhubung untuk membentuk suatu sumber informasi dan atau melaksanakan fungsi transaksi.

Wireless :

jaringan komunikasi dimana perangkat-perangkat di dalamnya (PC, komputer, ataupun *handphone*) dapat berkomunikasi tanpa kabel.

OTORITAS
JASA
KEUANGAN

BIJAK BER-eBANKING

TIDAK UNTUK DIPERJUAL BELIKAN

BIJAK BER-ELECTRONIC BANKING

Jakarta, Mei 2015

DISCLAIMER

Buku ini diharapkan dapat menjawab sebagian dari kebutuhan dan tantangan penyelenggaraan dan penggunaan e-banking. Meskipun demikian, isi buku ini tidak menjamin dan memastikan bahwa penyelenggara dan pengguna produk e-banking menjadi terbebas dari segala risiko baik *financial maupun non-financial* dalam menyelenggarakan dan bertransaksi dengan e-banking.

TIM PENYUSUN

A. Pengarah

Nelson Tampubolon	:	Dewan Komisioner OJK
Irwan Lubis	:	Deputi Komisioner Pengawas Perbankan III - OJK
Agus E. Siregar	:	Kepala Departemen Pengawasan Bank3 (DPB3) - OJK

B. Tim Perumus

Jasmi	:	Direktur - DPB3
Yusup Ansori	:	Direktur - DPB3
Irnal Fiscallutfi	:	Direktur - DPB2
Nahor P. Hutauruk	:	Direktur - DPB1
Ali Yusuf Asbi	:	Deputi Direktur - DPB3
Ridwan I. Situmorang	:	Deputi Direktur - DPB2
Guntar Kumala	:	Deputi Direktur - DPB1
Ahmad Nurdin	:	Kepala Bagian - DPB3
Pardiyono	:	Kepala Bagian - DPB3
Anton Sudharma	:	Kepala Bagian - DPB3
Budi Santoso	:	Kepala Bagian - DPB3
Iwan Irawan	:	Kepala Bagian - DPB1
Dayu Nawang M.	:	Kasubbag - DPB3

Rendra W. Prasetyo	:	Staf - DPB3
Rahayu Rianti	:	Staf - DPB3
Riris Grace Karolina	:	Staf - DPB2
Gozali Mulyono	:	Staf - DPB2

C. Kontributor/
Nara sumber : Bank Mandiri, BRI, BNI, BTN, BCA, Bank CIMB Niaga, Bank Danamon, Bank BII, Bank Panin, Bank Permata, Bank OCBC NISP, Bank UOB Indonesia, Bank Bukopin

DAFTAR ISI

KATA SAMBUTAN

Pertama-tama marilah kita mengucapkan puji syukur kehadirat Tuhan Yang Maha Kuasa, karena dengan kuasa dan kehendak-NYA-lah kita semua diberikan kesehatan dan kesempatan untuk menghadirkan buku ini. Selanjutnya saya juga ingin menyampaikan apresiasi kepada semua pihak yang telah menginisiasi, mengarahkan, menyumbangkan ide, tulisan, dan lain-lain hingga penerbitan buku ini dapat terealisir, sebagai bagian dari wujud tanggung jawab insan OJK terhadap pemangku kepentingan, terutama masyarakat luas pengguna maupun calon pengguna industri jasa keuangan, khususnya sektor perbankan.

Suatu keniscayaan bahwa seiring dengan perkembangan teknologi yang semakin maju, peningkatan kebutuhan dan tuntutan masyarakat yang semakin tinggi terhadap produk dan aktivitas perbankan baik dari sisi keberagaman, kecepatan, maupun fleksibilitas waktu bertransaksi, termasuk keamanan dan kenyamanan dalam bertransaksi serta disisi lain sejalan pula dengan upaya industri perbankan untuk beroperasi secara lebih efisien, maka berbagai kebutuhan tersebut dijawab oleh industri perbankan, antara lain dengan menghadirkan produk dan aktivitas *electronic banking* dengan *delivery channel* yang semakin beragam.

Sejalan dengan itu, otoritas pengawas telah, sedang dan akan terus mengawal perkembangan dan menjaga keseimbangan

kebutuhan dan tuntutan masyarakat terhadap produk dan aktivitas perbankan yang semakin kompleks dan efisien dimaksud dengan mengacu pada prinsip kehati-hatian dalam kerangka pengawasan secara mikro terhadap masing-masing individu perbankan sekaligus guna melindungi kepentingan nasabah industri perbankan khususnya dan masyarakat dan pada umumnya.

Penerbitan buku "Bijak Ber-eBanking" ini dinilai tepat dan diharapkan menjadi salah satu alternatif untuk ikut menjawab berbagai kebutuhan tersebut di atas. Buku ini dikemas dalam bentuk yang mudah dipahami mengenai apa dan bagaimana sebuah *electronic banking* dan beberapa contoh kejadian seputar transaksi *electronic banking* berikut ilustrasinya, baik yang terjadi di Indonesia maupun di luar negeri. Saya mengharapkan semoga buku ini dapat lebih meningkatkan pemahaman masyarakat pengguna/calon pengguna produk dan aktivitas *electronic banking*, termasuk bagi industri perbankan dalam kaitannya dengan potensi risiko yang mungkin timbul dari produk dan aktivitas dimaksud.

Semoga upaya ini mendapat berkah Tuhan Yang Maha Esa.

Selamat membaca.

Jakarta, Mei 2015

Nelson Tampubolon
Dewan Komisioner OJK

OTORITAS
JASA
KEUANGAN

Mengatur
Mengawasi
Melindungi

Untuk Industri Keuangan yang Sehat

OTORITAS JASA KEUANGAN

MENGATUR - MENGAWASI - MELINDUNGI

UNTUK INDUSTRI KEUANGAN YANG SEHAT

BAB I - PENDAHULUAN

A. Latar Belakang

Perkembangan perbankan saat ini memberikan dan menawarkan kemudahan bagi nasabah melalui layanan operasional yang sangat beragam, termasuk layanan e-banking *(electronic banking)*. Layanan e-banking saat ini dimiliki oleh hampir semua Bank Umum yang ada, baik dengan jenis *delivery channel* yang sangat umum (seperti ATM) maupun dengan jenis *delivery channel* lainnya seperti SMS, telephone, EDC (*Electronic Data Capture*) dan internet. Hal tersebut juga sejalan dengan kecenderungan perkembangan media sosial maupun kebijakan yang ada untuk mewujudkan atau mengarahkan transaksi pada masyarakat dilakukan tidak melulu dengan uang tunai *(less cash society),* sehingga telah banyak pelaku ekonomi atau masyarakat yang memanfaatkan layanan perbankan modern yang lebih efisien dan efektif melalui e-banking.

Transaksi yang dilakukan melalui e-banking setiap tahun mengalami pertumbuhan yang cukup besar pada beberapa bank. Berdasarkan data13 bank besar di Indonesia, frekuensi transaksi melalui e-banking pada tahun 2012 sebanyak 3,79 Milyar transaksi dan dengan nilai nominal Rp. 4.441 Trilyun, bertambah menjadi sebanyak 4,73 Milyar transaksi dengan nilai nilai nominal Rp. 5.495 Trilyun pada tahun 2013, pada tahun 2014 meningkat

masing-masing menjadi 5,69 Milyar transaksi dengan nilai nominal Rp. 6.447 Trilyun.

Pertumbuhan tersebut berpotensi meningkat sejalan dengan kecenderungan layanan bank mengarah pada *digital banking*. Hal ini dikarenakan antara lain layanan e-banking memiliki fitur yang menarik dan nyaman digunakan serta memberi kemudahan bagi nasabah untuk melakukan transaksi keuangan seperti transfer antar-bank, pembayaran kartu kredit, pembayaran listrik, pembayaran telepon, pembayaran tagihan ponsel, pembayaran asuransi, pembayaran internet, pembayaran tiket penerbangan, dan *virtual account*. Selain itu semakin marak bisnis daring *(online shop)* serta pertumbuhan jenis dan jumlah *smartphone* yang semakin meningkat telah memberikan andil dalam pertumbuhan transaksi melalui e-banking.

Pertumbuhan e-banking yang didukung dengan perkembangan teknologi, media sosial dan pola hidup masyarakat memberikan manfaat bagi industri perbankan antara lain menghasilkan pendapatan dari *fee-based income,* mengurangi biaya transaksi, pengembangan bisnis, dan meningkatkan kepercayaan/loyalitas nasabah. Penggunaan e-banking juga memberikan kenyamanan dan kemudahan bertransaksi secara bebas, tidak terbatas oleh waktu dan lokasi , khusus untuk *internet banking*, layanannya dapat dinikmati oleh nasabah *anytime, anywhere, dan by any*

device. faktor keamanan perlu mendapatkan perhatian yang cukup untuk meminimalkan potensi penyalahgunaan atau fraud melalui e-banking. Sebagai contoh, meskipun layanan *internet banking* dapat dinikmati oleh nasabah *anytime*, anywhere, dan by *any device*, tetapi dilengkapi dengan OTP (*One Time Password*), yaitu kode yang hanya dapat diperoleh melalui perangkat tertentu yang dimiliki oleh nasabah dan *password*, yaitu sesuatu yang hanya diketahui oleh nasabah.

B. Tujuan

Buku ini menjelaskan dan menguraikan gambaran umum mengenai jenis-jenis dan manfaat layanan serta modus kejadian penyalahgunaan e-banking, sehingga buku ini diharapkan dapat digunakan oleh nasabah, bank maupun pengawas bank terkait dengan tujuan antara lain:

- Memberikan pemahaman yang memadai kepada nasabah dalam melakukan transaksi melalui e-banking sehingga dapat meningkatkan rasa aman dan nyaman bertransaksi di e-banking.
- Menyusun langkah-langkah pengamanan maupun memberikan edukasi yang memadai oleh bank untuk mendukung penggunaan e-banking sebagai sarana transaksi oleh nasabah.
- Memberikan pemahaman kepada pengawas bankatas permasalahan pada e-banking, serta sebagai referensi

untuk melakukan langkah pembinaan atas kelemahan dan permasalahan pada e-banking sehingga bank diharapkan dapat menentukan langkah pencegahannya (mitigasi).

Selain itu,materi buku ini juga tersedia di website resmi OJK sehingga *stakeholder* lainnya dapat memperoleh informasi dan manfaatnya.

Uraian dalam buku ini lebih dititikberatkan sebagai salah satu wujud dari proses mengedukasi dan melindungi konsumen pengguna jasa produk/aktivitas perbankan terkait dengan e-banking, serta sekaligus dapat pula dimanfaatkan sebagai salah satu referensi pelaksanaan prinsip kehati-hatian bagi industri perbankan dalam menyelenggarakan e-banking.

C. Cakupan

Cakupan penyusunan buku ini meliputi layanan e-banking dan permasalahannya yang terjadi pada industri perbankan di Indonesia maupun di luar Indonesia. Adapun layanan e-banking yang ada pada industri perbankan tersebut antara lain meliputi ATM (*Automated Teller Machine*), *internet banking*, *mobile banking*, *SMS banking*, kartu kredit, kartu debet, *phone banking*, EDC (*Electronic Data Capture*) dan *video banking*.

Mengatur
Mengawasi
Melindungi

Untuk Industri Keuangan yang Sehat

OTORITAS JASA KEUANGAN

MENGATUR - MENGAWASI - MELINDUNGI

UNTUK INDUSTRI KEUANGAN YANG SEHAT

BAB II - GAMBARAN UMUM

A. Gambaran Umum *Electronic Banking* (e-Banking)

Perkembangan pesat Teknologi Informasi (TI) dan globalisasi mendukung Bank untuk meningkatkan pelayanan kepada nasabah secara aman, nyaman, dan efektif, diantaranya melalui media elektronik atau dikenal dengan *Electronic Banking* (e-banking). E-banking merupakan layanan yang memungkinkan nasabah Bank untuk memperoleh informasi, melakukan komunikasi, dan melakukan transaksi perbankan melalui media elektronik seperti *Automatic Teller Machine* (ATM), *Electronic Data Capture* (EDC)/ *Point Of Sales* (POS), *internet banking, SMS banking, mobile banking, e-commerce, phone banking*, dan *video banking*.

E-Banking memberikan banyak manfaat baik bagi nasabah, bank, dan otoritas. Bagi nasabah, e-banking memberikan kemudahan bertransaksi dalam hal waktu, tempat, dan biaya. Nasabah tidak perlu mendatangi kantor bank untuk memperoleh informasi atau melakukan transaksi perbankan. Bahkan untuk beberapa produk e-banking nasabah dapat bertransaksi selama 24 jam dengan menggunakan *laptop* atau perangkat *mobile* seperti telepon seluler yang dapat dibawa kemana saja selama terhubung dengan jaringan internet dan/atau SMS.

Bagi bank, e-banking meningkatkan pendapatan berbasis komisi *(fee based income)* dan mengurangi biaya operasional apabila dibandingkan dengan pelayanan transaksi melalui kantor cabang yang relatif besar untuk membayar karyawan, sewa gedung, pengamanan, listrik, dan lainnya.

Bagi otoritas, perkembangan teknologi e-banking mendorong mewujudkan masyarakat *less cash society. Less cash* society adalah gaya hidup dengan menggunakan media transaksi atau uang elektronik dalam bertransaksi sehingga tidak perlu membawa uang fisik. *Less cash society* selain dapat meningkatkan sistem pembayaran yang cepat, aman, dan efisien, untuk mempercepat perputaran aktivitas ekonomi dan stabilitas sistem keuangan, juga dapat mencegah tindak pidana kriminal maupun tindak pidana pencucian uang.

Di bawah ini merupakan beberapa produk yang termasuk dalam layanan e-banking.

Automated Teller Machine (ATM)

Definisi

ATM atau yang lebih dikenal dengan nama Anjungan Tunai Mandiri merupakan suatu terminal/mesin komputer yang terhubung dengan jaringan komunikasi bank, yang memungkinkan nasabah

melakukan transaksi keuangan secara mandiri tanpa bantuan dari *teller* ataupun petugas bank lainnya.

Sesuai dengan perkembangan teknologi, saat ini bank juga telah menyediakan 3 tipe mesin ATM lainnya, yaitu: mesin ATM yang hanya melayani transaksi non tunai, mesin ATM yang melayani transaksi penyetoran uang tunai *Cash Deposit Machine* atau CDM, dan mesin ATM yang dapat melayani semua transaksi yang telah disebutkan di atas.

Selain di kantor bank, saat ini nasabah dapat dengan mudah menemukan mesin ATM di berbagai tempat, seperti restoran, pusat perbelanjaan, bandar udara, pasar, dan lokasi-lokasi strategis lainnya.

Fitur

Melalui ATM, nasabah bank dapat mengakses rekeningnya untuk melakukan berbagai transaksi keuangan, yaitu transaksi penarikan tunai dan transaksi non tunai, seperti pengecekan saldo, pembayaran tagihan kartu kredit, pembayaran tagihan listrik, pembelian pulsa, dan sebagainya.

Cara Kerja

Untuk menggunakan ATM, nasabah harus memiliki kartu ATM/ debit/kredit dan PIN. PIN adalah kode (4-6 digit) angka yang dibuat oleh nasabah saat pertama kali menerima kartu ATM di bank. Kode tersebut harus dijaga kerahasiannya oleh nasabah supaya kartu ATM tidak dapat disalahgunakan oleh orang lain.

Nasabah memasukkan kartu pada slot kartu di mesin ATM dengan memperhatikan sisi kartu yang harus dimasukkan terlebih dahulu, kemudian nasabah akan diminta untuk memasukkan PIN. Setelah itu nasabah dapat melakukan transaksi dengan memilih menu yang tertera pada layar monitor ATM.

Electronic Data Capture (EDC)

Definisi

EDC merupakan suatu perangkat/ terminal yang dapat digunakan untuk bertransaksi menggunakan kartu debit/kredit/prabayar di *merchant* atau toko. Terminal tersebut terhubung ke jaringan komputer bank. EDC terdiri dari alat pembaca informasi pada pita

magnetis kartu *(card's magnetic stripe)* atau *chip*, tombol menu dan angka untuk memasukkan jenis transaksi, nilai transaksi, dan PIN, layar untuk melihat jenis dan nilai transaksi, dan printer untuk mencetak bukti transaksi.

Fitur

Saat ini, EDC digunakan di banyak toko untuk memudahkan nasabah melakukan transaksi, bahkan EDC dapat digunakan untuk pembayaran telepon, listrik, pulsa, tiket pesawat, dan transaksi lainnya. Pada umumnya EDC terhubung ke sistem bank menggunakan jaringan telepon *fixed line*, namun untuk beberapa pusat perbelanjaan yang memiliki banyak mesin EDC, ada juga yang menggunakan jaringan *leased line*. Seiring dengan perkembangan teknologi selular, EDC juga dapat menggunakan jaringan dengan sistem GPRS *(wireless)*.

Selain ditransaksikan dengan cara digesek, ada juga EDC yang yang digunakan dengan cara menempelkan kartu pada mesin (*card tapping*) seperti yang digunakan untuk membayar parkir, tol, alat transportasi, dan lainnya.

Cara Kerja

Untuk menggunakan EDC, nasabah harus memiliki kartu debit, kartu kredit, atau kartu elektronik. Cara menggunakannya yaitu dengan menggesekkan/memasukkan kartu pada mesin

kemudian pegawai *merchant* menginputkan jumlah uang yang akan dibayarkan, setelahnya nasabah akan diminta untuk menginputkan PIN pada mesin atau menyertakan tandatangan sebagai pembuktian keaslian nasabah *(authentication)* pada struk yang dikeluarkan oleh EDC. Namun pada EDC yang berjenis *card tapping,* nasabah cukup menempelkan kartu pada EDC saat melakukan pembayaran dan tidak perlu menginputkan PIN atau tanda tangan.

Internet Banking

Definisi

Internet banking adalah layanan untuk melakukan transaksi perbankan melalui jaringan internet. Merupakan kegiatan perbankan yang memanfaatkan teknologi internet sebagai media untuk melakukan transaksi dan mendapatkan informasi lainnya

melalui *website* milik bank. Kegiatan ini menggunakan jaringan internet sebagai perantara atau penghubung antara nasabah dengan bank tanpa harus mendatangi kantor bank. Nasabah dapat menggunakan perangkat komputer *desktop, laptop, tablet*, atau *smartphone* yang terhubung ke jaringan internet sebagai penghubung antara perangkat nasabah dengan sistem bank.

Fitur

Fitur layanan *internet banking* antara lain informasi umum rekening tabungan/giro, rekening deposito, kartu kredit, informasi mutasi rekening, transfer dana, baik transfer antar rekening maupun antar bank, pembelian pulsa, pembelian tiket, penempatan deposito, layanan informasi seperti suku bunga dan kurs, dan pembayaran, misalnya pembayaran telepon, internet, kabel TV, asuransi, listrik dan berbagai jenis pembayaran lainnya.

Cara Kerja

Untuk menggunakan *internet banking*, nasabah harus memiliki *user id, password*, media token atau *One Time Password* (OTP), dan jaringan internet. *User id, password,* dan media token dapat diperoleh dengan mendaftarkan diri ke bank. Saat menggunakan *internet banking*, nasabah harus memastikan *website* yang diakses adalah *website internet banking* milik bank, kemudian nasabah akan diminta untuk memasukkan *user id* dan *password* pada halaman muka atau *login*. Pada saat melakukan transaksi

finansial, nasabah akan diminta untuk memasukkan sandi OTP yang diperoleh dari media token atau SMS. Setelah transaksi selesai, nasabah harus memastikan telah keluar/*log out* dari halaman *internet banking*. Bank mengirimkan notifikasi melalui *e-mail* sebagai bukti bahwa transaksi telah berhasil. Notifikasi *e-mail* ini juga sebagai pengendalian agar nasabah mengetahui jika akun *internet banking*-nya digunakan oleh orang lain.

SMS Banking

Definisi

SMS banking adalah layanan perbankan yang dapat diakses langsung melalui telepon selular/*handphone* dengan menggunakan media SMS *(Short Message Service)*.

Fitur

Fitur *SMS Banking* antara lain layanan informasi (saldo, mutasi rekening, tagihan kartu kredit, dan suku bunga); dan layanan transaksi, seperti transfer, pembayaran tagihan (listrik, air, pajak, kartu kredit, asuransi, internet), pembelian (pulsa, tiket), dan berbagai fitur lainnya.

Cara Kerja

Untuk dapat menggunakan *SMS Banking*, nasabah harus mendaftarkan diri dan mendaftarkan nomor ponsel terlebih dahulu ke bank serta mendapatkan *password*, kemudian nasabah dapat bertransaksi dengan cara mengetik SMS sesuai dengan format SMS yang telah ditentukan. Format SMS berbeda-beda berdasarkan format yang telah ditentukan oleh masing-masing bank, contohnya: untuk melakukan transfer, nasabah dapat mengetik : Transfer <rek_sumber><rek_tujuan><nominal><password>. Pesan ini kemudian dikirim ke nomor tujuan yang telah ditentukan bank. Untuk menggunakan fasilitas ini nasabah sebaiknya mempelajari petunjuk format SMS yang tertera pada buku petunjuk *SMS banking* atau *website* bank.

Mobile Banking

Definisi

Mobile banking merupakan layanan yang memungkinkan nasabah bank melakukan transaksi perbankan melalui ponsel atau *smartphone*. Layanan

mobile banking dapat digunakan dengan menggunakan menu yang sudah tersedia pada SIM *(Subscriber Identity Module)* Card, USSD *(Unstructured Suplementary Service Data),* atau melalui aplikasi yang dapat diunduh dan diinstal oleh nasabah. Mobile banking menawarkan kemudahan jika dibandingkan dengan SMS banking karena nasabah tidak perlu mengingat format pesan SMS yang akan dikirimkan ke bank dan juga nomor tujuan SMS banking.

Fitur

Fitur-fitur layanan *mobile banking* antara lain layanan informasi (saldo, mutasi rekening, tagihan kartu kredit, suku bunga, dan lokasi cabang/ATM terdekat); dan layanan transaksi, seperti transfer, pembayaran tagihan (listrik, air, pajak, kartu kredit, asuransi, internet), pembelian (pulsa, tiket), dan berbagai fitur lainnya.

Cara Kerja

Untuk menggunakan *mobile banking*, nasabah harus mendaftarkan diri terlebih dahulu ke bank untuk mendapatkan *password*. Nasabah dapat memanfaatkan layanan mobile banking dengan cara mengakses menu yang telah tersedia pada *SIM Card* atau aplikasi yang terinstal di ponsel. Apabila nasabah menggunakan *mobile banking* melalui menu yang telah tersedia pada *SIM Card*, nasabah dapat memilih menu sesuai kebutuhan

kemudian nasabah akan diminta untuk menginputkan *PIN SMS Banking* saat menjalankan transaksi. Sedangkan apabila nasabah menggunakan *mobile banking* melalui aplikasi yang terinstal di ponsel, nasabah harus mengunduh dan menginstal aplikasi pada telepon seluler terlebih dahulu. Pada saat membuka aplikasi tersebut, nasabah harus memasukkan *password* untuk *login*, kemudian nasabah dapat memilih menu transaksi yang tersedia dan diminta memasukkan PIN saat menjalankan transaksi.

Electronic Commerce (e-Commerce)

Definisi

E-commerce atau perdagangan elektronik merupakan penyebaran, pembelian, penjualan, pemasaran barang dan jasa melalui sistem elektronik seperti internet atau televisi. Melalui *e-commerce*, pembeli dan penjual dapat melakukan transaksi secara *online.*

Jenis-jenis *e-commerce* antara lain:

a. *E-commerce* yang menggunakan sosial media atau forum untuk berjualan, namun transaksi tidak diselesaikan melalui *website* tersebut namun biasanya akan berkomunikasi secara langsung untuk bertransaksi.
b. *E-commerce* yang proses jual belinya dilakukan melalui *website* si penjual.

c. *E-commerce* yang proses jual belinya dilakukan di "lapak" *online*. Penjual bukanlah penyedia *website*, melainkan anggota-anggota yang mendaftar untuk berjualan di lapak *online* yang telah tersedia. Setiap transaksi yang terjadi pada lapak *online* tersebut, pengelola lapak akan menjadi pihak ketiga yang menerima pembayaran dan menjamin barang diterima oleh pembeli, lalu uang pembayaran akan diteruskan ke pihak penjual.

Fitur

Melalui *e-commerce*, masyarakat dapat melakukan jual beli, contohnya pembelian buku, alat elektronik, pakaian, kendaraan, bahkan rumah secara *online*. Pembayaran yang dilakukan pada saat bertransaksi secara *online* dapat menggunakan kartu kredit, debit, atau dengan menggunakan alat pembayaran *virtual* seperti *paypal.*

Cara Kerja

Untuk bertransaksi secara *online*, pembeli harus memiliki jaringan internet, alat pembayaran seperti kartu kredit, kartu debit, atau akun pembayaran *virtual*. Alur proses *e-commerce* pada umumnya

adalah sebagai berikut, pengguna mengakses *website* penjualan produk, melakukan pemesanan, menerima tagihan elektronik, kemudian pembeli dapat melakukan pembayaran secara elektronik. Beberapa perusahaan kartu kredit saat ini bekerjasama dengan perusahaan *internet security* untuk membuat standar enkripsi khusus demi keamanan bertransaksi, walaupun demikian nasabah diharapkan tetap menjaga keamanan bertransaksi misalnya dengan memperhatikan keamanan jaringan saat akan melakukan transaksi, memastikan perangkat dilengkapi dengan *antivirus, anti malware, firewall*, dan me-*review rating* si penjual sebelum melakukan transaksi *online.*

Phone Banking

Definisi

Phone Banking adalah layanan untuk bertransaksi perbankan atau mendapatkan informasi perbankan lewat telepon dengan menghubungi nomor layanan pada bank. Layanan tersebut antara lain bertujuan memberikan kemudahan kepada nasabah dalam melakukan berbagai transaksi perbankan melalui telepon. Nasabah tidak perlu lagi datang

ke bank atau mesin ATM untuk melakukan berbagai transaksi tersebut. Layanan *phone banking* ini merupakan salah satu dari perkembangan teknologi *call center.* Pada umumnya layanan *phone banking* dapat diakses selama 24 jam sehingga nasabah dapat menggunakannya dimana saja dan kapan saja.

Fitur

Fitur *phone banking* antara lain informasi perbankan misalnya informasi suku bunga, kurs, info produk bank, lokasi ATM dan kantor cabang, transaksi perbankan misalnya informasi saldo, pembayaran tagihan listrik, telepon pasca bayar, kartu kredit, pemindahbukuan, transfer antar bank, pembelian isi ulang pulsa, mutasi rekening, perubahan PIN dan data nasabah.

Cara Kerja

Phone banking dapat diakses oleh nasabah maupun non-nasabah bank untuk informasi umum bank. Bagi nasabah yang ingin menggunakan layanan *phone banking* dapat mendaftarkan diri terlebih dahulu ke bank untuk mendapatkan PIN *phone banking*. Setelah itu nasabah dapat menghubungi nomor *phone banking* bank dan nasabah akan dilayani oleh pegawai bank maupun IVR (*Interactive Voice Response*). IVR adalah teknologi yang dapat mendeteksi suara dan penekanan tombol telepon kemudian meresponnya kembali dalam bentuk suara atau media lain.

Video Banking

Definisi

Video Banking merupakan teknologi yang memungkinkan nasabah melakukan aktivitas perbankan jarak jauh menggunakan suatu perangkat khusus yang disediakan oleh bank yang memungkinkan nasabah berkomunikasi *audio visual* dengan petugas bank, menginput data, mencetak *statement*, dan mengeluarkan kartu baru. Pada umumnya bank menyediakan layanan *video banking* di lokasi-lokasi strategis seperti pusat perbelanjaan pada hari kerja maupun Sabtu dan Minggu. Jam operasionalnya pun lebih lama daripada jam operasional pelayanan melalui kantor bank.

Fitur

Fitur *video banking* di Indonesia pada saat ini antara lain pembukaan rekening, informasi produk, tarik dan setor tunai, transfer dana, pembelian pulsa, dan pembayaran tagihan seperti kartu kredit, listrik, dan telepon.

Cara Kerja

Untuk menggunakan layanan *video banking*, nasabah dapat mendatangi gerai perbankan digital yang menyediakan layanan ini. Selama bertransaksi nasabah akan dipandu oleh petugas bank, misalnya untuk melakukan pembukaan rekening baru melalui *video banking*, nasabah akan diminta untuk *memasukkan* data, *scan* kartu identitas, setoran awal, hingga cetak kartu sambil bertatap muka dan berkomunikasi dengan *customer service* bank melalui layar *video*.

B. Regulasi oleh Otoritas

Perbankan di Indonesia saat ini telah mengikuti perkembangan teknologi informasi dan komunikasi. Perkembangan ini ditandai dengan pesatnya penggunaan *electronic banking* (e-banking) untuk mendukung operasional kegiatan perbankan dan memudahkan nasabah melakukan transaksi.Walaupun demikian, penggunaan teknologi informasi tersebut perlu memperhatikan risiko yang dihadapi bank dan nasabah sehingga bank harus selalu menerapkan manajemen risiko teknologi informasi (TI) secara efektif.

Pengaturan dan pengawasan bank, khususnya manajemen risiko TI saat ini dilaksanakan oleh Otoritas Jasa Keuangan (OJK) sebagai lembaga pengawas industri jasa keuangan terpercaya, melindungi kepentingan konsumen dan masyarakat. Penerapan manajemen risiko TI bank diatur dalam PBI No.9/15/PBI/2007 tentang Penerapan Manajemen Risiko dalam Penggunaan

Teknologi Informasi dan SE No.9/30/DPNP perihal Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi Bank Umum. Beberapa hal yang diatur misalnya dalam kegiatan e-banking, bank wajib melaporkan rencana dan realisasi penerbitan produk e-banking yang bersifat transaksional dan harus memberikan edukasi kepada nasabah mengenai produk e-banking dan pengamanannya secara berkesinambungan. Pengaturan dan pengawasan terkait produk e-banking juga meliputi manajemen bank, kebijakan dan prosedur, penilaian risiko, mitigasi risiko, dan pengendalian pengamanan terkait e-banking.

C. Perkembangan Aktivitas E-banking Beberapa Bank di Indonesia

Penggunaan e-banking di Indonesia, baik dari jumlah nasabah pengguna transaksional, jumlah frekuensi e-banking dari tahun 2012 s/d 2014 secara umum meningkat. Peningkatan ini terjadi pada beberapa produk, misalnya *internet banking, mobile banking, SMS banking*, dan *phone banking*.

Jumlah Pengguna e-Banking Posisi 31 Desember 2014

Kartu Debit/ATM	82,006,699
Kartu Kredit	5,771,002
Kartu e-Money	9,788,145
Pengguna e-Money Berbasis Server	44,691
Pengguna *Internet Banking*	8,507,458
Pengguna *Mobile Banking*	14,738,817

Tabel 2.1 Perkembangan Frekuensi Transaksi e-banking di Beberapa Bank di Indonesia

Jenis Delivery Channel	*Frekuensi*				
	2012	*2013*	*2014*	*Perkembangan 2012 - 2013*	*Perkembangan 2013 - 2014*
ATM	*2,933,467,577*	*3,609,206,816*	*4,179,631,965*	*23.04%*	*15.80%*
EDC	*366,350,819*	*446,148,695*	*542,400,709*	*21.78%*	*21.57%*
Internet Banking	*235,957,566*	*311,880,376*	*437,798,960*	*32.18%*	*40.37%*
SMS /Mobile Banking	*224,876,666*	*325,550,038*	*473,196,941*	*44.77%*	*45.35%*
E-Commerce/ Merchant On-line	*2,790,843*	*3,707,515*	*7,778,488*	*32.85%*	*109.80%*
Phone Banking	*1,375,460*	*1,401,841*	*1,393,737*	*32.85%*	*-0.58%*
Video Banking	*7.684*	*16.418*	*28,097*		
Total Frekuensi Transaksi	*3,790,718,984*	*4,732,508,750*	*5,686,467,993*	*24,84%*	*20.16%*

Tabel 2.2 Perkembangan Nilai Transaksi e-banking di Beberapa Bank di Indonesia

Jenis *Delivery Channel*	Nilai Transaksi (dalam Milyar Rupiah)				
	2012	2013	2014	Perkembangan 2012 – 2013	Perkembangan 2013 – 2014
ATM	3,141,654	3,830,457	4,392,238	21.92%	14.67%
EDC	266,242	337,698	406,401	26.84%	20.34%
Internet Banking	669,607	860,546	1,062,820	28.52%	23.51%
SMS / Mobile Banking	343,441	437,853	544,371	27.49%	24.33%
E-Commerce/ Merchant On-line	5,514	10,849	16,134	96.76%	48.71%
Phone Banking	2,430	2,307	3,281	-5.05%	42.23%
Video Banking			104		
Total Nilai Transaksi	4,441,438	5,495,048	6,446,594	23.72%	17.32%

Mengatur
Mengawasi
Melindungi

Untuk Industri Keuangan yang Sehat

OTORITAS JASA KEUANGAN

MENGATUR - MENGAWASI - MELINDUNGI

UNTUK INDUSTRI KEUANGAN YANG SEHAT

BAB III –BIJAK DALAM MENGGUNAKAN LAYANAN E-BANKING

Electronic banking menawarkan berbagai kemudahan bagi nasabah, namun di sisi lain memiliki risiko yang harus diwaspadai. Berikut ini adalah beberapa contoh penyalahgunaan e-banking pada industri perbankan di Indonesia, termasuk di luar negeri 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:

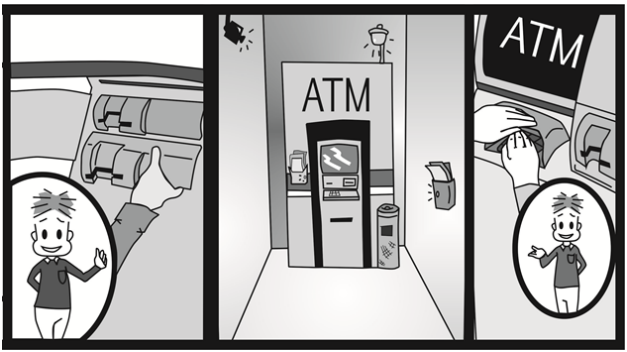
Delivery Channel	Media	Modus
ATM	Kartu, PIN, Mesin ATM.	- *Skimming* (menggunakan *skimmer*) - *Card Trapping* - *Card And PIN Sharing* - *Social Engineering* - *Call Center* palsu - Pencurian Data Kartu
EDC	Kartu, PIN, EDC, *Card Reader*.	- *Skimming* (menggunakan *skimmer*) - *Card Intercept* - Penggunaan *Card Reader Ilegal* - Pencurian Kartu/Data kartu - Gesek Tunai

Delivery Channel	Media	Modus
Internet Banking	User ID, Password, Token, Akun Medsos.	- P*hishing,* - *Man/Malware In The Browser (MIB)/* Sinkronisasi *Token* - *Typosite* - *Keylogger*
SMS Banking	PIN, Nomor Ponsel.	- Pencurian Ponsel, - Pembajakan Nomor Ponsel, - Ponsel digunakan oleh orang lain
Mobile Banking	PIN, Nomor Ponsel.	- Pencurian Ponsel - Pembajakan Nomor Ponsel - Clonning Nomor Ponsel
E-commerce	Data Kartu (Nomor Kartu, Masa Berlaku , Nama pada Kartu, CVV)	- *Carding*
Phone Banking	Nomor Rekening, PIN.	- *Call Center* palsu, - Menebak PIN Berulang-ulang.
Video Banking	Kartu Identitas, Penampakan Fisik.	- *Booth Video Banking* palsu.

A. ATM (*AUTOMATED TELLER MACHINE*)

CARD SKIMMING

Card Skimming adalah tindakan pencurian data kartu ATM dengan cara menyalin (membaca dan menyimpan) informasi yang terdapat pada strip magnetis secara ilegal. Strip magnetis adalah garis lebar hitam yang berada dibagian belakang kartu ATM. Fungsinya seperti pita kaset untuk menyimpan data nomor kartu, masa berlaku, dan nama nasabah. *Card skimming* dilakukan menggunakan alat pembaca kartu (*card skimmer*) yang ditempatkan pada slot kartu di mesin ATM.



Dalam *card skimming,* pelaku berusaha mendapatkan **data kartu** dan **PIN,** antara lain dengan cara:

1. Pelaku memasang alat *skimmer* pada mesin ATM;
2. Nasabah memasukkan kartu ke mesin ATM yang dipasangi alat *skimmer*, sehingga data kartu nasabah terbaca dan tersimpan pada alat tersebut;
3. Pelaku berusaha mendapatkan PIN ATM dengan cara mengintip tombol yang ditekan oleh nasabah atau dapat juga menggunakan kamera kecil yang dipasang oleh pelaku di mesin ATM;
4. Pelaku membuat kartu palsu menggunakan data yang telah diperoleh dan bertransaksi menggunakannya PIN yang telah diketahui (terekam).

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

- Memperhatikan kondisi mesin ATM sebelum digunakan. *Card Skimmer* seringkali tidak terlihat secara kasat mata karena warna dan bentuknya telah disesuaikan dengan mesin ATM;
- Hati-hati sebelum menekan tombol PIN. Usahakan agar tombol yang ditekan tidak terlihat oleh orang lain. Nasabah juga perlu mencermati adanya kamera yang dapat merekam tombol PIN yang ditekan oleh nasabah;
- Hindari menggunakan PIN yang mudah ditebak oleh orang lain, seperti tanggal lahir, nomor telepon, dan nomor kartu;

- Mengganti nomor PIN secara periodik, terutama jika ada indikasi bahwa PIN telah diketahui oleh orang lain.

CARD TRAPPING

Gbr. Contoh nomor call center palsu

Card trapping adalah mengambil fisik kartu dengan menggunakan suatu benda asing, seperti korek api, lidi, plastik, karet, benang, atau lem yang dipasang pada slot kartu di mesin ATM.

Dalam *card trapping*, pelaku berusaha mendapat fisik kartu dan PIN, antara lain dengan cara:

1. Pelaku memasang benda asing ke dalam slot kartu di mesin ATM.
2. Saat nasabah menggunakan mesin ATM tersebut, maka kartu ATM akan tersangkut oleh benda asing yang dipasang oleh pelaku, tidak dapat masuk maupun keluar.
3. Pelaku berusaha mendapatkan PIN nasabah dengan beberapa cara, misalnya:

- berpura-pura menawarkan bantuan dan meminta nasabah memasukkan PIN ke dalam mesin ATM. Pelaku memperhatikan dan mengingat nomor PIN nasabah;
- meminta nasabah untuk menghubungi *call center* palsu, lalu nasabah akan diminta menyebutkan PIN oleh petugas *call center* palsu tersebut; atau
- menggunakan kamera kecil yang dipasang oleh pelaku di mesin ATM.

4. Pelaku mengambil kartu ATM nasabah yang tersangkut di mesin ATM setelah nasabah meninggalkan mesin ATM. Modus lainnya untuk mendapatkan kartu nasabah, biasanya pelaku mendatangi nasabah di mesin ATM dan menawarkan bantuan, sementara pelaku lainnya akan mengalihkan perhatian nasabah, misalnya dengan menjatuhkan koin dan lain-lain. Selanjutnya, pelaku dengan cepat akan menukar kartu ATM nasabah dengan kartu ATM palsu yang sudah disediakan pelaku. Pelaku mendapatkan PIN nasabah dengan cara yang sama pada langkah sebelumnya.
5. Pelaku menggunakan kartu ATM dan PIN nasabah untuk mengambil tunai di mesin ATM atau transfer ke rekening lain.

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

- Memperhatikan kondisi mesin ATM sebelum digunakan. Nasabah perlu memperhatikan kondisi mesin ATM, sebelum

bertransaksi. Apabila terdapat hal yang tidak biasa seperti terdapat benda asing pada slot kartu ATM, nasabah hendaknya tidak melanjutkan bertransaksi, dan melaporkan hal tersebut melalui *call center* bank;

- Tidak panik. Nasabah tidak perlu panik saat kartu ATM tidak dapat masuk kedalam mesin ATM. Apabila terdapat seseorang yang menawarkan bantuan, sebaiknya nasabah tidak perlu melanjutkan transaksi;
- Mencari alternatif mesin ATM di lokasi lain;
- Tidak menginformasikan nomor PIN kepada orang lain, termasuk kepada petugas bank; dan
- Mewaspadai orang sekitar, jangan mudah percaya kepada orang yang tidak dikenal.

CALL CENTER 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:
   - Menyebutkan data rahasia nasabah, seperti seperti PIN, nomor kartu kredit, masa berlaku kartu kredit, dan kode pengaman kartu kredit atau *Card VerificationValue* (CVV).
   - 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:

- 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;

- Mencatat nomor telepon *call center* pada media lain, misalnya di ponsel atau catatan lainnya sehingga nasabah dapat menghubungi *call center* bank pada saat dibutuhkan; dan
- Tidak menginformasikan nomor PIN. Nasabah harus selalu merahasiakan nomor PIN, tidak memberitahukan kepada orang lain termasuk kerabat dekat dan pegawai bank atau *call center*.

PENCURIAN DATA KARTU

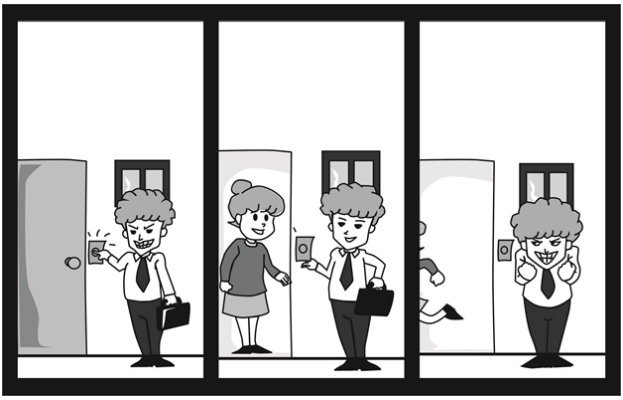
Pencurian data kartu (ATM/debit/kredit) dapat terjadi ketika nasabah berhadapan dengan petugas *marketing* palsu, menggunakan mesin EDC palsu (*dummy* EDC), atau menggunakan mesin ATM palsu (*dummy* ATM). Pelaku pencurian data kartu berusaha mendapatkan data nomor kartu kredit (atau data kartu debit yang menjadi *member principal* kartu kredit), masa berlaku kartu debit/kredit, dan kode pengaman kartu debit/kredit (CVV).

Dalam melakukan pencurian data kartu, pelaku melakukan hal-hal antara lain:

A. Petugas *marketing* palsu

1. Pelaku membuka kios sementara *(booth)* yang dilengkapi dengan spanduk *(banner)*, tanda pengenal, dan seragam yang mirip dengan bank tertentu.

2. Menawarkan produk bank, misalnya kartu kredit dan meminta nasabah:
   - menyerahkan kartu identitas dan/atau kartu kredit untuk difotokopi atau diambil oleh petugas dan menjanjikan penggantian dengan kartu kredit yang baru.
   - Mengisi formulir yang berisi data-data pribadi nasabah.
3. Pelaku dapat juga mendatangi nasabah ke rumah/kantor/ tempat usaha, menawarkan produk bank dengan modus seperti disebutkan pada nomor 2.



Hal-hal yang dapat dilakukan untuk meminimalisir pencurian data kartu, antara lain:

- Memastikan keaslian kios sementara (*booth*), spanduk (*banner*), tanda pengenal, dan seragam yang dikenakan oleh petugas *marketing*. Jika meragukan keasliannya, jangan lakukan transaksi, membuka rekening, atau memberikan data kartu kepada petugas kios sementara tersebut;
- Menghubungi layanan resmi atau kantor bank jika ingin mendaftar produk/layanan bank; dan
- Tidak memberikan fisik kartu atau fotokopi kartu kredit kepada pihak manapun, termasuk petugas bank.

B. Mesin EDC/ATM palsu

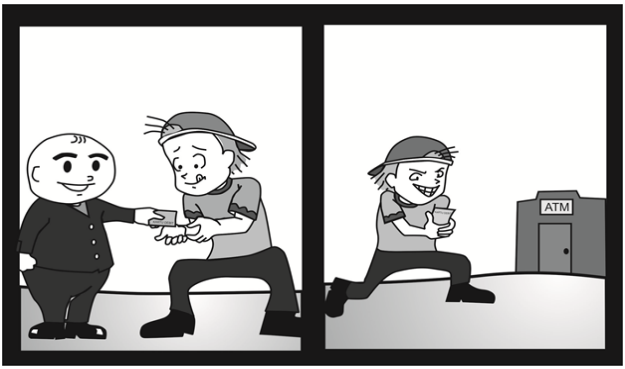
Pelaku memasang mesin EDC dan/atau ATM palsu di tempat umum. Pada saat nasabah menggunakan mesin tersebut, data kartu dan PIN nasabah akan terekam. Selanjutnya pelaku membuat kartu palsu menggunakan data yang telah diperoleh dan bertransaksi menggunakannya PIN yang telah diketahui (terekam).

Hal-hal yang dapat dilakukan untuk meminimalisir pencurian data kartu, antara lain:

- Mengamati mesin EDC/ATM sebelum digunakan. Jika ada kejanggalan (misalnya logo tidak sesuai atau tampilan layar tidak lazim) sebaiknya tidak menggunakan mesin tersebut;

- Segera mengganti PIN pada mesin lain yang resmi jika nasabah sudah terlanjur menggunakan mesin EDC/ATM palsu tersebut; dan
- Menginformasikan kepada bank jika menemukan adanya kejanggalan pada mesin EDC/ATM.

MEMINJAMKAN KARTU DAN PIN KEPADA ORANG LAIN



Nasabah harus memperlakukan kartu dan PIN sebagai sesuatu yang bersifat pribadi dan rahasia. Kartu dan PIN yang diberikan kepada orang lain, dapat disalahgunakan untuk bertransaksi di luar pengetahuan nasabah. Banyak kejadian pembobolan rekening nasabah oleh orang dekat seperti keluarga atau orang lain yang dipercaya oleh nasabah.

Hal-hal yang dapat dilakukan untuk meminimalisir risiko ini, antara lain:

- Nasabah hendaknya tidak meminjamkan kartu ATM dan/atau memberitahukan PIN kepada orang lain, sekalipun kepada keluarga, teman dekat, atau petugas bank; dan
- Hindari mencatat PIN dimanapun, termasuk di ponsel, dompet, buku, tempelan dinding, dll.

SOCIAL ENGINEERING

Social engineering adalah upaya yang memanfaatkan pendekatan sosial untuk mendapatkan data rahasia nasabah atau meminta nasabah melakukan sesuatu yang menguntungkan pelaku, seperti transfer uang, pembayaran tagihan, dan pembelian pulsa.

Dalam *social engineering,* pelaku menggunakan beberapa cara, antara lain:

1. Pelaku mengirimkan pesan melalui SMS, *e-mail*, atau media lain yang berisi pengumuman pemenang hadiah dan meminta nasabah untuk menghubungi nomor telepon atau membuka *website* tertentu;
2. Pelaku memandu nasabah untuk:
   - memberikan informasi rahasia seperti PIN, nomor kartu kredit, masa berlaku kartu kredit, dan kode pengaman kartu kredit (CVV, yaitu 3 angka yang tertera di belakang kartu); atau

- datang ke mesin ATM, menggunakan *internet banking*, atau menggunakan e-banking lainnya, dan melakukan transaksi transfer, pembelian, atau pembayaran yang menguntungkan pelaku tanpa disadari oleh nasabah.

Hal-hal yang dapat dilakukan untuk meminimalisir risiko *social engineering*, antara lain:

- Nasabah hendaknya tidak mudah tergoda dengan tawaran hadiah yang disampaikan melalui telepon, SMS, *e-mail*, atau media sosial;
- Mencari informasi ke sumber lain yang terpercaya untuk memastikan kebenaran informasi yang diterima;
- Tidak memberikan informasi rahasia seperti PIN, nomor kartu kredit, masa berlaku kartu kredit, dan kode CVV kepada orang lain.

B. EDC (*ELECTRONIC DATA CAPTURE*)

CARD SKIMMING

Seperti pada ATM, *card skimming* juga dapat terjadi pada transaksi melalui mesin EDC. Modus *card skimming* pada ATM dan EDC sedikit berbeda, pada ATM alat *skimmer* akan dilekatkan pada mesin ATM yang resmi, sedangkan pada EDC alat *skimmer*

terpisah dari mesin EDC yang resmi. Pelaku akan melakukan *double swipe* yaitu menggesek kartu nasabah pada mesin EDC Bank dan alat *skimmer* yang sudah disiapkan, seringkali alat *skimmer* tersebut dilekatkan pada mesin kasir milik *merchant.*

Hal-hal yang dapat dilakukan untuk meminimalisir bahaya *skimming* pada saat transaksi menggunakan mesin EDC, antara lain :

- Jangan serahkan kartu kepada pelayan tanpa didampingi. Seringkali nasabah lengah dengan memberikan kartu kepada pelayan untuk bertransaksi menggunakan mesin EDC, hal ini memungkinkan pelayan atau kasir menggesek kartu nasabah di mesin *skimmer* tanpa disadari oleh nasabah;
- Awasi pada saat kasir menggesek kartu. Nasabah harus mengawasi aktifitas kasir, pastikan bahwa kartu hanya digesekkan di mesin EDC resmi milik bank. Penggesekan kartu untuk transaksi perbankan hanya dilakukan sekali yaitu pada mesin EDC milik bank. Hal yang umum saat ini, kartu nasabah digesekkan dua kali yaitu pada mesin EDC dan mesin kasir untuk mencetak nama pembeli pada struk pembelian pada mesin *cash register* milik *merchant,* nasabah

harus berhati-hati dan berhak menolak untuk menggesekkan kartu di mesin kasir dengan alasan keamanan data; dan

- Hati-hati sebelum menekan nomor PIN di mesin EDC. Meskipun tidak seorangpun memperhatikan ketika nasabah memasukkan PIN, nasabah harus tetap berhati-hati kemungkinan adanya kamera tersembunyi. Akan lebih baik apabila dalam setiap menekan PIN, nasabah menutup dengan tangan.

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.

Hal-hal 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;
- Pastikan kartu yang dikembalikan oleh kasir setelah transaksi

adalah kartu yang benar. Nasabah harus mengecek kartu yang dikembalikan oleh kasir setelah bertransaksi adalah kartu yang benar. Sebaiknya nasabah menghapal atau mencatat nomer kartu ATM (minimal 4 digit terakhir) untuk memastikan kartu tidak tertukar atau ditukar dengan sengaja pada saat transaksi.

PENGGUNAAN *CARD READER ILEGAL*

Modus penggunaan *card reader ilegal* adalah tindakan pencurian saldo yang ada pada kartu *e-money* melalui proses *tapping* secara diam-diam oleh oknum *merchant* dengan menggunakan *card reader* atau mesin EDC yang bekerja dalam kondisi *online* maupun *offline*. Pelaku yang sudah dilengkapi dengan peralatan tersebut secara diam-diam (pada jarak tertentu yang memungkinkan terjadinya transaksi) melakukan *tapping* kepada calon korban, atau dilakukan secara acak tanpa disadari oleh korban dengan tujuan mengurangi saldo yang ada di dalam kartu *e-money* dalam jumlah tertentu sesuai keinginan pelaku. Saldo yang telah diambil tersebut baik secara otomatis ataupun tidak (bergantung kondisi *on-line/off-line* pada EDC), akan masuk ke dalam rekening pelaku.

Hal-hal yang dapat dilakukan untuk meminimalisir bahaya penggunaan *card reader ilegal*:

- Menyimpan kartu *e-money* dengan aman. Menjaga dan menempatkan kartu *e-money* di tempat yang memiliki penghalang memadai untuk menghindari *tapping;* dan
- Mengecek saldo kartu *e-money* setiap kali selesai melakukan suatu transaksi, untuk memastikan jumlah saldo berkurang secara wajar. Apabila nasabah menemukan saldo berkurang secara tidak wajar segera laporkan kepada bank penerbit untuk diketahui penyebabnya.

PENUKARAN (PENGAMBILAN) KARTU OLEH PETUGAS *MARKETING* PALSU

Penukaran atau pengambilan kartu dilakukan ketika nasabah pemilik kartu ditawari oleh petugas *marketing* palsu untuk melakukan penggantian kartu. Pelaku berusaha untuk mendapatkan kartu kredit nasabah, dengan cara sebagai berikut:

1. Pelaku membuka kios sementara *(booth)* dilengkapi dengan spanduk *(banner),* tanda pengenal, dan seragam yang mirip dengan bank tertentu atau dapat juga mendatangi nasabah ke rumah/kantor/tempat usaha.
2. Pelaku menjanjikan promo *upgrade* jenis kartu dari segi *limit*, jenis kartu, dan keuntungan lainnya.
3. Nasabah pemilik kartu menyerahkan kartu kredit yang dimiliki kepada *marketing* palsu.

4. Pelaku menggunakan kartu tersebut untuk bertransaksi atau penarikan tunai.

Hal-hal yang dapat dilakukan untuk menghindari penukaran kartu oleh petugas *marketing* palsu, antara lain :

- Memastikan keaslian kios sementara *(booth),* spanduk *(banner),* tanda pengenal dan seragam yang dikenakan oleh petugas *marketing*;
- Melakukan konfirmasi ke bank penerbit apabila menerima tawaran promo dari *marketing*;
- Menghubungi layanan/konter resmi jika ingin melakukan *upgrade* kartu; dan
- Tidak memberikan fisik kartu dan PIN kepada pihak manapun, termasuk petugas bank.

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 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.

KARTU HILANG

Nasabah pemegang kartu debit dan/atau kartu kredit dapat mengalami kehilangan kartu debit dan/atau kartu kredit. Kejadian kehilangan kartu tersebut dapat disebabkan kelalaian nasabah maupun disebabkan suatu tidak kejahatan yang dilakukan kepada nasabah, misalnya penjambretan, pencurian, dan penipuan.

Saat ini, penggunaan kartu debit dan/atau kartu kredit untuk berbelanja pada *merchant* memungkinkan dilakukan tanpa PIN, cukup dengan menandatangani struk transaksi. Kartu yang memungkinkan bertransaksi menggunakan tanda tangan adalah kartu debit dan kartu kredit yang tergabung dalam jaringan Visa

dan Mastercard. Oleh karena itu, meskipun nasabah tidak pernah mengungkapkan PIN kepada siapapun, tidak pernah menuliskan PIN pada kartu, ataupun merasa hanya nasabah tersebut saja yang mengetahui PIN kartu tersebut, risiko terhadap penggunaan kartu debit dan/atau kartu kredit tersebut oleh pihak yang tidak berwenang masih tetap ada.

Dalam kejadian nasabah kehilangan kartu, pelaku akan mencoba menggunakan kartu nasabah yang hilang, antara lain dengan cara:

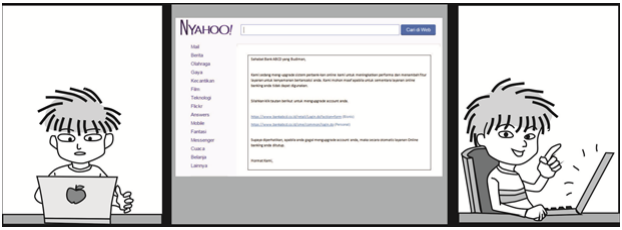
1. Pelaku mendapatkan kartu nasabah yang hilang. Apabila pada bagian belakang kartu terdapat tanda tangan nasabah, pelaku akan mencoba untuk menirukan tanda tangan tersebut untuk bertransaksi. Apabila pada bagian belakang kartu tidak terdapat tanda tangan nasabah, pelaku akan membiarkan tetap kosong atau dapat saja pelaku menandatangani bagian belakang kartu dengan tanda tangan palsu.
2. Pelaku akan bertransaksi (baik untuk membeli barang atau melakukan gesek tunai) melalui *merchant* yang tidak terlalu ketat dalam melakukan verifikasi tanda tangan pada kartu debet dan/kartu kredit. Selain itu, pelaku biasa mencari *merchant* yang tidak diawasi CCTV.

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

- Segera melaporkan kehilangan kartu dan melakukan blokir rekening untuk kartu-kartu yang hilang melalui kantor atau *call center* bank.
- Nasabah menjaga kartu dengan baik, dan jangan letakkan kartu pada sembarang tempat khususnya di tempat umum;
- Mengecek transaksi terakhir yang dilakukan melalui kartu yang hilang tersebut, pengecekan dapat dilakukan menggunakan fasilitas *internet banking, mobile banking, phone banking,* atau datang ke kantor bank; dan
- Melaporkan kejadian kehilangan kartu dan meminta surat keterangan kehilangan kartu kepada kepolisian.

C. INTERNET BANKING

PHISHING



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.

Selain ketiga hal di atas, suatu *phishing* dapat juga ditandai dengan adanya kesalahan ketik dan gaya bahasa yang kurang baik. Pesan *phishing* biasanya tidak melalui proses *review* dan *editing* yang baik, bahkan tidak jarang berupa terjemahan kasar dari bahasa asing. 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. Sebagai contoh, pelaku akan mengirimkan pesan bahwa saat ini sedang terjadi pemeliharaan *server* untuk transaksi *internet banking* sehingga nasabah diminta untuk memasukkan data-data sensitif dan penting. Apabila nasabah tidak memasukkan, maka rekening nasabah tersebut akan menjadi tidak aktif dan tidak dapat digunakan.

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

- 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.
- Menggunakan *anti virus* yang terkini.
- Jangan mengklik *link* apapun pada pesan (*e-mail*) yang terindikasi *phishing*.
- Mengkonfirmasikan kepada pihak bank melalui *call center* yang resmi jika ada permintaan yang mencurigakan.
- 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.
- Hati-hati mengunduh *attachment e-mail* karena dapat berisi *virus/malware* yang dapat mencuri data sensitif.

MAN/MALWARE IN THE BROWSER (MIB)

MIB adalah teknik pembobolan rekening *internet banking* dengan memanfaatkan *software* jahat (*malware*) yang telah menginfeksi *browser internet* nasabah. *Malware* tersebut dapat melakukan beberapa hal sesuai keingingan pembuatnya, misalnya:

- Mencuri data *user ID* dan *password* nasabah,
- Mengambil alih koneksi nasabah ke bank lalu memasukkan transaksi pemindahbukuan/transfer dari rekening nasabah ke rekening pelaku, dan
- Mengganti halaman *web* di *browser* nasabah sesuai keinginan pelaku.

Dalam melakukan MIB, pelaku menggunakan beberapa langkah, antara lain:

- Menyediakan program *malware* pada alamat *web* tertentu. Jika nasabah membuka *web* atau mengunduh sesuatu (*software*, gambar, *video*, dll) dari *web* tersebut, maka *malware* akan masuk ke komputer nasabah.
- Setelah *malware* terinstal di komputer nasabah, *malware* tersebut merekam apa saja yang diketik oleh nasabah sehingga pelaku bisa mendapatkan data *user ID* dan *password internet banking* nasabah.
- *Malware* mengambil alih koneksi *internet banking* milik nasabah lalu memasukkan transaksi sesuai keinginan pelaku, misalnya transfer dari rekening nasabah ke rekening pelaku.
- Jika *internet banking* dilengkapi dengan otentikasi token, *malware* mengirimkan pesan palsu kepada nasabah, meminta kode token kepada nasabah dengan alasan, misalnya: sinkronisasi token.

Hampir seluruh proses MIB bersifat transparan, berjalan di belakang layar, dan tidak dapat dilihat atau dirasakan oleh nasabah. Satu-satunya proses yang dapat dirasakan oleh nasabah adalah pada saat pelaku (*malware*) melakukan *phishing*, antara lain:

- Menampilkan layar *pop up* yang menginformasikan antara lain bank penyelenggara *internet banking* sedang melakukan pemeliharaan sistem atau data nasabah (misalnya sinkronisasi token).
- Meminta nasabah memasukkan kode token (*one time password* / OTP). Kode token tersebut digunakan oleh pelaku untuk menjalankan transaksi di *internet banking* nasabah.

Salah satu cara yang dapat digunakan nasabah sebagai tanda untuk lebih waspada yaitu adanya notifikasi melalui *e-mail* dari bank yang menginformasikan transaksi tertentu meskipun nasabah tidak melakukannya, misalnya informasi pendaftaran rekening tujuan transfer, informasi pendaftaran transaksi tunda, dan informasi transaksi berhasil dijalankan.

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

- Menggunakan komputer pribadi dan jaringan yang terpercaya untuk mengakses layanan *internet banking*. Sebaiknya menghindari penggunaan komputer publik, misalnya di

warnet, dan/atau jaringan yang tidak terpercaya, misalnya *wifi access point* yang disediakan oleh kafe atau toko di pusat perbelanjaan.

- Melengkapi komputer pribadi dengan *anti virus* yang terkini.
- Menghindari akses ke dan/atau mengunduh *file* dari alamat *web* yang tidak terpercaya.
- Mewaspadai permintaan informasi yang tidak wajar, misalnya permintaan untuk memasukkan kode token melalui layar *pop up*.
- Segera menindaklanjuti dengan menghubungi *call center* resmi apabila terdapat notifikasi dari bank mengenai adanya aktivitas pada rekening sementara nasabah tidak pernah melakukan hal tersebut.

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, namun biasanya

halaman *web* tersebut tidak terkini dan tidak dapat merespon secara interaktif, misalnya menampilkan ucapan selamat datang dengan menyebut nama lengkap nasabah. Halaman *web* palsu tidak dapat menampilkan nama lengkap nasabah karena pelaku tidak memiliki informasinya.

Dalam *typosite*, cara yang digunakan oleh pelaku, antara lain:

1. Membuat situs yang namanya mirip dengan alamat *web* suatu bank. Setiap orang dapat menamai situsnya dengan nama apapun sepanjang belum ada yang menggunakannya. Misalnya, situs resminya adalah www.ibanking-bankABC.com, sementara situs palsunya adalah www.ibank-bankABC.com, www.ibanking-ACBbank.com, dan sebagainya.
2. Menunggu hingga ada nasabah yang salah ketik sehingga masuk ke halaman web tersebut.
3. Mencatat/merekam *user ID* dan *password* yang dimasukkan oleh nasabah.
4. Menggunakan *user ID* dan *password* untuk membobol akun *internet banking* nasabah di situs yang resmi.

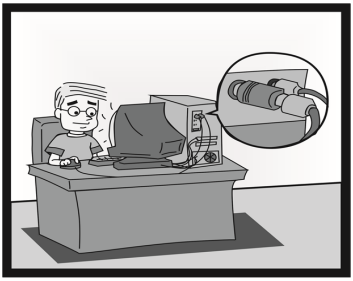
Jika *internet banking* dilengkapi dengan OTP, pelaku biasanya menggunakan teknik *phishing* untuk mendapatkan kode OTP, yaitu mengirimkan pesan disertai ancaman sehingga nasabah memberikan informasi OTP ke pelaku melalui halaman *web* palsu tersebut. Pelaku dapat juga menunggu hingga nasabah melakukan

transaksi tertentu, misalnya transfer keluar, lalu mengubah pesan (*challenge code*) sesuai kebutuhan pelaku, menangkap OTP yang dimasukkan oleh nasabah, dan menggunakan OTP tersebut untuk menjalankan transaksi pelaku di halaman *web* resmi.

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

- Selalu memeriksa kembali ejaan nama situs, jangan sampai ada kesalahan ketik, termasuk penggunaan sImbol.
- 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 baik tidak jadi mengakses situs tersebut atau mengecek ulang nama situs yang telah ketikkan.
- Menghentikan aktivitas transaksi jika merasa ada yang ganjil pada halaman *web* yang sedang diakses. Selanjutnya, tanyakan hal tersebut ke *call center* bank yang resmi.
- 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*.

KEYLOGGING (KEYLOGGER)



Keylogger adalah suatu perangkat yang dipasang di antara *keyboard* dan CPU, digunakan untuk merekam apapun yang diketikkan oleh nasabah di *keyboard*. Tujuannya adalah untuk mendapatkan *user ID* dan *password* nasabah. Meskipun saat mengetikkan *password* yang tampil di layar hanyalah '*****', namun isi *password* tersebut tetap dapat terekam dan terbaca oleh pelaku. Hasil rekamannya dapat dikirimkan melalui *e-mail* kepada pelaku atau dapat juga di-*copy* langsung dari perangkat *keylogger*.

Seiring dengan perkembangan teknologi, *keylogger* dapat berupa *software* yang terinstal di komputer nasabah.

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

- Memastikan bahwa komputer yang digunakan aman dari perangkat *keylogger*
- Menghindari penggunaan komputer publik, seperti di warnet, bandara, dan kafe.

- Menghentikan aktivitas transaksi jika merasa ada yang ganjil pada komputer yang sedang diakses.
- Berhati-hati dalam mengunduh dan/atau menginstal *software*.

D. SMS BANKING

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, auto-lock, screen-lock, pattern-lock*. Nasabah biasanya menyimpan informasi penting seperti PIN, *user id, password*, dll dalam ponsel agar tidak lupa dan memudahkan bertransaksi.

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

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:

- Mengaktifkan setting pengamanan pada ponsel seperti *password/passcode, auto-lock, screen-lock, pattern-lock* dll.
- Tidak menulis PIN atau informasi lainnya di dalam ponsel atau
- Tidak meminjamkan ponsel kepada pihak lain tanpa pengawasan sementara ponsel tersebut sudah sudah terdapat layanan untuk *SMS Banking*.
- 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.

PEMBAJAKAN NOMOR PONSEL DAN PENCURIAN PIN *SMS BANKING*

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

Dalam pembajakan nomor ponsel, pelaku menggunakan cara antara lain:

- Pelaku menggunakan surat kuasa palsu yang dilampiri fotocopy KTP nasabah.
- Jika berhasil mendapatkan SIM card pengganti, maka pelaku bisa mengirimkan dan menerima SMS ke bank seakan-akan ia adalah nasabah yang sebenarnya.
- Pelaku menghubungi *call center* bank, dan meminta untuk dilakukan reset PIN. Notifikasi perubahan PIN akan disampaikan ke *e-mail* / SMS nasabah, dimana ponsel nasabah sudah dikuasai pelaku.

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

- Merahasiakan PIN dan tidak menyimpan pada ponsel
- Menggunakan PIN yang tidak mudah ditebak
- Mengganti PIN secara berkala
- Senantiasa memperhatikan notifikasi *e-mail* dari Bank.

PONSEL DIGUNAKAN OLEH ORANG LAIN

SMS banking dapat disalahgunakan jika ponsel nasabah digunakan oleh orang lain, baik itu karena dipinjamkan, dicuri, atau hilang. Selain itu, ponsel mudah untuk disalahgunakan apabila *setting* pengaman dalam ponsel tidak diaktifkan, seperti

password/passcode, auto-lock, screen-lock, pattern-lock. Nasabah umumnya menyimpan informasi penting seperti PIN, *user id, password*, dll dalam ponsel agar tidak lupa dan memudahkan bertransaksi. Sebagai contoh, PIN *SMS banking* akan tersimpan pada *"sent items"* sehingga dapat diketahui dan disalahgunakan oleh orang lain.

Pelaku berusaha mendapatkan ponsel dan PIN antara lain dengan cara:

1. Pelaku memanfaatkan kelengahan nasabah dengan mengambil ponsel nasabah.
2. Pelaku mencari PIN yang tersimpan pada ponsel atau pelaku menghubungi *call center* bank meminta untuk dilakukan *reset* PIN.
3. Pelaku mendapatkan PIN dari notifikasi *e-mail* yang dikirimkan bank.

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

- Mengaktifkan *setting* pengamanan pada ponsel seperti *password/passcode, auto-lock, screen-lock, pattern-lock* dll
- Menghapus SMS yang berisi PIN dari *sent item* maupun dari *folder* lainnya.
- Menggunakan PIN yang tidak mudah ditebak.
- Mengganti PIN secara berkala

- Segera melakukan pemblokiran akun *SMS banking* dan/atau nomor ponsel jika kehilangan ponsel.
- Senantiasa memperhatikan notifikasi *e-mail* dari Bank.

E. MOBILE BANKING

PEMBAJAKAN NOMOR PONSEL DAN PENCURIAN PIN *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.

Dalam pembajakan nomor ponsel, pelaku menggunakan cara antara lain:

- Pelaku menggunakan surat kuasa palsu yang dilampiri fotocopy KTP nasabah.
- Jika berhasil mendapatkan *SIM card* pengganti, maka pelaku bisa mengirimkan dan menerima SMS ke bank seakan-akan ia adalah nasabah yang sebenarnya.
- Pelaku menghubungi *call center* bank, dan meminta untuk dilakukan *reset* PIN. Notifikasi perubahan PIN akan

disampaikan ke *e-mail* / SMS nasabah, dimana ponsel nasabah sudah dikuasai pelaku.

- Jika pelaku telah mengetahui PIN *SMS banking* nasabah, maka dapat digunakan untuk membobol rekening nasabah di bank.

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

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

PONSEL DIGUNAKAN OLEH ORANG LAIN

Mobile Banking dapat disalahgunakan jika ponsel nasabah digunakan oleh orang lain, baik itu karena dipinjamkan, dicuri, atau hilang. Selain itu, ponsel mudah untuk disalahgunakan apabila *setting* pengaman dalam ponsel tidak diaktifkan, seperti *password/passcode, auto-lock, screen-lock, pattern-lock*. Nasabah umumnya menyimpan informasi penting seperti PIN, *user id, password*, dll dalam ponsel agar tidak lupa dan memudahkan bertransaksi. Sebagai contoh, PIN *SMS banking* akan tersimpan pada *sent items* sehingga dapat diketahui dan disalahgunakan oleh orang lain.

Pelaku berusaha mendapatkan ponsel dan PIN antara lain dengan cara:

1. Pelaku memanfaatkan kelengahan nasabah dengan mengambil ponsel nasabah.
2. Pelaku mencari PIN yang tersimpan pada ponsel atau pelaku menghubungi *call center* bank meminta untuk dilakukan *reset* PIN.
3. Pelaku mendapatkan PIN dari notifikasi *e-mail* yang dikirimkan bank.

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

- Mengaktifkan *setting* pengamanan pada ponsel seperti *password/passcode, auto-lock, screen-lock, pattern-lock* dll
- Menghapus SMS yang berisi PIN dari *sent item* maupun dari *folder* lainnya.
- Menggunakan PIN yang tidak mudah ditebak.
- Mengganti PIN secara berkala
- Segera melakukan pemblokiran akun *SMS banking* dan/atau nomor ponsel jika kehilangan ponsel.
- Senantiasa memperhatikan notifikasi *e-mail* dari bank.

F. E-COMMERCE

CARDING

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*.

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

1. 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.
2. Pelaku menggunakan data-data tesebut untuk berbelanja secara *on-line*.

3. Transaksi terjadi dan tagihan akan dibebankan kepada nasabah yang memiliki kartu dengan data-data yang telah digunakan secara *illegal* oleh pelaku.

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

- Simpan dan perlakukan kartu debet dan/atau kartu kredit dengan baik.
- 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.
- Berhati-hati dalam menggunakan kartu kredit pada saat bertransaksi, untuk menghindarkan pencatatan data-data penting oleh *merchant*.
- 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.

G. PHONE BANKING

NOMOR *CALL CENTER* PALSU DAN/ATAU NOMOR *PHONE BANKING* PALSU

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:

1. 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.
2. Jika ada nasabah yang menghubungi nomor tersebut, pelaku akan berpura-pura bertindak sebagai petugas bank.
3. Pelaku meminta nasabah menyebutkan data rahasia nasabah, seperti PIN, nomor kartu kredit, masa berlaku kartu kredit, dan kode pengaman kartu kredit (CVV).
4. Setelah mendapatkan data-data rahasia dari nasabah melalui nomor *call center* palsu atau nomor *phone banking* palsu,

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

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

Hal-hal yang dapat dilakukan untuk meminimalisir bahaya nomor *call center* palsu :

- Meminta nomor *call center* atau nomor *phone banking* secara langsung dari kantor cabang, *website* resmi dan atau publikasi resmi dari bank.
- Simpan dan catat nomor *call center* dan/atau nomor *phone banking* pada daftar nomor telepon di ponsel.
- Batalkan transaksi jika nasabah curiga dengan nomor telpon tersebut ataupun curiga dengan respon dari nomor telpon tersebut.

MENEBAK PIN SECARA BERULANG-ULANG

Modus kejahatan dengan cara menebak nomor PIN *phone banking* nasabah secara berulang-ulang dapat dilakukan dengan memanfaatkan kelemahan sistem bank yang setiap hari melakukan *reset counter number* yang menampung jumlah kesalahan nomor PIN sehingga PIN tersebut tidak akan pernah terblokir. Pelaku yang telah memiliki kartu debit dapat mencoba memasukkan

nomor PIN berulang kali namun untuk menghindari terblokirnya kartu tersebut, sebelum mencapai frekuensi maksimum kesalahan PIN, pelaku berhenti mencoba memasukkan PIN dan mencobanya kembali pada keesokan harinya dengan metode yang sama hingga didapatkan nomor PIN yang benar.

Dalam melakukan aksinya, cara yang digunakan oleh pelaku antara lain:

1. Pelaku mencari beberapa data sensitif dan penting dari nasabah, antara lain nomor rekening, nomor kartu debet dan/ atau kartu kredit, tanggal *expired* atau masa berlaku kartu, limit kartu, dan beberapa data lainnya yang dapat digunakan untuk verifikasi transaksi *phone banking*.
2. Pelaku menghubungi nomor *phone banking*, dan mencoba melakukan verifikasi dengan memasukkan PIN. PIN yang dimasukkan tersebut merupakan tebakan dari pelaku.
3. Apabila kesalahan PIN sudah mendekati batas kesalahan yang diperkenankan, maka pelakukan akan menghentikan upayanya dan mencobanya di lain waktu.
4. Apabila tebakan PIN benar, maka pelaku dapat melakukan transaksi melalui fasilitas *phone banking* tersebut.

Hal-hal yang dapat dilakukan untuk meminimalisir bahaya menebak PIN secara berulang-ulang :

- Menjaga data-data rahasia dan sensitif seperti nomor rekening, nomor kartu debet dan/atau kartu kredit, tanggal *expired* atau masa berlaku kartu, limit kartu, dan beberapa data lainnya yang dapat digunakan untuk verifikasi transaksi *phone banking*.
- Secara periodik melakukan pengecekan transaksi pada rekening.
- Memanfaatkan fasilitas notifikasi transaksi *phone banking* melalui SMS apabila bank menyediakan layanan tersebut.

H. VIDEO BANKING

BOOTH VIDEO BANKING PALSU

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* yang cara kerjanya telah dijelaskan pada pembahasan sebelumnya.

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

1. Membuka *booth video banking* yang menyerupai dengan *booth* asli yang dimiliki bank.
2. Melengkapi *booth* tersebut dengan nomor *call center* palsu untuk mengelabui nasabah yang memerlukan bantuan langsung petugas.
3. 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*.
4. Mempergunakan informasi identitas dan kartu nasabah untuk bertransaksi.

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

- 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.
- Mencari nomor telepon bank yang sebenarnya dan kemudian menghubungi bank tersebut untuk melaporkan atau menanyakan kebenaran keberadaan *booth* tersebut.
- Tidak menyampaikan data identitas ataupun data kartu.

OTORITAS JASA KEUANGAN

Mengatur
Mengawasi
Melindungi

Untuk Industri Keuangan yang Sehat

OTORITAS JASA KEUANGAN

MENGATUR - MENGAWASI - MELINDUNGI

UNTUK INDUSTRI KEUANGAN YANG SEHAT

BAB IV - PENUTUP

Perkembangan operasional perbankan yang menggunakan modernisasi teknologi informasi dalam rangka memenuhi kebutuhan masyarakat terhadap pelayanan perbankan yang cepat dan efisien serta kebijakan *less cash society* menjadi *trend* perkembangan produk perbankan kedepan melalui layanan produk e-banking. Di sisi lain produk bank ini dapat menimbulkan risiko apabila tidak didukung dengan *environment, security,* prosedur dan manajemen risiko yang memadai dari bank yang menyediakan produk tersebut termasuk pemahaman yang memadai dari nasabah pengguna maupun calon pengguna produk e-banking.

Transaksi e-banking baik frekuensi maupun *volume* transaksi dari beberapa bank di Indonesia selama kurun waktu tahun 2012, 2013 dan 2014 menunjukkan perkembangan yang pesat. Kedepannya, sejalan dengan perkembangan teknologi, kebutuhan masyarakat dan tuntutan terhadap perbankan yang semakin efisien, maka transaksi dan nasabah termasuk bank yang menyelenggarakan produk e-banking diperkirakan semakin meningkat. Hal tersebut menimbulkan pula tantangan terhadap penyelenggaraan e-banking, kebutuhan pengawasan terhadap perbankan dan di sisi lain perlunya edukasi kepada masyarakat luas.

Selanjutnya, Otoritas telah, sedang dan akan terus melakukan pengaturan dan pengawasan terhadap produk e-banking untuk lebih meyakini bahwa operasional bank tekait dengan produk e-banking senantiasa mengacu kepada prinsip kehati-hatian sehingga aman dan nyaman bagi nasabah perbankan untuk melakukan transaksi dan menggunakan produk e-banking.

Buku ini diharapkan dapat menjawab sebagian dari kebutuhan dan tantangan penyelenggaraan dan penggunaan e-banking. Meskipun demikian, isi buku ini tidak menjamin dan memastikan bahwa penyelenggara dan pengguna produk e-banking menjadi terbebas dari segala risiko baik *financial* maupun *non-financial* dalam menyelenggarakan dan bertransaksi dengan e-banking.

GLOSSARY

3-D Secure:

pengamanan tambahan berupa kode sekali pakai atau *One Time Password* (OTP) untuk bertransaksi kartu kredit secara *on-line*. Sistem bank mengirimkan kode acak melalui SMS ke nomor ponsel nasabah pada saat nasabah melakukan transaksi *on-line*.

Access - akses:

jalan masuk. Suatu usaha untuk membuka suatu saluran komunikasi dengan perangkat *hardware* atau *software* tertentu, seperti *modem* yang digunakan untuk membuka akses internet. Perangkat *hardware* atau *software* tersebut selain untuk memberikan data juga digunakan untuk menerima data untuk disimpan.

Account:

penampungan data tentang seseorang, sedikitnya terdiri dari nama pengguna dan *password*. Di dalam sistem perbankan, *account* adalah satu data kepemilikan atas suatu produk perbankan, dapat terdiri dari nama nasabah, kode produk, nilai nominal yang dimiliki.

Access point:

perangkat keras yang memungkinkan perangkat *wireless* lain (seperti *laptop*, ponsel) untuk terhubung ke jaringan kabel menggunakan *Wi-fi, bluetooth* atau perangkat standar lainnya.

Auto-lock:

penguncian otomatis terhadap suatu perangkat (misalnya ponsel) dengan parameter waktu atau tombol tertentu sehingga perangkat tersebut tidak dapat digunakan oleh orang lain yang tidak memiliki akses.

Bisnis Daring atau online shop:

suatu kegiatan atau pekerjaan untuk memasarkan produk yang dimilikinya dengan mempergunakan jaringan internet dengan tujuan untuk memperoleh keuntungan.

Browser:

perangkat lunak yang berfungsi untuk menerima dan menyajikan sumber informasi di Internet.

Card reader:

alat untuk membaca kartu elektronik.

Card Verification Value (CVV):

tiga digit angka terakhir yang terdapat pada bagian belakang kartu kredit, biasanya berada di tempat tanda tangan pada kartu kredit.

Cash Deposit Machine (CDM):

mesin ATM yang memungkinkan nasabah dapat melakukan penyetoran tunai melalui mesin ATM secara *real time on-line* dengan rekening dan secara otomatis mesin ATM tersebut akan mendeteksi denominasi dan kondisi fisik uang (asli atau palsu, baik atau rusak).

Clonning:

penggandaan atau duplikasi terhadap suatu barang.

Closed Circuit Television (CCTV):

suatu sistem yang digunakan sebagai pelengkap keamanan dan pemantauan yang banyak digunakan untuk di perkantoran, toko, industri, militer, perumahan, di sekitar aset milik perbankan.

Customer Service:

petugas bank yang melayani nasabah untuk keperluan pembukaan rekening, perubahan data nasabah, pengaduan nasabah, dan layanan *non-financial* lainnya.

Delivery Channel:

jalur atau media yang digunakan oleh bank untuk memberikan layanan kepada nasabahnya baik secara konvensional ataupun elektronik, yang meliputi : *teller, SMS Banking, Mobile Banking, Phone Banking, EDC, Internet Banking*, ATM*, Video Banking, E-commerce.*

Digital Banking:

satu cara akses ke sistem perbankan yang dapat dilakukan kapan saja dan dimana saja dengan menggunakan jaringan internet.

Unduh:

adalah meminta sebuah *file* dari komputer lain (*web site, server* atau yang lainnya) dan menerimanya.

Electronic Banking (E-Banking):

layanan yang memungkinkan nasabah bank untuk memperoleh informasi, melakukan komunikasi, dan melakukan transaksi perbankan melalui media elektronik seperti *Automatic Teller Machine* (ATM), *phone banking, Electronic Fund Transfer* (EFT), *Electronic Data Capture* (EDC) / *Point Of Sales* (POS), *internet banking* dan *mobile banking.*

E-mail/surat elektronik:

sarana kirim mengirim surat melalui jalur jaringan komputer (misalnya Internet).

E-money atau stored value atau prepaid card:

produk yang merupakan media yang dipakai dalam mekanisme sistem pembayaran melalui pembayaran di *point of sales (merchant),* transfer antar dua media elektronik atau jaringan komputer menggunakan nilai uang yang tersimpan pada kartu atau produk tersebut.

Enkripsi:

alat untuk mencapai keamanan data dengan menerjemahkannya dengan menggunakan sebuah *key (password).* Enkripsi mencegah *password* atau *key* supaya tidak mudah dibaca pada *file* konfigurasi.

Fee-based income:

komisi yang diterima bank dari pemasaran produk maupun transaksi jasa perbankan yang dibebankan kepada nasabah sehubungan dengan produk dan jasa bank yang dinikmatinya.

File:

kumpulan data yang berisi informasi, dapat berupa dokumen atau elektronik dan dapat tersimpan di dalam suatu tempat penyimpanan fisik atau digital. Untuk *file* elektronik memiliki berbagai format dengan kegunaan yang berbeda.

Firewall:

peralatan untuk menjaga keamanan jaringan yang melakukan pengawasan dan penyeleksian atas lalu lintas data/informasi melalui jaringan serta memisahkan jaringan privat dan publik. Peralatan ini dapat digunakan untuk melindungi komputer yang telah terhubung ke jaringan dari serangan yang dapat mengkompromikan suatu komputer.

Fraud:

segala macam yang dapat dipikirkan dan diupayakan oleh seseorang untuk mendapatkan keuntungan dari orang lain dengan cara yang tidak jujur yang menyebabkan orang lain tertipu.

General Packet Radio Service (GPRS):

teknologi yang memungkinkan pengiriman dan penerimaan data dalam bentuk paket data, seperti *e-mail*, gambar, dll.

Interactive Voice Response (IVR):

teknologi telepon dimana pelanggan menggunakan telepon untuk terhubung dengan *database* yang berisi informasi tanpa harus berbicara dengan petugasnya.

Kartu kredit:

kartu yang dikeluarkan oleh pihak bank dan sejenisnya untuk memungkinkan pembawanya membeli barang-barang yang dibutuhkannya secara hutang. Kartu kredit merupakan suatu jenis penyelesaian transaksi ritel, yang diterbitkan kepada pengguna sistem tersebut sebagai alat pembayaran yang dapat digunakan dalam membayar suatu transaksi.

Kartu debit:

sebuah kartu pembayaran secara elektronik yang diterbitkan oleh bank yang berfungsi sebagai pengganti pembayaran dengan uang tunai.

Keyboard:

perangkat keras pada komputer yang berbentuk papan dengan berbagai macam fungsi perintah yang selanjutnya dikirim ke perangkat CPU. *Keyboard* terdiri dari banyak tombol ketik dengan simbol masing-masing.

Keylogger:

ancaman berupa perangkat lunak atau perangkat keras/*hardware* yang digunakan untuk memperoleh informasi (PIN, *password*) yang diketikkan pengguna pada *keyboard* (biasanya di warung internet).

Leased Line:

saluran koneksi telepon permanen antara dua titik yang disediakan oleh perusahaan telekomunikasi publik. Umumnya, *leased line* digunakan ketika terdapat kebutuhan komunikasi data jarak jauh yang harus dilakukan secara terus-menerus. *Leased line* memiliki beberapa tingkatan tarif yang bergantung kepada lebar jalur data *(bandwidth)* yang mampu dikirimkan melalui jaringan *leased line* tersebut.

Less cash society:

gaya hidup dengan menggunakan uang elektronik dalam bertransaksi, sehingga tidak perlu membawa uang fisik.

Login:

proses untuk mengakses komputer atau sistem atau aplikasi atau suatu layanan di media elektronis dengan memasukkan informasi yang telah terdaftar seperti *user id* dan *password.*

Malware:

perangkat lunak yang diciptakan untuk menyusup dan merusak sistem komputer tanpa izin dari pemilik.

Marketing:

proses menawarkan barang dan jasa kepada calon pelanggan.

Merchant:

penjual barang/jasa yang memiliki *physical store* maupun *on-line store* yang bekerja sama dengan bank dalam penyediaan layanan penerimaan pembayaran.

Media Sosial:

media *on-line* yang memungkinkan manusia untuk saling berinteraksi satu sama lain tanpa dibatasi ruang dan waktu.

On-line:

sistem atau komputer yang terkoneksi/terhubung dengan jaringan internet.

Off-line:

sistem atau komputer yang tidak terdapat hubungan jaringan atau tidak dapat berkomunikasi dengan sistem atau komputer lain.

One Time Password (OTP) :

kode verifikasi yang dikirimkan melalui SMS atau email untuk memastikan kebenaran transaksi oleh pemilik rekening.

Password:

kode atau simbol khusus untuk mengamankan sistem komputer yaitu untuk mengidentifikasi pihak yang mengakses data, program atau aplikasi komputer dan digunakan.

Pattern-lock:

penguncian layar perangkat (misalnya ponsel) menggunakan metode penguncian dengan pola, berfungsi seperti *password.*

Personal Identification Number (PIN):

rangkaian digit unik terdiri dari huruf, angka atau kode ASCII yang digunakan untuk mengidentifikasi pengguna komputer, pengguna ATM, internet banking, mobile banking,dll.

Pita magnetis (Card's magnetic stripe):

suatu pita perekam yang digunakan untuk media penyimpan data. Setiap karakter ditulis melintasi lebar pita dalam bentuk bintik-bintik yang diberi muatan magnet, pembacaan dari dan penulisan ke pita dilakukan dengan menggerakkan permukaan pita melintasi suatu *read/write head sebuah tape drive.*

Pop Up:

jendela yang muncul ketika mengunjungi halaman suatu web atau aplikasi.

Screen-lock:

penguncian layar perangkat (misalnya ponsel) sehingga *user* yang tidak memiliki akses tidak dapat mempergunakannya. Metode *screen-lock* dapat berupa penguncian dengan *password* atau pola.

Server:

sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer.

Setting:

pengaturan baik terhadap perangkat keras atau perangkat lunak.

Subscriber Identity Module (SIM) Card:

sebuah kartu pintar dalam berbagai ukuran yang menyimpan kunci pengenal jasa telekomunikasi sehingga dapat saling berkomunikasi.

Smartphone:

ponsel pintar atau ponsel cerdas yaitu telepon genggam yang mempunyai kemampuan dan fungsi menyerupai komputer.

Social Engineering:

teknik pembohongan melalui perilaku sosial yang dilakukan oleh hacker untuk mengelabui orang agar memberikan informasi rahasia seperti PIN, *Password*, dll.

Software / perangkat lunak:

sekumpulan program elektronik yang dapat menjalankan suatu perintah.

Teller:

petugas bank yang melayani transaksi simpanan, penarikan, pencairan cek, dan pelayanan perbankan tunai /non tunai lainnya kepada nasabah.

Token:

alat pengaman tambahan untuk melakukan transaksi finansial di *internet banking*.

Unstructured Suplementary Service Data (USSD):

sebuah protokol berbasis GSM untuk berkomunikasi dari *handphone* pengguna ke penyedia layanan telekomunikasi (dan sebaliknya).

Upgrade:

penggantian produk dengan versi yang lebih baru atau lebih baik dengan produk yang dihasilkan oleh perusahaan yang sama.

User Identification/User ID:

serangkaian huruf, angka, simbol atau kombinasinya untuk mengidentifikasi pihak yang mengakses data, program atau aplikasi komputer dan digunakan dengan tujuan mengamankan suatu sistem atau aplikasi tersebut.

Virtual account:

nomor identifikasi pelanggan yang dibuka oleh bank atas permintaan perusahaan untuk diberikan oleh perusahaan kepada pelanggannya (perorangan maupun non perorangan) sebagai nomor rekening tujuan penerimaan *(collection)*.

Virus:

program yang bersifat merusak dan akan aktif dengan bantuan orang (dieksekusi), dan tidak dapat mereplikasi sendiri, penyebarannya karena dilakukan oleh orang, seperti *copy,* biasanya melalui *attachement e-mail, game,* program bajakan dll.

Website:

web page atau informasi yang disampaikan melalui suatu *web browser* atau sekumpulan *web page* yang dirancang, dipresentasikan dan saling terhubung untuk membentuk suatu sumber informasi dan atau melaksanakan fungsi transaksi.

Wireless :

jaringan komunikasi dimana perangkat-perangkat di dalamnya (PC, komputer, ataupun *handphone*) dapat berkomunikasi tanpa kabel.

OTORITAS JASA KEUANGAN

MENGATUR - MENGAWASI - MELINDUNGI

UNTUK INDUSTRI KEUANGAN YANG SEHAT

Otoritas Jasa Keuangan
Gedung Soemitro Djojohadikusumo
Jalan Lapangan Banteng Timur 2-4
Jakarta 10720
(021) 385 8001
(021) 385 8321

CALL CENTER
LAYANAN KONSUMEN
(kode area) 500 655

OJK OTORITAS JASA KEUANGAN