KIAT KIAT PENGAMANAN MENGGUNAKAN bjb NET

Sistem bjb NET dirancang sedemikian rupa secara optimal untuk dapat memberikan proteksi keamanan bagi nasabah saat bertransaksi di bjb NET. Namun demikian setiap pengguna layanan keuangan melalui media Internet tidak terlepas dari berbagai ancaman kejahatan termasuk bjb NET. Berikut ini beberapa hal Kiat-Kiat Menggunakan bjb NET:

I. Umum

a. Peduli terhadap pentingnya sistem pengamanan saat bertransaksi melalui bjb NET;

b. Pendaftaran bjb NET dapat dilakukan melalui ATM bank **bjb**. Nasabah akan mendapatkan ACCESS CODE sebanyak 6 digit, sesegera mungkin lakukan aktivasi melalui bjb NET dan musnahkan *struk* jika telah selesai melakukan aktivasi bjb NET;

c. Jagalah keamanan UserID dan *Password* bjb NET anda dengan baik dan benar, *Password* merupakan salah satu kunci utama dari mekanisme Pengamanan anda dalam bertransaksi di bjb NET;

d. Akseslah bjb NET di tempat-tempat yang menurut anda aman, tidak ditempat publik seperti warnet;

e. Jangan meninggalkan *browser* dalam keadaan Login ke bjb NET;

f. Tetap waspada.

II. Khusus

Ancaman-ancaman saat menggunakan Internet Banking yang mungkin ditemui oleh nasabah dengan ciri-ciri serta kiat-kiat pengamanannya sebagai berikut :

a. Phising

Phishing merupakan suatu bentuk penipuan lewat internet, biasanya ditandai dengan adanya permintaan informasi penting yang dimiliki oleh Anda, seperti rekening kartu kredit, rekening bank, password, PIN dan lain sebagainya;

Terdapat beberapa cara dalam melakukan Phising yaitu :

- Para pelaku phishing tersebut biasanya akan mengirim e-mail ke pada korban yang menyatakan bahwa anda mendapat bonus atau suatu undian, dan menyamar sebagai orang yang benar-benar dapat dipercaya sehingga secara tidak sadar korban telah menyerahkan data-data yang sangat berharga;
- Para pelaku mengirimkan email kepada korban yang berisi halaman login untuk meminta nasabah memasukan *Username* dan *Password*;
- Mengirimkan alamat *website* yang dibuat semirip mungkin namun ternyata palsu sehingga dapat menangkap *Username* dan *Password* yang dimasukan nasabah.

Kiat-Kiat Pengamanan :

- Jika Anda menerima e-mail yang meminta Anda untuk memperbarui informasi bjb NET anda, pergi ke situs web dengan mengetikkan URL **https://ib.bankbjb.co.id** dalam bidang alamat *browser* anda, daripada mengklik link dalam e-mail tersebut. Bank **bjb** tidak pernah mengirimkan email kepada nasabah pengguna bjb NET untuk memperbaharui informasi nasabah;
- Apabila anda terjebak modus phising diatas dan merasa *Username* dan *Password* anda tidak rahasia lagi, segera ganti *Password* anda melalui menu **Profile Pengguna – Ubah Password**.
- Pastikan alamat bjb Net yang anda akses adalah **https://ib.bankbjb.co.id** serta pastikan pula pada alamat *browser* anda terlihat gambar gembok/kunci ( ).

b. KeyLogger

Keylogger adalah suatu program (walaupun jarang, tapi juga ada *keylogger* berbentuk *hardware*) yang dirancang khusus untuk mencatat segala aktifitas *keyboard* dan menyimpan hasilnya kedalam sebuah *log* atau catatan teks. *Keylogger* biasanya dipasang untuk mendapatkan suatu informasi rahasia seperti *Username*, *password*, nomor rekening dan PIN dan segala sesuatu yang anda ketik menggunakan *keyboard*.

Terdapat beberapa cara dalam melakukan KeyLogger :

- Para pelaku *keylogger* telah menanamkan sebelumnya *tools* yang akan digunakan untuk merekam segala aktivitas yang dilakukan melalui *keyboard*;

Kiat-kiat pengamanan :

- Pastikan untuk melakukan input beberapa hal yang sifatnya sensitif seperti UserID, *Password*, *Soft Token* dan Nomor Rekening menggunakan *On-Screen Keyboard*. Untuk beberapa form didalam bjb NET telah dilengkapi *On-Screen Keyboard* seperti pada halaman login, aktivasi input seluruh data nasabah serta *Update* profile nasabah. Namun untuk menambah keyakinan nasabah dapat menggunakan *On-Screen Keyboard* yang telah disediakan dari beberapa *Operating System* saat nasabah mengakses bjb NET. (contoh pada microsoft windows XP : Klik Start Pilih **Program > Accessories > Accessibility > On-Screen Keyboard**).
- Pastikan dengan menggunakan **Anti Virus** terbaru (karena beberapa anti virus akan dapat mendeteksi *keylogger* sebagai virus)
- Menggunakan **anti *keylogger*** bila memungkinkan.

c. Virus / Worm

Virus komputer adalah suatu program komputer yang menduplikasi atau menggandakan diri dengan menyisipkan kopian atau salinan dirinya ke dalam media penyimpanan / dokumen serta ke dalam jaringan secara diam-diam tanpa sepengetahuan pengguna komputer tersebut.

Worm dibuat untuk dapat menyebar dengan cepat ke banyak komputer. Walaupun umumnya worm tidak menimbulkan kerusakan seperti virus, namun worm dapat digunakan untuk membawa berbagai macam muatan/attachment termasuk yang berbahaya.

Ciri-ciri komputer yang terinfeksinya virus komputer sangat beragam dengan beberapa contoh sebagai berikut :

- Komputer berjalan lambat dari keadaan normal;
- Media penyimpanan seperti *disket*, *flashdisk*, dan sebagainya langsung melakukan *copy file* aneh tanpa adanya perintah *copy* dari kita ketika kita hubungkan ke komputer.
- Komputer adakalanya melakukan *restart* dengan sendirinya
- Tidak dapat mengakses harddisk
- Komputer melambat lalu "*hang*" atau berhenti memberikan respon
- Hilangnya beberapa fungsi dasar komputer
- Kehilangan data.

Kiat-kiat pengamanan :

- Lakukan *update* atau *patch* pada *software* atau *operating system* yang digunakan pada komputer anda yang bersumber dari perusahaan pembuat *software* atau *operating system*;
- Install program aplikasi komputer yang orisinil atau asli bukan bajakan sehingga tidak ditunggangi virus dan modus kejahatan komputer lainnya;
- Install Anti Virus yang anda yakini cukup aman, serta lakukan *update* anti virus secara berkala dan scan komputer anda secara *real-time*;
- Salah satu media penyebaran Virus dan modus kejahatan internet lainnya yaitu melalui email. Hati-hatilah dalam penggunaan email terutama bila mendapati email yang mencurigakan datang dari pengirim yang tidak dikenali.
- Scan *email attachment* sebelum dibuka;
- Pada beberapa *Operating System* telah tersedia *personal firewall.* Install dan atur sedemikian rupa untuk memberikan proteksi pada komputer anda;
- Tidak mengakses atau download dan install program aplikasi dari internet yang berasal dari situs yang tidak anda dikenali;
- Lakukan *scan* terlebih dahulu sebelum membuka *file* yang berasal dari berbagai media seperti berasal dari disket, CD, DVD, flashdisk ataupun media USB *drive* lainnya;

d. Spyware

Spyware adalah aplikasi yang membocorkan data informasi kebiasaan atau perilaku pengguna dalam menggunakan komputer ke pihak luar tanpa kita sadari. Biasanya *spyware* masuk atau menginfeksi komputer karena mendownload kontent dari internet atau menginstall program tertentu dari suatu situs.

Ciri terinfeksinya *Spyware* pada komputer diantaranya sebagai berikut :

- Kinerja komputer akan terasa lambat, terutama jika terhubung dengan internet.
- *Browser* terkadang atau seringkali macet (hang/crash) saat akan membuka halaman *web* tertentu;

- Alamat situs yang sudah di-set secara *default* sering berubah;
- Terkadang *browser* terbuka dengan sendirinya secara masal dan langsung mengakses situs tertentu.

Kiat-kiat pengamanan :
Secara umum kiat pengamanan sama dengan kiat pengamanan Virus / Worm, namun terdapat beberapa kiat tambahan yaitu :

- Hati-hati terhadap situs yang meminta installasi program tertentu.
- Untuk penggunaan aplikasi secara gratis, perhatikan *review* dari penggunanya, apakah terdapat *spyware* atau tidak.