Tutorial Mencegah Serangan Keylogger

Informasi tentang **tips atau cara mencegah serangan keylogger** di komputer. Semakin hari semakin bertambah penggunaan komputer dan koneksi internet oleh masyarakat di seluruh dunia. Baik itu digunakan sebagai sarana untuk belajar, bekerja, bisnis, bermain game, maupun sekedar sebagai media hiburan. Dengan kondisi yang demikian, penggunaan komputer baik itu di rumah, di kantor, di sekolahan, maupun di tempat-tempat yang lain, masih banyak yang belum menyadari bagaimana cara melindungi komputer dari serangan-serangan berbahaya yang mengancam. Serangan berbahaya yang mengancam komputer meliputi *serangan keylogger, virus komputer, spyware, malware, spam, adware, phishing*, dan upaya penipuan yang lain untuk mencuri identitas pribadi, akun pribadi, password, maupun data keuangan. Hal wajib yang harus dimiliki untuk *mengatasi serangan keylogger* dan sejenisnya terhadap komputer adalah dengan memasang antivirus yang selalu update, menginstal *security software* (memasang program pengaman seperti anti spyware, anti malware, anti keylogger, anti adware), dan perilaku si pengguna komputer atau user yang harus bisa melindungi informasi data pribadi, informasi akun dan password yang benar dan aman, terlebih lagi apabila tersambung dengan internet.

Keylogger atau **Key Stroke Recorders** disini adalah suatu jenis spyware yang diciptakan dan dijalankan untuk *mencuri informasi user ID*, password, dan input data, ketika seseorang masuk atau login ke dalam website tertentu. Apabila kita telah memasang anti virus dan software anti keylogger yang bagus, atau telah meng-instal *software anti malware* dan *anti spyware* yang bagus, maka komputer akan terlindungi dari serangan keylogger. Anti malware atau anti spyware yang bagus harus mencakup scanner keylogger, sehingga akan mendeteksi keberadaan program keylogger yang mengintai dan kemudian menghapusnya. Mereka yang menggunakan komputer pribadi, apakah itu di rumah, di sekolah, atau di kantor, harus memahami kebutuhan untuk melindungi komputer mereka dari *serangan keylogger, virus komputer, spyware, adware,* dan *malware*. Karena program-program jenis ini (*virus, spyware, malware, adware*) memang sengaja diciptakan untuk dapat menyebabkan banyak kerusakan komputer, ketidaknyamanan bagi penggunaan komputer, sampai pada tindakan kriminal atau *cyber crime* seperti *penipuan online, manipulasi data,* dan *pencurian*.

Penjahat cyber sering menggunakan infeksi virus, spyware dan malware dalam upaya untuk mencuri identitas pribadi seseorang dan informasi password, untuk mendapatkan akses ke rekening bank tertentu. Keylogger merupakan elemen yang paling sering digunakan dalam hal ini, keylogger akan *mendeteksi User ID* dan password ketika seseorang terhubung ke rekening bank secara online. User ID dan password yang telah berhasil diperoleh dari Keylogger kemudian akan digunakan (secara curang) untuk mencuri uang dari rekening bank orang tersebut. Para pengguna jasa keuangan atau bank online harus berhati-hati dengan kemungkinan adanya kecurangan atau serangan keylogger ini.

Tips atau cara mencegah serangan keylogger di bank online atau di situs lainnya

adalah :
- pasang antivirus yang selalu update
- pasang software anti keylogger atau anti spyware dan anti malware
- selalu mengikuti saran keamanan yang ada pada halaman keamanan (security page) dari situs bank online Anda.
- ketika Anda memasukkan user ID dan password pada form login, gunakanlah fasilitas *virtual keyboard* atau *on-screen keyboard* bawaan dari operating system di komputer. (untuk Windows 7 bisa ditemukan di Start > All Programs > Accessories > Ease of Access > On-Screen Keyboard)
- apabila tidak menggunakan *On-Screen Keyboard*, gunakanlah Notepad untuk menulis user ID dan password, lalu Anda Copy dan kemudian Paste ke Form Login.
- jangan pernah Anda konfirmasi ketika ada pop-up dari browser yang menanyakan tentang simpan otomatis user dan password yang baru saja Anda masukkan. (pilih saja NEVER)
- selalu logout ketika Anda sudah selesai melakukan aktivitas atau transaksi di bank online atau situs-situs yang lain.
- bersihkan cookies dan cache di browser yang Anda pakai. *Cara membersihkan cookies* dan cache di Mozilla Firefox adalah dengan menekan tombol *Ctrl-Shift-Del*, kemudian pada *Time range to clear* dipilih *Everything*, pada *Details* dicentangi semua, kemudian tekan *Clear Now.*

Serangan atau *penipuan online* yang juga peru diperhatikan adalah serangan yang disebut dengan "*phishing*". *Phishing* adalah serangan atau penipuan dengan menggunakan e-mail atau telepon untuk menyamar sebagai staf bank, atau undian berhadiah, dana hibah dan sejenisnya, dimana tujuannya untuk mengelabui pelanggan/calon korban untuk mengungkapkan rincian rekening bank dan passwordnya.
Cara mengatasi phishing atau penipuan online semacam itu adalah :
- perhatikan alamat pengirim email, apakah dari situs resmi bank Anda atau bukan
- kalimat sapaan dalam email, apabila berupa kaimat secara umum dan tidak spesifik menyebutkan nama Anda, maka Anda harus waspada
- untuk email yang berupa janji hadiah atau dana hibah onlline, maka Anda cari informasi yang lebih lengkap tentang hadiah atau dana hibah online tersebut di situs resminya atau cari informasi tentang penipuan online atau hadiah dan *dana hibah online* di forum-forum besar seperti di kaskus.co.id, atau di scam.com

Demikianlah tips atau **cara mencegah serangan keylogger** di komputer dan beberapa hal yang perlu diperhatikan sehubungan dengan *serangan keylogger* dan *tindakan phishing*, *penipuan online* maupun *tindakan kriminal online* yang sewaktu-waktu bisa menyerang kita. Semoga bermanfaat.