**Penipuan Komputer**

**Ahli setuju bahwa bisnis e-commerce di sini untuk tinggal.** Semakin banyak orang di seluruh dunia menjadi nyaman dengan proses pembelian secara online. Tapi karena lebih banyak orang mulai membeli barang secara online, penipuan komputer menjadi masalah yang lebih besar daripada siapa pun bisa menebak.

Penipu sekarang ini tidak hanya remaja bosan lagi. Para penjahat online saat ini ahli komputer terampil yang tahu bagaimana memanipulasi komputer Anda agar memberi mereka informasi yang mereka butuhkan untuk skema penipuan komputer mereka. Dan bagian terburuk adalah bahwa Anda dapat memiliki informasi penting dicuri dari Anda tanpa pernah mengetahui apa yang telah terjadi.

Jika Anda ingin melindungi diri dari **penipuan komputer,** maka hal terbaik yang dapat Anda lakukan adalah belajar lebih banyak tentang hal itu.

**Anatomi skema Penipuan Komputer:**

Sebuah kriminal online membutuhkan informasi pribadi Anda sebelum ia bisa melakukan apa saja. Jadi bagaimana dia mendapatkannya? Sebagian besar skema mulai dengan jenis program yang disebut spyware. Sebuah program spyware adalah software yang, setelah diinstal, mengumpulkan informasi tentang Anda dan kemudian mengirimkannya kembali ke sumbernya. Anda mungkin tidak tahu, tetapi komputer Anda menyimpan file penuh dengan informasi tentang Anda. Temporary Internet file, file cache, dan file browser history berisi informasi seperti nama, alamat, nomor telepon Anda, apa website yang Anda kunjungi, apa jenis pembelian online membuat Anda, dan bahkan nomor kartu kredit Anda. Jadi semua sepotong spyware harus lakukan adalah menemukan file-file dan laporan segala sesuatu yang ditemukan.

Spyware mendapat ke sistem Anda melalui manipulasi teknologi yang disebut [ActiveX](http://translate.googleusercontent.com/translate_c?depth=1&ei=b0r5UOGeCpHKrAf24YCACA&hl=id&langpair=en%7Cid&rurl=translate.google.com&twu=1&u=http://articles.winferno.com/web-browser-security/dangers-of-activex/&usg=ALkJrhguFlCqv7kFhB6uTUBDmTIx03K0Qg) . ActiveX dikembangkan untuk membuat website yang lebih baik. Anda bank atau toko online favorit mungkin menggunakan ActiveX. Tapi ketika seorang penjahat secara online memanipulasi ActiveX, dapat digunakan untuk jarak jauh menginstal perangkat lunak berbahaya di komputer Anda. Ini berarti bahwa dengan hanya mengunjungi website yang mencurigakan, Anda bisa terinfeksi spyware, dan Anda akan tidak tahu.

Setelah panen penipu semua informasi dari Anda bahwa dia membutuhkan, masalah nyata Anda dimulai. Dia dapat menggunakan informasi Anda untuk menjalankan utang atau bahkan lebih buruk, mencuri identitas Anda. Sebagian besar korban pencurian identitas menghabiskan bulan atau bahkan bertahun-tahun serta ribuan dolar dari uang mereka sendiri membersihkan nama mereka dan memperbaiki laporan kredit mereka. Dan sampai semua yang diperbaiki, korban dapat ditolak pinjaman, pendidikan, perumahan atau mobil, atau bahkan mungkin ditangkap karena kejahatan yang tidak mereka lakukan.

Penipuan komputer dapat menjadi hal yang paling dahsyat yang pernah akan terjadi pada Anda. Jika Anda ingin menyimpan penipuan komputer terjadi pada Anda, maka Anda berutang kepada diri sendiri untuk berinvestasi dalam perlindungan solid terhadap penipuan komputer.

# Berkontribusi  Keamanan Jaringan  dan  Penipuan Komputer & Keamanan

[Keamanan Jaringan](http://translate.googleusercontent.com/translate_c?depth=1&ei=b0r5UOGeCpHKrAf24YCACA&hl=id&langpair=en%7Cid&rurl=translate.google.com&twu=1&u=http://www.webvivant.com/nese.html&usg=ALkJrhglegnwO--WsN9n2Jvxq_ob0P_0-w) dan [Penipuan Komputer & Keamanan](http://translate.googleusercontent.com/translate_c?depth=1&ei=b0r5UOGeCpHKrAf24YCACA&hl=id&langpair=en%7Cid&rurl=translate.google.com&twu=1&u=http://www.webvivant.com/cfs.html&usg=ALkJrhhb34GwCKJM4tbSwqqYXi1lBUn35A" \o "Penipuan Komputer & Keamanan) kontribusi sambutan dari orang-orang yang memiliki pengetahuan yang berharga untuk berbagi - termasuk peneliti, akademisi, praktisi keamanan, vendor, integrator, lembaga, departemen pemerintah, perdagangan atau badan teknis, konsultan, analis, dll

Kami selalu tertarik pada artikel yang berhubungan dengan tren, masalah, dan teknologi - yang lebih rinci atau teknis yang lebih baik.

Artikel-artikel perlu berurusan dengan subyek yang sangat spesifik - kami tidak menjalankan fitur umum, 'pikir potongan' atau ikhtisar, atau potongan pendapat sederhana. (Dan tidak ada salinan pemasaran - copy harus vendor-netral.) Tapi jika Anda memiliki informasi nyata dan wawasan untuk berbagi, silakan lakukan menghubungi.

Seperti jurnal yang dibaca oleh para profesional infosec, berkontribusi memberikan kesempatan untuk meningkatkan profil Anda di sektor ini. Semua artikel juga dimasukkan dalam database langsung secara online Ilmu Elsevier, yang digunakan oleh para profesional, peneliti dan akademisi sebagai sumber daya penelitian utama dan sumber kutipan.

Penipuan dan pengamanan komputer

a. Proses penipuan

Tiga karakteristik penipuan:

· The theft of something

· The conversion to cash

· The concealment

Cara yang umum dan efektif untuk menyembunyikan suatu pencurian adalah untuk membebankan item yang dicuri kesuatu akun biaya,cara lain untuk menyembunyikan asset adalah dengan cara gali lubang tutup lubang (lapping). Pada skema kiting, pelaku menutupi pencuriannya dengan cara menciptakan uang melalui transfer uang antar bank.

b. Sebab – sebab terjadinya penipuan

· penelitian menunjukkan bahwa terdapat tiga kondisi yang biasanya terjadi sebelum terjadinya penipuan yaitu:

- tekanan atau motif

a. Dilihat dari tekanan ekonomi yaitu karena adanya gaya hidup melebihi kemampuan, tingginya utang pribadi, pendapatan yang tidak cukup, besarnya kerugian keuangan , besarnya utang judi dan rendahnya tingkat kredit.

b. Dilihat dari tekanan pekerjaan yaitu gaji yang rendah, tidak adanya pengakuan atas kinerja, ketidak puasan atas pekerjaan, dan rasa takut akan kehilangan pekerjaan.

c. Tekanan lainnya yaitu tantangan,tekanan keluarga/rekan kerja,ketidak stabilan emosi,kebutuhan akan kekuasaan dan harga diri/ambisi yang berlebihan.

- Peluang

Peluang adalah kondisi atau situasi yang memungkinakan seseorang untuk melakukan dan menutupi suatu tindakan yang tidak jujur. Peluang seringkalo berasal dari kurangnya pengendalian internal,peluang paling umum menimbulkan penipuan.berasal dari kegagalan perusahaan untuk menjalankan system pengendalian.

- rasionalisasi

kebanyakan pelaku penipuan mempunyai alas an atau rasionalisasi yang membuat mereka merasa perilaku yang illegal tersebut sebagai sasuatu yang wajar.

Berikut adalah sebagian dari rasionalisasi yang paling sering digunakan:

· Pelaku “hanya meminjam” asset yang dicuri

· Apa yang saya lakukan tidak seserius itu.

c. Penipuan komputer

Department kehakiman Ameriak Serikat mendefinisikan computer sebagai tinfak illegal apapun yang membutuhkan pengetahuan teknologi computer untuk melakukan tindakan awal penipuan, penyelidikan atau pelaksanaannya.contoh: pencurian, penggunaan,akses,modifikasi,penyalinan,perusakan software atau data secara tidak sah.

· Peningkatan penipuan komputer

Organisasi-organisasi yang melacak penipuan komputer memperkirakan bahwa 80% usaha di Ameriak Serikat telah menjadi korban paling tidak sati insiden penipuan computer dengan biaya mencapai $10 miliar pertahun

· Penipuan dan teknik penyalahguanaan computer

Beberapa teknik penipuan dan penyalahgunaan computer:

- Cracking(menjebol)

- Data diddling (mengacak data)

- Data leakage (kebocoran data)

- Denial of service attack(serangan penolakan pelayanan)

- Eavesdropping (menguping)

- E-mail forgery and threats (pemalsuan e-mail)

- Hacking (melanggar masuk)

- Internet misinformation and terrorism (informasi yang salah diinternet dan terorisme internet)

- Logic time bomb (bom waktu logika)

- Masquerading or impersonation (menyamar atau meniru)

- Password cracking (penjebolan password)

- Piggybacking (menyusup)

- Round-down (pembuatan kebawah)

- Salami technique (teknik salami)

- Software privacy (pembajakn software)

- Scavenging (pencarian)

- Social engineering (rekayasa social)

- Virus

- Cacing

- Kuda troya

- Pintu jebakan

- Serangan cepat

d. Mencegah dan mendeteksi penipuan komputer

· Membuat standar tertentu dapat secara signifikan mengurangi potensi terjadinya penipuan dan kerugian yang dapat dihasilkannya

- Membuat penipuan lebih jarang terjadi

- Meningkatkan kesulitan untuk melakukan penipuan

- Memperbaiki metode deteksi

- Mengurangi kerugian akibat penipuan

- Menuntut dan memenjarakan pelaku penipuan

v Kesimpulan:

- Review tentang pengendalian internal perusahaan harus dilakukan untuk menganalisis efektifitas s=dalam mencegah penipuan.

- Pengendalian-pengendalian harus dilakukan dengan benar untuk mendeteksi penipuan.

- Para pegawai dala suatu perusahaan harus dilatih mengenai kesadaran atas penipuan, standar keamanan dan isu-isu etika.

Romney, Marshall B., 2006, Sistem Informasi Akuntansi, Edisi 9, Buku 1, Salemba Empat, Jakarta

# Cara Meningkatkan Keamanan Komputer

Berikut sharing mengenai berbagai cara meningkatkan keamanan komputer, keamanan komputer terbaru, keamanan komputer 2011, tips kemanan komputer, trik kemanan komputer, cara menjaga komputer, cara menambah keamanan komputer, cara aman komputer, keamanan komputer, cara meningkatkan keamanan komputer terbaru, cara menjada komputer dari cracker, tingkatkan keamanan komputer, tambah keamanan komputer, maksimalisasi keamanan komputer, maximal keamanan komputer. increase keamanan komputer, update keamanan komputer, tipss mengamankan komputer, tips meningkatkan komputer, cara membuat komputer aman, cara membuat komputer secure, cara bikin komputer supaya lebih aman, cara supaya komputer aman,, cara aman komputer 2011, keamanan komputer Indonesia.

LANGKAH UTAMA MENGAMANKAN KOMPUTER

Bagi para pengguna komputer baik yang terhubung dengan internet atau tidak, sudah saatnya untuk mengetahui bahwa bahaya akan kejahatan komputer terus mengintai baik disadari atau tidak, tinggal menunggu waktu yang tepat untuk menghancurkan isi komputer anda.

Terkait dengan berita di media online, tentang melesatnya penyebaran virus-virus buatan lokal yang tidak kalah merepotkannya dengan virus luar negeri, maka saya ingatkan untuk sebaiknya teman-teman pembaca selalu waspada. Dan waspada itu saya rangkum menjadi 9 langkah awal dalam mengamankan komputer. Ingat, ini adalah 9 langkah awal, kewaspadaan dan memperbaharui pengetahuan anda tentang cara-cara baru yang digunakan penjahat tetap senantiasa dibutuhkan.

Saat ini, pengguna komputer di Indonesia sebagian besar menggunakan Microsoft Windows sebagai sistem operasi, dan langkah ini memang ditujukan untuk sistem operasi tersebut.

1. Upgrade Sistem Operasi

Meng-upgrade sistem operasi ke yang lebih baru, setidaknya tetap mengikuti program terakhir yang disediakan.

Pengguna Microsoft Windows XP meng-upgrade ke Microsoft Windows XP Service Pack (SP) 2.

Untuk pengguna Microsoft Windows 95/98/ME/NT, disarankan meng-upgrade ke yang lebih tinggi.

Menutup celah keamanan pada sistem operasi dengan memasang security patch terkini.

2. Gunakan Firewall

Firewall membantu melindungi komputer dari hacker jahat, worm, dan beberapa spyware.

Gunakan Windows Firewall (tersedia pada Windows XP SP2) atau produk-produk firewall lainnya baik yang harus beli maupun yang gratis. Beberapa program firewall komersial adalah ZoneAlarm, Agnitum Outpost Personal Firewall, Checkpoint Firewall, dll. Sedangkan yang gratis seperti Comodo Personal Firewall, Sunbelt Personal Firewall,

Untuk pengguna internet broadband, pastikan router sudah memiliki firewall.

3. Install Antivirus

Antivirus melindungi kita dari akses virus pada komputer dan serangan-serangan jahat lain seperti trojan dan worm. Antivirus bisa mencari virus, trojan, dan worm yang berdiam di komputer dan melakukan pemindai terhadap email yang masuk maupun email yang keluar. Yang terpenting adalah:

Pastikan Antivirus anda selalu diset untuk meng-update pengetahuannya tentang virus-virus terbaru.

Pastikan juga program Antivirus anda adalah versi yang terakhir.

Jangan membuka attachment email dari orang yang tidak anda kenal.

Lakukan pemindai (scanning) terhadap removable device seperti hard disk external, USB disk, maupun CD/DVD yang terkadang mengaktifkan auto-run.

4. Selalu Update

Sama seperti sistem operasi, piranti lunak yang terus di-update akan terbebas dari masalah kelemahan keamanan. Selain itu, gunakan program-program terkini agar terus mengikuti perkembangan keamanan program.

5. Mencegah Spyware

Spyware adalah program kecil yang hinggap di komputer kita untuk merekam dan mengirimkan semua data-data dan kegiatan yang terjadi di komputer, tentunya hanya kegiatan yang diinginkan si pembuatlah yang direkam, seperti aktivitas keyboard oleh keylogger.

Mencegah spyware dapat dilakukan dengan:

Waspada terhadap file yang anda buka atau download lewat internet atau email.

Jangan menginstall program yang tidak jelas pembuatnya.

Jangan sembarangan berselancar ke situs yang memiliki tingkat risiko tinggi. Sebagai contoh: Banyak situs porno yang mengandung spyware.

Menghilangkan spyware bisa menggunakan program AntiSpyware seperti Windows Defender, Ad-Aware, Spybot Search & Destroy, dll lalu lakukan pemindai di seluruh komputer. Yakinkan program selalu melakukan update otomatis dan memindai komputer setiap hari sebelum anda memulai kerja.

6. Amankan Koneksi Nirkabel (Wireless)

Apabila anda memiliki jaringan nirkabel, selalu ikuti dokumentasi instalasi dan :

Gunakan MAC filtering untuk membatasi penggunaan pada komputer yang dipercaya saja.

Gunakan enkripsi WPA atau WPA2 yang lebih aman untuk mengurangi risiko penyadapan.

7. Membatasi Resiko Email Spam

Ada beberapa hal yang dapat dilakukan untuk mengurangi resiko terhadap spam:

Jangan meng-klik apapun terhadap email yang telah diidentifikasi sebagai spam.

Pisahkan antara email pribadi / kantor dengan email yang digunakan khusus untuk melakukan registrasi online.

Gunakan email client yang sudah terintegrasi dengan spam filter atau pasang program spam filter.

8. Backup

Selalu backup file-file penting dan simpan di tempat lain yang aman, pastikan file-file terbackup dengan baik dan tidak mengandung malware.

9. Keamanan Fisik

Buat tanda “keamanan” pada komputer anda dan benda lain yang anda anggap penting, agar selalu ingat bahwa barang tersebut butuh keamanan.

Pastikan tidak meninggalkan catatan-catatan kecil di sembarang tempat.

Catat setiap nomor serial dan jangan sampai orang lain tahu.

Pastikan pintu rumah, jendela, garasi terkunci dengan baik. Alat pendeteksi gerak dan alarm meningkatkan pengamanan rumah anda.

Jangan biarkan komputer terlihat dari luar rumah, tentu akan mengundang pencuri.

Pakai kunci pengaman tambahan untuk laptop, misal: fingerprint, usb dongle, dll.

Gunakan tas yang memiliki pengaman tambahan untuk laptop.

Hati-hati saat kendaraan anda mengalami gangguan dijalan, misal: ban bocor, yang seringkali dimanfaatkan oleh penjahat untuk mencuri laptop anda.

Src: http://think[.]securityfirst[.]web[.]id

MENGAMANKAN KOMPUTER DARI VIRUS

Apakah komputer anda terkena Virus? Apakah anda menemukan pesan aneh di layar anda yang sebelumnya tidak muncul? Apakah anda merasa komputer anda semakin lama semakin lambat? Baik, ini adalah masalah umum yang ditemukan oleh pemilik komputer di seluruh dunia. Terdapat berbagai virus dan worm di luar sana yang dapat menginfeksi komputer anda.

Beberapa efek yang ditimbulkan virus sangat beragam. Ada pada kategori level biasa saja, artinya hanya memperngaruhi kinerja sistem pada komputer anda. Pada level yang lebih tinggi virus juga dapat menghapud data-data penting anda. Sangat fatal sekali, bahkan virus juga dapat merusak sistem komputer anda. Untuk komputer yang terhubung jaringan, bisa jadi virus dapat mengubah komputer anda sebagai komputer zombie (komputer yang dikuasai oleh orang lain).

Bagaimana, mengerikan bukan efek dari serangan virus pada komputer anda. Tip-tip di bawah ini mungkin perlu anda ketahui untuk menanggulangi atau paling tidak mencegah serangan virus dari luar.

1. E-mail adalah satu cara penyebaran virus yang paling mudah dan paling berbahaya. Pastikan anda membuka e-mail dari sumber yang anda pastikan kebenaranya. Jika e-mail yang anda dapatkan berasal dari sumber yang anda tidak ketahui atau tidak berasal dari daftar kontak yang anda miliki, segera hapus e-mail tersebut. Pastikan daftar SPAM yang masuk segera dikosongkan. Jangan sekali kali untuk membukanya.

2. USB Flash disk adalah metode penyebaran virus paling banyak kedua setelah e-mail. Jadi pastikan anti virus anda terupdate dengan baik sebelum USB Flash Disk masuk terhubung di komputer anda. Scan terlebih dahulu sebelum dibuka. Cara membukanya juga jangan di double klik, tapi dengan klik kanan kemudian pilih Open. Cara ini lebih aman untuk menghindari virus yang masuk melalui autoruns yang disertakan dalam USB Flash Disk.

3. Hati-hati menggunakan program e-mail client misalnya Microsoft Outlook. Pastikan program tersebut terupdate dengan baik. Jika sistem operasi yang anda gunakan adalah bajakan, saya menyarankan anda menggunakan e-mail client yang sifatnya free dan dapat update secara otomatis, misalnya Mozilla Thunderbird atau Pegasus.

4. Semua orang pasti mengetahui internet adalah sumber penyebaran virus terbesar di dunia. Hampir 80% virus disebarkan melalui jalur itu. Berikut tip aman saat anda melakukan selancar di ranah dunia internet: – Jangan melakukan klik pada jendela pop-up yang ditampilkan. Misalnya pemberitahuan bahwa anda adalah pemenang sebuah undian atau klik beberapa kali makan anda akan menang sebuah undian. Sebenarnya itu adalah program jahat yang otomatis akan mengirim trojan atau spyware ke komputer anda. – Anda dapat menggunakan fitur atau program atomatis blok pada pop-up yang akan ditampilkan. Fitur ini biasanya sudah disertakan dalam web browser yang anda gunakan.

5. Mesin pencari, misalnya Google terkadang tidak dapat menyaring situs-situs yang dianggap sebagai berbahaya. Untuk itu anda dapat menginstal sebuah program yang dapat mendeteksi otomatis situs- situs yang tidak layak dikunjungi atau berbahaya. Program gratis yang dapat anda gunakan adalah AVG Link Scanner. Program gratis buatan AVG ini mampu mendeteksi situs-situs hasil pencarian google. Jika situs tersebut mengandung virus berbahaya, maka akan ditampilkan peringatan atau situs tersebut akan otomatis diblok tidak dapat dibuka.

6. Install anti virus yang dapat anda percaya. Tidak harus anti virus berbayar, untuk pengguna rumahan/pribadi anda dapat menggunakan anti virus free yang tidak kalah populer dengan anti virus berbayar, misalnya Avira, AVG, Clamav, dan lain-lain. Pastikan anda melakukan update secara rutin untuk menjamin anti virus yang anda install mampu menahan virus yang semakin lama semakin berkembang kemampuanya.

7. Instal juga anti Spyware untuk mencegah masuknya Malware dan spyware. Kedua program jahat tersebut selain dapat membuat komputer berjalan lambat, juga dapat mengahantarkan komputer anda sebagai komputer zombie yang dapat dikendalikan orang- orang di luar sana. Beberapa program anti spyware gratis yang cukup terkenal adalah Spyware Doctor, Spyware Terminator, dll

8. Jangan pernah membuka lampiran yang disertakan dalam e-mail dari sumber yang tidak diketahui dengan baik. Meskipun lampiran file yang disertakan adalah format file yang jarang membawa virus seperti .txt, .jpeg, .gif, .bmp, .tif, .mp3, .htm, .html, and .avi, namun pastikan anda melakukan scan terlebih dahulu.

9. Gunakan disk (CD/DVD) untuk mengimpan/membackup data- data penting agar tidak mudah terinfeksi virus. CD/DVD sifatnya hanya read only (hanya dapat dibaca), namun pastikan sebelum dipindahkan kedalam disk, data telah terbebas dari virus. Karen jika datanya bervirus, maka percuma saja disimpan di dalam disk.

10. Atur sistem operasi yang anda gunakan agar selalu melakukan update secara rutin. Ini dapat mengurangi resiko serangan virus dari luar karena celah masuknya virus telah ditutup oleh update yang anda lakukan. Namun update hanya dapat berhasil jika sistem operasi yang anda gunakan adalah asli. Jika tidak saya sarankan gunakan sistem operasi yang gratis misalnya linux.

11. Ketika anda mendownload program-program dari situs warez, pastikan anti virus anda terpasang dan terupdate dengan baik. File yang berasal dari situs-situs tersebut kadang sengaja disusupi oleh virus yang berbahaya.

12. Terakhir saya sarankan, jangan mengunjungi situs-situs berbahaya yang mengandung virus dan program-program jahat yang dapat membahayakan komputer anda sendiri, misalnya situs warez, crack, serial, porno, dan lain-lain.

Demikian 12 tip yang dapat anda lakukan untuk mengamankan komputer anda dari serangan virus. Satu hal yang perlu anda pahami “menjaga/merawat lebih baik dibanding menyembuhkan”.

Src: http://idecapung[.]blogspot[.]com/

MENGAMANKAN KOMPUTER DARI CRACKER

1. Memblokir Remote Access. Untuk mencegah PC anda diambil alih oleh Hacker,

nonaktifkan Remote Access. Dlm menu Start, klik kanan pada “My Computer” & pilih “Properties”.

Maka ada tampilan “System Properties”, kemudian pilih tab “Remote”,

singkirkan/hilangkan tanda (V) yg ada didepan semua option yang ada untuk menonaktifkannya. Kemudian klik “OK”.

2. Menghapus User Account yang tidak terpakai => Pada “Windows XP Professional” terdapat beberapa user account

yang dapat diakses melalui trojan & dimanfaatkan utk melakukan penyerangan.

Utk menyingkirkannya pilih menu Start, pilih “Control Panel”, pilih “Performance and Maintenance”.

Kemudian pilih “Administrative Tools”, Klik 2 kali “Computer Management”. Pilih “Local Users and Groups”,

pada sisi kanan klik 2 kali pd bagian “Users”. Hapuslah account-account lama yang tdk anda gunakan

( gambar users yg ada tanda X ). Kemudian tutuplah tampilan2 tadi.

3. Menutup celah NetBIOS => File2 dokumen anda bisa diakses melalui Internet maka nonaktifkanlah NetBIOS.

Dlm menu Start, klik kanan pada “My Network Place” & pilih “Properties”. Maka ada tampilan “Network Connections”.

Kemudian klik kanan icon koneksi internet yg tersedia, pilih “Properties”. Jika ada tampilan, pilih tab “Networking”. Beri tanda ( V ) yg ada didepan “Internet Protocol (TCP/IP), kemudian klik tab “Properties” yg ada dibawahnya. Maka ada tampilan “Internet Protocol (TCP/IP) Properties”, pilih tab “Advanced”. Tampilan ada lagi “Advaced TCP/IP Settings”, pilih tab “Wins”, lalu pilih “Disable NetBIOS over TCP/IP. Klik ‘OK”.

4. Penanggulangan terhadap BO2K pada Windows 9x. BO2K dapat dilacak dgn scanning port.

Biasanya pd Windows 9x yg terbuka portnya hanya satu yaitu port 139 (NetBios).

Oleh karena itu perlu dicurigai jika kita mengetahui ada port lain selain port 139 yg terbuka.

Program anti virus yg beredar saat ini dapat mendeteksi keberadaan program ini.

Pastikan anda sudah melakukan download versi terbaru dari program anti virus. Rajin2 lah membuka registrasi Windows. Biasanya pd Windows 9x, karena BO2K menanamkan dirinya pada

“HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices”

atau pada

“HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run”.

5. Pengamanan BIOS pada Server => BIOS merupakan perangkat lunak aras rendah yg berguna utk melakukan konfigurasi

atau manipulasi hardware pada PC berbasis x86. MS Windows maupun Lilo dari Linux menggunakannya utk

menentukan prosedur melakukan booting pada PC anda. Anda perlu memproteksi BIOS anda dgn memberi password padanya.

Cara ini juga berguna utk mencegah penggunaan booting up melalui floppy disk. Cara ini tdk memberi perlindungan secara maksimal pada PC anda, namun dapat mempersulit org lain utk mengacak2 PC anda. Perlu diingat bahwa BIOS saat ini menggunakan metode flashroom, yg memungkinkan kita utk mengubah konfigurasi atau bahkan menghapusnya sama sekali.

6. Penyalahgunaan CGI Shell pada Unix/Linux => Ada beberapa cara yg cukup ampuh utk menanggulanginya :

a. Anda pasang Chrooted-Jail pada Apache anda sehingga perintah yg dapat dijalankan dapat anda batasi.

b. Utak-atik Source Code dari fasilitas CGI yg akan anda berikan misalnya Perl,

kemudian anda matikan fasilitas fungsi system ( )…Smile

c. Minimalisasi terjadinya eksploit local pada sistem anda dgn sering mengutak-atik & mengikuti perkembangan berita

seputar sekuriti.

7. Menghapus komponen COM yg tdk dibutuhkan pd Windows 2000/XP/Etc => Beberapa komponen COM yg tdk dibutuhkan oleh

hamper semua aplikasi harus dihapus. Pertimbangkan dulu sebelum menghapusnya karena setiap komponen saling

berhubungan dgn file system & dictionary object. Dalam menu Start pilih Internet Explorer,

pada menu”Tools” pilih “Internet Options”. Jika ada tampilan, pilih tab “Connections”.

Didalam “Dial-up and Virtual Private Network Setting” hapus COM yg tdk dibutuhkan dgn mengkliknya lalu pilih

“Remove”. Kemudian klik “OK’.

8. Mengaktifkan Firewall => Agar Hacker & penyerang tidak sampai ke PC anda, dibutuhkan sebuah Firewall.

9. Menginstalasi Anti Virus => Software antivirus tidak hanya menyingkirkan virus, worm, atau file perusak lainnya

tetapi juga melindungi PC dari ancaman serangan Script di website.

10. Jangan anda melakukan chatting di MIRC sebelum tips diatas dipraktekkan,

kalo ngak kompi lo akan diserang oleh Hacker karna IP temen” bisa diliat melalui MIRC.

Src: http://www[.]okeaja[.]co[.]cc

Selamat mencoba cara meningkatkan keamanan komputer, cara menjaga komputer, cara menambah keamanan komputer, cara aman komputer, keamanan komputer, cara meningkatkan keamanan komputer terbaru, cara menjada komputer dari cracker, tingkatkan keamanan komputer, tambah keamanan komputer, maksimalisasi keamanan komputer, maximal keamanan komputer. increase keamanan komputer, update keamanan komputer, tipss mengamankan komputer, tips meningkatkan komputer, cara membuat komputer aman, cara membuat komputer secure, cara bikin komputer supaya lebih aman, cara supaya komputer aman.

Semoga bermanfaat

<http://www.binushacker.net/cara-meningkatkan-keamanan-komputer.html>

### Aspek Keamanan Komputer

Sebelum membahas tentang keamanan komputer, kita harus mengenal apa yang dimaksud dengan keamanan komputer. Cukup banyak pendapat yang dilontarkan oleh para pakar mengenai keamanan komputer, misalnya seperti :

*Computer Security is preventing attackers from achieving objectives through unauthorized access or anauthorized use of computers and networks.*  
*(John D. Howard, “An Analysis Of Security Incidents On The Internet 1989 - 1995”)*  
*A computer is secure if you can depend on it and its software*

*to behave as you expect. (Garfinkel and Spafford)*

Menurut Garfinkel, aspek keamanan komputer terdiri dari :

1. **Privacy/Confidentiality** => Usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Menggunakan Enkripsi merupakan salah satu usaha yang dapat dilakukan.
2. **Integrity** => Usaha untuk menjaga informasi agar tetap utuh, tidak diubah, baik ditambah maupun dikurangi kecuali mendapat izin dari pemilik informasi. Virus maupun Trojan Horse merupakan salah satu contoh dari masalah dan penggunaan antivirus,enkripsi dan digital signatures merupakan salah satu usaha untuk menangkalnya.
3. **Authentication** => metoda untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud. Penggunaan Acces Control seperti Login dan Password adalah salah satu usaha untuk memenuhi aspek ini. Digital Signature dan Watermarking merupakan salah satu usaha untuk melindungi *intelectual property.*
4. **Availability** => Informasi tersedia manakala dibutuhkan. Contoh serangannya adalah *DoS attack* dan *MailBomb.*

Berkaitan dengan aspek security diatas, menurut W Stallings ada beberapa kemungkinan serangan terhadap keamanan sistem informasi, yaitu :

1. **Interruption** => Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan (availability) dari sistem. Contoh serangan adalah “denial of service attack”.
2. **Interception** => Pihak yang tidak berwenang berhasil mengakses aset atau informasi. Contoh dari serangan ini adalah penyadapan (wiretapping).
3. **Modification** => Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset.Contoh dari serangan ini antara lain adalah mengubah isi dari web site dengan pesan-pesan yang merugikan pemilik web site.
4. **Fabrication** => Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti e-mail palsu ke dalam jaringan komputer.

Menurut G. J. Simons, keamanan informasi adalah *bagaimana kita dapat mencegah penipuan (cheating) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana*  
*informasinya sendiri tidak memiliki arti fisik.*

<http://achmadmauludi.blogspot.com/2012/04/aspek-keamanan-komputer.html>

Pengamanan merupakan bidang yang sangat luas dan kompleks bila diterapkan sistem informasi berdasarkan komputer. Pengamanan dalam hal ini tidak saja meliputi perlindungan sehari-hari atas perangkat keras dan perangkat lunak komputer, melainkan juga integritas data, kerahasiaan data, perlindungan atas semua fasilitas fisik dan pencegahan kemungkinan kehilangan yang sangat merugikan. Tindakan pengamanan dapat di klasifikasikan dengan berbagai cara. Dalam hal ini kita menggunakan ancangan yang memisahkan tindakan-tindakan tersebut dalam tiga kategori:

1. Tindakan pengamanan yang mengamankan semua kekayaan fisik selain perangkat keras komputer

Sebagian besar tindakan pengamanan dalam kategori ini bertujuan membatasi akses orang-orang yang tidak berwenang, umumnya untuk mencegah pencurian atau tindak kekerasan. Seperti, tindakan pengamanan lain melindungi kekayaan fisik dari bencana alam. Sistem penyemprotan air (sprinkler system) dipasang untuk memadamkan kebakaran yang mungkin terjadi di gudang, misalnya. Lemari tahan api digunakan untuk melindungi uang dan surat-surat berharga dari kebakaran dan juga berfungsi membatasi akses orang-orang yang tidak berhak.

2. Tindakan pengamanan yang utamannya mengamankan fasilitas perangkat keras komputer

Sistem komputer dan peralatan-peralatan terkaitnya, seperti perlengkapan masukkan-keluarkan off-line, memerlukan perlindungan terhadap sebab-sebab yang sama mengancam kekayaan fisik non-komputer.

\*Perlindungan terhadap akses tanpa izin\*

Akses fisik ke fasilitas-fasilitas komputer haruslah dibatasi hanya bagi orang-orang yang berwenang. Beberapa cara untuk membatasi akses ke fasilitas komputer adalah (1) mengunci pintu ruang komputer,(2) satpam ditempat-tempat strategis (3) pemantau televisi (4) kartu magnetik berkode untuk membuka pintu ruang komputer (5) tanda pengenal karyawan (6) alarm yang berbunyi bila ada pelanggaran masuk.

3. Tindakan pengamanan atas data

Pengamanan data di artikan sebagai upaya untuk menjaga integritas dan kerahasiaan data, sumber daya penting bagi setiap perusahaan. Pembatasan akses ke data dapat di terapkan dengan cara-cara seperti isolasi, identifikasi pengguna-pengguna yang sah, pembatasan pengguna terminal, enkripsi dan perusakan.

– Isolasi :

Data yang bersifat rahasia atau sangat penting bagi operasi perusahaan hendaklah diisolasikan secara fisik guna mencegah akses yang tidak sah.

– Identifikasi pengguna-pengguna yang sah :

Penggunaan dan modifikasi data yang sah harus ditetapkan secara jelas oleh manager yang bertanggung jawab.Pembatasan penggunaan: Peralatan dan pengguna dapat dikenai pembatasaan penggunaan. Contoh, terminal dapat dilengkapi dengan papan tombol yang dapat di kunci sehingga tidak dapat digunakan diluar kerja.

– Enkripsi:

Untuk menanggulangi penyadapan jalur komunikasi, data yang peka dan rahasia dapat diproteksikan dengan enkripsi. Artinya, data yang dimasukkan pada terminal yang jauh dapat di enkode, dikirimkan dalam bentuk tersandi (coded form), dan kemudian didekode pada saat tiba di kantor pusat perusahaan.

– Perusakan :

Untuk mencegah kemungkinan dibaca secara tidak sah, data rahasia harus di hancurkan setelah digunakan. Sebagai contoh, kertas berisi data rahasia harus di hancurkan setelah digunakan.