Home Computer Security

A personal computer connected to the Internet without a firewall can be hijacked in just a few minutes by automated hacker ''Bots''. The only way to make your computer 100% secure is to turn it off or disconnect it from the Internet. The real issue is how to make your computer 99% secure when it is connected. Not having protection is like leaving your car running with the doors unlocked and the keys in it which a thief might interpret as "please steal me". Stated another way, when was the last time you handed a stranger your wallet and encouraged them to take your social security card, drivers license, cash and credit cards? Locking a car, using a "club" or installing a security system makes stealing a car more difficult. Internet security and privacy products provide adequate protection by making it difficult for "outlaws" to find and take control of your computer.

A layered approach is best to protect your security and privacy:

- Use personal firewall, anti-spyware, anti-virus, anti-Trojan, anti-spam, anti-phishing, and privacy software on your desktop computer.
- Update and tighten Windows before installing new security software.
- To avoid conflicts, do not use two software firewalls or two anti-virus products at the same time. Completely uninstall one before installing another.
- After installing any security software, **immediately** check for updates at the vendor's website.

Guidelines to secure your PC on your own

Securing your Windows

Microsoft Windows XP is being used by a growing number of users. Windows XP is potentially much more conducive to security than its predecessors such as Windows 95 and 98—a good reason for you to upgrade your desktop system to Windows XP if you have not already done so. Following checklist describes the measures you will need to take to achieve baseline security in your Windows XP system.

Baseline Security Measures for securing your computer:

Your system will achieve a baseline level of security if you deploy the following measures:

- Use only Windows XP Professional. Windows XP Home has too many major security flaws (e.g., in XP Home every default account has superuser privileges and cannot belong to any domain) to enable it to achieve even a baseline level of security.

- Install Windows XP only from trusted media.

- Ensure that every partition is an NTFS partition. If any volume is FAT-formatted, enter

convert <partition letter>: /fs:ntfs

For example, to convert the D partition into an NTFS partition, enter

convert d: /fs:ntfs

and then reboot your system.

- Check to see whether Service Pack 2 (SP2) has been installed by going from Start to Run, then entering “winver”.

- Install the latest post-SP2 hotfixes from www.windowsupdate.com

  - An "unprotected share" is a share that permits everyone to connect to it; the worst case is a share that allows everyone to assume full control or to write and delete. Many Windows systems users have unprotected shares. The result is greater likelihood that their systems will be successfully attacked by hackers, worms, etc. Unprotected shares are one of the major causes of security-related incidents in Windows systems.

  - Leave the Guest account disabled. Double-click on this account name and ensure that "Account is Disabled" is checked.

  - Activate the screen saver. This will help protect against unauthorized physical access. Go to the Control Panel, then Display, then Screen Saver (or right click on the desktop to Properties and click on the Screen Saver tab). Be sure to password-enable the screen saver and also to set the activation period to 30 minutes.

  - Be sure to run AntiVirus on your system, and to keep its signatures updated every day.

Block NetBIOS ports over TCP/IP

Block NetBIOS ports over TCP/IP to all Internet traffic if you need to enable file sharing for your machine so no one from the outside can access the contents of your hard drives through these ports. This can be accomplished with either one of these two methods:

Preferred method: Block incoming and outgoing access to ports 135, 137-139, and 445 with your firewall. ZoneAlarm (a free personall firewall) does this by default when you set the Internet Zone Security to "high". (The "medium" Internet Zone Security default settings only block incoming access to NetBIOS ports and you can manually change that to include outgoing, but remember - any Internet Zone Security setting lower than "high" is not recommended for use in the Internet Zone.)

Backup your files

Keep current backups of all personal and system files. A backup can restore lost data in the event your system's security is compromised or your critical files become corrupt.

What system files to backup?

Daily backups of your registry files are recommended. In addition, always create a backup before installing any new program or making any changes to your system settings.
Since system files in Windows XP cannot be simply copied while they are in use, XP users should use System Restore to create restore points. (A shortcut is placed by default under System Tools in the Start Menu, or you can find it at %SystemRoot %System32restorerstrui.exe.)

Disable File and Print Sharing

Disable File and Printer Sharing in your network settings if you are using a computer that is not connected to a Local Area Network (LAN). This will shut all NetBIOS ports - those which are used for the sharing of files. Even if you are using a router and a firewall, this is giving you added protection by disabling something you don't need.

Five Steps to Safety while surfing:

1. Ensure your Operating System is up to date and safely configured

- Windows 2000, XP or ME can be set to download security updates **automatically** and prompt you for permission to install them. http://windowsupdate.microsoft.com/
- Make sure the security settings on your Web browser are at medium or **high**. If you are using Internet Explorer this can be done by going to Tools>Internet Options>Privacy.
- Consider using a more secure browser such as **Firefox** or **Opera**.

2. Check your system for viruses

A **virus** is so called because it reproduces itself by using the facilities of the host PC to copy itself to removable media and attach itself to emails, without your knowledge. There are variants, which may be technically characterised as worms or Trojans, but you don't want any of these. Most commonly you get one by opening an email attachment or copying (from deceptive software on the Internet or a bootleg CD) a program containing the virus, on to an unprotected PC. They take over the compromised PC and either **trash your data** or use your PC like a **zombie** to send hundreds or thousands of emails containing copies of itself, and/or spam, maybe with copies of your **confidential** data, to everybody in your address book.

There are many virus checking services offered **free** by the various Anti Virus vendors, such as **House Call** from Trend Micro:

http://uk.trendmicro-europe.com/consumer/products/housecall_launch.php

These checks are only effective during the time that they are run and do not provide continued protection afterwards. You will need to install an Anti-Virus package for continuous protection. It is very important that it is updated regularly, ideally every day.

3. Install a Firewall

A personal **firewall** blocks unauthorised network connections from either entering or leaving the computer. This helps protect you either from malware entering your PC, or using it to attack others. You can download the following personal firewall from:

http://www.zonelabs.com/store/content/company/products/znalm/freeDownload.jsp

4. Block SpyWare and Identity Theft

"**Spyware**" is any technology that aids in gathering information about a person or organization without their knowledge. On the Internet, it gathers information such as email addresses, passwords, phone numbers, and credit card numbers, and relays it to advertisers or other interested parties. It is not to be confused with "**Cookies**" which are small files that contain a record of the last time you visited a web site; many e-commerce sites require their use to recognise returning visitors.

Ad-aware is a free product that will search for Spyware and report items found.

http://www.lavasoftusa.com/software/adaware/

5. Be vigilant to protect your privacy

- **Identity theft** can ruin your credit rating and take months of effort to recover from. Exercise caution in your business affairs.
- If you receive an email allegedly from your bank, or Ebay, PayPal, FedEx, etc, asking you to verify your credit card data, it is almost certainly a **scam**, called "**phishing**". Sometimes it is inexpertly done and the web site address is not the real address but some variation on it. For example, ebay-accounts.com rather than ebay.com; or yourbankname.kr rather than yourbankname.ie. Report such attempts to the financial institution involved.
- Actually read the **privacy policy** and terms and conditions of a site before you give them **personal data**. Look for the check box that sometimes says "Allow third parties to send me emails" and sometimes "I do not want my address given away". Legitimate companies will allow you to unsubscribe from an e-mail list by replying with '**remove**'. Best practice is not to send unsolicited commercial email at all. But **never reply to spammers**, as your reply verifies that they have found a valid e-mail address, and you'll be on their list and everyone else's that they can sell that verified address to.

E-Mail Security

HTML E-Mail

Disable HTML for e-mail or choose to view all messages as plain text if your e-mail client has such options - the better ones do; or use an e-mail content filter for web bugs and embedded content originating from a server other than the one belonging to the sender of the e-mail. Today's cleverly-coded e-mail worms can execute just by viewing HTML-formatted e-mail.

E-Mail Attachments

- Never allow your e-mail client to "View Attachment Inline" ...unless you are sure it arrived from a trusted sender.

- Never open e-mail attachments from strangers.

- Use encryption software for sending your most private e-mail messages. If you don't, keep in mind that what you are sending is the equivalent of a postcard.

- Never, ever use e-mail to send confidential information such as credit card numbers, bank account numbers, or your Social Security number.

- Never respond to e-mail asking for confidential information. Any e-mail you receive requesting your credit card numbers, bank account numbers, or Social Security number either via e-mail or a web site link is surely an identity theft or phishing scam.

How to disable JavaScript in e-mail programs:

Outlook

1. Select the "Options..." command under the Outlook "Tools" menu.
2. Select the "Security" tab in the "Options" dialog box.
3. Under "Secure Content" section, select "Restricted sites" in the Zone Window.
4. Click on the "Zone settings..." button.
5. Click "OK" for the warning dialog box which pops up on the screen.
6. In the "Security" dialog box, make sure that the "Restricted sites" icon is selected.
7. Make sure that the security level slider control for the zone is set to "High".
8. Click on the "Custom Level..." button.
9. Scroll down to the "Active scripting" entry in the settings list in the "Security Settings" dialog box.
10. Select "Disable" for "Active scripting" entry.
11. Press the "OK" button in the "Security Settings" dialog box.
12. Press the "OK" button in the "Security" dialog box.
13. Press the "OK" button in the "Options" dialog box.

Note on Outlook: By following this procedure, you will accomplish two things. First, you will configure the e-mail client so that all of its network activity happens in the "Restricted" security zone. Second, you will increase the security of the Restricted zone beyond its default setting so that "Active scripting" is disabled. The end result is that your e-mail program will disable Active scripting (which includes JavaScript) whenever it shows you an e-mail, thereby preventing the e-mail wiretap exploit.

Mozilla Mail

1. Select "Edit" from the menu bar.
2. Select "Preferences" from the drop-down list.
3. Select "Advanced" from the Category list.
4. Select "Scripts & Windows" from the Advanced list.
5. Uncheck the box next to "Mail & Newsgroups" under "Enable JavaScript for:"
6. Important: Leaving "Navigator" checked applies to your browser window only. The option in step 5 applies to e-mail only.
7. Click on "OK" to save your settings and close the "Preferences" window.

8. (NOTE: Unlike with Netscape or Outlook, in Mozilla this option is unchecked by default... but it is a good idea to look for yourself.)

Mozilla Thunderbird

1. Select "Tools" from the menu bar.
2. Select "Options" from the drop-down list.
3. Select "Advanced" from the Category list.
4. Uncheck the box next to "Enable JavaScript in mail messages".
5. Click on "OK" to save your settings and close the "Preferences" window.
6. (NOTE: Unlike with Netscape or Outlook, in Thunderbird this option is unchecked by default... but it is a good idea to look for yourself.)

Netscape Messenger

1. Select "Edit" from the menu bar.
2. Select "Preferences" from the drop-down list.
3. Select "Advanced" from the Category list.
4. Uncheck the box next to "Enable JavaScript for Mail and News".
5. Important: Leaving "Enable JavaScript" (version 4.x) or "Enable JavaScript in Navigator" (versions 6/7) checked applies to your browser window only. The option in step 4 applies to e-mail only.
6. Click on "OK" to save your settings and close the "Preferences" window.

Eudora

1. Click on "Tools".
2. Click on "Options".
3. Click on "Viewing Mail".
4. Uncheck the box "Allow executable in HTML content".

(NOTE: Unlike with Netscape or Outlook, in Eudora, this option is unchecked by default, but it is a good idea to look for yourself.)

Beware of Spywares

"Spyware is the name which was given to software that - without the user of the program knowing that the software performs this kind of action - traces the user's usage of the internet and sends this information - again without the user knowing this is happening - to a computer ("Server") designated by the developer of the Spyware software."

Run spyware detection/removal software frequently to search your hard drives for spyware, adware, keyloggers, spy-related modules, browser hijackers, to check for security leaks and registry inconsistencies, and clean up tracks from web sites, opened files, started programs, and cookies.

Install Microsoft's Anti-Spyware to keep your system protected from Trojans/Spywares.

http://www.microsoft.com/downloads/details.aspx?FamilyID=321cd7a2-6a57-4c57-a8bd-dbf62eda9671&displaylang=en

Internet privacy protection

- Use a web content filter (or browser filter) to prevent remote site contact through ad banners and embedded web bugs. They are built into most browsers, but third-party programs usually offer better filtering and configuration options.
- Enable the popup blocker in your web browser. The better browsers have this built in.
- Disable HTML for e-mail or choose to view all messages as plain text if your e-mail client has such options - the better ones do; or use an e-mail content filter for web bugs and embedded content originating from a server other than the one belonging to the sender of the e-mail.
- Disable cookies in e-mail if your e-mail client has such an option - the better ones do.
- Encrypt your stored passwords. Most browsers include an option to store your online passwords. Be sure yours are stored encrypted and you set a master password for access.
- Set your browser for maximum privacy, forcing it to prompt you for permission for everything possible from cookies to downloads as well as security permissions for Java Classes (Mozilla, Firefox, Opera, and Netscape) and ActiveX Controls (Internet Explorer) as mentioned above. Once you become familiar with a site you can always add it to an 'approved' or 'trusted' sites list in your content filter or browser to avoid the annoyance of continuous prompts, but apply some caution as this is for absolutely trusted sites only.
- Clear your browser cache (called "Temporary Internet Files" in IE) and browser history often, and always after visiting any site where you performed personal business - online banking, making a purchase, etc.
- Read a site's privacy policy. The presence of a privacy policy does not mean that a company won't collect or sell your information. Read it carefully. If it is vague or unclear, watch out. If you can't find one, get out! .
- Never respond to spam by using their "click here to unsubscribe" or "follow this link for removal from our list". The one and only thing this does is verify that the spam was delivered to a valid e-mail address and confirm that you saw it. In fact, by responding you are guaranteed the delivery of even more spam from the same sender plus those who were sold your confirmed-valid address. Destroy the spam without responding to anything.
- Never reveal personal details to strangers.

Cookies

Companies try to personalize web site experiences for their visitors. Some remember your login name and password for your convenience upon subsequent visits. Others offer news, stock quotes, and weather tailored to people's interests and location. This is done with a cookie, a small file created by the site, that collects specific information about your preferences or web browsing activities and stores it on your PC. Allowing all cookies, however, is unacceptable for those who care about privacy.

Tracking networks such as DoubleClick and MSN LinkExchange use cookies to monitor which site you were on when you clicked a particular banner ad and what you did once you got to the advertiser's site. They can put cookies on your PC and then read them across many sites - tracking your surfing habits and building a profile about your preferences.

Though this can be alarming, you are not left without the option to take control of the cookies that are used to invade your privacy. You can completely close this privacy gap as long as you apply basic cookie management techniques. Cookie filters will allow you to accept or deny each cookie upon arrival. Cookie filters can also be instructed to always deny "third-party" cookies - those that do not directly originate from the site you are currently visiting. Third-party cookies are most often used by advertisers and marketers.

Handling Spam

Take advantage of the built-in junk mail filters inside your e-mail client. In addition, configure your own filters to automatically trash or delete incoming e-mail that contains certain keywords. By using a combination of various filters you can noticeably reduce the amount of spam reaching your inbox.

You can set up as many filters as you like in your e-mail client. It is always wise, though, not to automatically delete the filtered mail until you are certain the filter is properly configured. You can always change it later.

ActiveX and Java Class

Never accept and run an "ActiveX Control" or "Java Class" unless it comes signed and from a trusted site. It is best to force your browser to prompt you for permission. If you are using Internet Explorer, these settings are located under Control Panel - Internet Options - Security - Internet, Custom Level. Mozilla, Opera, and Netscape users are prompted by default.

Install on Demand

Disable "Install on Demand" if you are using Internet Explorer so your browser will be forced to prompt you if additional components are needed in order to display certain content. This setting is located under Control Panel - Internet Options - Advanced.

Use a Personal Firewall

Use a good bi-directional firewall that will monitor all incoming and outgoing traffic and will alert you for access permission if such traffic is detected. It also has the ability to hide your presence from intruders by completely blocking access to the ports that are used for the transfer of information. Select the highest security level for your Internet zone and set all programs to prompt you for access - even those you use frequently. When in doubt, deny access of a program until you know for sure its identity.

It also has the ability to hide your presence from intruders by completely blocking access to the ports that are used for the transfer of information. A firewall plus anti-virus protection are rule number 1 to Internet security. For Windows XP users, be aware that although its Internet Connection Firewall (ICF) will detect inbound traffic,

it is useless for detecting outbound traffic - you need a bi-directional firewall - one that will detect both.

Use Anti-Virus software

Use a virus scanner (anti-virus), keep the virus data files current (check for updates at least once a week), enable the "Heuristics" or "Bloodhound" feature (for detection of virus-like activity of yet-to-be discovered viruses), and set it to scan all downloads and e-mail attachments - before they are opened. Let it quarantine and destroy anything suspicious. If it has settings for scanning ActiveX Controls and Java Classes for potentially harmful content, use that too. For even greater protection and a wider range of configuration options, combine the use of a virus scanner with a trojan scanner.

Installing an anti-virus or anti-virus/anti-trojan program on your system is probably the easiest of all security measures you'll find. Upon detection of a virus, the program will move the infected file to a quarantine area for disinfection or removal before it has the opportunity to make contact with you or any other program. Configuration is simple and detection is reliable as long as you keep the virus data files or rulesets up to date (check at least once a week), and apply all updates and program or scan engine patches as they are released.

Trojan Scanners

Trojans, or often referred to as Trojan Horses, are disguised as innocent programs and most often arrive hidden inside e-mail attachments or programs that are downloaded from the Internet. Upon execution, they place sets of instructions in various places then wait silently until you restart your computer to begin their nasty deeds.

Some anti-virus programs will also detect trojans, yet the use of a separate anti-trojan program is a popular and recommended option that provides you with a wider range of configurations and more extensive Trojan Horse protection. These programs are meant to be used in conjunction with your anti-virus program.

Peer-to-Peer Security

Be extremely careful when using any P2P (peer-to-peer) network service like Kazaa, Gnutella for sharing/swapping files across the Internet. Be sure you are not exposing any drive folder other than the one designated for access by these services, and keep your virus scanner active at all times.

Instant Messenger Security

Secure your IMs (Instant Messengers). It is wise to use an IM encryption utility to secure your AIM, ICQ, MSN, or Yahoo! Messages, but be aware that the encryption will only be effective if the utility is used on both ends.

Disable file transfers in IM programs, as this feature, if configured incorrectly, can enable the sharing of more than you intend. AIM, .NET Messenger, and others let you disable file transfers from the Preferences or Options menus. If someone wants to

send you an image or file, use e-mail to verify that the request is legitimate.

Protect Your Registry

Use a registry guard to protect your registry, startup directories, and startup files from malicious programs. Incoming Trojans can go undetected. They will place a specific set of instructions in the registry or other system files and will activate the next time you shutdown/restart your computer. A registry guard will alert you before the damage is done. It is also a useful tool for alerting you of changes when installing new software.