

Secure Your Home Computer

by: TomCat Internet Solution, 03/06/2005

<http://www.securitydocs.com/library/3080>

These topics are brought to you from [TomCat Internet Solutions "Secure Your Home Computer" Version 2.0](#)

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.

If you do nothing else, you **MUST** at least use a good personal firewall. It will monitor all incoming and outgoing traffic by inspecting each individual packet of data 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. 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.

Not only should a firewall be used with your anti-virus program, but firewalls can also be used along with a variety of other programs such as content filters, proxies, anti-trojans, and port scanners to expand your arsenal of protection. Some are bundled with an assortment of these other programs as a package or suite, some are stand-alone. There are many from which to choose for a variety of combinations.

Anti-Virus

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.

Virus Scanners - the rundown:

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. A firewall plus anti-virus protection are rule number 1 to Internet security.

Whichever program you choose, be sure to set it to scan all downloads and e-mail attachments, enable the "Heuristics" or "Bloodhound" feature (for detection of virus-like activity of yet-to-be discovered viruses), and if it has settings for scanning ActiveX Controls and Java Classes for potentially harmful content, use that too! Also be sure to allow the program to create 'clean boot' disks, as you never know when you might need them for an infected system.

Trojan Scanners - the rundown:

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. Many anti-trojan programs have an option to stay active at all times working much like an anti-virus program, but there can sometimes be conflicts - especially when your anti-virus program is set to scan files when they are opened or executed. If you notice odd behavior such as intermittent system freezes, look here first. Disable active scanning in the anti-trojan program, NOT the anti-virus program.

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.

Peer-to-Peer Security

Be extremely careful when using any P2P (peer-to-peer) network service 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. 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.

Your IP Address

Know your IP. If you know the IP address of your internet connection (and the IP ranges used by your local network), you will recognize when an outsider is trying to break in.

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 'rearguard' will alert you before the damage is done. It is also a useful tool for alerting you of changes when installing new software

Careful when Executing Files

Never allow a downloaded application or any downloaded executable content to launch on its own, and be especially careful of downloading files that end in exe, bat, vbs, and com.

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. Not only could you be granting permission for the installation of something malicious, you could become a victim of browser hijacking. 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.

Browser Hijacking

Your browser's default start and search pages are changed by malicious web sites and/or software. This most commonly affects users of Microsoft Internet Explorer usually through the download and installation of ActiveX controls and plug-ins on browsers where the options for "download" and "run" are set to "enable" through your Internet settings. This is either executed through some action of your own - a mouse click or a click on a link - while browsing the site, or by simply visiting a site - code is executed upon loading a page for you to view. Sometimes Internet shortcuts are also added to your Favorites folder without your permission.

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.

Careful with JavaScript

While JavaScript may be fine for internet browsing, it can be dangerous when enabled for e-mail. Many internet users keep JavaScript disabled for everything in their browsers. The fear of this widely used internet programming language results mostly from the discovery of security holes in browsers and e-mail clients, especially Microsoft Internet Explorer and Outlook. In fact, the first thing Microsoft will advise when a new security hole is discovered is "disable active scripting in your Internet Security settings". Although this is certainly one method of controlling what a hostile script might do until the next browser patch or update is issued, it makes far more sense to understand what scripting can and cannot do. While the vulnerabilities are especially a risk in programs where patches and updates are not applied, the threat is persistent in every program since new vulnerabilities have yet to be discovered. Still, it takes a wide-open, unprotected system plus your authorized permission before JavaScript can allow anything damaging to enter your computer through your browser.

One way to begin understanding how JavaScript behaves is know how it is used. JavaScript can control the appearance and content of the web browser, open new windows and display HTML dynamically, open links to new sites, pop up dialog boxes, click forward and back through the user's browser history, and set and read cookies. In addition, JavaScript can interact with Java applets and with browser plug-ins. Although some of the scripted behavior, for example pop-up ads, unnecessary cookies and/or information gathering such as referers (transmission of your last visited address), is undesirable and downright unwanted, much more is there to simply enhance the appearance and performance of the sites you visit. By disabling JavaScript you will miss the entire web experience as it is designed to be seen, and you will lose all interactivity from mouseover effects to form input and everything in between.

Yes, scripts can get nosy - they can look for your browser version, look for your IP address, look for your cookies, and record the referer address; but there are better ways to control this than entirely disabling JavaScript. Consider this, too... in knowing your browser version you will be shown a page that is designed specifically for you, as the coding and display elements are different for each one. Your IP address is no secret anyway since you can't even get past your ISP and connect to the Internet without one; and in order for you to use the Internet at all, information must be able to find its way back to your computer. Besides, it is going to take more than disabling JavaScript to keep your IP address a secret from everyone. As for cookies, banner ads, pop-up windows, referers and the like, they are more effectively controlled with a cookie/content filter that will allow you to accept what you want while discarding everything else.

If completely hiding your IP address from the world is that important to you, anonymizer services are available - some are free, some charge small monthly fees. An anonymizer is used as a proxy, or a "middle man", to mask your IP address between you and the rest of the Internet. For obvious reasons, though, you might still need to disable this proxy in order to connect to certain sites (for example online banking). And keep in mind that anonymizer services cannot guarantee anonymity 100%. Also keep in mind that you are not anonymous from them - they cache a trail of every site you visit. It is far better to avoid the sites where you feel an anonymizer might be needed.

But what about intrusions into your computer?

Fact: JavaScript cannot read or write local files and cannot open network connections except within the confines of browser capabilities... and you are in control of setting those rules!

JavaScript alone is not a threat. The threat comes when JavaScript is used to execute some "other action" such as placing hostile active content in the form of an ActiveX Control, Java Class file, or some other executable content on your computer. These are little programs, much like plug-ins, that are downloaded to your computer in order to allow a certain event to take place such as auto-installing a program or update, or running some visual or interactive effect. They should ALL be signed - proof of who they say they are, like a digital certificate you might use for your own e-mail. They should always come from the site you are visiting and they should always be forced with browser settings to ask for permission before they come in - they won't get in if you say "no".

If your guard is down, though, something nasty can get in, but this has nothing to do with whether you have JavaScript enabled or not ...a trojan - the most aggressive of all intruders. Trojans are disguised as innocent programs and most often arrive hidden inside e-mail attachments or programs that are downloaded from the Internet. They are mentioned here only because you need to know, and we repeat - they can get into your computer whether you have JavaScript enabled or not! Your best defense here is to always use a virus and trojan scanner along with a good, reliable firewall ...and of course, don't allow anything to execute on your computer without your permission. Remember... permission must be authorized by you before JavaScript can allow anything damaging to enter your computer through your browser.

Basic JavaScript Rules

- Never, ever, enable JavaScript for e-mail or e-mail attachments. While JavaScript may be fine for internet browsing, it can be dangerous when enabled for e-mail. See How to disable JavaScript in e-mail programs for step-by-step instructions.
- 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. Period.
- Never allow a downloaded application or any downloaded executable content to launch on its own, and be especially careful of downloading files that end in exe, bat, vbs, and com.
- 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.
- 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.
- Never visit untrusted sites. If you do, be extremely cautious.
- 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.
- 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.
- Visit BrowserSpy, a testing site that shows you what information can be gathered from your visits to web sites. Switch JavaScript on/off and compare each set of results. This will give you a better idea of what JavaScript is capable of doing, and it will also show you its limitations.

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

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. In Mozilla Mail and Thunderbird click on View from the main menu, select Message Body As, then select Plain Text. Also uncheck Display Attachments Inline so this setting is used by default. In Outlook click on the Security tab, select Change Automatic Download Settings, and place a check next to Don't download pictures or other content automatically in HTML 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. Period

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. Also remember that encryption is for the message body only - it does not hide the subject line nor does it hide the message headers.

Never, ever use e-mail to send confidential information such as credit card numbers, bank account numbers, or your Social Security number. Even if you use encryption and the correspondence is for legitimate business, you cannot be certain that the recipient will protect this information once it is delivered and decrypted. It will only be as secure as the recipient's system permits.

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.

Other Online Security Tips

Keep your OS and browser up-to-date, in addition to any service or application that has access to the Internet. Apply updates and patches as they are released.

Learn to identify which system services and applications are known to compromise security and do not allow them to have open access to the Internet. When in doubt, have your firewall prompt you for permission.

Be sure your browser is SSL-capable (Secure Socket Layer) and the encryption strength, or cypher strength, is not less than 128-bit.

Never submit a secure form on an insecure server. Period.

Avoid using easily recognizable passwords such as the names of family members or pets, birthdays, or anniversaries. Make them as cryptic as possible; and if you must write them down, do not store them on your computer or any other place where someone may have access to them. If you must use your browser's password manager, never use it to store important passwords such as those used for banking.

Never visit untrusted sites. If you do, be extremely cautious.

Spyware

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.

"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."

"By performing these actions, detailed userprofiles may be collected - without the user's knowledge and approval - which then can be used for commercial or other purposes. By gathering and sending this information both resources on the user's computer as well as bandwidth on the Internet is abusively used, not to mention the breach of privacy such a userprofile would be."

-- Dick Hazeleger, Creator "Packet Sniffing - A Crash Course" and founder of the original "Spyware List"

Additional guidelines for LAN Security

Use a Router with NAT

Use a router between your LAN and the Internet if you have an 'always-on' connection using DSL, cable, or any connection where you are assigned a static IP address. If your ISP advises against this, FIND ANOTHER ISP. A router uses Network Address Translation (NAT) to mask the IPs of your internal network from the outside world. A router that also combines a hardware firewall is even better.

Network Address Translation (NAT):

NAT acts as an interpreter between two networks. In the case of a home network, it sits between the WAN (wide area network, or Internet) and your LAN (local area network, or your home computers). The Internet is considered the public side and your home network is considered the private side. When a computer in the private side requests data from the public side, the NAT device will open a conduit between your computer and the destination public computer. When the public computer returns results from the request, it is passed back through the NAT device to the requesting private computer.

Routers:

Basic NAT devices are not 'true' firewalls, but they are usually considered good enough for most home networks. By not forwarding requests or probes that originate from the Internet to your LAN, a NAT device blocks most mischief. A simple NAT device cannot keep hackers from running DoS (Denial of Service) attacks on you - something that is extremely rare with private networks, but it will keep out people looking for file shares, rogue mail servers and web servers, and most port-based exploits. Most also protect against SMURF and WinNuke attacks. When combining a NAT device with a software firewall and a good anti-virus program, you should be safe from the most common kinds of Internet attacks.

Hardware firewalls:

Some NAT routers have an advanced form of built-in firewall that performs Stateful Packet Inspection (SPI). This allows the NAT device to filter out specific kinds of data on your router like SYN flood attacks, IP Spoofing, Teardrop attacks and others. SPI is a general term that can describe a router that filters more kinds of attacks than basic NAT by closely examining packet data structures and not just the source and destination addresses and ports. Each manufacturer will implement different kinds of SPI so not all SPI routers are equal, yet most routers with SPI can log attacks.

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 LAN 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:

1. **Preferred method:** Block incoming and outgoing access to ports 135, 137-139, and 445 with your firewall. ZoneAlarm 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.)
2. **Alternate method:** Manually disable NetBIOS over TCP/IP. This method is for advanced users only and is something we now consider unnecessary in these modern days of routers and bi-directional firewalls like ZoneAlarm. Be aware that with Windows XP, the results can be unpredictable and highly dependent on how your network is configured.

Other Home Network Security Tips

Periodically check for heavy traffic on your router's LEDs and check each PC's log files for new entries that are unfamiliar. These factors could indicate malicious activity.

Turn on WEP (Wired Equivalent Privacy) on your wireless router or access point if you are connected to a "wireless" network.

Require a login user name and password for every computer connected to your LAN. For any hard drives that are configured as shared: Windows 98 users - require a user name and password there, too. Windows XP users - do not configure share permissions to allow 'anonymous logon' or any access by groups or users outside your LAN.

Secure your sensitive files on any computer you use to connect to the Internet. Never place sensitive files on drives or inside folders that are configured as shared. Even better, the best place to store these files is on a CD or some other removable media. Another option is to install a third-party file guardian program but be very careful when using such tools as misconfiguration can result in complete inability to access to your OS.

And remember that even though only one computer is actually making the internet connection, any other computer sharing that connection, or is sharing files on a network with that computer, needs the same protection!

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.
- Don't tell sites anything you don't want them to know. Use common sense when filling out forms or submitting any personal information unless you are absolutely sure it won't be misused.
- 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!
- Don't install spyware, and use adware cautiously. Many freeware, shareware, and adware programs not only contain

spyware, but can contain viruses or worse - trojans! Make your selections carefully and always do a Google search on software titles for all the information you can gather.

- Opt out of everything from mailing lists to requests to use your personal information for whatever purpose is intended, and beware of sites that offer some sort of reward or prize in exchange for your contact or other information.
- 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. The sender has no intention what so ever in honoring your request. 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 give your personal e-mail address to a commercial vendor. This applies to anything from making a purchase online to responding to an online survey. Apply for a free Webmail account or subscribe to a Disposable E-mail Service and use that address instead. You can always dispose of it and acquire a new one quite easily if necessary.
- Never use your personal e-mail address when posting to message boards or newsgroups. Always use a webmail address if a valid address must be supplied. Spiders are constantly crawling these places for addresses to use for spam. If you must use your personal address, or any valid address you plan to keep, always insert some text that the viewer will know to remove when responding to you. No one will question your intent - this is standard practice.
- Never reveal personal details to strangers. Period.
- Realize you may be monitored at work. Avoid sending highly personal e-mail to anyone including mailing lists, and keep sensitive files on your home computer.
- Use anonymizers cautiously. They are not as private and secure as you might think. It is far better to avoid the sites where an anonymizer might be needed.
- Keep informed. Visit privacy sites frequently. Read the news. Apply what you learn.

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.

Although cookies are often used in such ways that are beneficial to you as you move across the Internet, many more are not. Such cookies are used with the sole purpose of gathering information and are beneficial only to those who place them on your computer. 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. They will also allow you to set automatic handling rules for future cookies - always accept those from sites you trust and visit frequently or always deny those from sites that have no business knowing your own. 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.

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.

Dealing with Spam

Automated reporting systems used to be the preferred choice when dealing with spam but for all practical purposes are simply just a waste of time. A more effective way of dealing with this nuisance is by setting up your own e-mail filters to weed out and destroy the junk. Mozilla and Mozilla Thunderbird have excellent built-in junk mail filters that with a little training are quite effective. Still, you might want to manually set a few rules.

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.

Our example below shows you how to filter for spam arriving from a certain country, but you can set your filters to test for just about any string of text found in the e-mail header and/or message body. We are routing mail from that country into a specific folder, keeping it out of our inbox, but saving it somewhere else to be manually deleted later. Once we are certain the filter is working properly, the action performed can later be changed to "delete".

For e-mail that is malicious or threatening, contact your ISP immediately! Many ISPs destroy their server log files after 48 hours and that evidence is critical. Your ISP should be able to advise you how to proceed with filing your complaint. Also, be sure to include all headers that are embedded in the e-mail, as every piece of information is needed to trace its origin.

Configuring Spam filters in Mozilla Mail and Mozilla Thunderbird

1. Click Tools >> Message Filters
2. In the Message Filters window click "New"
3. In "Filter Name:" enter "Slovenia Spam Filter" (or any name you like without the quotes)
4. Under "For incoming messages that:" select "Match any of the following"
5. In the first drop down box select "Sender"
6. In the second drop down box select "Contains"
7. In the textbox, enter ".si" (without the quotes)
8. Under "Perform these actions:" select "Move to folder"
9. Click the "New folder..." button
10. In the New Folder window under "Name:" type "Slovenia" (or any name you like without the quotes)
11. Under "Create as a subfolder of:" select "Local Folders", "Inbox", "choose this for the parent"
12. Click OK to close the New Folder window
13. Click OK to close the Filter Rules window
14. Be sure a check mark appears next to your new filter under "Enabled"
15. Just click on the "x" at upper right to Message Filters window

Configuring Spam filters in Netscape Messenger

1. Click Edit >> Message Filters
2. In the Message Filters window, click "New"
3. In "Filter Name:" enter "Slovenia Spam Filter" (or any name you like without the quotes)
4. Under "For incoming messages that:" select "Match any of the following"
5. In the first drop down box select "Sender"
6. In the second drop down box select "Contains"
7. In the textbox, enter ".si" (without the quotes)
8. Under "Perform these actions:" select "Move to folder"
9. Click the "New folder..." button
10. In the New Folder window under "Name:" type "Slovenia" (or any name you like without the quotes)
11. Press the "Click here to select" button
12. Specify a choice and click OK
13. Click OK to close the Filter Rules window
14. Be sure a check mark appears next to your new filter under "Enabled"
15. Click OK to close the Message Filters window

Configuring Spam filters in Microsoft Outlook

1. Click Tools >> Rules Wizard >> New
2. Select "Start creating a rule from a template"
3. Select "Move new messages from someone"

4. Click Next
5. Under "Which condition(s) do you want to check?" click the box next to "with specific words in the sender's address" (Clear any other boxes that are checked.)
6. In the "Rule description" box, click "specified"
7. Select the Slovenia folder, or click New to create the Slovenia folder
8. In the "Rule description" box, click "specific words"
9. The Search Text box will open. Type ".si" (without the quotes) in the "Specify a word or phrase..." box
10. Click Add >> OK
11. Click Next
12. In the "What do you want to do..." field, select "move it to the specified folder"
13. Click Next >> Next
14. In "Please specify a name for this rule," enter Slovenia Spam Filter
15. Select "Turn on this rule"
16. Click Finish
17. Click OK

Configuring Spam filters in Eudora

1. Click Tools >> Filters
2. Under Match, check Incoming
3. Under Header, choose From:
4. In the drop down box below Header, select Contains
5. In the textbox to the right, enter ".si" (without the quotes)
6. In the Action area, in the first drop down box, select Transfer To
7. Click the long command button to the right (it says "In")
8. Select the box to which you want to send Slovenian e-mails (If you don't yet have a box, select New and create one.)
9. Click File and Save

Test for Security Vulnerabilities

Use an online service to test the security of your computer's connection to the Internet. Be sure to include a check for identity vulnerabilities and port scanning.

Examine the results and make adjustments to your firewall and/or network settings and apply software patches wherever required for maximum defense. Closed ports are good - stealthed ports are better - but keep in mind that more often than not, security problems exist with the software and not with the ports through which they are granted access.

Use Common Sense

Examine your firewall and router logs frequently for suspicious incoming or outgoing traffic. If you suspect you are a victim of a hack attack, that someone did in fact compromise your system, go to www.fbi.gov for instructions on gathering proof and filing a report. Also look for changes on your hard drive such as unknown or changed files and folders and decreased hard drive space. Do not delete but rather quarantine anything suspicious mainly because you will need this information for evidence, but also because a file that looks suspicious is not always bad - it might be critical system or program file that you need to restore.

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. Keep copies of everything you would need for both a simple restore (the replacement of just one or two damaged files) and a major restore (bringing your system back to its original state). And in the event of something very serious - like a hard drive crash or trojan damage - you should always be prepared to re-install your OS from scratch. This means not only keeping your installation CD for Windows in a safe place, but also the installation CDs for all of the other programs you have installed plus any personal files (address books, e-mail, documents, etc.) that will certainly be destroyed when you re-format a hard drive partition. If you backup your files to another hard drive partition for easy access, ideally you should also place copies onto external media such as a CD, Zip disk, or removable hard drive.

What system files to backup? Daily backups of your registry files are recommended and you should keep at least 7 of the most recent copies. In addition, always create a backup before installing any new program or making any changes to your system settings.

For Windows 98 users - keep backup copies of WindowsSystem.dat and WindowsUser.dat. If you are using User Profiles, you will also find a copy of User.dat under each WindowsProfilesprofilename. Simply copy these files to another location for safe keeping. If you need to restore these files, just boot to a command prompt and copy the files back to their original locations.

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%\System32\restorerstrui.exe.) In addition, we recommend a wonderful freeware utility called ERUNT (The Emergency Recovery Utility NT). ERUNT is a Registry Backup and Restore for Windows NT/2000/XP and will copy your critical system files in their original form to any location you specify. ERUNT will create a backup set which includes a utility for restoring the files to their original locations. To restore the registry from outside Windows, just copy the files back to their original locations.

If you are selling your computer, thoroughly clean your hard drive. Deleting files and reformatting is not enough. Reformatting does not overwrite every sector, and private information can remain retrievable. Use a secure delete or disk wiping utility to overwrite every sector on all hard drives. Be sure to use a utility that supports the U.S. DoD standard of seven passes or wipes. While this method is good enough for most people, be aware that the only absolute way of destroying all traces of everything your hard drives is to have these disks degaussed (demagnetized) and physically destroyed.

Copyright 2005 TomCat PC Systems