

Safe Computing

By: Bill Woelk

Copyright© 2002-2004, Bill Woelk - User Friendly Computers of Royal Oak

To avoid expensive computer repairs and loss of your data I recommend you follow these Do and Don't suggestions for safe computing. This is especially important if you have an always-on Internet connection; however, dial-up modem users also need to exercise caution on the Internet. The Internet is a public network, and like all public places must be used carefully since you have no control over others who frequent the Internet.

A special note for those with high speed connections: Many hackers purposely seek out computers attached to always-on Internet connections due to their higher speed and constant availability. Hackers can use PCs attached to high speed networks to attack other computers that belong to either private individuals, businesses, or governmental agencies. They can commandeer your computer to use it in what is known as a Denial of Service attack, or DoS attack for short.

A DoS attack is accomplished by loading a backdoor program onto your computer via an email attachment or via a directed attack on your TCP/IP ports, browser, or other susceptible software running on your PC. Your PC is then turned into what is known as a Zombie in hacker parlance. Your PC, without your knowledge, is then used to direct malformed or corrupt packets at another computer or web site on the Internet. It could be either a server, mainframe computer, or another private PC. Many hackers accumulate hundreds of Zombie computers under their control. This way they can direct millions of bad data packets at the victim computer or website essentially knocking it off-line. This can be done in the background without your knowledge. You might only notice a slight slow down in your computer's response time.

Many large SPAM operators are now hiring hackers to use their Zombie computers to relay email SPAM messages to other Internet users. This is similar to techniques used by money launderers to cover their tracks over. By relaying SPAM through a third party Zombie PC the owner/victim of the Zombie gets the blame for sending the SPAM. This can result in the Zombie owner's ISP cutting off their Internet service access, or their ISP being black listed by Anti-SPAM sites. The Zombie victim could also be left open to any resulting prosecution or law suits. The burden of proof would then be on him or her to prove they did not originate the SPAM, or receive compensation for relaying it. This is why a personal firewall is so important these days.

Here is a list of Do's and Don't's to help you maintain a secure environment on your computer:

- * Do install and maintain a good software firewall. This helps keep your data in

and while keeping unwanted people and software out of your computer while it is connected to the Internet. It does this by blocking, or stealthing, your Windows TCP/IP ports. ZoneAlarm and Sygate both offer excellent free firewalls. Black-Ice and Norton Internet Security are two common commercial offerings. (Independent tests indicate the free software above is as good or better at protecting your PC). ZoneAlarm is available here: <http://www.zonelabs.com>, or you can download Sygate here: <http://soho.sygate.com>.

- * Don't get into the habit of blindly agreeing to alerts from your firewall programs when new programs ask for Internet access. Be especially wary of program names you don't recognize, or did not click-on, or those requesting server rights. Very few if any programs need server rights to function. Going server allows them to broadcast data packets from your PC across the Internet. These could contain personal information, or be used to conduct a DoS attack.

- * Do maintain a good antivirus program and keep the virus detection signatures up to date. Updating your antivirus signature files daily is not too often, since new viruses are spread on the Internet every day. Enable the auto update feature to automate this process. Keep both the background and email scan protection activated. Most modern Trojan Horses and script viruses arrive as email attachments, or embedded in downloaded files. AVG (Grisoft Corp.), Computer Associates, Dr. Solomon's, McAfee's, Symantec Norton, Sophos, and Trend Micro are all good antivirus program vendors. AVG is available in an older version for free.

- * Do a full antivirus scan of your hard drive at least once per week.

- * Don't forget to scan Zip disks, homemade CD-ROM's and floppy disks since these can spread viruses, or re-infect a cleaned system.

- * Do keep informed about newly released viruses and what to watch out for. Both McAfee's and Symantec Norton Antivirus have free newsletters you can subscribe to on their web sites. These will automatically be sent to your email box whenever new viruses are released into the wild that you should know about.

- * Another excellent security newsletter that I subscribe to that is: <http://www.securityspace.com>. This is published weekly as the: Weekly Security News Headlines email newsletter. It is available for free by signing up here: <http://www.securityspace.com/secnews/subscribe.html>.

- * Do test your antivirus software to make sure it has not been compromised by a virus. To do this is simple. Go to: http://www.eicar.org/anti_virus_test_file.html and download the EICAR test virus and save it to your hard drive. This is an industry test virus that does not contain any harmful instructions in it. Next, run your antivirus scanning software. Your antivirus program should detect and offer to remove the EICAR test virus if it is working correctly.

- * Don't open emails from people or companies you don't recognize.
- * Don't open SPAM messages. Never reply to SPAM messages.
- * Don't open email attachments except from people you know closely and trust. If you were not expecting an attachment from a trusted individual, call or email them first to confirm they sent it and that it is safe to open before opening it.
- * Don't open an email or attachment if the subject line seems strange or out of character. Even a friend could send you an email with a Trojan unknowingly, if his/her system has been compromised without their knowledge. Most Worm viruses replicate by emailing every person in the infected computer's email address book. This is done secretly in the background without the victim's knowledge. Many victims do not even know they are infected with a worm. One of the latest exploits used by email worms is to address an infected email as if it came from a friend with the pitch that they are sending you a cure for a previously transmitted email infection. Never open these emails.
- * Do keep your email preview screen closed. A preview window will automatically open and display any email message your cursor happens to land on. If its infected, now your computer is too! Always read the subject line and know the author before opening any email. Only open email messages in a separate new window.
- * Don't install new downloaded software without first reading the full End User License Agreement (EULA) text completely. Be especially wary of free, or ad supported software. Nothing is free in life, there is usually a catch involved. Most trial shareware is safe to install, but read the EULA first.
- * Don't load free software like: Gator, search bars, time setting software, free icon software, free weather bugs, or any other free software that promises to make your life easier without first reading the complete EULA. As stated elsewhere in this publication, nothing is ever free in life. Most of these programs contain a Catch-22 in the form of ad serving back-door programs that can turn your PC into a 24-hour advertising display machine. This will, in turn, slow down your machine and eat away at your Internet bandwidth.
- * Do run the Ad-aware scan software at least once per week to remove any ad serving software and cookies that accumulate on your computer. Run the auto-update feature first to insure your Ad-aware scanner files are up to date. Go to Ad-aware's website to check for the latest version of Ad-aware:
<http://www.lavasoftusa.com>
- * Do install pest removal software. The two most popular are Pest Patrol and Spybot Search & Destroy. You have to purchase Pest Patrol, but Spybot is offered for free as a public service. Use either of these programs to scan your system at least once per week for backdoor programs, keyboard loggers, spyware, malware,

web bugs and Trojan horse software. Ad-aware mainly detects advertising software, Pest Patrol and Spybot are designed to find more harmful programs that might be missed by Ad-aware and antivirus software. You can order Pest Patrol by going to the following Internet site: <http://www.PestPatrol.com>, or call their toll free phone number at 866-235-7163 to speak directly with an authorized representative.

* Note: Zone Systems the parent company of ZoneAlarm has been running a special offer if you purchase the "Pro" version of ZoneAlarm you can often get Pest Patrol for free, or at a substantial discount as an add on. Spybot can be downloaded for free at: <http://www.safer-networking.org>.

* Don't visit hacker web sites, or sites run by independent webmasters with unknown, or dubious credentials. Avoid game hack sites. Many of these have files uploaded by hackers or other users who may not bother to scan them for viruses, or who may intentionally plant viruses or Trojans in their postings to infect others.

* Do run Windows Update at least once per week to check for critical security updates. Better yet you can now set Windows Update to check for updates automatically as soon as they are released. Most of these updates are to correct for security problems in Windows or other related Microsoft programs. Install all critical updates ASAP.

Addendum: Lately it has been popular for hackers to quickly develop exploits based on newly discovered security defects in Microsoft applications and operating systems. Many of these exploits now appear within days of Microsoft releasing a critical update, or even before an update patch is released. Because of this, it is recommended to install Microsoft updates ASAP to protect your computer. In the past it was recommended to hold off for 30 days in case an MS-Update had harmful side effects that were not detected during the normal prerelease testing.

This advice has now changed based on the speed with which the hacker community has been implementing new hacks that take advantage of Microsoft's security breaches. I recommend using System Restore to create a set point prior to installing any Critical Updates in Windows ME, or XP. This way if an update creates a problem, you can easily reverse the damage. Run ERU first on older versions of Windows. Call me if you need help.

* Do not conduct monetary (credit card or PayPal transactions) or private business over non-encrypted connections. SSL encryption scrambles and encodes your data transmission so that others who might intercept it can not read its contents. Your browser should notify you when entering or leaving an encrypted connection. Netscape also has a small padlock in the lower right corner of the screen. When the padlock is open you are on a non-encrypted (unsafe) connection.

* Don't visit Internet Relay Chat (IRC) chat rooms. IRC is inherently insecure and is inhabited by many hackers.

* Don't use AOL, MSN, Trillian, or Yahoo instant messenger software on business computers, or home computers with sensitive data. More hacker exploits are taking advantage of holes in IM software to compromise computers. IM software is typically not essential for conducting normal business communications.

* Don't install File Sharing software such as Kazaa, Limewire, Morpheus, Napster, etc. Not only can this software expose you to expensive lawsuits by the MPAA, or RIAA, but it also turns your PC into an Internet server. To do this the file sharing software opens TCP/IP ports up to the Internet that are normally kept closed. This makes your PC highly visible to hackers looking for potential Zombies to infect. The FTC has published a web page at: <http://www.ftc.gov/bcp/online/pubs/alerts/sharealrt.html>, warning consumers about the dangers in using file sharing software.

* Do perform regular backups of important data on to floppy disks, Zip drives, CD/RW or DVD/RW, tape, or other removable media. Store a second backup copy off site at another location in case a fire, flood, or other disaster destroys your primary location. You can always replace your computer; however, without a backup you cannot replace your lost data.

* Do create a Zip, or floppy based emergency recovery disk set, mark it and save it. Update it at least once per month, or after any major system changes. Many antivirus programs have a feature or wizard to walk you through how to do this.

* Don't visit porn sites. Many of these sites can infect your computer with scripts or other backdoor programs simply by clicking on them. These programs can vary from simply turning your PC into a porn ad server, or even go so far as to scan your PC for credit card numbers to steal.

* Do beware of Phishing exploits. Phishing is pronounced like fishing and is similar in meaning. This is a fairly new exploit that hackers and crooks are using to steal personal financial information such as: your online banking account numbers, private passwords, PayPal account information, and especially credit card numbers. The way the scheme works is simple:

The crook sets up a mirror image of a legitimate web site such as: eBay, or PayPal, or a credit card site for example. He then sends you an official looking email including real company logos, fonts etc., advising you to visit and update your online banking, eBay, or PayPal account. When you click on the convenient link provided in the email alert, the crook redirects your browser to his realistic looking mirror site versus the real site.

His goal is to trick you into typing in your private financial information, such as your credit card number and expiration date, online banking user name and password, etc. Once the crook has collected this information he or she can then easily steal you blind.

To avoid being phished, be leery of emails that are worded strangely, have spelling or grammar errors, have oddly named URLs, or in other words don't look legitimate. Call the company in question and ask if the email is real or not before responding to it. Most licit companies will never send these kind of emails in the first place. If you visit the web site link make sure the web site is using SSL encryption and verify the site certificate. Most crooks don't bother to incorporate secure connections, or maintain valid site certificates. This could change though. Try clicking on other links in the website to make sure they all work. A web site with many broken links is a sure sign of a fake site.

* Do take advantage of the free Microsoft ERU (Emergency Recovery Utility) program provided on the Windows 9x CD-ROM disk, to backup your windows registry and startup files at least once per month. This nifty program can accomplish this task in only seconds. Windows 2000 and NT users can download a freeware program called ERU-NT. WinME and XP users can use the built-in System Restore feature to create a restore point before installing new software or making any significant changes to your computer's configuration. System Restore allows you to roll your computer's configuration back in time before the new configuration changes took place in case the new changes caused it to crash or misbehave. Ask me for help on how to do this.

* Do stay abreast of the latest on-line security news. Visit sites like: <http://www.grc.com>, GRC ShieldsUp!, <http://www.grisoft.com>, <http://www.us.mcafee.com>, <http://www.informationweek.com>, <http://www.sophos.com>, <http://www.symantec.co> and <http://www.zdnet.com>. All of these sites can be found by typing the URLs above into your browser or by searching on Google.

* Here is a great article about keeping your home computer secure by the Carnegie Mellon Software Engineering Institute, CERT® Coordination Center: <http://www.cert.org/homeusers/HomeComputerSecurity>.

* Do check out the Langa-List at: <http://www.langa.com>. The LangaList is an email newsletter that is published twice weekly. It is full of important news and recommendations on how to maintain and improve your computer. The cost is free for the basic email list, the "Plus List" is \$12.00 per year. Most of the proceeds go to children's charities. Fred Langa (the author) is a well known computer columnist that is careful about testing software and other products before recommending them to his Langa-List readers.

* Do consider joining a computer user group. There are many computer user groups that meet monthly in the Detroit Area. Check out the SouthEastern Michigan Computer Organization, or SEMCO as they are better known at: <http://www.semco.org>.

SEMCO held their first meeting in 1976 and has been going strong ever since. Visit one of their local meetings, or see their Hot Links section for information on other

computer user groups in the Detroit area.

Note: The advice given in this white paper is based solely on my own personal research of other security articles and papers. It is not intended to be a comprehensive document on computer security. I will not be held responsible for any detrimental effects, loss of data, or loss of business that may result as a consequence of implementing any of these suggestions.

Copyright© 2002-2004, by Bill Woelk - User Friendly Computers of Royal Oak. Contents of this article may be redistributed or republished freely, so long as the contents is not modified and credit to the original creator and contributors is maintained.