

Home Computer **HELP!**

Serving the greater North Hills communities of Pittsburgh
 (412) 480-9969 *We make Housecalls!*



Practice Safe Surfing

- Don't click on links contained in Spam emails
- Just Say NO to online file-sharing (Music or Movies)
- Look out for Phishing and Pharming (see article on page 2)

Internet Explorer Keyboard Shortcuts

- **Ctrl-D** Adds the current page to your Favorites list.
- **Ctrl-B** Open the "Organize Favorites" dialog box
- **Alt-Up Arrow** Move the selected page up on the list in the "Organize Favorites" dialog box
- **Alt-Down Arrow** Move the page down on the "Organize Favorites List

Inside this issue:

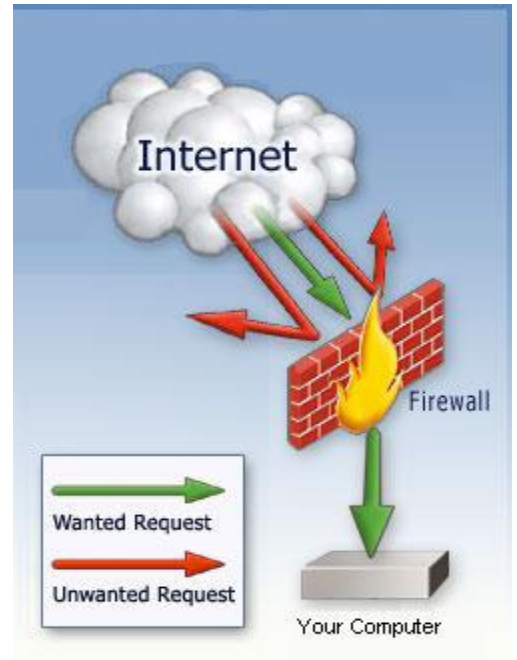
Internet Nasties Glossary.....	2
Backups Made Easy.....	4

Firewalls—Don't Go Online Without One!

Before the internet, a Firewall was a device used in construction, and could be found in any engineered building. It was part of the structure, and acted as a barrier, designed to prevent a fire (or at least slow it down) from spreading past a certain point. Firewalls are required by the building code and save lives – they work.

Internet Firewalls serve much the same purpose for computers. They are designed to keep the countless "internet bad guys" from gaining access to your computer (see the article "Internet Nasties Glossary" on page 2 for a frightening list). Firewalls can be either software (a program that runs on your computer) or hardware (a box that sits between your computer and the internet), and there are many different ones available.

If you have a dial-up connection to the internet, right now you may be saying to yourself that "I've never had a firewall, and I've never gotten a virus". If this is true, you should consider yourself lucky. You may want to go out and buy some lottery tickets right now, lucky. It's true that some bad guys ignore dial-up connections because it would take too long to download their nefarious pay-



load, but that is changing rapidly.

The fact is that most of these "bad-guy" programs are completely automated. They scan thousands upon thousands of random internet addresses automatically looking for vulnerable computers. Your risk comes from

(continued on page 2)

Ad-Aware Personal SE Version 1.06 Released

This software has been on our recommended list for a long time, and the release of version 1.06 continues to be one of our favorite tools to keep your computer free of adware and spyware. Visit www.lavasoftusa.com and click on **Downloads** to get the new version. After the installation, be sure you download the latest

signature file before you start using the software. Unless you are a heavy internet user, running the software about once per week should be enough to keep ahead of the bugs. As always, this program is free for personal use (we love free!).





If you are running Windows XP (Home or Professional) you should install “Service Pack 2” to take advantage of the many security enhancements.

SP2 is available via the Windows Update Web Site, but can be as much as 220 megabytes in size — way too big to download if you have dialup access to the internet.

We can save you time and frustration by installing Service Pack 2 directly from CD — usually in less than an hour.

Give us a call, we here to help!

“Firewalls work by preventing connections to your computer and by making your computer (mostly) invisible to automated scans from the internet. If the bad guys can’t see you, they can’t infect you.”

Firewalls—Don’t Go Online Without One!

(continued from Page 1)

just being online, not because you are sharing music or visiting questionable web sites (although those behaviors do carry an elevated risk).

Firewalls work by preventing connections to your computer and by making your computer (mostly) invisible to automated scans from the internet. If the bad guys can’t see you, they can’t infect you.

So, how do you choose what kind of firewall to use? Here are some Pros and Cons to help with the decision:

Hardware Firewall Advantages:

- Highest Level of Protection
- “Set It And Forget It” – little ongoing maintenance required
- One device works for all computers that share a single internet connection

Hardware Firewall Disadvantages:

- More expensive (\$60 - \$300 for home use models)
- More difficult to set up

Software Firewall Advantages:

- Less expensive -- \$30-\$50 for most retail “security suites”, many free softwares available
- Most softwares have installation “wizards” that make setup very easy

Software Firewall Disadvantages:

- Must install on each computer if you have more than one sharing a single internet connection
- Since program runs all the time, it reduces the amount of computer resources available for other work.
- Ongoing user input required. You may have to “train” the software over time to recognize those things that you **want** to allow (like virus software updates, etc.).

If you have a dial-up connection, you should use a software firewall.

Retail Security Suite softwares are available from Norton, McAfee, and others. Free softwares I like are Sygate (www.sygate.com) and Zonealarm (www.zonealarm.com). Windows XP has a built-in firewall which provides some protection, but should not be the only security you have.

Hardware firewalls include those made by Linksys, Netgear, and Watchguard.

Warnings & Suggestions

- Never run more than one software firewall on the same machine. This includes the Windows XP firewall. If you are using the Sygate firewall, for example, you should disable the Windows firewall.
- If you have a hardware firewall, feel free to run a software firewall as well – this gives you the highest level of protection.

Feel free to call us if you have any questions. We would be happy to install a firewall for you!



Internet Nasties Glossary

Whether or not you realize it, every time you connect to the internet or download an email, your computer is doing battle. If you’ve followed our advice, your computer is prepared for this battle with a properly installed and configured firewall, updated anti-virus software, and one or more spyware scanners. . You can only be properly prepared, however, if you know your enemy. What follows is a short primer on the various types of bad-guys that are trying to break through your defenses, and what to do about them.

(Continued on page 3)



Internet Nasties Glossary *(continued from page 2)*

Adware – A program secretly installed or downloaded to your computer that tracks what sites you visit on the internet for the purposes of delivering targeted advertising (refer to the in-depth article in our Fall/Winter 2004 newsletter for a more detailed explanation). These programs should be detected by your spyware scanner program.

Cookies – Text files that store information used to personalize web sites you visit often. See the article “Toss Your Cookies” in our Fall/Winter 2004 newsletter for a detailed explanation.

Harvesting – The act of stealing your email address book and sending it to purveyors of spam or other malware.

Macro Virus – Another name for a vbs program that delivers a virus to your computer. See “Vbs” later in this article.

Malware – Generic term (Mal is French for “Bad”) describing any program that is “up to no good.”

Phishing – An identity theft scam perpetrated via email.

You receive an email that looks like it is from a legitimate source (perhaps your bank or credit card company). This email asks you to verify your personal information for security purposes (or other such trumped-up reason), and provides a link for you to click on for this purpose. The link takes you to a site setup specifically to look like the legitimate site, but in fact is a bogus web site used solely to collect your name, account number and password. Once the bad guys have your information, it can be used to steal your identity, the funds in your accounts, or charge merchandise using your credit card. Defense against Phishing is simple – NEVER click on an email link for purposes of “verifying” your personal information. Your bank or credit card company or brokerage firm will NEVER ask for your information in this fashion.

Pharming – Much like Phishing, except you don’t get an email. Instead, a program is downloaded secretly to your computer, and waits for you to go to your bank or credit card company’s web site. When you do, this program wakes up and interrupts the process, sending you instead to a bogus site designed to imitate the real thing. This bogus site then collects your personal information. To help defend yourself against Pharming, do the following:

Whenever you go to your bank or credit card’s web site (or other web site where your personal information is used like ebay, Merrill Lynch, etc.), for your first logon attempt, use a *completely made-up user name and password*. The real web site will reject this attempt and tell you the information is invalid. You can then use your real name and password for the second attempt. **A bogus web site will accept the made-up information without question.** You may get a message that “we are having computer problems, please try again later”, but your logon with the made-up user name and password will be accepted. If you happen to identify a Pharming attempt in this way, you should immediately scan your computer for viruses and spyware using the latest updates for your scanning software. Make sure you clear your browser’s history and temporary files before trying again.

You may also wish to use the internet’s numerical (“IP” or “Internet Protocol”) address instead of it’s name for any web sites where you enter personal information. This can bypass the normal trigger for a Pharming program. For example, one of the numeric addresses for the popular web search site Google is 64.233.161.147 – to use this address, open your browser and type the following directly into the address bar:

`http://64.233.161.147`

Then, click on the “Go” icon next to the address bar, or merely press the Enter key.

To find out the numeric address of almost any web site you want to visit, use this slightly geeky, but foolproof, method:

1. Open the Run box (Hit the Start Button and choose Run).
2. Type the letters “cmd” into the run box and click OK. Note if you are running a version of Windows earlier than XP, type “command.com” instead of cmd.
3. This will display a black box on the screen with a Command Prompt visible.
4. Type the following (replace www.google.com with the name address of the site you want to look up, then press Enter.


```
nslookup www.google.com
```
3. Several lines of text will display. Look for the “Addresses” line, like this:

Addresses: 64.233.161.147, 64.233.161.104, 64.233.161

6. Write down the numeric address, then type the word “Exit” at the command prompt and press Enter. This will close the command box and return you to Windows.

“Every time you connect to the internet or download an email, your computer is doing battle.”



Home Computer **HELP!**

130 Pine Road
Pittsburgh, PA 15237

Phone: 412.480.9969

Email: help@home-computerhelp.com

We provide affordable, in-home computer service to customers in the greater North Hills region of Pittsburgh. Evening & Weekends, whenever it fits into YOUR schedule.

Call us for an appointment!

**Repairs, Troubleshooting, Upgrades, Training,
Custom-Built Computers**

WE'RE ON THE WEB!

WWW.HOME-COMPUTERHELP.COM

Internet Nasties Glossary *(continued from page 3)*

Spyware – Delivery and function much like adware for the purpose of monitoring your computer (without your knowledge or consent), looking for credit card numbers, passwords, and other personalized data. These programs should be detected by your spyware scanner program.

Trojan Horse – Like it's namesake, a Trojan Horse arrives disguised as or inside of a innocent-looking program. Perhaps it's a free screensaver featuring your favorite pet, a funny cursor replacement, or a song you downloaded from one of the sharing services. Hidden within the downloaded program, the Trojan Horse program runs when you install the file. The program scans your computer for private information and clandestinely sends it to the creator of the program. These programs should be detected by your anti-virus software.

Backups Made Easy

The more you use your computer, the more important it is to have a backup of your data. Things can (and do!) go wrong – parts fail, lightning strikes, you mistakenly overwrite an important file – the list is endless.

And yet, most of us don't backup on a regular basis. Why? Because it's too hard, too expensive or takes too much time and effort.

The USB Flash Drive (a.k.a. "Thumb Drive" or "Memory

Vbs – Visual Basic Scripting – "Macro" programming language used to store programs inside of Word Documents or Excel Spreadsheets. Useful in the right hands, but dangerous in the wrong hands. NEVER click on an email attachment whose name ends with "vbs". Better yet, NEVER click on ANY email attachment unless 1) you were expecting it, and 2) it comes from a known source.

Virus – A program that replicates itself for the purpose of spreading to other computers. Viruses can range from benign (but annoying) to dangerous (corrupting or deleting valuable files). They can be spread via email, removable media, or over the internet. New viruses are identified every single day. While many are just variations on already-existing viruses, some are new and can't be identified by your anti-virus software until it is updated to recognize the new threat. These are the most dangerous since they can infect your computer even if you are fastidious about updating your anti-virus program.

Key") is an inexpensive and easy solution to this problem. These little devices are available very inexpensively, and under Windows XP, require no installation. Just insert them into a free USB slot, and they show up in My Computer as another Hard Drive. You can copy or move files just as you would use a floppy, and they are much faster than burning a CD.

We can even help you automate the process so you can backup your most important files with just one click!