SoHo E-spirin E-zine
brought to you by
Funai Pty Ltd
IT Handyman Services
For Small Office/Home Office and Small Business. IT Tips & Tricks.

How You at Home Can Protect Your Windows PC from the Evils of the Internet... For Free.

Allan Naguit
03-Feb-04

Of course the Internet isn't necessarily evil. But there are definitely bad things out there from which you should be protecting yourself: ***Viruses, Worms, Trojans and Spyware***. If you simply want to know **what to do about them**, then this guide is for you. Along the way, this guide also offers an overview of **what they are** and **what they do**.

What To Do

There are three things that your computer should have. These should give you a significant (if basic) level of security and privacy when connected to the Internet:

1. **A Personal Firewall**
2. **Anti-Virus Software**
3. **Anti-Spyware Software**

This guide is structured so it opens each section with one of the three **main items** above, followed by a short explanation, then the good stuff: where to get **Your Free, (software)**. For those interested, this is followed by more in-depth explanations on what the item is and what it protects against. Otherwise, just jump to the next **Section**.

A Personal Firewall is a software application that normally filters traffic entering or leaving a single computer. Basically, a firewall protects your computer in two ways: it stops someone on the Internet from getting into your computer, and it stops your computer from secretly leaking your computer's information to the Net.

Your Free, Personal Firewall

There are many Personal Firewalls out there but arguably the best known (and FREE for personal use) is **ZoneAlarm**. Experts like Steve Gibson of the Gibson Research Corporation recommend it. He has a **Personal Firewall Scoreboard** at http://grc.com/lt/scoreboard.htm from which you can make your own choice. However, ZoneAlarm is a good choice if you're not so technically oriented. It's available at the Zone Labs website: www.zonelabs.com (try navigating through their Site Map, look at Home/Office Products, and look for ZoneAlarm – Free Download).

Keeping the Barbarians at the Gates

Usually, for malicious stuff (evil hackers/evil programs) to target computers, they have to know which computers are connected to the Internet. They can fish for these by casting a wide net of a particular type of "computer prodding". If your computer responds to this prodding (usually automatically) they can focus their attention on your computer. A personal firewall can protect your computer by not responding to this electronic prodding. To the malicious programmers, it's as if your computer were not connected at all (invisible) or has its doors ("ports") shut.

Plugging the Leak (Shutting Your Computer Up)

Another problem is "leaking". You could already have some bad things (like "spyware") hiding in your computer. They could secretly be sending out private information (like your Net-surfing habits) from your computer and to interested parties on the Internet. A personal firewall should let you know when something on your computer is trying to access the Internet. It should let you know instead of just slamming the door shut because oftentimes, it could be a valid action: it could be you trying to use your web browser to find out today's horoscope.

If your firewall lets you know whenever something is trying to reach out to the Internet – and before it actually does – then you can first: check what it is, and second: you can "teach" your firewall to remember whether or not it's ok to do it. For example, you'd say it's okay for your web browser (e.g., Internet Explorer, Opera, Mozilla) to talk to

the Net so it doesn't ask you again the next time you surf the Net. But if your firewall pops up an alert telling you that your computer is trying to access the Net, and you're not actively Net-surfing or e-mailing, it ***could*** be something that's leaking your private data to the Net.

It could also be quite innocent. It could be your antivirus automatically updating its database. But at least this way you have the chance to double-check and do something about it. You could disallow whatever it is from talking to the Net and just wait and see if you can still do your usual stuff. If you don't recognise what it is and can't work it out, the alert might convince you that it's time to scan your machine for viruses, spyware and other bad stuff.

Testing your Personal Firewall
ShieldsUP! is a useful, web-based "firewall checker" from a company called Gibson Research Corporation. You run it directly from their website. The **ShieldsUp!** utility pretends (with your permission) to act like a hacker or virus and systematically probes various parts of your computer. It then gives you the results of its efforts to get past your firewall.

The best result is to get "Stealth" ratings, meaning it looks like your computer isn't even connected to the Net. Next best is "Closed", meaning it looks like your computer exists but isn't responding to any prodding. If your computer is found to have "Open" ports, and you're not actually running "Internet servers or offering services to the public," you should take steps to close those open ports. It's recommended that you explore the site. It gives plenty of useful advice and information.

You can try **ShieldsUp!** at the Gibson Research Corporation's website: http://grc.com/default.htm.

Anti-Virus Software programs are computer programs that can be used to scan files to identify and eliminate computer viruses.

Your Free, Anti-Virus Software

You have the choice of four Free Antivirus solutions here. For an in-depth review, look at an on-line article from PC World at: http://www.pcworld.com/howto/article/0,aid,113462,00.asp
The title is "Free Antivirus: Finally Ready for Prime Time".

Grisoft's AVG Anti-Virus System	http://www.grisoft.com/us/us_dwnl_free.php
Alwil's Avast 4 Home Edition	http://www.asw.cz/i_idt_153.html
H+BEDV Datentechnik's AntiVir Personal Edition	http://www.free-av.com/index.htm
Softwin's BitDefender Free Edition Version 7	http://www.bitdefender.com/bd/site/products.php?p_id=24

Viruses - What They Are

A computer **virus** is a piece of program code that, like a biological virus, makes copies of itself and spreads by attaching itself to a host, often damaging the host in the process. The host is another computer program, often a computer operating system, which then infects the applications that are transferred to other computers. Viruses usually spread as attachments on emails, but you could also get them through files transferred from floppy diskettes or other media.

For an in-depth explanation on **Viruses**, see the original Wikipedia article at http://en.wikipedia.org/wiki/Computer_virus

A **Trojan horse** is also a relatively dangerous computer program that tries to do something malicious to your computer without letting you know.

For an in-depth explanation on the **Trojan Horse**, see the original Wikipedia article at http://en.wikipedia.org/wiki/Trojan_horse.

A Trojan horse differs from a virus in that it's a stand-alone program; the Trojan doesn't attach to another program. It differs from a

worm in that it doesn't move from one computer to another on its own. A person must transfer it intentionally, such as by email.

For example, an attacker might email a Trojan with an innocent filename attached to an email message that makes you want to see what that attachment is. When you double-click on the attachment, it might cause all kinds of havoc (like delete all your files).

It's a good idea to always scan e-mail attachments with updated antivirus software before opening them. A typical Trojan doesn't infect other programs and is usually easily deleted.

A **computer worm** is a self-replicating computer program, similar to a computer virus. The main difference between the two is that a virus attaches itself to, and becomes part of, another executable program, while a worm is self-contained; it does not need to be part of another program to propagate itself. In addition to replication, a worm may be designed to do any number of things, such as delete files on a host system, or send documents via email. It should be pointed out that worms are not always bad, and in fact can be occasionally useful, for instance they could be used to upgrade software on a very large privately run network. But even if worms do not have malicious intent if they reproduce quickly enough they can consume a lot of bandwidth and slow down networks.

Anti-virus software typically uses two different techniques to identify and eliminate computer viruses:

- Examining files to look for known viruses by means of a virus dictionary
- Identifying suspicious behaviour from any computer program which might indicate infection

Most commercial anti-virus software uses both of these approaches, with an emphasis on the virus dictionary approach.

In other words, a typical anti-virus program checks the contents (files) of your computer, looks for matches against its list (dictionary) of known viruses, and acts accordingly. It could delete the virus, quarantine the file with the virus so it can't spread, or even repair the affected file by removing the virus from the file. Of course, the anti-virus software is limited by how up-to-date its dictionary is, which is why it's recommended to update it as often as possible (e.g., daily).

Anti-Adware/Anti-Spyware

programs are computer programs that can be used to scan files to identify and eliminate **adware** and **spyware** from your computer.

To combat both, a very effective way is to have two software programs on your home computer: **Spybot Search & Destroy** (from PepiMK Software)and **Ad-Aware** (from Lavasoft). In practice, Spybot sometimes finds spyware that Ad-Aware misses and vice-versa. Used side-by-side, they catch most Adware and Spyware floating around the Internet.

Your Free, Anti-Adware(/Spyware)

Ad-aware	www.lavasoftusa.com
Spybot Search & Destroy	www.safer-networking.org

Similar to Antivirus Software, both Ad-Aware and Spybot S&D work by comparing your files to their database of known spyware. Each one also allows you to update their database by connecting to their websites. It's recommended that you install both of these programs on your computer and run them regularly (and don't forget to update the dictionaries, at least weekly).

What are Spyware and Adware?

Spyware is computer software that aids in gathering information about a person or organisation without their knowledge. The most common use of spyware is to gather information about the user and relay it to advertisers or other interested parties. It has also been used by law enforcement to collect evidence against criminal suspects.

For an in-depth explanation on Spyware, see the original Wikipedia article at http://en.wikipedia.org/wiki/Spyware

Spyware can be installed on a computer by a virus, by an e-mail trojan, or it may be hidden within the otherwise-innocent installation of a new program. Data collecting programs installed with the user's knowledge are not, properly speaking, spyware, if the user fully understands what data is being collected and with whom it is being shared.
Spyware is usually installed by some stealthy means. If you read the user agreements for the software you download and install, references (sometimes vague) are cited for allowing the issuing company of the software to record your internet usage and website surfing. Some software vendors allow you to buy the same product without this overhead.

Adware or **advertising-supported software** is any software application in which advertisements are displayed while the program is running. These applications include additional code that displays the ads in pop-up windows or through a bar that appears on a computer screen. Adware helps recover programming development costs, and helps to hold down the price of the application for the user (even making it free of charge)--and, of course, it can give programmers a profit, which helps to motivate them to write, maintain, and upgrade valuable software. Some adware is also shareware, in that users are given the option to pay for a "registered" or "licensed" copy, which typically does away with the advertisements.

For an in-depth explanation on Adware, see the original Wikipedia article at http://en.wikipedia.org/wiki/Adware

Links & Resources

Grisoft's AVG Anti-Virus System	www.grisoft.com/us/us_dwnl_free.php
Alwil's Avast 4 Home Edition	www.asw.cz/i_idt_153.html
Grisoft's AVG Anti-Virus System	www.grisoft.com/us/us_dwnl_free.php
H+BEDV Datentechnik's AntiVir Personal Edition	www.free-av.com/index.htm
Softwin's BitDefender Free Edition Version 7	www.bitdefender.com/bd/site/products.php?p_id=24
ZoneAlarm	www.zonelabs.com
Shields Up!	http://grc.com
Ad-aware	www.lavasoftusa.com
Spybot Search & Destroy	www.safer-networking.org
Wikipedia, the Free Encyclopedia	http://en.wikipedia.org/wiki/Main_Page

What's Next?

The next steps to making your PC more secure include things like regular **File Backups**, **Windows Critical Updates**, using more secure **Web Browsers**, **Email Encryption** and we haven't even mentioned **SPAM**. Although these are currently beyond the scope of this guide, perhaps an updated version will cover them. In the meantime, you're encouraged to find out more about these things for yourself. Just do what we did: go to www.google.com and search away! And don't forget about the excellent Wikipedia, the Free Encyclopedia. You just might get hooked.

About this Guide

This guide came into being to help people take the basic steps to making their PCs more secure from the bad elements of the Internet. Prevention definitely beats the cure, and the less virus-carriers there are, the better for the rest of us.

Allan Naguit is an IT Consultant for Funai Pty Ltd, an outfit that provides "IT Handyman Services" for small businesses and SoHos based in the Sydney Metropolitan Area (Australia). This monthly e-zine is part of their services, giving ideas for curing IT headaches, and exposing people to their IT opportunities.
If you found this e-zine helpful go and subscribe!
Visit their website at www.funai.com.au.