

Secure Your PC & Communications

By Aaron Turpen

Secure Your PC & Communications

Aaron Turpen
aaron@aaronzwebworkz.com

Aaronz WebWorkz <http://www.AaronzWebWorkz.com>

In today's world of online connections, hackers, information nabbing, and other nefarious Internet deeds, many wonder what they can do to protect themselves. This is especially true with those who have an "always-on" or static IP connection to the Internet (cable modem, DSL, etc.).

There are many tools out there to help, but by far the best is ZoneAlarm from Zone Labs. A free version for private use is available from their website (<http://www.zonelabs.com>) while the commercial and Pro version are about \$50. The paid versions include one year of upgrades and support.

Whichever version you choose, you'll be well covered from most Internet attacks by this handy little firewall. After first installing ZoneAlarm, you'll be bombarded with messages from the software asking whether this program or that should have access to the Internet. This will be your first clue as to how great this program is. Once you've chosen who can have access and who can't (obvious choices like your web browser, proxy service, email client, etc. will need access), you'll rarely see anything from the program unless something is wrong. If you aren't sure about a program, you can click on information and if Zone Labs has that software in their database, they'll inform you as to what it is.

The software is highly configurable for different types of connections or security levels, but for most people, the default settings are good enough. I prefer the Pro version, which includes a free piece of software that checks your system for "spyware" and "adware" (programs which spy on you or use advertisements to pay for themselves – in both cases usually at the expense of your privacy). The Pro version also has the ability to "map" where an intruder is attempting to come from. Sometimes this is useful in at least tracking down the would-be hacker's ISP so you can complain.

Once you have your new firewall set up, you'll want to consider anti-virus software. There are many to choose from, but I've always preferred the highly acclaimed Norton Anti-Virus, made by Symantec. It is available off-the-shelf or through their website and several other vendors (Amazon.com and the like) as well. Expect to pay around \$50 for this software, but it's the best \$50 you'll ever spend on your computer. Norton scans all incoming and outgoing emails, your hard drive, all downloaded files and email attachments, and even disks, CDs, and other media when you put them into the drive. Most of this is in the background and you won't even notice it happening. The drag on your system is minimal in most cases as well. There are a lot of configuration options, but again, the default settings are best for most people. Watch for it to scan your system every Friday night for viruses. This can be changed or disabled completely at your discretion.

Finally we come to file downloads and other online sharing. While the majority of virus and Trojan horse attacks are made through email file attachments or shareware/freeware downloads, this is no reason to stop using or accepting either. I myself run many useful shareware and freeware programs and receive literally dozens of file attachments to emails daily.

The anti-virus software you've installed is your first line of defense. The next few steps may seem like common sense to some, but may have been overlooked by others.

Make sure the person sending the file/email is someone you know and that the subject line of their email is "normal" for the type of subject they'd put in (rather than something strange like "L@@K at this!"). If you're downloading freeware/shareware, be sure that the site is reputable and fairly well known. If you've used the site in the past and not had problems, you've established trust and should guard it carefully. I personally prefer cnet.com and tucows.com for most of my shareware requirements.

Whatever your chosen download site, make sure they have reviews of the software – either by professionals or by other users (many have both). Before you install software, read the software agreement (usually long and boring, but you NEED to do this) before you install it. If the program is adware or spyware, it will HAVE to list their information-gathering techniques in this agreement. Otherwise the software is illegally collecting information. You may also want to double-check the software at <http://www.spychecker.com> – a free public database of known spyware and adware programs.

When the program first attempts to access the Internet, if you have ZoneAlarm or another firewall installed, you should receive an alert that the program is attempting to access the Internet. If you don't know what the program is doing or why it needs to access the Internet, you probably should block it from doing so. If software doesn't inform you of its intentions before doing something, it may be attempting to do things behind your back. In my book, this is ground for dismissal.

Regardless of how you access the Internet, your security and the welfare of your PC is always of concern. The simple steps I've outlined here and the recommendations I've made should protect you most of the time. While nothing is 100%, putting the odds in your favor is definitely better than playing against a stacked deck.

[Get-Articles.com : 1000's of reprintable business and internet marketing-related articles.](#)

[Submit your article for reprint.](#)