



Four basic security rules for every computer that connects to the Internet:

1. Install a Firewall between the PC and the Internet.
2. Use Antivirus software, and keep it current.
3. Regularly run "Windows Update" and install all Critical Patches.
4. Regularly scan drives using "Spyware" detection and removal software.

### Additional Information Security Resources

**Sinclair Community College**

<http://www.sinclair.edu/departments/infosec/index.cfm>

**FTC Consumer Protection Advice**

<http://www.ftc.gov/bcp/menu-internet.htm>

**US-CERT Security Tips**

<http://www.us-cert.gov/cas/tips>

**National Cyber Security Alliance**

<http://www.staysafeonline.info/>

**Microsoft 'Security at Home'**

<http://www.microsoft.com/athome/security/default.mspx>



**NOTE:** This is intended as a basic guide to illustrate some effective practices and some of the tools available to home PC users. *Sinclair Community College does not endorse, or offer technical support for, any of the software or vendors listed in this document.*

Current as of February, 2005  
Daniel V. O'Callaghan, Jr., CISSP  
Chief Information Security Officer  
<http://www.sinclair.edu/departments/infosec/index.cfm>  
Sinclair Community College  
444 West Third Street  
Dayton, Ohio 45402



**How to  
Protect Your  
Home PC  
from Internet  
Threats  
for  
*FREE!***

**Do you have a  
computer in your home?  
Do you use it for email or  
the Internet?**

**If so,  
you need to protect it  
from hackers, viruses,  
worms, and other  
malicious attacks.**

# Protect Your Home PC from Internet Threats— for Free!

Do you have a computer in your home? Do you use it to check email or access the Internet? If so, you need to protect it from hackers, viruses, worms, and other malicious attackers.

There are four basic security tools every computer that connects to the Internet should have and use:

1. An Internet Firewall
2. Antivirus Software
3. Regularly run “Windows Update” (Windows 2000, ME, or XP can do automatically)
4. “Spyware” detection and removal software.

Fortunately, there are companies who, in the name of good “netizenship,” will help home users protect themselves with some free software tools. Here’s who they are and how to get the tools.

## Internet Firewall

The purpose of a firewall is essentially to block unwanted Internet traffic from your PC. If you use Windows XP, it has a built-in basic firewall, all you need to do is make sure it is turned on (see Windows XP ‘help’ files). For other versions of Windows, a good software firewall is **ZoneAlarm**, available from [www.zonelabs.com](http://www.zonelabs.com). While their premium products are very effective and well worth the cost, especially for the advanced PC user, the free version they offer is effective for most users. To obtain the software, click on the link “[ZoneAlarm \(free\)](#)” on the Zone Labs home page. Follow the instructions for download and installation. (The default program settings are adequate for most users.)

## Antivirus Software

Anti-virus software detects and prevents known viruses and other malicious code from infecting your system. It is only effective against the viruses in the “signature file”, so it must be updated frequently (**Recommendation: Update your signature files at least daily**).

There are many reputable antivirus software programs. The two most well known are Symantec’s Norton Anti-Virus, and McAfee’s VirusScan. If you don’t want to purchase Norton or McAfee, another vendor, **Grisoft**, offers a good “free” AV tool. The free version is offered to “single-seat” home users, **AVG Free** doesn’t allow scheduled scanning and full scans must be triggered manually, but it does scan email and downloaded files “on-demand”. It is available for download from [www.grisoft.com](http://www.grisoft.com). Users have to complete a survey and submit a valid email address to obtain an activation key.

### On-Line AntiVirus Scan

**Recommended: After downloading AVG, (or other AV software) but before installing it,**

Visit **Trend Micro** and run their free on-line virus scanner <http://housecall.trendmicro.com/> to ensure the PC is virus-free before installing any new software. Some viruses actually prevent antivirus software from installing or scanning properly. (Trend Micro also sells an excellent Anti-virus product and security suite, PC-cillin).

## Windows Update

Windows Update is the tool Microsoft provides to keep Windows software updated with the latest security patches. As long as you have an Internet connection and Internet Explorer browser, you can run this tool. You should run Windows Update at least once a week.

- From the Internet Explorer browser toolbar, click Tools, then Windows Update (you may be prompted to install software from Microsoft...click “yes” or OK)
- After the page loads, click the “Scan for Updates” link.
- You should install all “Critical Updates” found during the scan, including ‘SP2’ if you are using Windows XP.

If you are using Windows 2000, ME, or XP, you can set your PC to automate the Windows Update process. Instructions are different for each version of Windows and are available on the Microsoft Security Web site <http://www.microsoft.com/security/articles/swupdates.asp>.

## Spyware Scanners/Removers

Spyware is a generic—and controversial—term for software that collects information about you and/or your PC, and transmits this information to its “home” computer. Some spyware is harmless or even marginally beneficial as it simply tracks your Internet usage habits to deliver targeted advertising; this allows some Web sites to remain free of charge. However, illicit spyware is a threat that is growing and has the potential to cause damage or steal personal information.

As a minimum, users should occasionally scan their systems to ensure they know if any spyware programs are running, and should also eliminate any unwanted spyware. An effective, proven free anti-spyware tool is **Ad-Aware SE**, available from:

<http://www.lavasoftusa.com/>. Another good spyware detector is **SpyBot S&D** (Search & Destroy) available from: <http://www.safer-networking.org>. Be very careful to type the URL (Web Address) exactly as listed above because some unscrupulous companies actually use very similar addresses to trick the unsuspecting into *installing* spyware instead of the spyware removers!

Microsoft is also developing a free antispyware tool. As of this publication date, this software is ‘beta’ (test). If you are comfortable testing software, the URL is: <http://www.microsoft.com/athome/security/spyware/default.msp>

*The Internet-based threats to your PC are real—and growing—but they do not outweigh the benefits of the access to information and communication offered (and, of course, shopping!). With a little effort, understanding and practicing basic Information Security habits, and by using the free tools listed above, you can not only “surf” more safely and privately, but also help prevent your PC from being used to help generate the next malicious code tsunami on the Internet.*

Current as of February, 2005

Daniel V. O’Callaghan, Jr., CISSP  
Chief Information Security Officer

<http://www.sinclair.edu/departments/infosec/index.cfm>  
Sinclair Community College  
444 West Third Street  
Dayton, Ohio 45402