

# KEEP YOUR COMPUTER SAFE AND SECURE WHILE YOU ARE ON THE INTERNET

Beginners' Kaffee Klatch  
Presented by Bill Wilkinson  
February 3, 2007

It is a fact: the Internet is just not a safe place on which to connect your computer. If you access the Internet from an unprotected computer, there is a good chance that the computer will be compromised within the first 23 minutes! That figure, provided by the SANS Institute's Internet Storm Center, reveals a troubling issue. In less time than it takes to download and install all the various fixes and patches to secure Windows, your PC can fall victim to a malicious worm, virus, or other form of malware. It's an Internet-era Catch-22. There are worms constantly scanning for vulnerable computers to infect, Trojans disguised as helpful programs, but actually installing malicious ones, spyware that reports your activities back to their makers, and hijackers that take control of your web browser and browsing experience.

For those people who have been the victim of one of these infections, removing them and getting your computer back under your control can be a daunting and frustrating experience. The purpose of this presentation is to teach you how to setup your computer in such a way that you minimize the risks of contracting one of these nasties.

Each step is very easy to do and regardless of your computer experience you will have no trouble following along. It is also important to note that there is not one step listed below that is more important than the other. They are all equally important to keeping your computer safe and secure.

**USE ANTIVIRUS SOFTWARE.** It is very important that your computer has an antivirus software running on your machine. By having an antivirus program running, files and emails will be scanned as you use them, download them, or open them. If a virus is found in one of the items you are about to use, the antivirus program will stop you from being able to run that program and infect your computer.

**It is important to have only one anti-virus program installed on your computer at any one time. (Any anti-virus program that comes bundled with your Internet service provider does not count!)**

**Three recommended anti-virus programs (all free):**

**AVG Anti-Virus Free Edition.** Although you'll get a fraction of the features found in AVG Professional, Grisoft's AVG Anti-Virus Free Edition still leaves you with a reliable utility that catches practically all viruses—with no hassle. Regular updates

keep this program constantly on top of the latest threats, and automatic scanning makes sure your system is clean, even if you forget to use the scanner. A rudimentary interface provides quick access to scanning and resident shield options, including email scanning, as well as other tools. <http://tinyurl.com/czbxm>

**AntiVir PersonalEdition Classic.** With the ability to detect and remove more than 80,000 viruses, Avira's AntiVir provides solid protection against most of today's viral beasties. AntiVir even protects against previously unknown viruses using heuristic detection, which watches for virus-like patterns to catch new malware. Through its System Tray icon, the utility's on-access scanner provides an instant view of its current status, including the name of the last file it scanned. <http://www.free-av.com>.

**avast! 4 Home Edition.** This free, feature-packed utility integrates elements typically found in premium products, including Web Shield, which monitors and filters HTTP (Hypertext Transfer Protocol) traffic for malware, and Network Shield, which works on systems using Windows XP to protect against Internet-based attacks such as worms. The avast! 4 program's resident protection offers multiple settings to fine-tune your antivirus environment exactly as you see fit, including email options for scanning various protocols and a separate plug-in for Microsoft Outlook.

<http://tinyurl.com/oagc8>

**Virus Repair Utility:** If your anti-virus program is not able to quarantine or remove a virus from your system, select the virus that you need to remove from your computer and download the solution for free. Since this program is Web-based, it can be used as a complement to your installed anti-virus program.

<http://tinyurl.com/fa2ag>

**UPDATE YOUR ANTIVIRUS SOFTWARE.** - There is no point running an antivirus program if you do not make sure it has all the latest updates available. If you do not update the software, it will not know about any new viruses, Trojans, worms, etc. that have been released into the **wild** since you installed the program. Then if a new infection appears in your computer, the antivirus program will not know that it is bad and will not alert you. Therefore it is imperative that you update your Antivirus software whenever new definitions are available so that you are protected from all the latest threats. (Both AVG and Avast4Home will update your definitions automatically.)

**OCCASIONALLY RUN ONLINE VIRUS SCANS.** Unfortunately not all antivirus programs are created equal. Each program may find infections that another antivirus program does not and vice-versa. It is recommended that you occasionally run some free **online** (Web-based) antivirus scanners to make sure that you are not infected with items that your particular antivirus program does not know how to find.

Two highly recommended online scanners are:

<http://housecall.antivirus.com/>

<http://www.pandasoftware.com/activescan/>

**At least once each month, run one or both of these scanners to see if they find anything that may have been missed by your locally installed antivirus software.**

### **VISIT MICROSOFT'S WINDOWS UPDATE SITE FREQUENTLY.**

Open INTERNET EXPLORER, click on TOOLS, then WINDOWS UPDATE. This site is a Microsoft site that will scan your computer for any patches or updates that are missing from your unit. It will then provide a list of items that it can download and install for you.

You can set up Windows XP to automatically perform the tasks mentioned above by clicking on START, right-clicking on MY COMPUTER, selecting PROPERTIES, then clicking on the AUTOMATIC UPDATES tab.

Of the four choices offered, choose either **“Download updates for me, but let me choose when to install them”** or **“Notify me but don’t automatically download or install them.”** DO NOT select “Automatic” or “Turn off automatic updates.”

**USE A FIREWALL.** It is extremely important that you use a Firewall on your computer. Without a firewall your computer is susceptible to being hacked and taken over. You may say "Why do I need a firewall? I have all the latest updates for my programs and operating system, so nobody should be able to crack into my computer". Unfortunately that reasoning is not valid. Many times crackers discover new security holes in a software or operating system long before the software company does and therefore many people get cracked before a security patch is released. If you use a firewall, the majority of these security holes will not be accessible as the firewall will block the attempt.

### **Free Personal Firewalls (Software) INSTALL ONLY ONE OF THESE!**

All four of these products control both **incoming** and **outgoing** malware.

**Zone Alarm.** <http://tinyurl.com/qbzqd>

**Kerio Personal Firewall.** <http://tinyurl.com/aaspz>

**Adorons Firewall:** <http://tinyurl.com/2sumvv>

**Sygate Personal Firewall.** <http://tinyurl.com/33enen>

**Hardware Router/Firewalls. NEEDED IF YOU HAVE A BROADBAND INTERNET SERVICE [examples: Cox or Embarq digital subscriber line (DSL)].**

Belkin: <http://www.belkin.com/networking/>

D-Link: <http://www.dlink.com/>

Linksys: <http://www.linksys.com/>

Netgear: <http://www.netgear.com/>

**INSTALL ANTI-SPYWARE.** Just as you use an antivirus program, it is essential these days to use good Spyware protection and removal programs.

**According to many experts, you should have a "cocktail" of anti-spyware programs installed on your computer, including all of these.**

**Microsoft Windows Defender.** Previously known as Microsoft AntiSpyware, Windows Defender is the antispyware tool that is included with Vista, Microsoft's newest operating system. However, it is freely available to any WinXP SP2 user. This utility features a slick interface that's easy to navigate and understand, in addition to a powerful scanner that catches a wide range of threats. As Windows Defender identifies such threats, the program alerts users with pop-up messages that indicate suspicious activity. <http://tinyurl.com/47cus>

**The Microsoft Windows Malicious Software Removal Tool** checks computers running Windows XP for infections by specific, prevalent malicious software and helps remove any infection found. When the detection and removal process is complete, the tool displays a report describing the outcome, including which, if any, malicious software was detected and removed. Microsoft releases an updated version of this tool on the second Tuesday of each month. New versions are available through the Microsoft Download Center at: <http://tinyurl.com/hsxvt>

**SpywareBlaster.** Although today's free antispyware apps are getting better at preventing spyware infections, their main focus remains on identifying and removing spyware after the threats infect your computer. However, SpywareBlaster works primarily on the prevention side, blocking spyware-related threats from installing and executing. <http://tinyurl.com/3vcux>

A tutorial on installing & using Spyware Blaster can be found here:

<http://www.bleepingcomputer.com/tutorials/tutorial49.html>

**Spybot Search & Destroy.** If you need an effective, no-frills, spyware-scanning app that can identify and remove most threats, Spybot Search & Destroy is a wise choice. In addition to basic scanning tools that target cookies, Internet dialers, browser

hijackers, keyloggers, Trojans, and other malware, Spybot S&D features immunization tools for Internet Explorer that help block suspicious plug-ins and other downloads. Spybot S&D also provides a wealth of fine-tuning options that let you alter the way the program scans and removes spyware. <http://tinyurl.com/2b7s7>

A tutorial on installing & using Spybot S&D can be found here:

<http://www.bleepingcomputer.com/tutorials/tutorial43.html>

**Ad-Aware SE Personal Edition.** Long regarded as a trusted ally in the war against spyware, Lavasoft's Ad-Aware program remains an effective tool for identifying and removing threats. This free utility is now better than ever, featuring a scanning engine that scours extended memory (including modules loaded by processes) and can even identify new and unknown variants.

<http://tinyurl.com/ahklk> or <http://tinyurl.com/fh7cs>

A tutorial on installing & using Ad-Aware can be found here:

<http://www.bleepingcomputer.com/tutorials/tutorial48.html>

**CWSredder:** The best defense against malware that tries to hijack your browser.

<http://tinyurl.com/pgxct>

A tutorial on installing & using CWSredder can be found here:

<http://www.bleepingcomputer.com/tutorials/tutorial47.html>

**Bazooka Adware and Spyware Scanner** detects a multitude of spyware, adware, Trojan horses, keyloggers, and trackware components. The scanning process only takes a fraction of a second and tells you how to uninstall the invasive spyware or puts you in contact with the spyware developer for the most up-to-date and safe uninstall instructions. Spyware and adware often are bundled with free software and in many cases are installed without your knowledge. Some send information about your surfing habits to ad companies, which target you with pop-up ads that fit your preferences. <http://tinyurl.com/9bxnz>

## **UPDATE ALL THESE ANTI-SPYWARE PROGRAMS**

**REGULARLY.** If you do not update your programs, they will not be able to find the newest infections that may be racing around the Internet. It is important that you upgrade the software and spyware/virus definitions for a particular program so that it will run effectively.

## **DO NOT PERMIT "UNINVITED" PROGRAMS TO RUN AT STARTUP.**

**StartupMonitor** is a small utility that runs transparently (it doesn't even use a systray icon) and notifies you when any program registers itself to run at system startup. It prevents those utterly useless tray applications from registering themselves behind your back, and it acts as a security tool against trojans like BackOrifice or Netbus.

<http://tinyurl.com/33j pz>

**SWITCH TO ANOTHER BROWSER, LIKE FIREFOX, OR MAKE YOUR INTERNET EXPLORER MORE SECURE.** Internet Explorer is inherently insecure. Your best choice is to switch to another browser like **Mozilla Firefox**. It's an excellent browser and tends to be much more secure.

<http://www.mozilla.com/firefox/>

If you still decide to continue using Internet Explorer, then follow these steps to make it more secure:

1. From within Internet Explorer click on the **TOOLS** menu and then click on **Internet Options**.
2. Click once on the **Security** tab
3. Click once on the **Internet** icon so it becomes highlighted.
4. Click once on the **Custom Level** button.
5. Change the **Download signed ActiveX controls** to **Prompt**
6. Change the **Download unsigned ActiveX controls** to **Disable**
7. Change the **Initialize and script ActiveX controls not marked as safe** to **Disable**
8. Change the **Installation of desktop items** to **Prompt**
9. Change the **Launching programs and files in an IFRAME** to **Prompt**
10. Change the **Navigate sub-frames across different domains** to **Prompt**
11. When all these settings have been made, click on the **OK** button.
12. If it prompts you as to whether or not you want to save the settings, press the **Yes** button.
13. Next press the **OK** button to exit the Internet Properties page.

## **BLOCK POPUPS**

You click a search result and are suddenly bombarded with porn pop-ups. Back out immediately by either clicking the **X** in the upper-right corner of the Website window or by pressing **Alt+F4** to close your browser. Then run a malware scanner to assess and fix the damage. Many **pop-up blockers** are available for Internet Explorer 6 or 7, including the one built into the IE browser (click on **Tools** from the Menu Bar to find **Popup Blocker**). Both Firefox and Opera include blocking features.

**By following the ten (10) suggestions listed above in CAPITALIZED BOLD FACE, you are assured of keeping your computer at minimal risk to future infections or cracker attempts. Unfortunately, there is no fool proof method of securing your computer as new risks are released almost every day, but your susceptibility to these attacks will be diminished greatly.**