

Protecting Your Home Computer from Internet Threats

Improperly configured home PCs are one of the biggest risks to the Internet. At any given time there are hundreds of thousands or possibly millions of home PCs infected with viruses, worms, adware, spybots, or spambots. These users are causing a large volume of malicious traffic, which at the very least is a nuisance, and at the worst is infecting other PCs on the Internet. In the days where everyone connected using dialup, the impact of these infected PCs was minimal. But today when most home PCs are connected via an always-on high-speed connection, these machines are causing a significant impact to the Internet and the users on it. There is no reason for your machine to be one of these. A few basic security steps can virtually ensure a home PC will never be infected.

This document details the strategy I use when securing a home computer. I am a security professional by trade, but nothing in this document is difficult, or requires any special security knowledge. Anyone who can turn on a computer and surf the Internet is more than capable of performing the steps in this document.

For those of you who don't like to read the instructions before assembling Christmas toys, here are the steps in brief:

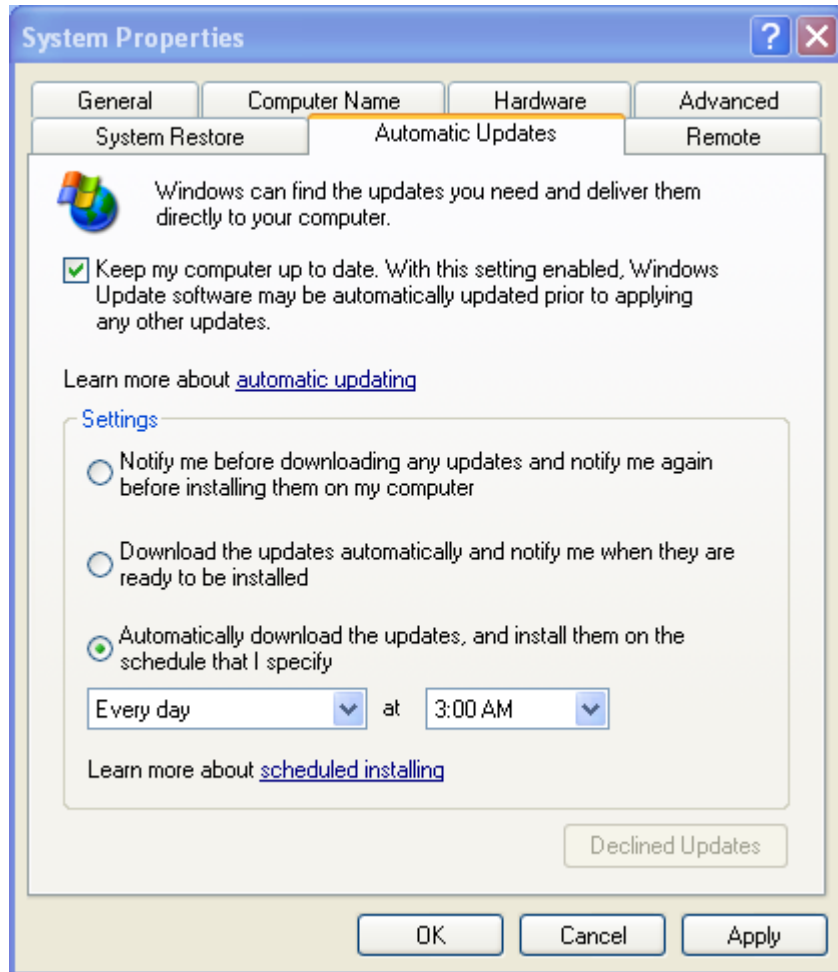
- Enable automatic Microsoft updates.
- Install and keep anti-virus software up to date.
- Install anti-adware software
- Install a gateway router

The screenshots in this document come from Windows XP Professional, but all of this functionality exists in any recent Windows version, i.e. any version Windows 98 or newer. If you are running on an operating system older than that, you should probably start by upgrading to Windows XP.

Step 1: Enable Microsoft Updates

Most viruses and worms take advantage of vulnerabilities in the Microsoft Windows Operating System. Microsoft provides patches for any known vulnerabilities at least once a month. By configuring your PC to download these fixes as soon as they are available, you will be made aware of these fixes within a day or two of when they are released, and can apply them in most cases before the vulnerability can be exploited causing your machine to be infected.

Automatic updates can be enabled by clicking on Start -> Settings -> Control Panel -> System then clicking on the "Automatic Updates" tab and setting it to download and install the updates automatically. The screen is displayed below.



Anti-Virus Software

Ok. So now you are installing Microsoft updates, so you are safe? Correct? Unfortunately not. There are two major problems. The first is that the updates don't always get distributed before malicious code reaches the Internet to exploit it. The second is that not all attacks against your machine are against the operating system and applications. For example a lot of attacks in the last few years have propagated via email attachments.

In the early days of the PC revolution, anti-virus software was used to stop files on your machine from becoming infected via diskette borne viruses. Viruses and their progeny are typically called malware nowadays. The new name refers the fact that a large family of malicious code has evolved from the simple virus to numerous types of malicious code with numerous attack methods. Fortunately anti-virus software has evolved along with them to cover all sort of malware and to protect various applications present on your machine, including common email clients. Anti-virus will check and clean the email coming into your system, and more importantly, will check the email going out of your system to make sure you have not accidentally become infected and are propagating the problem to your friends in your email address book.

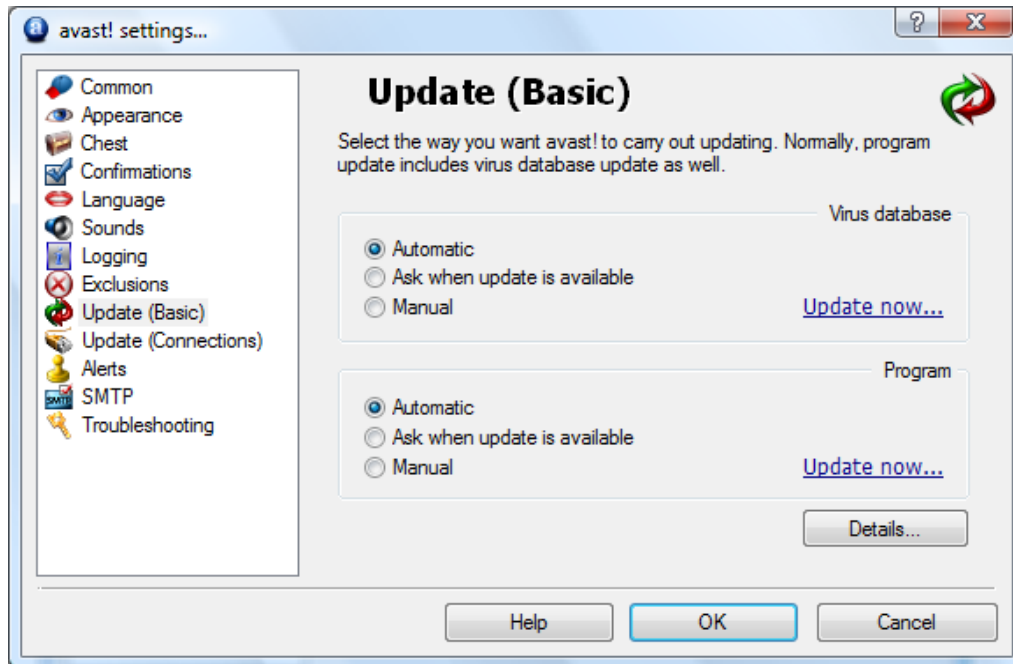
[Symantec](#) and [McAfee](#) seem to own the majority of the anti-virus market, although other companies such as [Trend Micro](#) and [E-Secure](#) also have excellent competing products. The point is that there are a lot of competing products out there, and the difference is negligible both in functionality and in price. You should be able to purchase anti-virus for less than \$50 plus a small yearly subscription fee for the anti-virus software and signature updates. If you really don't want to pay for anti-virus, the good people at [Avast](#) provide a version of their commercial product free for non-commercial use. The free version can be found at <http://www.avast.com/eng/download-avast-home.html>. It has most of the features of the commercial offerings and is far better than nothing.

Once anti-virus is installed, it does not require much care and feeding and it will make it extremely difficult for malware to take hold on your computer.

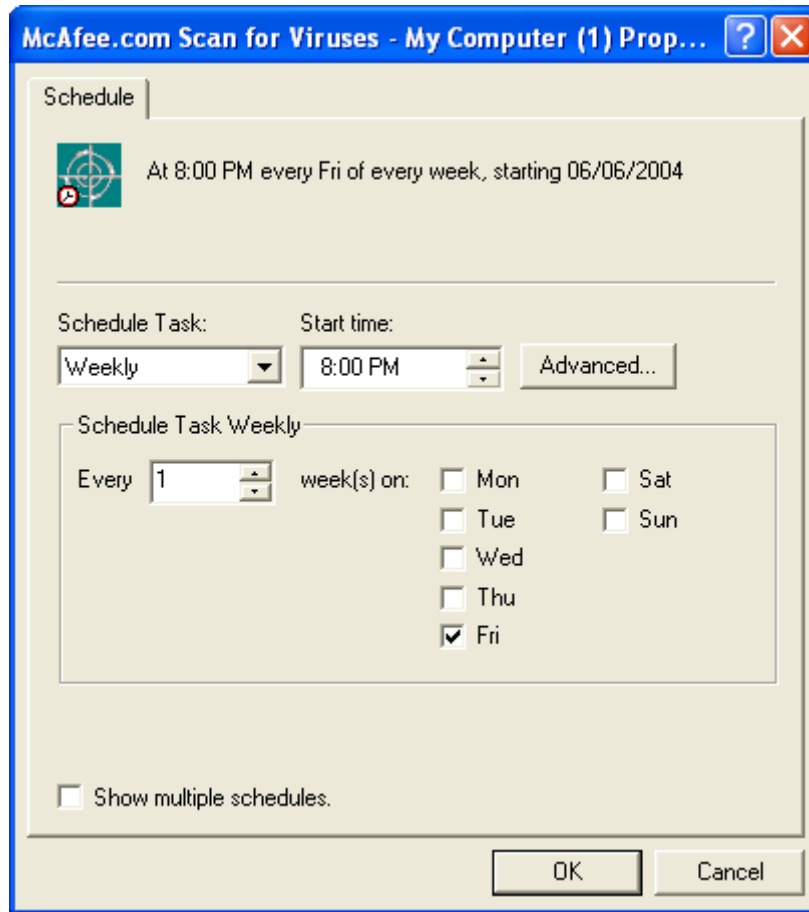
Whichever product you choose, you should ensure that it is configured to get anti-virus program and signature updates automatically. The screenshot below is for McAfee VirusScan, but all products have similar configuration screens.



Here is the corresponding screen for Avast:



Also, it is possible that you have gotten infected by a zero-day exploit, or malware that has gotten in before the anti-virus signature update which recognized it was released. Because of this you should configure your anti-virus to run a weekly scan on your computer. This will catch anything that snuck in under the radar. Again, the screenshot below is for McAfee VirusScan, but all products have similar configuration screens.



If you shut down your computer at night, be sure to configure it to run at a date and time when your computer is usually on.

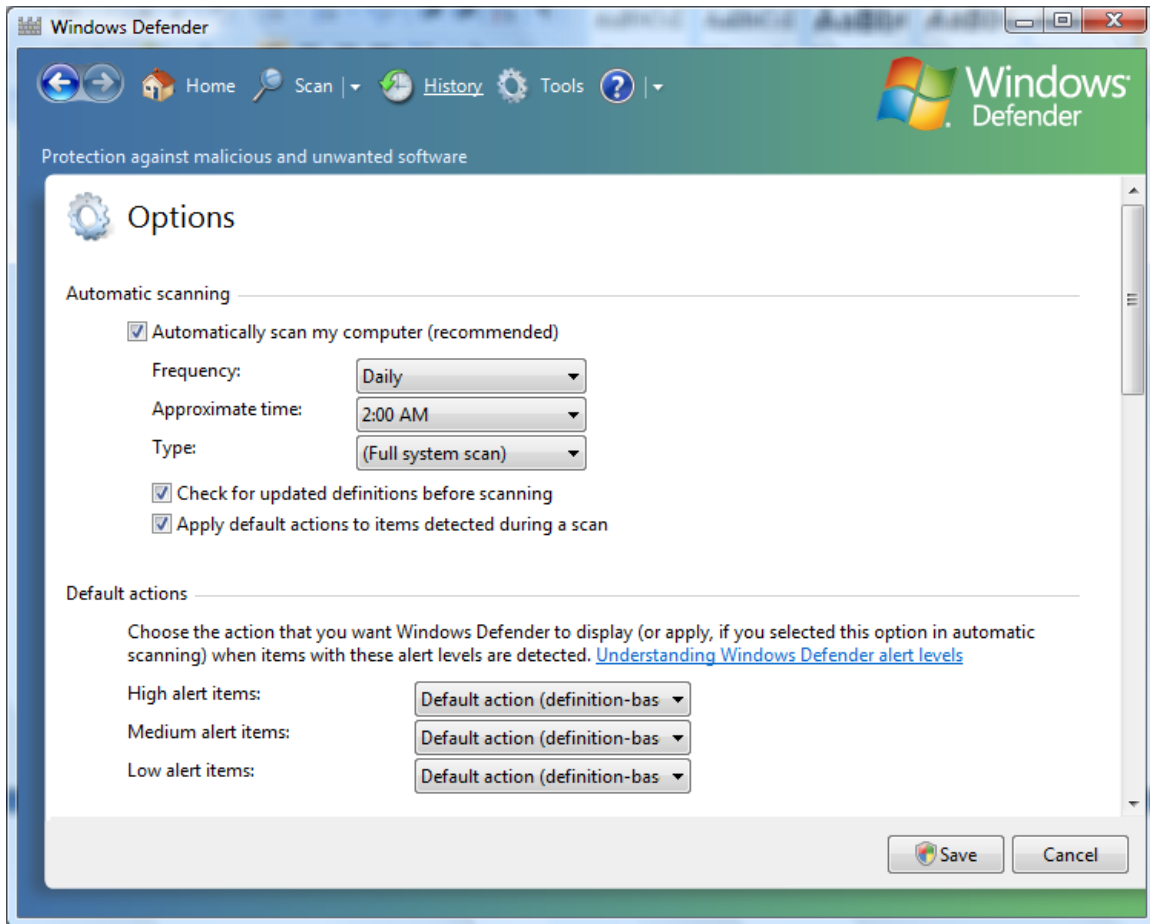
Anti-Adware Software

Unfortunately there is another set of pseudo-malware which anti-virus software does not always stop. This is because some consider it legitimate. Adware is software which is often installed along with legitimate software, and it is used to generate targeted advertising such as pop-ups and pop-unders even when the original software is not in use. It does this by providing information about your surfing and software usage patterns to Internet advertisers. It also may capture and send personal information like your email address to advertisers and make you a target of spam and other unsolicited email.

There are several free software packages which can be used to block adware. A couple of the better ones are [Spybot Search and Destroy](#), and [Adaware](#) and Microsoft's [Windows Defender](#). Once they are installed and configured they will block adware coming into your computer.

I used to use Spybot, but it does require periodic care and feeding. In the recent past I switched to Windows Defender. Once it is installed and configured it is completely hands off as far as operations go.

Like the anti-virus, make sure it is set up to do periodic scans.



Install a Gateway Router

If you do all of the previous steps, you will be in great shape. But to be truly safe, you should go one step further. Install a Cable/DSL router. A Cable/DSL Router is a device which goes between your DSL or Cable modem and your computer. It creates a buffer between your home PC and the Internet. Basically your PC can communicate out, and return traffic can get back in, but any unsolicited inbound traffic will not be allowed to reach your home PC.

To be clear, I am talking about routing devices sold by companies like [Linksys](#), [DLink](#), [US Robotics](#) and [NetGear](#), and others, which provide some firewall capabilities, as well as a switch which will permit you to run multiple computers on your home network. Myself, I am a fan of the [Linksys BEFSR41](#) or its wireless equivalent, the [WRT54G](#), and that is what I usually install for my clients. But all of the major vendors' products provide roughly the same functionality, and they are all easy to install and use. For the most part you just plug them in to your DSL or Cable Modem, plug your PC into one of the switch ports, turn them on and they work. If there is something out of the ordinary about your ISP's setup, most of the products have web-based interfaces, and quick setup wizards. From a users' point of view you cannot even tell they are there, but they are blocking threats from the Internet which will try and infect your PC.

These devices don't cost a whole lot of money either, brand new, you can generally get them for under \$50. If you are prepared to settle for refurbished or end of life components you can get them for a lot less. All of the chain electronics stores carry several varieties of routers, and the online guys carry them as well, often at substantial discounts.

Finale

I am giving away all my secrets. These are the exact steps that I take for my clients. I hope that everyone with a home PC uses this document and puts me out of business. No technology can prevent all possible attacks that may infect your computer, but a few simple steps can substantially reduce the likelihood that your computer will become the victim of an attack and contribute to an already serious problem on the Internet. This is not difficult, and it is not expensive, and I hope that you will take this advice to heart.

Cerberus Security Technology provides security services and wireless network setup and configuration for home users, and small offices in Regina, Saskatchewan, Canada and outlying areas. For more information please email cerberus@whitehats.ca.