

## KEEPING YOUR COMPUTER SAFE WITH FREE DOWNLOADS

Galen Garretson

<http://rascal.galenswebsite.com>

Let's start by talking about what we are protecting our computers from.

- **Malware:** A term used to describe a "malicious software" program. Malware includes things like spyware (for example tracking cookies) which are used to monitor your internet surfing habits. It also includes more sinister items, such as viruses, Trojan horses, worms, and keyloggers.
- **Spyware:** Programs that use your internet connection to send information from your personal computer to other computers, normally without your knowledge or permission. Most often this information is a record of your ongoing browsing habits, downloads, or it could be more personal data like your name and address.

Different strains of spyware perform different functions. Some might also hijack your browser to take you to an unexpected site, replace the Home Page setting in your browser with another site, or serve you personal ads, even when you're offline.

Some programs that have included spyware, like RealPlayer, disclose this information in their terms and conditions as the program is installed, though most users don't read the terms and conditions when they install software, particularly if it is free. KaZaa, a free file sharing program, also includes spyware and there are many others.

But spyware doesn't have to come bundled with another application to find its way on to your computer. In fact most spyware is installed secretly. You might visit a website that pops up a window informing you the site won't display correctly unless you allow it to install a file or plug-in. Answering yes to a prompt that you don't understand can allow spyware to be loaded. You might also agree to load a program that, unbeknownst to you, has spyware included.

- **Viruses:** A virus is a small piece of software that piggybacks on real programs. For example, a virus might attach itself to an Excel spreadsheet. Each time the spreadsheet program runs, the virus runs, too, and it has the chance to reproduce (by attaching to other programs) or wreak havoc.
- **E-mail Viruses:** An e-mail virus travels as an attachment to e-mail messages, and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book. Some e-mail viruses don't even require a double click -- they launch when you view the infected message in the preview pane of your e-mail software.
- **Trojan Horses:** A Trojan horse is simply a computer program. The program claims to do one thing (it may claim to be a game) but instead does damage when you run it (it may even erase your hard disk). Trojan horses have no way to replicate automatically.
- **Worms:** A worm is a small piece of software that uses computer networks and security holes to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well.
- **Keylogger:** A program that logs every keystroke you make and then sends that information, including things like passwords, bank account numbers, and credit card numbers, to whomever is spying on you.
- **Phishing:** Phishing is a type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information.

Now that we know what we're protecting ourselves from, let's take a look at how we protect our computers and do it for **FREE**.

#### **FOUR STEPS TO PROTECTING YOUR COMPUTER**



Keep your firewall turned on. A firewall helps protect your computer from hackers who might try to delete information, crash your computer, or even steal your passwords or credit card numbers. Windows has a built-in firewall. Or, you may use a third party firewall.



Keep your operating system up-to-date. Though we may despise the name Microsoft, each of the security updates and fixes is designed to improve the function and/or security of the Windows operating system.



Install and keep your antivirus software up-to-date. Windows does not have built-in antivirus protection. Once installed **BE SURE** to run a full system scan. Install and run system maintenance software. Run weekly if you spend a lot of time on the internet .



Install and keep your antispysware program up-to-date. Again, run weekly if you spend a lot of time on the internet.

Take a look at the Security Center in Windows XP. Click Start/Control Panel/Security Center. You can check settings for the Windows firewall, automatic updates and whether or not you have antivirus software running.



If necessary, click on "Windows Firewall" and/or "Automatic Updates" at the bottom of the screen to change the settings.

## DOWNLOADING FREE PROGRAMS

There are plenty of free programs available on the internet. Free programs may have limited technical support. One of the main things to be careful of with freeware is that some applications secretly install other potentially malicious programs on your computer when you run the setup file.

**Always** have your antivirus software running and up-to-date when downloading and installing unfamiliar software.

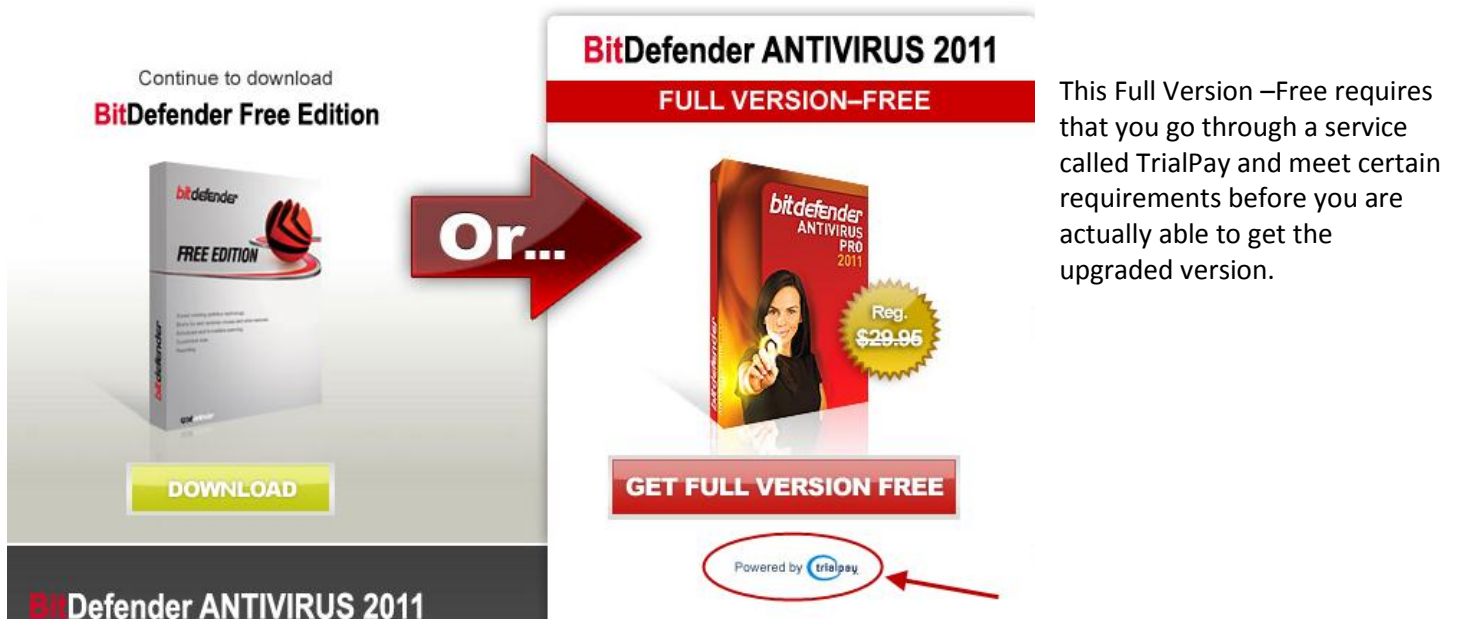
Almost all new computers come with trial versions of antivirus programs. While you are still within the trial period download a free antivirus program, then disconnect your computer from the internet, uninstall your trial version antivirus program, install your new free antivirus software, then connect back to the internet. You're good to go!

**Never** give out any credit card information to get a free program.

You may occasionally be required to provide your email address and even your name or street address in order to use the free software. It is most common to just provide you email address. If you are concerned about the company's use of your email address you will need to read the terms and conditions for use.

There are some sites that allow you to download programs that would otherwise cost you a pretty penny. These sites may charge you an initial "membership" fee or monthly charge which entitles you to then download well known programs for free. Avoid these sites as the software is more often than not pirated.

**Avoid** the "Free" upgrades to the "Professional" versions. You'll end up having to satisfy a number of requirements such as applying for a new credit card, sign up for Netflix, etc. before you get the "Free" upgrade.



Continue to download  
**BitDefender Free Edition**

**Or...**

**BitDefender ANTIVIRUS 2011**  
**FULL VERSION-FREE**

Reg. \$29.96

**GET FULL VERSION FREE**

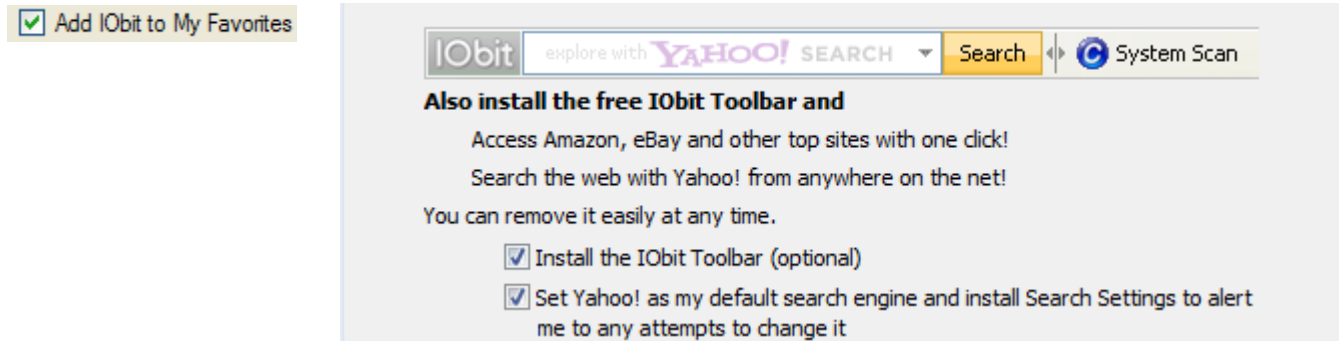
Powered by **trialpay**

This Full Version –Free requires that you go through a service called TrialPay and meet certain requirements before you are actually able to get the upgraded version.

**Always** carefully read the screens you are clicking through to get your free software. Remember "Free Download" does not necessarily equate to "Free Program". Watch for key words like "Advertisement or Ad". You'll know they're trying to sell something.

## **INSTALLING FREE PROGRAMS**

During the installation of your free program, **read** each screen carefully. For example Advanced System Care will add iobit.com to your favorites list, install the IObit Toolbar and change your default search engine if you are not careful.



Take your time with the install process. Avoid clicking on the “Next” button without reading the entire screen.

## **FREE PROGRAMS TO KEEP YOUR COMPUTER SAFE**

Some programs have multiple functions and are listed more than once. The lists below are not all inclusive. Please do your own research to determine which is best suited for your needs and easy for you to use.

### **Antivirus\***

1. Avast Home Edition
2. Avira Antivirus
3. ClamWin Antivirus
4. PC Tools Antivirus Free Edition
5. AVG Free Antivirus
6. Bit Defender
7. Comodo Antivirus + Firewall
8. Windows Security Essentials

### **Firewalls**

1. Comodo Security Suite
2. Netdefender Firewall
3. Outpost Firewall
4. PC Tools Firewall Plus
5. R-Firewall
6. Zone Alarm Personal

### **Spyware Removal**

1. Ad-Aware
2. Malwarebytes
3. Advanced System Care
4. Microsoft Windows Defender
5. Spybot Search and Destroy
6. Super AntiSpyware

### **System Maintenance**

1. Advanced System Care
2. Auslogics Registry Cleaner
3. Auslogics Disk Defrager
4. Ccleaner
5. Defragger
6. Eusing Free Registry Cleaner
7. Smart Defrag
8. Wise Registry Cleaner

\*Want to test your antivirus program? Go to: [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm) and try downloading and/or running the eicar files. These files are not harmful in any way, but should trigger your antivirus program to alert you.