

29 June 2008

By: Stefan Fintea, Software News Editor



Don't let your  
computer become a  
biohazard!

## **Basic Computer Protection In Just A Few Steps - Part I**

### *The programs you should install to ensure PC safety*

Nowadays, keeping your computer clean and secure is not a very easy thing to do. Threats may come in all shapes and sizes; so, if you don't have the necessary programs and knowledge, you might find yourself in a very dangerous situation. The following article is a small tutorial of the basic measures you should take to make sure you and your computer are safe from today's most often encountered Internet threats. And as I have already written in my previous articles on Softpedia, you won't need to buy anything, it's all about freeware software and advice. First of all, you'll have to install a reliable antivirus program, of course. We recommend Avira AntiVir Personal, but you can also give [Avast! Home Edition](#), [BitDefender Free Edition](#), [Gucup Antivirus](#), [ClamWin](#) or [a-squared Free](#) a try. An alternative to this first step is using virus cleaners like [McAfee AVERT Stinger](#), [Microsoft Malicious Software Removal Tool](#), [Kaspersky Free Cleaner](#), [Avira AntiVir Removal Tool](#), [avast! Virus Cleaner](#) or [Multi Virus Cleaner](#), but all these applications are designed to remove only a small percentage of viruses, compared to what an antivirus software will delete and, furthermore, most of them are not updated as often as an antivirus is. Besides these two, antivirus programs have one more, very important advantage: if you use them to scan an infected application before installing it on your computer, not only will they detect viruses, but other types of malicious software like spyware, rootkits or suspicious toolbars. And since I've mentioned spyware, we'll take a look at another way to remove this harmful type of software from your computer. But before we get into that, for those of you who don't know what spyware is or what it may do to your computer, here's a little insight: spyware is a privacy-invasive software that intercepts the way your computer and computer applications are configured without your consent, but it can also collect private information about your Internet surfing habits (the websites you visit or enter most often) and send it to a third-party, again, without your consent. If spyware is already installed on your computer, the safest way to remove it is by installing an antispyware program. Here are your freeware alternatives: [Ad-Aware](#), [Spyware Terminator](#), [SpyBot - Search & Destroy](#), [Microsoft Windows Defender](#), [SUPERAntiSpyware](#). The most important thing you must remember about antispyware and especially antivirus programs is: be sure to keep them up-to-date. Performing an update at least once a day is a must. Another important computer threat, besides viruses and spyware, are rootkits. The general problem with rootkits is that, as opposed to viruses and spyware, they are not so easy to detect or evade. Therefore, in case your security programs do not offer a very reliable protection against them, it's better to run a scan using an application created solely to find and remove rootkits. First of all, let's start with a short definition, which will help you understand why you should take this type of threat very seriously: Rootkits are created to take fundamental control of a PC, once again, without your consent. Allowing Administrator access to your computer is even worse if you realize that, in most cases, rootkits use this type of access to conceal malicious activities performed by trojans, backdoors, sniffers, keyloggers or spam distributors, that will not only put your computer in grave danger, but may affect the security of other people's computers with which you interact. So, here are a few programs to help you detect any rootkits that may be found on your computer: [AVG Anti-Rootkit](#), [RootkitRevealer](#), [F-Secure BlackLight Rootkit Detection](#), [Panda Anti-Rootkit](#), [Trend Micro RootkitBuster](#), [McAfee Rootkit Detective](#), [Sophos Anti-Rootkit](#), [Rootkit Unhooker](#), [RootKit Hook Analyzer](#), [BitDefender RootkitUncover](#) and [DarkSpy Anti-Rootkit](#). These are the programs you should use to detect and remove any malicious software from your computer. In the second part of our tutorial, we'll take a look at some of the ways to prevent the installation of malware components on

any PC, no matter if it's yours, whether it has a security program installed or not.