

Title:

Staying safe on the net

Word Count:

761

Summary:

In conclusions, Malware is a common name for computer worms such as adware, spyware, trojan horses, viruses, browser hijackers, and even dialers. Having a working knowledge of these malicious codes brings awareness and prepares you to be better able to deal with them. Anti virus, firewalls, scan and remove applications are good defenses and are indispensible, but more importantly is a little good old commonsense in the fight against malware.

Keywords:

adware removal spyware, assassin spyware, registry spyware, kazaa spyware, clean spyware, fix spyware, removal software spyware, check spyware

Article Body:

11 Names you must know

When a problem is properly identified, half of the battle is already won. You may not necessarily win the war, but you have a clear view of your path. Staying safe on the net is the same way. When you know what you are dealing with, you have a better strategy on how to deal with it. It is a little like "the devil you know". So, here are 11 things or names you must know to shore up your safety on the net.

1. Malware: A common name for computer worms, malware is short for malicious software. Malware is software script or code written to inflict damage to a computer (hope not yours), a server, or a network of computers or servers. One of the difficult things about malware is that they have the ability to hide deep inside files and can reinstall even after you remove them. Malware has the ability to distabilize your system.
2. Adware: Adware scripts are designed to place advertisements on your computer screen for program owners. These ads can come as pop-ups, pop-unders, and sometimes are embeded in programs. Such pop-ups can show up even when you are not surfing. Adware pop-ups are targetted to the content of the website that you are surfing when online.
3. Spyware: These are another group of malware. As the name implies, these

software scripts are written to spy on you. They work behind the scene to gather information about your internet behavior and even your computer usage. Some of the information relayed to the program owners include search terms that you type into the search box, credit card information, your name, login names and passwords etc. Spyware owners can and do use these information for marketing and may sell your information to other entities.

4. Trojan Horses: A trojan horse is designed to infiltrate your computer without raising an alarm. They often disguise themselves by pretending to be what they are not. They can present themselves as a useful program, may be an important update.

Trojans are written speicifically to cause damage by destroying or changing the data on your hard drive. They can erase an entire hard drive, mine data such as credit card information, personal passwords and logins.

5. Browser hijackers: Hijackers are scripts designed to arrest your browser and browser components. They are known to redirect to pages of their own choosing. More often than not, the pages they redirect to, leave much to be desired.

6. Dialers: Dialers are another type of malware. As the name implies, these scripts dial telephone number through your modem. A malware dialer installs secretly to your computer to dial 900 numbers, attracting charges and large telephone bills for you and fat bank deposits for program owners.

7. Toolbars: Normally, legitimate toolbars such as Yahoo toolbar or Google toolbar provide additional functionality to the browsing experience. Malware toolbars on the contrary, mimick the behavior and funtionality of legitimate toolbars while serving up owner ads and mining data from your computer.

8. Cookies: A cookie is a bit of text file placed in your compute memory that tags you to a particular website. Cookies store information that visited website deem important to them. Cookies are used legitimately by online merchants to facilitate and enhance visitor's online transactions. For example, an incomplete transaction can be cookied for future reference.

9. Viruses: Viruses are computer scripts or program codes written to spread from one file to another or from computer to computer. They are not always written with the intent to cause damage. But intent or not, that is not important. The truth is that viruses cause damage, even though the damage may not be intended.

10. Worms: Worms are viruses designed to propergate by making copies of

themselves on a computer or across a computer network.

11. Commonsenseware: Having talked all about the bad stuff, I believe now is the time to talk about the good stuff. You can call it whatever you want to call it but I call it commonsenseware. This is probably the most important of all the names that we talked about. Why? Because it is your best defense against all the wares and worms- the bad stuff. While deploying software tools such as antivirus, firewalls, and scan and remove applications are a great and indispensable defense against all the bad stuff, a little "commonsenseware" will take you a long way in your battle against malware. Remember, malware has serious privacy implications and should not be taken lightly.

This article is brought to you by <a href="http://www.allspywarefree.com">www.allspywarefree.com</a>