



Web Security and Maintenance Services

McAfee Security



Privacy, Security & Virus Information

Computer Threats to Come

Even if you are unsure of exactly what a computer virus is, you are likely familiar with the concept. In fact, even people who are very computer savvy are unsure, since the concept of the computer virus changes almost daily due to new inventions by hackers.

One of the most recent and dangerous trends in hacker activity is to launch multi-layered attacks, such as those that use a chat message directing the user to a website that contains a Trojan horse.

Another common form of attack is to exploit computer code that can combine a dangerous virus with useful software. This program can then hunt down vulnerabilities in the operating systems and browsers of infected computers. After finding the system's Achilles Heel, the virus will launch an assault.

You may have heard of worms. These are frequently used hacker tool that will burrow into a program and find out where your system or software is vulnerable. The worm will then send this information back to the hacker who can quickly send out a dangerous type of malware, infecting your computer before you've had a chance to protect it. This is all done very quietly, without you or your computer noticing the invasion – the only thing you may see is that your computer has been running a little slower for an hour or so.

Although you may feel safe sitting at your computer in the privacy of your home or office, it is an unfortunate reality that computer anonymity does not exist. Whether a hacker is reaching you as one of many subjects in mass attack, or they have singled you out as a high value victim, your computer can become quickly infected with programs designed specially for data theft.

Do you use peer-to-peer networking programs with browse hosting? P2P programs can be manipulated by hackers to plunder a user network and search for credit reports, chat logs, IDs, and passwords. This information can then be used for fraud or even worse, for blackmail.

All of these threats can be thwarted with the right protection and a little vigilance on your part. You need a safeguard on your files and a way to protect you personal identify information.

Here are some tips:

- **Only use ISPs that are security conscious** and have strong antispam and anti-phishing protection.
- **Do not open attachments from unfamiliar senders**, and use caution when opening attachments from those you know.
- **Do not use your preview pane to open an attachment.** If the site that you are opening is programmed to do so, it could remember you email address and sell it.
- **Never open P2P files with extensions** such as .exe, .scr, .lnk, .bat, .dll, .bin or .cmd.



Web Security and Maintenance Services

McAfee Security



- **Keep your browser updated** by consistently downloading the latest version.
- **Do not set your instant messaging to open automatically.** This can allow unauthorized downloads to take place.
- **Turn off your computer at the end of each session** and be sure to disconnect your modem cable. Scary as it is, a hacker and their viruses can be working on your computer even when you aren't there.