



Overview

This article contains helpful tips on protecting yourself against the infection of viruses and spyware. It will inform you how to detect and remove infections. It is also intended to give you helpful tips on adopting new habits to protect your computer.

In today's world there is a plague of harmful viruses, worms, and spyware spreading across the internet. It is likely that you, or someone you know, has been infected. Computers frequently become infected without the user being aware or knowledgeable.

Having the best virus scanning and removal software alone can no longer be considered sufficient protection. The number and variety of threats are spreading in a variety of different forms. There are two primary means of protecting yourself, and understanding the differences will provide you with a greater level of protection; but you will still need to know that you are still vulnerable to becoming infected.

It is important to understand the differences between viruses and spyware. Some anti-virus software programs will detect and remove spyware, and vice versa. The optimal form of defense is to install and run both anti-virus and anti-spyware software.

Viruses & Worms

Today, viruses and worms primarily spread via email attachments and transmissions, peer-to-peer file sharing, or visiting a malicious website. There are numerous tools and software programs that will help you detect and remove infections, but having even the best tools available can no longer be considered adequate protection. The frequency of new virus creations increases annually. Software companies are finding themselves only being able to address the infections that pose the greatest possible threat of spreading. Therefore, the possibility exists that the virus protection software you are using may not detect an infection on your computer.



An Ounce of Prevention is Worth a Pound of Cure

Some form of virus protection software is to be considered a must have. You should also consider adopting practices and habits that can stop viruses in their tracks. Over the past few years, the level of security with software operating systems has increased substantially. However, even with the highest level of protection, they cannot stop users from being tricked into unknowingly infecting their computers. So, it is best to be aware that many of today's viruses rely heavily on attempting to lure you into their trap.

Email Attachments

Even if you receive an email that was sent from a known and trusted source, do not open it until you confirm that its attachment was intended for you. To achieve this, simply reply to the sender, and confirm that they had intended sending you the attachment.

Web Sites that Request Installs

If you're visiting a website and you encounter a popup window that attempts to convince you that it needs you to install software or a plug-in before you can view the page, ask yourself if the website publisher is a known and reliable source. If you are unfamiliar with the software manufacturer, or if the software that requests to be downloaded does not seem necessary.

Peer-to-Peer File Sharing

Many of today's viruses are spread via peer-to-peer file sharing. A good practice is to always use caution when encountering files posted on these sites.



Spyware

Spyware is a category of malicious software designed to intercept or take partial control of your computer without your consent. The primary intent of spyware is to monitor your computer's activity and operation for the benefit of a third party.

Unlike viruses or worms, spyware typically does not self-replicate. Spyware by design is intended to exploit infected computers for commercial gain. Typical tactics include the delivery of unsolicited popup advertising, theft of personal information (including financial information such as credit card numbers, monitoring of web browsing activity for marketing purposes; or redirecting your internet browsing to advertising sites.

Most spyware programs attempt to deceive users by either by piggybacking on desirable free software, or by tricking users into doing something that installs the software without their realizing it.

Beware of untrusted sites that offer free software, it may be a trick to enticing you into installing malicious software. Also, if you notice that the frequency of popups seems unreasonably high, then you are probably infected.

Useful Links

General Knowledge

[Straight Talk on Mac Security Risks](#)
[Howstufworks.com: How Computer Viruses Work](#)
[Wikipedia: Spyware](#)
[Spamlinks.net: Client Side Spam Filters](#)

Free Anti-Virus Tools

[AVG Anti-Virus Free - Windows / Linux](#)
[AntiVir Personal Edition - Windows](#)
[avast! Home Edition - Windows / Linux](#)
[Comodo AntiVirus - Windows](#)
[ClamWin - Windows](#)

Free Anti-Spyware Tools

[AVG Anti-Spyware Free - Windows / Linux](#)
[Windows Defender - Windows](#)
[Ad-Aware SE Personal Edition for Windows - Windows](#)
[Spybot Search & Destroy - Windows](#)

Paid Subscription Anti-Virus Tools

[McAfee](#)
[Norton](#)
[Trend Micro](#)
[Panda](#)
[AVG](#)