

## Internet security

When a computer connects to a network and begins communicating with others, it is taking a risk. Internet security involves the protection of a computer's internet account and files from intrusion of an unknown user.[1] Basic security measures involve protection by well selected passwords, change of file permissions and back up of computer's data.

Security concerns are in some ways peripheral to normal business working, but serve to highlight just how important it is that business users feel confident when using IT systems. Security will probably always be high on the IT agenda simply because cyber criminals know that a successful attack is very profitable. This means they will always strive to find new ways to circumvent IT security, and users will consequently need to be continually vigilant. Whenever decisions need to be made about how to enhance a system, security will need to be held uppermost among its requirements.

Internet security professionals should be fluent in the four major aspects:

\* Penetration testing \* Intrusion Detection \* Incidence Response \* Legal / Audit Compliance Anti-virus For more details on this topic, see Malware.

Programs can be made to help your computer, but some users can also create programs with intentions of destroying the computers data by being deceptive. Such programs are known as Trojan horses, worms, viruses and spyware.

\* Trojan horses are programs which pretend to do one thing, but in reality snoop out your personal data or damage it. These types conceal their identity or true intentions and are usually quite hard to detect. \* Worms are programs which are able to replicate themselves over a computer network and in turn perform malicious actions. As a result it has the ability to affect other programs on the computer. \* Viruses are programs which are able to log into the personal files on a computer it has affected and as a result, can end up removing all of them. It can have serious side effects on a computers system. \* Malware can be classified as trojans with a limited payload and are often not detected by most antivirus software. They may require the use of other software designed to detect other classes of malware, including spyware.

Software programs such as antivirus software are the most useful in protecting your computer from harmful viruses. These programs are used to detect and eliminate viruses. Anti-virus software can be purchased from any software vendor or downloaded off the internet. Care should be taken in the selection of anti-virus software, as some programs are not very effective in finding and eliminating viruses or malware. Also, when downloading anti-virus software from the Internet, one should be cautioned that some websites say they are providing protection from viruses with their software, but they are really trying to install malware on your computer by disguising it as something else.

Anti-spyware For more details on this topic, see Malware.

There are two major kinds of threats in relation to spyware:

Spyware collects and relays data from the compromised computer to a third-party.

Adware automatically plays, displays, or downloads advertisements. Some types of adware are also spyware and can be classified as privacy-invasive software. Adware often are integrated with other software.

Email Security An significant part of the Internet, E-mail encryption is an important subset of this topic.

Browser choice Almost 70% of the browser market is occupied by Internet Explorer[1]. As a result, malware writers often exploit Internet Explorer. Often malware exploit ActiveX vulnerabilities. Internet Explorer market share is continuously dropping (as of 2009; see list of web browsers for statistics) as users switch to other browsers, most notably Firefox, Opera and Google Chrome.

Buffer overflow attacks For more details on this topic, see Buffer overflow. A buffer overflow is a attack that could be used by a hacker to get full system access through various methods. It is similar to "Brute Forcing" a computer in that it sends an immense attack to the victim computer until it cracks. Most internet security solutions today lack sufficient protection against these types of attacks.

## About the Author

Professional editor working for [Satellite Signal Finder](#) products.