

Local Security is Crucial to Internet Use

by Leon J. Pezok, Sr.

The Internet has become a critical tool in education and entertainment, as well as communications – business and personal. With the internet and the ability to share information comes great risk; exposure to malicious software that steals your information and damages your computer system. This malicious software (MALWARE for short) is categorized as Adware, Spyware, and Viruses.

E-mail as an Infection Route

“Forward this to everyone in your address book” is a common phrase in chain mail over the internet. Well – many malicious types of software will do this for you, without your knowledge or consent. Persons receiving a file from a friend or colleague may promptly open it without considering the circumstances. This is the intent from the programmer of these particular malicious softwares (often called worms); they will masquerade the dangerous attachment to be a funny video, pictures, or some other file from a friend or colleague.

Best Practice: Do not open an attachment or link from an e-mail that you were not expecting – even if you know the person that sent it.

Surfing the Web

Malicious websites take advantage of scripting features and security errors within common internet browsers and operating systems. Dialogue boxes may appear on your computer warning of detected conditions, intending to scare you, and suggesting you install their software to repair the issue. Other sites require you to install their “driver” to view the content, like videos or pictures.

In both these cases, by clicking OK or YES you are expressly allowing these sites to install their potentially malicious software on your computer, regardless of any protective software installed on your computer.

Best Practice: Do not install applications or drivers from web-sites that are not trusted.

Internet File Sharing

Ares, Bearshare, BitTorrent, Frostwire, Limewire, mIRC, and Morpheus are common internet-based file sharing applications. The applications themselves are not malicious software; however their functionality does provide a substantial path for intrusion.

Internet File Sharing allows files to be shared with other people around the world; be it documents, videos, music, applications, or viruses. The tools for sharing do not discriminate or understand the difference between a safe file and something malicious. Malware is frequently made available masquerading as your favorite song or program.

Best Practice: Do not use this type of internet file sharing.

Types of Malicious Software (MALWARE)

Adware	Places advertisements, often as pop-ups, on your computer desktop and internet browser windows, usually pertaining to the content found on your computer or the keywords typed in documents and internet browser.
Spyware	Tracks your internet and computer use with the intention of reporting information back to its author or other party, possibly including programs, keywords, account numbers and passwords.
Virus	Typically destructive, intending to disable your computer or programs. Virus are sometimes tied to other malware. Many virus automatically spread via e-mail or a network.

Malicious softwares are often classified by their infection mechanism or payload type:

Rootkit	Infect the disk boot sector or core operating system files. These are the most difficult to remove and usually will critically damage the operating system.
Trojan	Installs malicious software, posing to provide some other purpose; commonly creating a backdoor into a system.
Dialer	Use the modem to redirect internet traffic or connect to pay services without the computer operator’s consent – typically distributed by Trojans.
Downloader	Often part of web scripts or startup routines, these are used to download virus and other malicious content without detection.
Worm	Self propagating program spreads from computer to computer across networks, particularly in peer-to-peer environments.