

## Keep the Viruses Out!

By Ken Meyer, Solbrekk Sr. Network Engineer

Viruses are out on the internet and are trying to attack your users and network. One of our network engineers gave a great analogy the other day. He said, "Having Antivirus Software is like having a lock on your door. You feel secure when it is locked, but someone could still kick the door in."



Over the last month virus attacks have again been in the news, and we have seen an increase in the number of virus attacks on customer networks. We feel this is due in large part to the companies' user's internet activities while at work. Our network engineer team has compiled a list of what you can do to mitigate your exposure to these attacks.

1. Keep your computers up to date with Microsoft updates. Having Windows updates downloaded and installed on a regular schedule helps by installing fixes to holes or software flaws that have been found. These flaws are what the attackers are looking for when they write a virus.
2. Keep your antivirus up to date with the current definitions that are supplied by your antivirus company. These should be programmed to get the new definitions every day, and need to be checked to verify all is working correctly.
3. Limit access to certain websites to prevent attacks on your computer. They can be blocked at the firewall by products such as WatchGuard WebBlocker.
4. Check on the feasibility of upgrading to a more secure operating system, such as Vista, and a more secure Internet Browser, such as Internet Explorer 7 or Mozilla.
5. Train your users on how to navigate the internet safely. This starts with them knowing the basics of what could happen if they click on the wrong link, click on a pop-up window, or just general clicking out of a need to click.

The definitions below are from Wikipedia and are most of the words used to describe unwanted software attacks. I would like to stress the importance of your internet users becoming familiar with the terms and how they could affect their computer, because it will improve your network security. All the infections we have seen lately have come from a click on a web site that was crafted to look like something it was not!

**Phishing** is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites (YouTube, Facebook, MySpace, Windows Live Messenger), auction sites (eBay), online banks (Wells Fargo, Bank of America, Chase), online payment processors (PayPal), or IT Administrators (Yahoo, ISPs, corporate) are commonly used to lure the unsuspecting. Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Even when using server authentication it requires skill to detect that the website is fake. Phishing is an example of social engineering techniques used to fool users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

**Adware** or advertising-supported software is any software package which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used. Some types of adware are also spyware and can be classified as privacy-invasive software.

**A computer virus** is a computer program that can copy itself and infect a computer without the permission or knowledge of the user. The term "virus" is also commonly but erroneously used to refer to other types of malware, adware and spyware programs that do not have the reproductive ability. A true virus can only spread from one computer to another (in some form of executable code) when its host is taken to the target computer; for instance because a user sent it over a network or the Internet, or carried it on a removable medium such as a floppy disk, CD, or USB drive. Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by another computer.

**A computer worm** is a self-replicating computer program. It uses a network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

**Malware**, a portmanteau from the words malicious and software, is software designed to infiltrate or damage a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. The term "computer virus" is sometimes used as a catch-all phrase to include all types of malware, including true viruses.

**Spam** is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, Online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, and file sharing network spam.

**Spyware** is computer software that is installed surreptitiously on a personal computer to intercept or take partial control over the user's interaction with the computer, without the user's informed consent.

**Trojan horse**, also known as a trojan, is a form of malware that appears to perform a desirable function but in fact performs undisclosed malicious functions that allow unauthorized access to the host machine. As such, a computer worm or virus may also be classed as a Trojan horse if they display these characteristics.

**Keystroke logging** (often called keylogging) is a method of capturing and recording user keystrokes. The technique and name came from before the era of the graphical user interface; loggers nowadays would expect to capture mouse operations and screenshots. Keylogging can be useful to determine sources of errors in computer systems, to study how users interact and access with systems, and is sometimes used to measure employee productivity on certain clerical tasks. Such systems are also highly useful for both law enforcement and law-breaking—for instance, providing a means to obtain passwords or encryption keys and thus bypassing other security measures. Keyloggers are widely available on the Internet.