



# Security Jargon

**Adware** – Program that displays advertising through pop-up windows while you are surfing the web.

**AntiVirus** – AntiVirus software scans your computer (files and memory) for certain patterns that indicate an infection. The patterns it scans for are the signatures, or definitions, of known viruses. Since virus writers are continually releasing new viruses, it is important that you keep your antivirus definitions updated.

**Backdoor** – A backdoor is an undocumented or hidden opening that allows access to a system. Some viruses and trojans install backdoors.

**Blended threat** – A blended threat has combined characteristics of two or more viruses, worms and/or trojans. By using multiple methods and techniques, they can spread rapidly and cause more damage.

**Bot** – Short for robot. The term describes little programs designed to perform automated tasks. Bots may also be used in a coordinated attack on network computers.

**Exploit** – A program that takes advantage of a security hole in a computer program.

**Firewall** – Software that monitors incoming and outgoing internet traffic to your computer and checks for suspicious patterns. A firewall may alert you to spyware or a Trojan installed on your computer.

**Identify Theft** – Identity theft occurs when someone uses your personal information without your knowledge or consent to commit a crime, such as fraud or theft.

**Intrusion Detection** –

**Keylogger** – A program that records anything typed on the keyboard.

**Malware** – Malware is the term used for malicious software. It typically refers to viruses, worms, and trojans.

**Password sniffer** – A program that seeks out passwords on your computer, then sends them to a hacker.

**Personal Firewall** – A personal firewall is a software application used to protect a single Internet-connected computer from intruders. Often compared to anti-virus applications, personal firewalls work in the background at the device (link layer) level to protect the integrity of the system from malicious computer code by controlling Internet connections to and from a user's computer, filtering inbound and outbound traffic, and alerting the user to attempted intrusions.

**Pharming** – Pharming is simply a new name for a relatively old concept: domain spoofing. Rather than spamming you with email requests, pharmers work quietly in the background, “poisoning” your local DNS server by redirecting your web request somewhere else. As far as your browser's concerned, you're connected to the right site. The danger here is that you no longer have to click an email link to hand over your personal information to identity thieves.

**Phishing** – Phishing is a form of social engineering. Phishing attacks use e-mail or malicious web sites to solicit personal information. Attackers may send e-mail seemingly from a reputable credit card company or financial institution that requests account information, often suggesting there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

**Sniffer** – A program or device used to monitor packets as they cross the network.

**Social Engineering** – Social Engineering is the term used to describe how an attacker uses social skills to obtain or gather information.

**Spam** – Spam is the term used for unsolicited email.

**Spyware** – A program that surreptitiously monitors your actions. While they are sometimes sinister, such as a remote control program used by a hacker, software companies have been known to use spyware to gather data about customers. Spyware is a program or technology that aids in gathering information about a person or organization, often without their knowledge, and includes programs like hijackers and keyloggers. Spyware is easy to install but often difficult to remove without downloading specialized anti-spyware programs. You may have unknowingly installed spyware or adware when you download programs from the internet.

**Trojan** – A program that disguises itself as another program. These programs are hidden and usually cause an unwanted effect, such as installing a back door in your system that can be used by hackers. They differ from viruses and worms because they typically are not designed to replicate. A Trojan might look like a game, but instead it steals your personal information.

**Updates** – Antivirus and other security tools need frequent and detailed updates to work effectively; they can't block a piece of malware that they haven't seen before. Consequently, these programs always suffer a period of vulnerability between the time a new worm hits and the time the antivirus definitions to block or clean the infection are available.

**Virus** – A self-replicating computer program that can be destructive to files or other programs. Requires human intervention to spread.

**Virus signature** – The “fingerprint” of a virus, which antivirus programs use to identify and isolate viruses. Users should regularly update their antivirus programs online by downloading the latest virus signatures, so they're protected against new viruses.

**Worm** – Worms spread without any human intervention typically by exploiting a flaw in popular software. Once activated, they will self-propagate through the network.