

Patches/Software Patches—Software updates that fix a particular problem or vulnerability within a program.

Pharming—Similar in nature to email phishing, pharming seeks to obtain personal or private information through domain spoofing.

Phishing—A scam that involves Internet fraudsters who send spam or pop-up messages to lure personal information (credit card and bank account numbers, Social Security numbers, passwords, etc.) from unsuspecting victims.

Pop-up Messages or Ads—Unsolicited advertising that appears as its own browser window.

Secure Socket Layer (SSL)—A protocol used to transmit sensitive data, like credit card information, securely by way of the Internet.

Sock Puppet—A secret alias used by a member of an Internet community, but not acknowledged by that person.

Spam—Unsolicited commercial email, often sent in bulk.

Spam Zombies (a.k.a. Zombies)—Home computers that have been taken over by spammers who then use them to send spam in a way that hides the true origin.

Spammer—Someone who sends unsolicited commercial email, often in bulk.

Spoofing—Forging an email header or Web addresses to make it appear as if the message or website came from somewhere or someone other than the actual source.

Spyware—A software program that may be installed on your computer without your consent to monitor your use, send pop-up ads, redirect your computer to certain websites, or record keystrokes, which could lead to identity theft.

Trojans—Programs that, when installed on your computer, enable unauthorized people to access it and sometimes to send spam from it.

Virus—A program that can sneak onto your computer, often through an email attachment, and then make copies of itself, quickly using up all available memory.

Worm—A program that reproduces itself over a network and can use up your computer's resources and possibly shut your system down.

Excerpts from "Learning the Language,"
The Washington Times, April 23, 2007.

Online Speak

Technology Terminology for the Security Savvy Web User



Prepared by

Chris Bednar and Kevin Sol
Advanced Multimedia Productions
Luther Jackson Middle School

You don't have to know everything about a computer to use the Internet, but you will be much more web literate if you are familiar with technology vocabulary. Here are some technology terms specifically for those of you who want to be more security savvy when you are online.

Adware—Software that often comes with free downloads. Some adware displays ads on your computer, while some monitors your computer use and displays targeted ads based on your use.

Anti-Virus Software—Protects your computer from viruses that can destroy your data, slow your computer's performance, causes a crash, or even allow spammers to send e-mail through your account.

Blocking Software—Computer programs that filter content from the internet, blocking access to websites or content-based on specified criteria.

Browser Hijacker—A common spyware program that changes your Web browser's home page automatically, even if you change it back.

CAN-Spam Act—A law that prohibits senders of unsolicited commercial email from using false or misleading header information or deceptive subject lines.

Cookies—A small text file that a website can place on your computer's hard drive to collect information about your activities on the site or to allow other capabilities on the site.

Drive-by Downloads—Software that installs on your computer without your knowledge when you visit certain websites. To avoid drive-by downloads, make sure to update your operating system and Web browser regularly.

End User Licensing Agreement—A provider's legal terms. You, as the "end user," may be required to "click" to accept before you can download software.

Exposure—When sensitive data is released to someone without authorization.

Filter—Software that screens information on the internet, classifies its content, and allows the user to block certain kinds of content.

File Sharing—Accessing files on one computer from another computer.

Firewall—Hardware or software that helps keep hackers from using your computer to send out your personal information without your permission. Firewalls watch for outside attempts to access your system and block communications to and from sources you don't permit.

Hacker—Someone who uses the Internet to access computers without permission.

Hidden Dialers—Programs that you may unknowingly download that can use your computer to silently dial expensive phone calls, which later show up on your phone bill.

Monitoring Software—Programs that allow a parent or caregiver to monitor the websites a child visits or email messages he or she reads, without blocking access.

Online Profiling—Compiling information about consumers' preferences and interests by tracking their online movements and actions to create targeted ads.

Opt-in—When a user explicitly permits a website to collect, use, or share his or her information.

Opt-out—When a user expressly requests that his or her information not be collected, used and/or shared. Sometimes a user's failure to "opt-out" is interpreted as "opting-in."

Parental Controls—Tools that allow parents to prevent their children from accessing certain Internet content they might find inappropriate.