

Glossary of Online Security Terms

Antivirus Software - A computer software program that detects and responds to viruses and worms, blocking access to infected files and performing frequent updates.

Browser - A computer software program that is used to view and interact with Internet material on the World Wide Web. Netscape Navigator and Microsoft Internet Explorer are two of the most popular browsers.

Dumpster Diving - Thieves rummage through trash looking for bills or other paper that includes your personal information.

Encryption - A process in which data is scrambled before it is transferred so that it cannot be read by unauthorized parties.

Enhanced Security Login - Provides security at login, no matter what computer you sign in from, using additional end user authentication that helps to protect against online fraud.

Firewall - A gateway supported by hardware or software that limits access between computer networks. Firewalls can protect your home computer from hackers and your family from web sites that may contain offensive material.

Hacker - A person who tries to gain unauthorized access to a computer system. Hackers are known to modify computer programs and security systems that protect home and office computers.

Keystroke Capture - A spyware program or device that records what users type on their computer. Also referred to as Keystroke Logger.

Malware - Also known as 'malicious software', malware is designed to harm, attack or take unauthorized control over a computer system. See Virus, Trojan and Worm.

Opt-In - Permission granted to a business or organization to use your email address for promotional or marketing purposes, or to rent your email address to another organization.

Opt-Out - The opposite of Opt-In- not granting permission for a business or organization to use your email address for promotional or marketing purposes, or to rent your email address to another organization.

Patch - A new software release created to update a computer software program. Updates may include security, performance, or usability enhancements.

Pharming - Pharming takes place when users type in a valid URL and you are illegally redirected to a web site that is not legitimate in order to capture personal information through the internet such as credit card numbers, bank account information, Social Security number and other sensitive information.

Phishing - The process of seeking to obtain personal information illegally through email or pop-up messages in order to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, or other sensitive information.

Pop-Up Ads - A form of web advertising that appears as a "pop-up" on a computer screen, they are intended to increase web traffic or capture email addresses. However, sometimes popup ads are designed with malicious intent like when they appear as a request for personal information from a financial institution.

Privacy Policy - A standard policy included on most corporate websites that explains how personal information collected about visitors to a company's site is handled.

Service Pack - A software program that updates, fixes and/or enhances a software program found on your computer, typically delivered in the form of a single, installable package.

Skimming - When an unauthorized second copy of a credit or debit card is taken by an employee at a store by using a storage device that copies the details held within the card's magnetic strip.

Spam - Unsolicited bulk electronic "junk" messages sent to huge numbers of people via email, instant messaging, Usenet newsgroups, and more.

Spoofing - A form of phishing, a way for cyber criminals to send emails that look legitimate, but are not, to falsely represent a legitimate company or organization. The false email from phishing will include a phony link to what closely resembles a legitimate website address. Once click upon, the victim is asked to provide personal information which is then forwarded to criminals.

Spyware - Loaded onto your computer unbeknownst to you, spyware is a type of program that watches what users do and forwards information to hackers over the Internet.

Trojan Horse - A malicious program that is disguised or embedded within legitimate software program that, when activated, unwittingly allows hackers to gain unauthorized access to the computer.

Virus - A self-replicating computer program, loaded on to your computer without your knowledge that spreads by making copies of itself and clogging up your computer's memory.

Worm - Similar to a computer virus, a worm attaches itself to, and becomes part of, another executable program. Able to self-propagate, worms generally harm the network and consume bandwidth.