

## IT Security Glossary

**Adware** -- Software that serves up ads based on your previous searches. Free software can come with adware that pays for its use. Generally adware differs from spyware in that it notifies the user of how the program works and its intent.

**Antispyware** -- Software that removes or blocks spyware.

**Antivirus** -- Antivirus software protects your computer against malware. It scans the hard drive for viruses and removes them. It also looks for aberrant behavior in programs that can signal an infection.

**Authentication** -- The process of verifying identity.

**Bot** -- Short for robot. A computer program that performs automated tasks. Can be used maliciously to scan for passwords, search browsing history, capture keystrokes, send spam and report information to a third party across the Internet.

**Dual-facto rules** -- Requires banks to implement some form of additional password in addition to the standard username and password combination. It's often accomplished by presenting a picture or something else that the consumer chooses in addition to their password in order to recognize the bank.

**Firewall** -- A security system that protects individual computers or networks from intruders. Firewalls can be either hardware or software or a combination of the two.

**Identity cloning** -- When a fraudster lives as the victim, getting married, working, paying taxes and possibly committing crimes.

**Identity fraud** -- Occurs when a transaction happens in a person's name without their knowledge.

**Identity theft** -- An umbrella term used for everything from a one-time fraudulent credit card transaction to identity cloning. Technically refers only to situations when identifying information is taken and used for fraudulent purposes.

**Image spam** -- A spam e-mail whose content contains text embedded inside an image.

**Malware** -- A general term for malicious software. Examples include viruses, Trojan horses, spyware and worms.

**Nigerian scam** -- Also called the 419 after the code in Nigerian criminal law, the Nigerian scam is an advance fee scam in which unsolicited e-mails claim to offer large sums of money in return for helping someone in trouble.

**Phishing** -- A scam perpetrated via e-mail wherein the scammer spoofs a well-known brand or entity, for instance a big national bank or the IRS. The e-mails contain a link to a Web page which purports to be the legitimate site and asks for personal information.

**Plug-in** -- Software or hardware that is used to modify or add to an existing program. Flash and QuickTime are both plug-ins for Web browsers, for example.

**Red flag rules** -- Regulations included in the Fair Credit Reporting Act requiring

financial institutions to institute a program to identify red flags signaling possible ID theft or fraud.

**Social Security number tumbling** -- Taking a valid Social Security number and changing it slightly. For instance, 123-45-6789 is changed to 123-45-6790. This is a technique used in a new type of identity fraud called synthetic identity theft.

**Spam** -- The transmission of unsolicited electronic messages in bulk. Usually used in reference to junk e-mail.

**Spim** -- Spam over instant messaging.

**Spit** -- Spam over Internet telephony, or VoIP spam.

**Spoofing** -- Mimicking a legitimate e-mail address or Web site for the intent of fraud. Scammers spoof the e-mail address, logos and design of legitimate businesses in e-mail scams trying to steal account numbers or identifying information by copying the look of the business. Links in the e-mail send victims to the spoofed Web site.

**Spyware** -- Software installed either unbeknownst to the user, or without revealing the intent of the program. Spyware collects data on the user and shares it with the parent company. More annoyingly, spyware programs can also take control of the computer, reroute the Web browser to pages to install more programs and change settings.

**Synthetic identity fraud** -- A type of ID fraud in which thieves literally create new identities either by combining real and fake identifying information to establish new accounts with fictional identities or create the new identity from totally fake information. In typical synthetic fraud, a fraudster uses a real Social Security number and combines it with a name other than the one associated with that number. The combination often doesn't hit the consumer's credit report.

**Trojan horse**-- A software program, usually downloaded, which purports to do one thing but actually damages other programs. Trojan horses can arrive as attachments in e-mails, IMs or by download.

**Virus** -- A program which hides inside another program. When that program is run, the virus also runs and can copy itself into other programs.

**Vishing** -- A voice phishing scam that involves getting consumers to dial into a voicemail system that records personal information. Can involve first a spoofed e-mail that appears to come from a major company or banking institution that directs the recipient to call a number, or a cold call attempting to retrieve sensitive information. Cold calls may be live or automated. Like phishing scams, the message usually sounds urgent and stresses the existence of a problem with the recipient's account.

**Worm** -- A computer virus capable of copying itself without needing a host program.