

Definitions

Administrator	a user with access to all files, programs and security functions on the computer, and who is responsible for the administration of the computer.
Adware	applications that can launch pop-up ads on the computer. Freeware and shareware applications frequently install adware during their own installation procedures.
Anti-virus	application that protects the computer by inspecting data (files, emails, network input) for viruses and by isolating infected data.
DMZ	a special network used to isolate publicly accessible computers from the rest of the corporate network.
Encryption	protection methodology used to make data unreadable without the relevant key.
Firewall	device, software or hardware, allowing the user control over the traffic coming into, and leaving, the user's computer. Note that some firewalls provide protection only over incoming traffic.
Hub	network device for sharing a single network connection between multiple computers.
Malware	software that performs tasks other than those advertised; frequently those unadvertised tasks are malicious.
Modem	device that allows two computers to talk to each other indirectly over varying network types.
Phishing	email sent in the hopes of collecting private information for the purposes of committing fraud.
PKI	an encryption methodology that enables secure authentication and communication.
Router	network device used to direct traffic between networks.
Social Engineering	the art of influencing people to do what you want, frequently without them realizing the gravity of what they have done (for example, convincing a user to give you his password).
Service Pack	a major collection of updates.

SPAM	unsolicited commercial email.
Spyware	software that collects information from a computer and sends it to another computer without the user's knowledge or approval.
Strong Password	password that is difficult to guess. Typically consists of more than 8 characters including a mix of uppercase, lowercase, digits, and other characters.
Switch	network device that allows several devices to talk to each other.
Trojan	a program that, when installed on a computer, gives a remote user some measure of control over that computer, typically without the approval of the computer's owner.
Updates	software that repairs problems or security weaknesses in applications or the operating system.
Virus	a program that spreads from computer to computer - without the knowledge or approval of the users - as a result of users' legitimate activities and which may perform harmful activities on the infected computers.
VoIP	allows a regular phone, using an adaptor, to make calls over the internet.
VPN	methodology for creating a private secure network using the public network.
Weak Password	password that is easy for a computer to guess. Typically a short simple word or number (such as a date).
WiFi	common name for wireless networking.
Worm	a program that spreads from computer to computer without the knowledge or approval of the users as a result of normal operating system activities (no user activity is required). The worm may perform malicious activities on infected computers.
Zombie	a form of malware controlled by a third party for malicious activities such as denial of service attacks.