

Special Holiday Edition: OUCH Glossary

1. *The Internet and the World Wide Web* – 2. *Getting Connected* –
3. *Your Computer* – 4. *Malware* – 5. *Bad Guys*

1. The Internet & the WWW

The Internet is a vast collection of thousands of interconnected networks across the world, all of which use the TCP/IP protocol (transmission control protocol/Internet protocol). This common protocol acts as a global electronic language, allowing dissimilar computers to talk with each other easily. The Internet is used for many types of communication--text, graphics, email, audio, video, telephony, and television--by means of thousands of software applications or programs, the most popular and widely used of which is the Web browser. The Internet is the network. The World Wide Web is a network application.

2. Getting Connected

BROADBAND: Short for "broad bandwidth". Any of several kinds of two-way, high-speed network connection, such as Cable Internet and DSL (Digital Subscriber Line), which can carry several channels of voice, data, and video simultaneously (ex. TV + Internet and telephone calls + Internet respectively).

BANDWIDTH: The amount of information that can be sent over a network connection in a given period of time. Bandwidth is usually measured in bits per second (bps), kilobits per second (kbps), or megabits per second (Mbps).

DSL: - Digital Subscriber Line. One of the most common ways of bringing several channels of high-bandwidth information (telephone calls + Internet) to homes and small businesses over ordinary copper telephone lines. Its ancestor, the dialup modem, had a maximum speed (or bandwidth) of 56 kilobits/second. DSL, at 6 Megabits/second, can move information up to 100 times faster.

CABLE OR CABLE INTERNET: Another common way of bringing several channels of high-bandwidth information (cable TV + Internet) to homes over local cable TV lines. Its speed or bandwidth ranges from 1.5 to 6 Megabits/second. Cable Internet has proven very popular with Internet gamers.

ETHERNET: Ethernet is a local area network (LAN) standard for hardware, communication, and cabling. The smallest network consists of two computers, or one computer and a network printer. When you connect two LANs together, you get a WAN (wide area network). When all the WANs are connected together, you have the Internet.

ROUTER: A device that finds the best route between any two networks. Routers are to networks what crossing guards are to busy streets, and Traveler's Aid booths are to airports. Routers keep traffic flowing efficiently as networks

get larger and more complex. Small home networks can work OK without a router because they generally contain a small number of devices.

SWITCHES AND HUBS: A switch is a networking device that connects computers or networks together. A switch is “smart.” It learns and memorizes where devices are located on a network (like where the printer is) and this speeds up sending information to the device. A hub connects things together too, but it is “dumb.” That means every time you send a job to the printer on a hub, the hub has to hunt around and talk with every device on the network until it finds the printer.

IP ADDRESS: Each computer or other device connected to the Internet has a unique number known as an Internet Protocol address. The IP address usually takes the form of four numbers separated by dots, for example: 122.132.167.251. Non-IT people refer to IP addresses, especially on the Web, by their easier-to-remember alias (a.k.a. Domain Name or URL), like <http://www.amazon.com>.

NAT: Network Address Translation is primarily a security measure that translates a public IP address into one or more private IP addresses that are used within a private network, such as your home network. NAT helps protect your computer by hiding its IP address from hackers and crackers on the Internet, providing some security through obscurity.

Wi-Fi: Short for “Wireless Fidelity,” a.k.a. “radio networking.” A kind of local area network (LAN) that communicates via radio waves rather than wires. (See “Ethernet.”) Wi-Fi operates at various frequencies and bandwidths. The current standard is 56 Mbps.

EVDO: or Evolution Data Only/ Evolution Data Optimized is an emerging technology that provides wireless broadband Internet service directly to your laptop. Unlike Wi-Fi, EVDO works in large areas, like an entire city. Based on cell phone technology, EVDO is currently provided in many metropolitan US cities by Verizon and Sprint. Bandwidth will vary, but at its best, you can expect 300-400 kbps, pleasantly fast for Web browsing.

FIREWALL: A software or hardware device that prevents outsiders from accessing a computer or network. If you have DSL or Cable Internet at home, chances are good that the box (or modem) supplied by your service provider acts a hardware firewall.

3. Your Computer

WINDOWS COMPUTER

ADMINISTRATOR: One of the three types of users created when you install Windows 2000 or XP. An administrative user has complete privileges on a system, including the ability to change passwords, access files created by any user, install and uninstall all software, add printers and other peripheral devices, change settings, create and delete user accounts, etc. The other types of default user accounts are Windows Limited User and Guest. (See also Windows Limited User)

WINDOWS LIMITED USER: Another type of user created when you install Windows 2000 or XP. A limited user is permitted to make only certain kinds of changes to a system. A common downside is that Limited Users may be unable to launch some software

applications or install new software (See also Windows Computer Administrator).

WINDOWS GUEST USER: The third type of user created when you install Windows 2000 or XP. A guest has almost no privileges on a computer other than logging in and running applications specifically allowed by the Windows Computer Administrator.

LOCKING DOWN A WINDOWS SYSTEM:

The Windows 2000 and XP operating systems allow a Windows Administrator to set permissions-restricted access to critical files (such as the Registry) and to the file system, preventing users from installing, modifying, or removing software applications without the knowledge or permission of other users. In corporate settings, it is not uncommon to find Windows systems that have been locked down in this way.

SPOOLING: When printing a document, the whole thing does not go directly to the printer all at once. Instead, the document is spooled — saved in a temporary file — and then sent when the printer is ready to process the job. If the printer is not ready, i.e., busy with another job, powered off, out of paper, etc., your job will be saved until the printer is ready.

PASSWORDS: A series of characters that enables you to access a file, computer or program. Passwords are a very common and basic security tool and can be weak or strong. A weak password is one that could be guessed easily, thus allowing unauthorized or unwanted access. Using a weak password contributes to identity theft and other computer crimes.

PASSWORD CACHING: Having your computer “memorize” a password so you no longer have to type it in. While

convenient, this creates an automatic and serious security problem because a password is no longer required to gain access to a file, computer, program or website.

DATA FILES: Files created by a computer user within an application, such as a word processing document, a spreadsheet, a database file, a graphic, a chart, etc. Some people refer to all data files as “documents.”

LOGS AND LOGGING: Logging refers to the feature in operating systems and software applications that compiles records of events (logs) that occur on your computer. Information stored in Application and System logs can help with troubleshooting problems, like a program quitting unexpectedly or a system crash. Security log information can tell you when and how someone tried to gain unauthorized access to your computer either at the keyboard or over the network.

4. Malware

VIRUS: A self-replicating program, often written to cause damage or mischief, which inserts itself into a software application without leaving any obvious sign of its presence. Your computer can pick up a virus when you copy an apparently normal file from a diskette, CD or memory stick, when you open an infected email attachment, or when you download an infected file from the Internet.

WORM: Like a virus, a worm is a self-replicating program, often written to cause damage or mischief. Unlike a virus, a worm is self-contained and does not need to become part of another program to propagate itself. Instead a worm infects the operating system, acts

like a program in its own right, and spreads via the network.

TROJAN HORSE: A malicious program that appears harmless, but conceals other malware that can compromise the security, data, and proper functioning of your computer. The damage can range from printing silly messages on your screen, to sending sensitive information out to a Bad Guy, or even trashing your entire hard drive. Trojan horses spread via the network and are sometimes referred to as “network viruses.”

SPYWARE AND ADWARE: Spyware is a general term for a program that installs itself on your computer surreptitiously and monitors and reports your actions to the maker of the spyware. While spyware sometimes has nasty and even sinister purposes, like stealing personal information or allowing your computer to be controlled remotely by a hacker, software companies have been known to use adware to gather data about customers, and their browsing and purchasing habits, as a routine business practice. Adware is often bundled subtly along with free downloadable software.

BACKDOOR: A piece of software that bypasses normal authentication methods, such as a username and a password, and allows a Bad Guy access to your computer without your knowledge. A backdoor may take the form of an installed program or an illegitimate modification to a legitimate program. Trojan horses are a common kind of backdoor threat.

BLENDED THREATS: An attack on your computer from the network specially crafted to maximize the severity of damage and speed of contagion by combining several kinds of malware. This could be, for example, a blend of a virus and a worm that also takes

advantage of vulnerabilities in your computer and the network to which it is connected, or virus sent to you as an email attachment, along with a Trojan horse embedded in a HTML file that is part of the email message.

KEYLOGGERS: Spyware that monitors your keystrokes surreptitiously and sends the information back to a Bad Guy. Keyloggers spread most commonly by email attachments or in a drive-by download when you visit a rigged website. They are often used to gather email and online banking usernames and passwords as a prelude to identity theft.

5. Bad Guys

HACKERS AND CRACKERS: Historically, “hacker” was not derogatory, but simply a slang term for a computer enthusiast, or a programmer who lacked formal training. In current popular speech, hacker and cracker mean the same thing: someone who breaks into systems, destroys data, steals copyrighted software, and performs other destructive or illegal acts with computers and networks.

SCRIPT KIDDIE (a.k.a. script bunny or script kitty): A derogatory term for inexperienced crackers who use scripts and programs developed by others to compromise computers and launch attacks on whole computer systems (see also DoS). In general, script kiddies do not have the ability or experience to write malicious programs on their own.

DoS: Short for denial-of-service attack. An automated attack designed to bring a network to its knees by flooding it with useless traffic or to overwhelm a computer so it can no longer respond to legitimate requests.

VULNERABILITIES AND EXPLOITS: Your system is said to be vulnerable when a weakness in its hardware or software design makes it possible to compromise the security and smooth functioning of your computer. An exploit is a software application or program that takes advantage of a vulnerability (a.k.a. bug, glitch, or flaw) in order to attack your system.

SNIFFING: A computer, deliberately placed in “promiscuous mode,” and connected to a network by an attacker so that it sniffs or listens in on everything you are doing on the network and captures all of your data traveling on that network. Sniffers, which can operate on both wired and wireless networks, provide an easy way to steal clear-text passwords as well as other information that can be used to gain unauthorized access.

SPOOFING: A generic term covering a range of computer network attacks in which a person or program you shouldn’t trust masquerades as a person or program you do trust. In email spoofing, the attacker forges an email address in order to hide its origin and make you believe that the message comes from a legitimate source. In IP spoofing, the Bad Guy’s device attempts to impersonate another system illicitly by using its IP address. Webpage spoofing, a common phishing ploy, is the act of creating a phony website that looks like the real one with the intention of misleading you into believing that the

website is the work of another person or organization.

PHISHING: A widespread form of Internet fraud that aims to steal valuable information such as credit cards, social security numbers, user IDs, and passwords. The most common ploy consists in luring unsuspecting persons to visit phony websites by means of an email. Recipients visit the bogus, look-alike website and enter personal information which is then used to defraud them.

IDENTITY THEFT: The fastest growing crime in America. In addition to traditional methods of obtaining personal information fraudulently, such as dumpster diving, mail theft and lost/stolen wallets, modern criminal methods include stealing information by overhearing conversations on cell phones, intercepting faxes and emails, hacking into computers, telephone and email scams, and phishing the users of online vendors and banks.

*Copyright 2007, SANS Institute
(www.sans.org)*

Editorial Board: Bill Wyman, Alan Reichert, Barbara Rietveld, Alan Paller. Permission is hereby granted for any person to redistribute this in whole or in part to any other persons as long as the distribution is not being made as part of any commercial service or as part of a promotion or marketing effort for any commercial service or product. Readers are invited to subscribe for free at <https://www.sans.org/newsletters/ouch>