COMPUTER NEWS from the

JAN 2014 Volume 2 NO. 1

As found on the web and other sources

FYI

I ran across this and thought it would make a good addition to your computer dictionary. It is a little long but makes for interesting reading.

Plausible Denial of Terms of Service?

FROM: Askbobrankin.com

Maybe that's mixing too many metaphors, but it sounded more fun than 'Hackers Dictionary' or 'Dark Deeds Defined.' Anyway, when we discuss the issues surrounding all the bad stuff that bad guys do online, and the good stuff that the good guys do to keep things running smoothly, we run into a bunch of jargon. And even if you're just an ordinary user, you should be familiar with these terms and their definitions. At the very least, you'll sound smarter at your next social gathering...

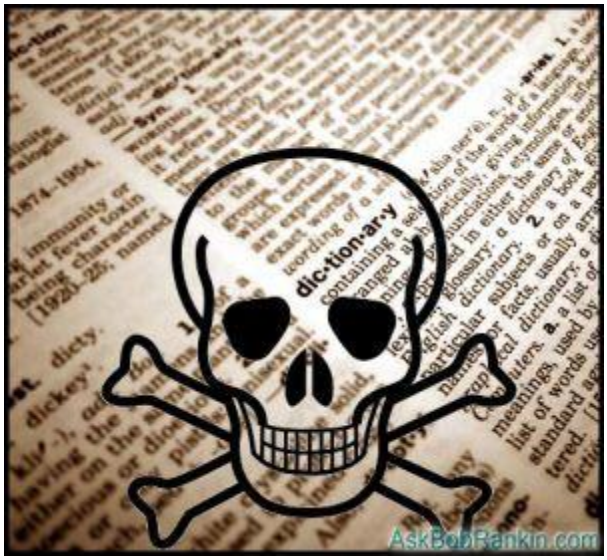
The Lexicon of Online Evil

Hackers, crackers, black hats, cyber-criminals, identity thieves, and spam kings -- these are some of the Bad Guys in the online world. And because of them, we've had to invent a whole new

vocabulary to describe the dastardly deeds they do. Here are plain English definitions of some words you should know, that deal with the darker side of the Internet...

Adware - A piece of software that displays advertisements on a computer after the software is installed. Adware can be benign, as in the case of a free program that displays ads in a manner that is agreed upon in advance. Or adware can be a nuisance, displaying unwanted ads with no apparent way to remove the program. The nuisance variety is often silently downloaded along with some other desired software, such as a game or toolbar. See Download Alert: Foistware Warning.

Arbitrary Code Execution - When a security vulnerability is discovered in a piece of software, sometimes it is said that it allows for "arbitrary code" to be executed on the machine. This really means that the vulnerability can be used to cause that program to execute ANY set of commands or instructions on that computer.



Back Door - A secret or unpublished feature of a software program that allows a third party to surreptitiously gain access to data or resources. For example, it is sometimes rumored that an encryption program may have a back door that allows for government agents to decrypt encoded messages without having the decryption keys.

Black Hat - A "bad guy" or hacker who breaks into computer networks, creates viruses, sends spam, or uses unethical tactics to influence search engine results.

Botnet - A collection of ordinary home and office computers that have been compromised by rogue software. The term "botnet" is short for "robot network" and describes the situation rather well. Computers that have been caught up in a botnet have been effectively taken over, and can be used to perform almost any task by the person or persons who control the botnet. Botnets are controlled by criminals and other miscreants whose motives include spewing spam to sell

products, operating financial scams and crippling websites through coordinated attacks. See BOTNET ALERT: Are You Vulnerable?.

Buffer Overrun - This is a flaw in a computer program that occurs when the length of a user input is not validated. For example, if a program is expecting a 9-digit social security number as input, it should discard any input beyond the 9th character. If the program blindly accepts a longer input string, it could "overrun" the input buffer, thereby trashing some other part of the currently running program with the extraneous characters. In some cases, this flaw can be used to overwrite the existing program with code that comes from the input string. (See "Arbitrary Code Execution")

Cookies - Actually, cookies are not evil, despite what you may have heard. See my article A Closer Look at Cookies for details.

Denial of Service Attack (DOS) - an attempt to flood a website with a barrage of meaningless requests for data, in order to make it crash under the load, or render it unable to service legitimate users. Most commonly, this comes in the form of a Distributed Denial of Service Attack (DDOS), which employs computers in many locations to attack a server anonymously. (See also: Botnet)

Ethical Hacker - A "good hacker" who uses a variety of techniques to test the safety of a computer network or system software. Typically an ethical hacker (also known as a "White Hat") is hired by a company to see if there are any flaws in their systems that might allow Black Hats to gain entry.

Exploit - A method of taking advantage of a bug or security hole in a computer program. It's possible that a hole may be known to exist, but no exploit has yet been created to capitalize on it.

Firewall - Hardware or software that limits access to a computer from an outside source. See Do I Really Need a Firewall?

Keylogger - a spying program that silently records all keystrokes on a computer, and optionally sends that information to a third party. See How To Detect and Defeat Keyloggers.

Malware - Any form of malicious software. This can include computer viruses, spyware, worms, trojan horses, rootkits and other software that is deliberately harmful, destructive, or invasive. See Protect Your Computer With Free Anti-Virus Software.

Patch - A fix for a software bug or security hole. When a bug is discovered, often there is a race by software vendors to provide a patch before an Exploit is created. Patches must be applied to the affected computers in order to prevent exploitation of the flaw.

Phishing - The act of stealing information using lies or deception as bait. Online scammers try to trick people into voluntarily providing passwords, account numbers and other personal information by pretending to be someone they trust. An example of phishing is an email that appears to be from a bank, asking recipients to login to a rogue site that looks exactly like the

real one. When the victim logs in, the operators of the fake site then have that person's login credentials and can access their bank account. See Would You Click on This? for more information on phishing and how to defend against it.

Polymorphic Virus - a virus that is designed to mutate, in order to avoid detection by anti-virus programs.

Ransomware - A type of malware that locks your computer and demands the payment of money (ransom) in order to unlock it. For a classic example, see Is The FBI Holding Your Computer for Ransom?

Rootkit - A rootkit is a software tool (or a set of programs) designed to conceal files, data or active processes from the operating system. Because of their ability to hide deep in the operating system, rootkits are hard to detect and remove. Although rootkits may not cause damage when installed, they are often piggy-backed with additional code written for the purpose of taking control of a computer, disabling certain functions, or spying on the user and reporting activities back to the rootkit creator. See Rootkits: Evil, Nasty and Sneaky!

Scareware - Software that is created for the purpose of tricking people into downloading or purchasing it, when in reality it's either unnecessary, marginally useful, or outright dangerous. Online ads that display fake warnings such as "Your computer may be infected -- click here to scan for viruses" or "ERROR! Registry Damage Detected -- click to download Registry Cleaner" would qualify as scareware. Scareware programs often run a fake or cursory scan, then present the user with a list of hazards that must be corrected. Fixing these "problems" then requires the user to pay a fee for a "full" or "registered" version of the software. See Don't Fall Victim to Scareware.

Skimming - The act of stealing credit or debit card information while a legitimate transaction is taking place at an ATM machine. Skimming involves an unauthorized device that is attached to the card slot of the ATM, which reads the magnetic strip as the card passes through. A hidden camera may also be used to capture the victim's PIN number.

Social Engineering - Manipulating people with trickery or deception, in order to gain confidential information that can be used to access a computer system, or perpetrate some other fraud. Social engineering is different from what is usually thought of as computer hacking, in that the information is gained from a person with legitimate access to the system, instead of by trying break into the system. (See also: Phishing)

Spyware - Spyware is a type of malicious software designed to take action on a computer without the informed consent of the user. Spyware may surreptitiously monitor the user, reporting personal information to a remote site, or subvert the computer's operation for the benefit of a third party. Some spyware tracks what types of websites a user visits and send this information to an advertisement agency. Others may launch annoying popup advertisements. More malicious versions try to intercept passwords or credit card numbers.

Trojan Horse - A Trojan horse is a malicious program that is disguised as or embedded within other software. The term is derived from the classical myth of the Trojan Horse. Such a program may look useful or interesting, but is actually harmful when executed. Examples may include web browser toolbars, games and file sharing programs. A Trojan horse cannot operate or spread on it's own, so it replies on a social engineering approach (tricking the user into taking some action) rather than flaws in a computer's security.

Virus - A computer virus is a malicious self-replicating computer program that spreads by inserting copies of itself into other programs or documents, similar to the way a real virus operates. When the infected program or document is opened, the destructive action (payload) is repeated, resulting in the infection, destruction or deletion of other files. Sometimes the infected programs continue to function normally, albeit with the side effects of the virus; in other cases the original program is crippled or destroyed.

Wardriving - the act of driving through an area while looking for unsecured wifi networks. See Avoid These Five WiFi Security Mistakes to make sure your wifi is secured with a password.

Worm - A worm is a malicious computer program that is self-contained and does not need help from another program to propagate itself. They can spread by trying to infect other files on a local network, or by exploiting the host computer's email transmission capabilities to send copies of themselves to everyone found in the email address book. Some even look in the cache of recently visited web pages and extract other email addresses to target.

Zero-Day Exploit - An attack that tries to exploit unpatched security vulnerabilities. The term "zero day" derives from the fact that software vendors sometimes have a window of time to fix a problem before an exploit is developed, or before news of a vulnerability is made public. But when the exploit already exists before a patch is released, the vendors have "zero days" to fix it because users are already exposed. See Avoiding Zero-Day Exploits.

Zombie - A computer that has been compromised, and can be controlled over a network to do the bidding of a criminal or miscreant. Computers that have been caught up in a Botnet are zombies, and can be used by the controller of the Botnet to send spam or participate in a coordinated denial of service attack.

Got a bone to pick? Want to beat me up over Hacker vs Cracker? Or maybe you want to add a word to the list. Post your comments and questions below...

Read more:
http://askbobrankin.com/plausible_denial_of_terms_of_service.html#ixzz2nwKBKJu2

Miss Quote of the month

Ken Olson

Kenneth Harry Olsen (February 20, 1926 – February 6, 2011 was an American engineer who co-founded Digital Equipment Corporation (DEC) in 1957 with colleague Harlan Anderson.

One quote of his is frequently taken out of context, and is indeed among the least understood in the industry.

Here is one from 1977: **There is no reason for any individual to have a computer in his home**.

He was referred to having the computer run the house, with automated doors, voice-activated faucets et cetera. He had a computer in his home for general use and promulgated the idea.

Note: Are we not heading in that direction with all the cell phone APP'S et cetera!

Bob