Glossary of Internet Threats

In using the internet and emails there are hundreds perhaps thousands of terms you may come across. Some of these are less important to users than others.

Safe Communities Algarve has put together some commonly used terms that are relevant to computer security and keeping your computer safe from attack. The terms are explained as definitions to help you understand what these mean. The list has been compiled from various sources, to provide a comprehensive guide. We hope you find it useful.

Adware

Generically, adware (spelled all lower case) is any software application in which advertising banners are displayed while the program is running. The authors of these applications include additional code that delivers the ads, which can be viewed through pop-up windows or through a bar that appears on a computer screen. Adware has been criticized because it usually includes code that tracks a user's personal information and passes it on to third parties, without the user's authorization or knowledge

Anti-Spam

Program that installs on your computer to avoid the reception of electronic junk mail, known as spam.

Antivirus (also written "anti-virus" or simply "AV")

Is software designed to prevent, detect, and remove viruses from a computer. Once installed, most antivirus programs run in the background, scanning new files for viruses and performing regular system checks. You can also use an anti-virus utility to scan individual files or folders directly.

Auction fraud

Someone selling something on an online auction site such as E-bay or Craigslist that appears to be something it really isn't. For example, someone may claim to be selling tickets for an upcoming concert that really are not official ticket

Botnets

A botnet is a network of computers that are controlled from a single source. While some botnets are used for legitimate cluster computing purposes, most botnets are created for malicious activity. Some examples include sending spam messages, spreading viruses, and attacking Internet servers.

Catfish

A person who creates a fake online profile with the intention of deceiving someone. For example, a woman could create a fake profile on an online dating website, create a relationship with one or more people and then create a fake scenario that asks others for money.

Firewall

A computer firewall limits the data that can pass through it and protects a networked server or client machine from damage by unauthorized users. Firewalls can be either hardware or software-based. A router is a good example of a hardware device that has a built-in firewall.

Hacker

It is now more commonly used to refer to someone who can gain unauthorized access to other computers. A hacker can "hack" his or her way through the security levels of a computer system or network. This can be as simple as figuring out somebody else's password or as complex as writing a custom program to break another computer's security software. Hackers are the reason software manufacturers release periodic "security updates" to their programs.

HTTPS

Stands for "Hypertext Transport Protocol Secure." HTTPS is the same thing as HTTP, but uses a secure socket layer (SSL) for security purposes. Some examples of sites that use HTTPS include banking and investment websites, e-commerce websites, and most websites that require you to log in.

Malware

Short for "malicious software," malware refers to software programs designed to damage or do other unwanted actions on a computer system.

Pharming

Pharming is yet another way hackers attempt to manipulate users on the Internet. While phishing attempts to capture personal information by getting users to visit a fake website, pharming redirects users to false websites without them even knowing it.

Phishing

Phishing is similar to fishing in a lake, but instead of trying to capture fish, phishers attempt to steal your personal information. They send out e-mails that appear to come from legitimate websites such as eBay, PayPal, or other banking institutions. The e-mails state that your information needs to be updated or validated and ask that you enter your username and password, after clicking a link included in the e-mail. Some e-mails will ask that you enter even more information, such as your full name, address, phone number, social security number, and credit card number. However, even if you visit the false website and just enter your username and password, the phisher may be able to gain access to more information by just logging in to your account.

Ransomware

Virus software that blackmails users by encrypting their hard drives or locking them out of the computer. It then demands payment to restore it. A favourite ploy is an FBI message claiming the user has child pornography on the computer, and a fine must be paid or else risk arrest. After paying the blackmail on any of these ransomware attacks, the user's machine may or may not be restored.

RFID

RFID is short for "Radio-Frequency Identification." RFID tags are small integrated circuits that can be scanned with a radio transmitter. This means they can be simply passed into the range of the transmitter rather needing to be swiped or scanned directly, like a credit card or UPC label. RFID tags have many applications, including inventory tracking, retail loss prevention, electronic toll booth payments, and keyless entry.

Spam

Now also refers to junk e-mail or irrelevant postings to a newsgroup or bulletin board. The unsolicited e-mail messages you receive about refinancing your home, reversing aging, and losing those extra pounds are all considered to be spam.

Trojan horses

Are software programs that masquerade as regular programs, such as games, disk utilities, and even antivirus programs. However if they are run, these programs can do malicious things to your computer.

For example, a Trojan horse might appear to be a computer game, but once you double-click it, the program starts writing over certain parts of your hard drive, corrupting your data. While this is certainly something you want to avoid, it is good to know that these malicious programs are only dangerous if they are given a chance to run.

Worm

A computer worm is a type of virus that replicates itself, but does not alter any files on your machine. However, worms can still cause havoc by multiplying so many times that they take up all your computer's available memory or hard disk space. If a worm consumes your memory, your computer will run very slowly and possibly even crash

Spyware

As the name implies, this is software that "spies" on your computer. Nobody likes to be spied on, and your computer doesn't like it either. Spyware can capture information like Web browsing habits, e-mail messages, usernames and passwords, and credit card information. If left unchecked, the software can transmit this data to another person's computer over the Internet.

Viruses

Computer viruses are small programs or scripts that can negatively affect the health of your computer. These malicious little programs can create files, move files, erase files, consume your computer's memory, and cause your computer not to function correctly. Some viruses can duplicate themselves, attach themselves to programs, and travel across networks. In fact opening an infected e-mail attachment is the most common way to get a virus.

419

Alternatively known as the Nigeria scam this scam lets the person think they have come to gain a large amount of money and only requires bank information to deposit the money or what seems to be a small deposit in order to get a large reward. In reality, the bank information is used against the person or the deposits are kept with no reward.

Posted 8 November 2014