LOGANSPORT
SAVINGS BANK FSB
“Leading the Way” ™

Address Munging: the practice of disguising, or munging, an e-mail address to prevent it being automatically collected and used as a target for people and organizations that send unsolicited bulk e-mail address.

Adware: or advertising-supported software is any software package which automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used. Some types of adware are also spyware and can be classified as privacy-invasive software.
Adware is software designed to force pre-chosen ads to display on your system. Some adware is designed to be malicious and will pop up ads with such speed and frequency that they seem to be taking over everything, slowing down your system and tying up all of your system resources. When adware is coupled with spyware, it can be a frustrating ride, to say the least.

Backdoor: in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice), or could be a modification to an existing program or hardware device.
A back door is a point of entry that circumvents normal security and can be used by a cracker to access a network or computer system. Usually back doors are created by system developers as shortcuts to speed access through security during the development stage and then are overlooked and never properly removed during final implementation. Sometimes crackers will create their own back door to a system by using a virus or a Trojan to set it up, thereby allowing them future access at their leisure.

Backscatter (also known as outscatter, misdirected bounces, blowback or collateral spam): a side-effect of e-mail spam, viruses and worms, where email servers receiving spam and other mail send bounce messages to an innocent party. This occurs because the original message’s envelope sender is forged to contain the e-mail address of the victim. A very large proportion of such e-mail is sent with a forged From: header, matching the envelope sender. Since these messages were not solicited by the recipients, are substantially similar to each other, and are delivered in bulk quantities, they qualify as unsolicited bulk email or spam. As such, systems that generate e-mail backscatter can end up being listed on various DNSBLs and be in violation of internet service providers’ Terms of Service.

Black Hat: the villain or bad guy, especially in a western movie in which such a character would wear a black hat in contrast to the hero’s white hat. The phrase is often used figuratively, especially in computing slang, where it refers to a hacker that breaks into networks or computers, or creates computer viruses.
Just like in the old westerns, these are the bad guys. A black hat is a cracker. To add insult to injury, black hats may also share information about the “break in” with other black hat crackers so they can exploit the same vulnerabilities before the victim becomes aware and takes appropriate measures… like calling Global Digital Forensics!

Bluebugging: a form of bluetooth attack. A Bluebug program allows the user to “take control” of the victim’s phone. Not only can they make calls, they can send messages, essentially do anything the phone can do. This also means that the Bluebug user can simply listen to any conversation his victim is having in real life.

Bluejacking: the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers,

Bluesnarfing: the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs. This allows access to a calendar, contact list, emails and text messages, and on some phones users can steal pictures and private videos.

Bot - A bot is a software “robot” that performs an extensive set of automated tasks on its own. Search engines like Google use bots, also known as spiders, to crawl through websites in order to scan through all of your pages. In these cases bots are not meant to interfere with a user, but are employed in an effort to index sites for the purpose of ranking them accordingly for appropriate returns on search queries. But when black hats use a bot, they can perform an extensive set of destructive tasks, as well as introduce many forms of malware to your system or network. They can also be used by black hats to coordinate attacks by controlling botnets.

Botnet: a jargon term for a collection of software robots, or bots, that runs autonomously and automatically. They run on groups of zombie computers controlled remotely.
A botnet is a network of zombie drones under the control of a black hat. When black hats are launching a Distributed Denial of Service attack for instance, they will use a botnet under their control to accomplish it. Most often, the users of the systems will not even know they are involved or that their system resources are being used to carry out DDOS attacks or for spamming. It not only helps cover the black hat’s tracks, but increases the ferocity of the attack by using the resources of many computer systems in a coordinated effort.

Cookies – A cookie is a small packet of information from a visited webserver stored on your system by your computer's browser. It is designed to store personalized information in order to customize your next visit. For instance, if you visit a site with forms to fill out on each visit, that information can be stored on your system as a cookie so you don't have to go through the process of filling out the forms each time you visit.

Cracker - When you hear the word hacker today, in reality it is normally referring to a cracker, but the two have become synonymous. With its origin derived from "safe-cracker" as a way to differentiate from the various uses of "hacker" in the cyber world, a cracker is someone who breaks into a computer system or network without authorization and with the intention of doing damage. A cracker may destroy files, steal personal information like credit card numbers or client data, infect the system with a virus, or undertake many others things that cause harm. This glossary will give you an idea of what they can do and some of the means they use to achieve their malicious objectives. These are the black hats.

Click fraud: a type of internet crime that occurs in pay per click online advertising when a person, automated script, or computer program imitates a legitimate user of a web browser clicking on an ad, for the purpose of generating a charge per click without having actual interest in the target of the ad's link. Click fraud is the subject of some controversy and increasing litigation due to the advertising networks being a key beneficiary of the fraud.

Computer Virus: a computer program that can copy itself and infect a computer without permission or knowledge of the user. The term "virus" is also commonly used, albeit erroneously, to refer to many different types of malware and adware programs.

Computer Worm: a self-replicating computer program. It uses a network to send copies of itself to other nodes (computer terminals on the network) and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Many worms have been created which are only designed to spread, and don't attempt to alter the systems they pass through. However, as the Morris worm and Mydoom showed, the network traffic and other unintended effects can often cause major disruption. A "payload" is code designed to do more than spread the worm – it might delete files on a host system (e.g., the ExploreZip worm), encrypt files in a cryptoviral extortion attack, or send documents via e-mail. A very common payload for worms is to install a backdoor in the infected computer to allow the creation of a "zombie" under control of the worm author – Sobig and Mydoom are examples which created zombies. Networks of such machines are often referred to as botnets and are very commonly used by spam senders for sending junk email or to cloak their website's address.

Crapflooding: the practice of disrupting online media such as discussion websites or Usenet newsgroups with nonsensical, inane, and/or repetitive postings (flooding with crap) in order to make it difficult for other users to read other postings. It can also be motivated by a desire to waste the targeted site’s bandwidth and storage space with useless text.

Cybercrimes: offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS).

Cyber-stalking: repeatedly sending message that include threats of harm or are highly intimidating; engaging in other online activities that make a person afraid for his or her safety.

Denial-of-Service Attack (DoS attack): or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to, motives for, and targets of a DoS attack may vary, it generally consists of the concerted, malevolent efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely.
A Denial of Service attack is an attack designed to overwhelm a targeted website to the point of crashing it or making it inaccessible. Along with sheer numbers and frequency, sometimes the data packets that are sent are malformed to further stress the system trying to process the server requests. A successful Denial of Service attack can cripple any entity that relies on its online presence by rendering their website virtually useless.

Distributed Denial of Service Attack (DDOS) - A Distributed Denial of Service attack is done with the help of zombie drones (also known as a botnet) under the control of black hats using a master program to command them to send information and data packets to the targeted webserver from the multiple systems under their control. This obviously makes the Distributed Denial of Service attack even more devastating than a Denial of Service attack launched from a single system, flooding the target server with a speed and volume that is exponentially magnified. As is normally the case with zombie drones and botnets, this is often done without the user of the controlled system even knowing they were involved.

Dumpster Diving - The act of rummaging through the trash of an individual or business to gather information that could be useful for a cyber-criminal to gain access to a system or attain personal information to aid them in identity theft or system intrusion. One person’s garbage can indeed can be a cyber-criminal’s treasure.

Easter Egg - A non-malicious surprise contained in a program or on a circuit board installed by the developer. It could be as simple as a text greeting, a signature, or an image embedded on a circuit board, or be comprised of a more complex routine, like a video or a small program. The criteria that must be met to be considered an Easter Egg are that it be undocumented, non-malicious, reproducible to anyone with the same device or software, not be obvious, and above all – it should be entertaining!

E-mail spoofing: a term used to describe fraudulent email activity in which the sender address and other parts of the email header are altered to appear as though the email originated from a different source. E-mail spoofing is a technique commonly used for spam e-mail and phishing to hide the origin of an e-mail message.

False flag operations: covert operations conducted by governments, corporations, or other organizations, which are designed to appear like they are being carried out by other entities.

Firewall - A firewall is a security barrier designed to keep unwanted intruders “outside” a computer system or network while allowing safe communication between systems and users on the “inside” of the firewall. Firewalls can be physical devices or software-based, or a combination of the two. A well designed and implemented firewall is a must to ensure safe communications and network access and should be regularly checked and updated to ensure continued function. Black hats learn new tricks and exploit new techniques all the time, and what worked to keep them out yesterday may need to be adjusted or replaced over time.

Flaming: online fights using electronic messages with angry and vulgar language.

Gray Hat – A gray hat, as you would imagine, is a bit of a white hat/black hat hybrid. Thankfully, like white hats, their mission is not to do damage to a system or network, but to expose flaws in system security. The black hat part of the mix is that they may very well use illegal means to gain access to the targeted system or network, but not for the purpose of damaging or destroying data: they want to expose the security weaknesses of a particular system and then notify the “victim” of their success. Often this is done with the intent of then selling their services to help correct the security failure so black hats can not gain entry and/or access for more devious and harmful purposes.

Griefers: differ from typical players in that they do not play the game in order to achieve objectives defined by the game world. Instead, they seek to harass other players, causing grief. In particular, they may use tools such as stalking, hurling insults, and exploiting unintended game mechanics. Griefing as a gaming play style is not simply any action that may be considered morally incorrect.

Hacker: someone involved in computer security/insecurity, specializing in the discovery of exploits in systems (for exploitation or prevention), or in obtaining or preventing unauthorized access to systems through skills, tactics and detailed knowledge. In the most common general form of this usage, "hacker" refers to a black-hat hacker (a malicious or criminal hacker).

This is the trickiest definition of the group and controversy has followed its use for decades. Originally, the term hacker had a positive connotation and it actually had nothing to do with computer systems. In 1946, the Tech Model Railroad Club of MIT coined the term to mean someone who applies ingenuity to achieve a clever result. Then, when computers came along, "hacker" took on the meaning of someone who would "hack" away on a program through the night to make it better. But in the 80s everything changed, and Hollywood was the catalyst. When the personal computers onslaught started invading our daily lives, it didn't take long for clever screen-writers to bring the black hat villains of the cyber world to the forefront of our collective consciousness, and they haven't looked back since. They associated our deepest fears with the word hacker, making them the ones that unraveled our privacy, put our safety in jeopardy, and had the power to take everything from us, from our material possessions to our very identities. And they could do it all anonymously, by hacking away in a dark room by the dim light of a computer monitor's glow. Needless to say, right or wrong, it stuck! Even many professionals in the computing field today have finally, albeit grudgingly, given in to the mainstream meaning of the word. "Hacker" has thus become the catch-all term used when in fact it should be "cracker."

Internet Bots: also known as web robots, WWW robots or simply bots, are software applications that run automated tasks over the Internet.

Internet troll (or simply troll in Internet slang): someone who posts controversial and usually irrelevant or off-topic messages in an online community, such as an online discussion forum or chat room, with the intention of baiting other users into an emotional response[1] or to generally disrupt normal on-topic discussion.

Joe Job: a spam attack using spoofed sender data. Aimed at tarnishing the reputation of the apparent sender and/or induce the recipients to take action against him **(see also e-mail spoofing)**.

Keylogger – A keylogger is a non-destructive program that is designed to log every keystroke made on a computer. The information that is collected can then be saved as a file and/or sent to another machine on the network or over the Internet, making it possible for someone else to see every keystroke that was made on a particular system. By breaking down this information, it can be easy for a black hat cracker to recreate your user names and passwords, putting all kinds of information at risk and susceptible to misuse. Just imagine your online banking login information falling into the wrong hands! Finding out you have a keylogger installed, however, does not necessarily mean you were the victim of a black hat, as some companies install them on employee computers to track usage and ensure that systems are not being used for unintended purposes. Keyloggers are, for obvious reasons, often considered to be spyware.

Keystroke Logging (often called keylogging): a method of capturing and recording user keystrokes. Keylogging can be useful to determine sources of errors in computer systems, to study how users interact and access with systems, and is sometimes used to measure employee productivity on certain clerical tasks. Such systems are also highly useful for law enforcement and espionage—for instance, providing a means to obtain passwords or encryption keys and thus bypassing other security measures.

Logic Bomb – A logic bomb is a malicious program designed to execute when a certain criterion is met. A time bomb could be considered a logic bomb because when the target time or date is reached, it executes. But logic bombs can be much more complex. They can be designed to execute when a certain file is accessed, or when a certain key combination is pressed, or through the passing of any other event or task that is possible to be tracked on a computer. Until the trigger event the logic bomb was designed for passes, it will simply remain dormant.

Lurker: a person who reads discussions on a message board, newsgroup, chatroom, file sharing or other interactive system, but rarely participates.

Malware: software designed to infiltrate or damage a computer system without the owner's informed consent. The term is a portmanteau of the words malicious and software. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.
Simply put, malware is a malicious program that causes damage. It includes viruses, Trojans, worms, time bombs, logic bombs, or anything else intended to cause damage upon the execution of the payload.

Master Program - A master program is the program a black hat cracker uses to remotely transmit commands to infected zombie drones, normally to carry out Denial of Service attacks or spam attacks.

Money Mule: a person who transfers money and reships high value goods that have been fraudulently obtained in one country, usually via the internet, to another country, usually where the perpetrator of the fraud lives. The term money mule is formed by analogy with drug mules.

The need for money mules arises because while a criminal in a developing country can obtain the credit card numbers, bank account numbers, passwords and other financial details of a victim living in the first world via the internet through techniques such as malware and phishing, turning those details into money usable in the criminal’s own country can be difficult. Many businesses will refuse to transfer money or ship goods to certain countries where there is a high likelihood that the transaction is fraudulent. The criminal therefore recruits a money mule in the victim’s country who receives money transfers and merchandise and resend them to the criminal in return for a commission.

Nigerian 419 Fraud Scheme (or an advance fee fraud): a confidence trick in which the target is persuaded to advance relatively small sums of money in the hope of realizing a much larger gain.

Payload – The payload is the part of the malware program that actually executes its designed task.

Peer to Peer (or "P2P"): computer network that uses diverse connectivity between participants in a network and the cumulative bandwidth of network participants rather than conventional centralized resources where a relatively low number of servers provide the core value to a service or application. P2P networks are typically used for connecting nodes via largely ad hoc connections. Such networks are useful for many purposes. Sharing content files (see file sharing) containing audio, video, data or anything in digital format is very common, and realtime data, such as telephony traffic, is also passed using P2P technology.

Pharming (pronounced farming) is a hacker's attack aiming to redirect a website's traffic to another, bogus website.

Phishing is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. PayPal, eBay and online banks are common targets. Phishing is typically carried out by e-mail or instant messaging, [1] and often directs users to enter details at a website, although phone contact has also been used.
Phishing is a form of social engineering carried out by black hats in electronic form, usually by email, with the purpose of gathering sensitive information. Often these communications will look legitimate and sometimes they will even look like they come from a legitimate source like a social networking site, a well-known entity like Paypal or Ebay, or even your bank. They will have a link directing you to a site that looks very convincing and ask you to verify your account information. When you log in to verify your information on the bogus site, you have just given the black hat exactly what they need to make you the next victim of cybercrime. Phishing is done in many forms – sometimes it’s easy to spot, sometimes not.

Phreaking: a slang term coined to describe the activity of a subculture of people who study, experiment with, or explore telecommunication systems, like equipment and systems connected to public telephone networks. The term "phreak" is a portmanteau of the words "phone" and "freak". It may also refer to the use of various audio frequencies to manipulate a phone system. "Phreak", "phreaker", or "phone phreak" are names used for and by individuals who participate in phreaking. Additionally, it is often associated with computer hacking. This is sometimes called the H/P culture (with H standing for Hacking and P standing for Phreaking). Considered the original computer hackers, phreakers, or phone phreakers, hit the scene in the 60s and made their mark by circumventing telecommunications security systems to place calls, including long distance, for free. By using electronic recording devices, or even simply creating tones with a whistle, phreakers tricked the systems into thinking it was a valid call. One of the first to find prominence was "Captain Crunch," a phreaker who realized the toy whistle that came as a prize in a box of Captain Crunch cereal could be used to mimic the tone frequencies used by telecommunications companies to validate and route calls.

Pigeon Drop: the name of a confidence trick in which a mark or "pigeon" is convinced to give up a sum of money in order to secure the rights to a larger sum of money, or more valuable object. In reality the scammers make off with the money and the mark is left with nothing.

Piggybacking: a term used to refer to access of a wireless internet connection by bringing one's own computer within the range of another's wireless connection, and using that service without the subscriber's explicit permission or knowledge. It is a legally and ethically controversial practice, with laws that vary in jurisdictions around the world. While completely outlawed in some jurisdictions, it is permitted in others. Piggybacking is used as a means of hiding illegal activities, such as downloading child pornography or engaging in identity theft. This is one main reason for controversy.

Pod Slurping: the act of using a portable data storage device such as an iPod digital audio player to illicitly download large quantities of confidential data by directly plugging it into a computer where the data is held, and which may be on the inside of a firewall. As these storage devices become smaller and their storage capacity becomes greater, they are becoming an increasing security risk to companies and government agencies. Access is gained while the computer is unattended.

Polymorphic Virus - A polymorphic virus is a virus that will change its digital footprint every time it replicates. Antivirus software relies on a constantly updated and evolving database of virus signatures to detect any virus that may have infected a system. By changing its signature upon replication, a polymorphic virus may elude antivirus software, making it very hard to eradicate.

Rootkit: a program (or combination of several programs) designed to take fundamental control (in Unix terms "root" access, in Windows terms "Administrator" access) of a computer system, without authorization by the system's owners and legitimate managers. Access to the hardware (i.e., the reset switch) is rarely required as a rootkit is intended to seize control of the operating system running on the hardware. Typically, rootkits act to obscure their presence on the system through subversion or evasion of standard operating system security mechanisms. Often, they are also Trojans as well, thus fooling users into believing they are safe to run on their systems. Techniques used to accomplish this can include concealing running processes from monitoring programs, or hiding files or system data from the operating system.

Without a doubt, the biggest fear in IT security is an undetected intrusion. A rootkit is a tool that can give a black hat the means for just such a perfect heist. A rootkit is a malware program that is installed on a system through various means, including the same methods that allow viruses to be injected into a system, like email, websites designed to introduce malware, or downloading and/or copying to the system with an unsafe program. Once a rootkit is introduced, this will create a back door for a black hat that will allow remote, unauthorized entry whenever he or she chooses. What makes a rootkit particularly lethal: it is installed and functions at such low system levels that it can be designed to erase its own tracks and activity from the now vulnerable system, allowing the black hat to navigate through entire networks without being exposed. Often, black hats will use social engineering to gain physical access to particularly well protected system so the rootkit can be directly installed from CD or a tiny USB drive (it only takes a minute) in order either to circumvent a particularly troublesome firewall or gain access to a system that is not normally accessible from the outside. Once the rootkit is introduced, the black hat has free reign and even skilled IT security departments will have a lot of trouble even seeing the activity as it's happening. Rootkits are a definite 10 on the scary scale of cyber intrusions.

Scam Baiting is the practice of pretending interest in a fraudulent scheme in order to manipulate a scammer. The purpose of scam baiting might be to waste the scammers' time, embarrass him or her, cause him or her to reveal information which can be passed on to legal authorities, get him or her to waste money, or simply to amuse the baiter.

Script kiddie (occasionally script bunny, skiddie, script kitty, script-running juvenile (SRJ), or similar): a derogatory term used for an inexperienced malicious hacker who uses programs developed by others to attack computer systems, and deface websites.

An individual who does not possess, or just doesn't use, their own skills and know-how to hack or crack a computer system or network, but uses a pre-written program or piece of code, a script, to do the dirty work. While they may not possess the computing talent, they can be just as dangerous!

Shareware: a marketing method for computer software in which the software can be obtained by a user, often by downloading from the Internet or on magazine cover-disks free of charge to try out a program before buying the full version of that program. If the "tryout" program is already the full version, it is available for a short amount of time, or it does not have updates, help, and other extras that buying the added programs has. Shareware has also been known as "try before you buy". A shareware program is accompanied by a request for payment, and the software's distribution license often requires such a payment

Smishing: short for "SMS phishing" (SMiShing) is an attempt to get cellular phone and mobile device owners to download a Trojan horse, virus or other malware by clinking on a link included in a SMS text message.

Sneakernet: a tongue-in-cheek term used to describe the transfer of electronic information, especially computer files, by physically carrying removable media such as magnetic tape, floppy disks, compact discs, USB flash drives, or external hard drives from one computer to another.

Snarfing: information theft or data manipulation in wireless local-area networks (WLAN).

Social engineering: the art of manipulating people into performing actions or divulging confidential information.[1] While similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access and in most cases the attacker never comes face-to-face with the victim.
In the realm of the black hats, social engineering means to deceive someone for the purpose of acquiring sensitive and personal information, like credit card details or user names and passwords. For instance, when fictitious Mr. Smith calls from IT services to inform you of new user name and password guidelines being implemented by the company and asks you to reveal yours so he can make sure they meet the new guidelines, you have been a target of social engineering. They can be very clever and resourceful, and very, very convincing. The only way to make sure you are not a victim of social engineering is never to give your personal and sensitive information to anyone you are not absolutely sure about. There are very few occasions that anyone legitimate would ever ask you for a password, and you should always be the one contacting them, not the other way around.

Sockpuppet: an online identity used for purposes of deception within an Internet community. In its earliest usage, a sockpuppet was a false identity through which a member of an Internet community speaks while pretending not to, like a puppeteer manipulating a hand puppet.[1] A sockpuppet-like use of deceptive fake identities is used in stealth marketing. The stealth marketer creates one or more pseudonymous accounts, each one claiming to be owned by a different enthusiastic supporter of the sponsor's product or book or ideology. A single such sockpuppet is a shill; creating large numbers of them to fake a "grass-roots" upswelling of support is known as astroturfing.

Software cracking: the modification of software to remove protection methods: copy prevention, trial/demo version, serial number, hardware key, CD check or software annoyances like nag screens and adware.

Spam – Spam is simply unsolicited email, also known as junk email. Spammers gather lists of email addresses, which they use to bombard users with this unsolicited mail. Often, the emails sent are simply advertising for a product or a service, but sometimes they can be used for phishing and/or directing you to websites or products that will introduce malware to your system. When you receive spam, the best practice is to delete it immediately. Sometimes you will see a note in a spam email that gives you instructions on how to be removed from the list – never do it! This will only confirm to the spammer that they have a valid email address and the spam will just keep coming. They could also then sell your email address to another spammer as a confirmed email address and more spam will show up in your inbox. Most mail services have spam filters and these should be employed whenever possible.

Spamming: the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, mobile phone messaging spam, Internet forum spam and junk fax transmissions.

Spear Phishing: Targeted versions of phishing have been termed spear phishing.[19] Several recent phishing attacks have been directed specifically at senior executives and other high profile targets within businesses, and the term whaling has been coined for these kinds of attacks.

Spoofing – Spoofing is the art of misdirection. Black hat crackers will often cover their tracks by spoofing (faking) an IP address or masking/changing the sender information on an email so as to deceive the recipient as to its origin. For example, they could send you an email containing a link to a page that will infect your system with malware and make it look like it came from a safe source, such as a trusted friend or well-known organization. Most of the true sources have security measures in place to avoid tampering with sender information on their own mail servers, but as many black hat spammers will launch attacks from their own SMTP (Simple Mail Transfer Protocol), they will be able to tamper with that information. When in doubt, check with the source yourself.

Sporgery: the disruptive act of posting a flood of articles to a Usenet newsgroup, with the article headers falsified so that they appear to have been posted by others. The word is a portmanteau of spam and forgery.

Spyware: is computer software that is installed surreptitiously on a personal computer to intercept or take partial control over the user’s interaction with the computer, without the user’s informed consent.While the term spyware suggests software that secretly monitors the user’s behavior, the functions of spyware extend well beyond simple monitoring. Spyware programs can collect various types of personal information, such as Internet surfing habit, sites that have been visited, but can also interfere with user control of the computer in other ways, such as installing additional software, redirecting Web browser activity, accessing websites blindly that will cause more harmful viruses, or diverting advertising revenue to a third party. Spyware can even change computer settings, resulting in slow connection speeds, different home pages, and loss of Internet or other program.

Spyware is software designed to gather information about a user’s computer use without their knowledge. Sometimes spyware is simply used to track a user’s Internet surfing habits for advertising purposes in an effort to match your interests with relevant ads. On the other side of the coin, spyware can also scan computer files and keystrokes, create pop-up ads, change your homepage and/or direct you to pre-chosen websites. One common use is to generate a pop-up ad informing you that your system has been infected with a virus or some other form of malware and then force you to a pre-selected page that has the solution to fix the problem. Most often, spyware is bundled with free software like screen savers, emoticons and social networking programs.

Stealware: refers to a type of software that effectively transfers money owed to a website owner to a third party. Specifically, stealware uses an HTTP cookie to redirect the commission ordinarily earned by the site for referring users to another site.

Time Bomb – A time bomb is a malicious program designed to execute at a predetermined time and/or date. Time bombs are often set to trigger on special days like holidays, or sometimes they mark things like Hitler’s birthday or 9/11 to make some sort of political statement. What a time bomb does on execution could be something benign like showing a certain picture, or it could be much more damaging, like stealing, deleting, or corrupting system information. Until the trigger time is achieved, a time bomb will simply remain dormant.

Trojan horse (or simply Trojan): a piece of software which appears to perform a certain action but in fact performs another such as transmitting a computer virus. Contrary to popular belief, this action, usually encoded in a hidden payload, may or may not be actually malicious, but Trojan horses are notorious today for their use in the installation of backdoor programs. Simply put, a Trojan horse is not a computer virus. Unlike such malware, it does not propagate by self-replication but relies heavily on the exploitation of an end-user (see Social engineering).

A Trojan, or Trojan Horse, is a malicious program disguised to look like a valid program, making it difficult to distinguish from programs that are supposed to be there. Once introduced, a Trojan can destroy files, alter information, steal passwords or other information, or fulfill any other sinister purpose it was designed to accomplish. Or it may stay dormant, waiting for a cracker to access it remotely and take control of the system. A Trojan is a lot like a virus, but without the ability to replicate.

Virus - A virus is a malicious program or code that attaches itself to another program file and can replicate itself and thereby infect other systems. Just like the flu virus, it can spread from one system to another when the infected program is used by another system. The more interconnected the host is, the better its chances to spread. The spread of a virus can easily occur on networked systems, or it could even be passed along on other media like a CD or memory stick when a user unwittingly copies an infected file and introduces it to a new system. A virus could even be emailed with an attachment. "Virus" is often incorrectly used as a catch-all phrase for other malicious programs that don't have the ability to self-replicate, like spyware and adware.

Vishing: is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private personal and financial information from the public for the purpose of financial reward. The term is a combination of "voice" and phishing. Vishing exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations which are known to the telephone company, and associated with a bill-payer. The victim is often unaware that VoIP allows for caller ID spoofing, inexpensive, complex automated systems and anonymity for the bill-payer. Vishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.

VoIP Spam: the proliferation of unwanted, automatically-dialed, pre-recorded phone calls using Voice over Internet Protocol (VoIP). Some pundits have taken to referring to it as SPIT (for "Spam over Internet Telephony").

War dialing: a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for unknown computers, BBS systems or fax machines. Hackers use the resulting lists for various purposes.

Wardriving: the act of searching for Wi-Fi wireless networks by a person in a moving vehicle using such items as a laptop or a PDA.
Wardriving is the act of driving around in a vehicle with the purpose of finding an open, unsecured Wi-Fi wireless network. Many times, the range of a wireless network will exceed the perimeter of a building and create zones in public places that can be exploited to gain entry to the network. Black hats, and even gray hats, will often use a GPS system to make maps of exploitable zones so they can be used at a later time or passed on to others. Wardriving is not the only way this task is performed – there are Warbikers and Warwalkers too. As you can see, it is imperative that your WiFi network is secure because there are entities out there looking for any opening to ply their trade.

Warspying: detecting and viewing wireless video; usually done by driving around with an x10 receiver. Warspying is similar to "Wardriving" only with wireless video instead of wireless networks.

Web crawler (also known as a web spider or web robot or – especially in the FOAF community – web scutter): a program or automated script which browses the World Wide Web in a methodical, automated manner. Other less frequently used names for web crawlers are ants, automatic indexers, bots, and worms. This process is called web crawling or spidering. Many sites, in particular search engines, use spidering as a means of providing up-to-date data.

White Hat: the hero or good guy, especially in computing slang, where it refers to an ethical hacker that focuses on securing and protecting IT systems. Such people are employed by computer security companies where these professionals are sometimes called sneakers.[citation needed] Groups of these people are often called tiger teams.
While black hats use their skill for malicious purposes, white hats are ethical hackers. They use their knowledge and skill to thwart the black hats and secure the integrity of computer systems or networks. If a black hat decides to target you, it's a great thing to have a white hat around. But if you don't, you can always call on one of ours at Global Digital Forensics.

Worm – A worm is very similar to a virus in that it is a destructive self-contained program that can replicate itself. But unlike a virus, a worm does not need to be a part of another program or document. A worm can copy and transfer itself to other systems on a network, even without user intervention. A worm can become devastating if not isolated and removed. Even if it does not cause outright damage, a worm replicating out of control can exponentially consume system resources like memory and bandwidth until a system becomes unstable and unusable.

Zero Day Threat/Exploit - Every threat to your computer security has to start somewhere. Unfortunately, the way most of us protect ourselves from cyber threats and intrusions, is to use detection programs that are based on analyzing, comparing and matching the digital footprint of a possible threat to an internal database of threats that have been previously detected, reported and documented. That's why we all have to go through those seemingly never-ending updates to our anti-virus programs, that's how the database is updated and the newest threats are added to the list of what the scanners look for. That inherent flaw in our scanners is what makes a Zero Day threat so dangerous. A Zero Day threat is pristine and undocumented. From the very first day a particular threat is ever deployed (zero day) until that threat is noticed, reported, documented and added to the index, it is an unknown. As far as standard protection goes, unknown means invisible – and when it comes to cyber threats, invisible can definitely mean trouble.

Zombie / Zombie Drone – A zombie is a malware program that can be used by a black hat cracker to remotely take control of a system so it can be used as a zombie drone for further attacks, like spam emails or Denial of Service attacks, without a user's knowledge. This helps cover the black hat's tracks and increases the magnitude of their activities by using your resources for their own devious purposes. Rarely will the user infected with a zombie even know it's there, as zombies are normally benign and non-destructive in and of themselves. Zombies can be introduced to a system by simply opening an infected email attachment, but most often they are received through non-mainstream sites like file sharing sites, chat groups, adult websites and online casinos that force you to download their media player to have access to the content on their site, using the installed player itself as the delivery mechanism.

Zombie computer (often shortened as Zombie): a computer attached to the Internet that has been compromised by a hacker, a computer virus, or a Trojan horse. Generally, a compromised machine is only one of many in a Botnet, and will be used to perform malicious tasks of one sort or another under remote direction.