Threats

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. The word is a neologism created as a homophone of fishing due to the similarity of using fake bait in an attempt to catch a victim. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting victims. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

A **computer worm** is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer. Users can minimize the threat posed by worms by keeping their computers' operating system and other software up-to-date, avoiding opening unrecognized or unexpected emails, and running firewall and antivirus software.

A **computer virus** is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into othercomputer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected". Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts,logging their keystrokes, or even rendering the computer useless. However, not all viruses carry a destructive payload or attempt to hide themselves—the defining characteristic of viruses is that they are self-replicating computer programs which install themselves without user consent.

A **Trojan horse**, or **Trojan**, in computing is any malicious computer program which misrepresents itself as useful, routine, or interesting in order to persuade a victim to install it. The term is derived from the Ancient Greek story of the wooden horse that was used to help Greek troops invade the city of Troy by stealth. Trojans are generally spread by some form of social engineering, for example where a user is duped into executing an e-mail attachment disguised to be unsuspicious, (e.g., a routine form to be filled in), or by drive-by download. Although their payload can be anything, many moderns forms act as a backdoor, contacting a controller which can then have unauthorized access to the affected computer. While Trojans and backdoors are not easily detectable by themselves, computers may appear to run slower due to heavy processor or network usage.Unlike computer viruses and worms, Trojans generally do not attempt to inject themselves into other files or otherwise propagate themselves.

In computing, a **denial-of-service** (**DoS**) **attack** is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. A **distributed denial-of-service**(**DDoS**) is where the attack source is more than one–and often thousands–of unique IP addresses. Criminal perpetrators of DoS attacks often target sites or services hosted on high-profile web servers such as banks, credit card payment gateways; but motives of revenge, blackmail or activism can be behind other attacks. A **SYN flood** occurs when a host sends a flood of TCP/SYN packets, often with a forged sender address. Each of these packets are handled like a connection request, causing the server to spawn a half-open connection, by sending back a TCP/SYN-ACK packet (Acknowledge), and waiting for a packet in response from the sender address (response to the ACK Packet).

A **Dictionary attack** is an attempt to identify your password by using common words, names of loved ones, pets, birth dates, addresses, and phone numbers. A dictionary attack begins with the dictionary, essentially a database of commonly used words to which the attacker can add custom words or conduct a forensic analysis, in which software scans text documents and adds all words to the dictionary. Some passwords are so simple or poorly formed that the intruder can easily guess them. You would be surprised how many users use a password that is the same as their user name. Some users use a street name, a maiden name, or the name of a child for a password, and some use easily guessable character combinations, such as 123456, abcde, or zzzzzz. A **Brute force attack.** A hacker uses a computer program or script to try to log in with possible password combinations, usually starting with the easiest-to-guess passwords. (So just think: if a hacker has a company list, he or she can easily guess usernames. If even one of the users has a “Password123”, he will quickly be able to get in.)

Referencies:

https://en.wikipedia.org/wiki/Phishing

https://en.wikipedia.org/wiki/Computer_worm

https://en.wikipedia.org/wiki/Computer_virus

https://en.wikipedia.org/wiki/Trojan_horse_(computing)

https://en.wikipedia.org/wiki/Denial-of-service_attack

http://insights.scorpionsoft.com/3-types-of-password-security-attacks-and-how-to-avoid-them