Cybersecurity Terminology

Botnet (also zombies) - A collection of computers subject to control by an outside party, usually without the knowledge of the owners, using secretly installed software robots. The robots are spread by trojan horses and viruses. The botnets can be used to launch denial-of-service attacks and to transmit spam.

Card Skimming - The act of using a skimmer to illegally collect data from the magnetic stripe of a credit, debit or ATM card. This information, copied onto another blank card's magnetic stripe, is then used by an identity thief to make purchases or withdraw cash in the name of the actual account holder. Skimming can take place at an ATM. Be aware of attachments, cameras, or anything that does not seem right with an ATM. Skimming can also occur at restaurants, taxis, or other places where a user surrenders his or her card to an employee.

Cybersecurity - Measures taken to protect computers or critical infrastructure.

Denial-of-service attack - Flooding the networks or servers of individuals or organizations with false data requests so they are unable to respond to requests from legitimate users.

Hacker - A person with special expertise in computer systems and software. A hacker who attempts to gain unauthorized access to computer systems is a "cracker."

Hacktivist - An individual who breaches Web sites or secured communications systems to deliver political messages, including those related to foreign policy, or propaganda

Identity management - A method of validating a person`s identity when he/she tries to access a network.

Malicious code (also malware) - Any code that can be used to attack a computer by spreading viruses, crashing networks, gathering intelligence, corrupting data, distributing misinformation and interfering with normal operations.

Pharming - The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a website where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information

Phishing - Using fake e-mail to trick individuals into revealing personal information, such as Social Security numbers, debit and credit card account numbers and passwords, for nefarious uses.

Spam - Unsolicited bulk e-mail that may contain malicious software. Spam is now said to account for around 81 percent of all e-mail traffic.

Spear Phishing - A type of phishing attack that focuses on a single user or department within an organization, addressed from someone within the company in a position of trust and requesting information such as login IDs and passwords. Spear phishing scams will often appear to be from a company's own human resources or technical support divisions and may ask employees to update their username and passwords. Once hackers get this data, they can gain entry into secured networks. Another type of spear phishing attack will ask users to click on a link, which deploys spyware that can thieve data.

Spoofing - Making a message or transaction appear to come from a source other than the originator.

Spyware - Software that collects information without a user`s knowledge and transfers it to a third party.

Trojan horse - A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

Virus - A program designed to degrade service, cause inexplicable symptoms or damage networks.

Worm - Program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down. A worm, unlike a virus, has the capability to travel without human action and does not need to be attached to another file or program.