- **Adware –** Adware refers to any piece of software or application that displays advertisements on your computer.
- **Advanced Persistent Threat (APT)** – An advanced persistent threat is an attack in which an unauthorized user gains access to a system or network without being detected.
- **Anti-Virus Software** – Anti-virus software is a computer program used to prevent, detect, and remove malware.
- **Artificial Intelligence** – Artificial intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions.
- **Attachment** – An attachment is a computer file sent with an email message.
- **Authentication** – Authentication is a process that ensures and confirms a user's identity.
- **Back door** – A backdoor is used to describe a hidden method of bypassing security to gain access to a restricted part of a computer system.
- **Backup** – To make a copy of data stored on a computer or server to reduce the potential impact of failure or loss
- **Baiting** – Online baiting involves enticing a victim with an incentive.
- **Bluetooth** – Bluetooth is a wireless technology for exchanging data over short distances.
- **Blackhat** – Black hat hacker refers to a hacker that violates computer security for personal gain or malice.
- **Blog** - Online journal – stands for "web log"
- **Botnet** – A botnet is a collection of internet-connected devices, which may include PCs, servers and mobile devices that are infected and controlled by a common type of malware.
- **Broadband** – High-speed data transmission system where the communications circuit is shared between multiple users.
- **Browser** – A browser is software that is used to access the internet. The most popular web browsers are Chrome, Firefox, Safari, Internet Explorer, and Edge.
- **Brute Force Attack** – Brute force attack is an activity which involves repetitive successive attempts of trying various password combinations to break into any website.
- **Bug** – A bug refers to an error, fault or flaw in a computer program that may cause it to unexpectedly quit or behave in an unintended manner.
- **BYOD** – Bring your own device (BYOD) refers to employees using personal devices to connect to their organizational networks.
- **Clickjacking** – Clickjacking, also known as a UI redress attack, is a common hacking technique in which an attacker creates an invisible page or an HTML element that overlays the legitimate page.
- **Cloud Computing** – The practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.
- **Cookie** – Cookies are small files or info packets which are stored on a user's computer. Cookies provide a way for the website to recognize you and keep track of your preferences.
- **Critical Update** – A fix for a specific problem that addresses a critical, non-security-related bug in computer software.
- **Cyber Bullying** - The act of one individual harassing or intimidating another individual via the Internet.
- **Cyber Warfare** – Cyber warfare typically refers to cyber-attacks perpetrated by one nation-state against another.
- **Cryptography** - protecting information or hiding its meaning by converting it into a secret code before sending it out over a public network

- **Data Breach** – A data breach is a confirmed incident where information has been stolen or taken from a system without the knowledge or authorization of the system's owner.
- **Data Server** – Data server is the phrase used to describe computer software and hardware that delivers database services.
- **Denial-of-service (DDoS) attack** - a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.
- **Deepfake** – Deepfake refers to any video in which faces have been either swapped or digitally altered, with the help of AI.
- **Domain name** – The part of a network address which identifies it as belonging to a particular domain.
- **Domain Name Server** – A server that converts recognizable domain names into their unique IP address
- **Download** – To copy (data) from one computer system to another, typically over the Internet.
- **Electronic Data**: means files, documents, information and "programs and applications" in an electronic format and that are stored on "media".
- **Electronic Vandalism** - means "computer hacking", "computer virus" or a "denial of service attack". Does not include the "theft" of any property or services.
- **Exploit** – A malicious application or script that can be used to take advantage of a computer's vulnerability.
- **Firewall** – A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet.
- **Fraudulent instruction** - An electronic, telegraphic, cable, teletype, tele facsimile or telephone instruction which purports to have been transmitted by you, but which was in fact fraudulently transmitted by someone else without your knowledge or consent;
- **Hacking** – Hacking refers to an unauthorized intrusion into a computer or a network.
- **Hacktivism** – a politically or ideologically motivated cyber-attack or hack
- **Honeypot** – A decoy system or network that serves to attract potential attackers.
- **HTML** – Hypertext Markup Language (HTML) is the standard markup language for creating web pages and web applications.
- **Identity theft** – Identity theft is a crime in which someone uses personally identifiable information to impersonate someone else.
- **Incident Response Plan** – An incident response policy is a plan outlying organization's response to an information security incident.
- **Internet of things (IoT)** – The Internet of Things, or IoT, refers to the billions of physical devices around the world that are now connected to the internet, collecting and sharing data.
- **IP Address** – An IP address is a unique 32-bit binary identifying number for a piece of network hardware. Having an IP address allows a device to communicate with other devices over an IP-based network like the internet.
- **IOS** – An operating system used for mobile devices manufactured by Apple.
- **Keystroke logger** – A keystroke logger is software that tracks or logs the keys struck on your keyboard, typically in a covert manner so that you are unaware actions are being monitored.
- **Malware** – Malware is shorthand for malicious software and is designed to cause damage to a computer, server, or computer network.
- **Malvertising** – The use of online advertising to deliver malware.
- **Man-in-the-Middle Attack:** Eavesdropping: when attacker secretly relays computer communication through themselves between two parties enabling them to compromise the integrity and confidentiality of the message.

- **Media:** means an instrument that is used with "hardware" and on which "electronic data", "programs and applications", and "proprietary programs" can be recorded or stored. "Media" includes, but is not limited to, films, tapes, cards, discs, drums, cartridges, cells, DVDs, CD-ROMs and other portable data devices.
- **Memory stick** – A memory stick is a small device that connects to a computer and allows you to store and copy information.
- **MP3** – MP3 is a means of compressing a sound sequence into a very small file, to enable digital storage and transmission.
- **Multi-Factor Authentication** – Multi-Factor Authentication (MFA) provides a method to verify a user's identity by requiring them to provide more than one piece of identifying information.
- **Packet Sniffer** – Software designed to monitor and record network traffic.
- **Padlock** – A padlock icon displayed in a web browser indicates a secure mode where communications between browser and web server are encrypted.
- **Patch** – A patch is a piece of software code that can be applied after the software program has been installed to correct an issue with that program.
- **Penetration testing** – Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.
- **Phishing** – Phishing is a method of trying to gather personal information using deceptive e-mails and websites.
- **Policy Management** – Policy Management is the process of creating, communicating, and maintaining policies and procedures within an organization.
- **Proxy Server** – A proxy server is another computer system which serves as a hub through which internet requests are processed.
- **Pre-texting** – Pre-texting is the act of creating a fictional narrative or pretext to manipulate a victim into disclosing sensitive information.
- **Ransomware** – A type of malicious software designed to block access to a computer system until a sum of money is paid.
- **Rootkit** – Rootkits are a type of malware designed to remain hidden on your computer.
- **Router** – A router is a piece of network hardware that allows communication between your local home network and the Internet.
- **Scam** – A scam is a term used to describe any fraudulent business or scheme that takes money or other goods from an unsuspecting person.
- **Scareware** – Scareware is a type of malware designed to trick victims into purchasing and downloading potentially dangerous software.
- **Security Awareness Training** – Security awareness training is a training program aimed at heightening security awareness within an organization.
- **Security Operations Centre (SOC)** – A SOC monitors an organization's security operations to prevent, detect and respond to any potential threats.
- **Server** – A server is a computer program that provides a service to another computer programs (and its user).
- **Smishing** – Smishing is any kind of phishing that involves a text message.
- **Spam** – Spam is slang commonly used to describe junk e-mail on the Internet.
- **Social Engineering** – Social engineering is the art of manipulating people, so they disclose confidential information.
- **Software** – Software is the name given to the programs you will use to perform tasks with your computer.

- **Spear Phishing** – Spear phishing is an email-spoofing attack that targets a specific organization or individual, seeking unauthorized access to sensitive information.
- **Spyware** – Spyware is a type of software that installs itself on a device and secretly monitors a victim's online activity.
- **Tailgating** – Tailgating involves someone who lacks the proper authentication following an employee into a restricted area.
- **Tablet** – A tablet is a wireless, portable personal computer with a touchscreen interface.
- **Traffic** – Web traffic is the amount of data sent and received by visitors to a website.
- **Trojan** – A Trojan is also known as Trojan horse. It is a type of malicious software developed by hackers to disguise as legitimate software to gain access to target users' systems.
- **Two-Factor Authentication** – Two-factor authentication (2FA), often referred to as two-step verification, is a security process in which the user provides two authentication factors to verify they are who they say they are.
- **USB** – USB (Universal Serial Bus) is the most popular connection used to connect a computer to devices such as digital cameras, printers, scanners, and external hard drives.
- **Username** – A username is a name that uniquely identifies someone on a computer system.
- **Virus** – A computer virus is a malicious software program loaded onto a user's computer without the user's knowledge and performs malicious actions.
- **VPN (Virtual Private Network**) – A virtual private network gives you online privacy and anonymity by creating a private network from a public Internet connection. VPNs mask your Internet protocol (IP) address, so your online actions are virtually untraceable.
- **Vulnerability** – A vulnerability refers to a flaw in a system that can leave it open to attack.
- **Vishing** – Vishing is the telephone equivalent of phishing. It is an attempt to scam someone over the phone into surrendering private information that will be used for identity theft.
- **Whaling** – Whaling is a specific form of phishing that's targeted at high-profile business executives and managers.
- **Whitehat** – White hat hackers perform penetration testing, test in-place security systems and perform vulnerability assessments for companies.
- **Wireless Hotspot** - A location where individuals can connect to the Internet wirelessly. This may be in a larger area in a public space or a small space created by a cell phone
- **Worm** – A computer worm is a malware computer program that replicates itself to spread to other computers.
- **Wi-Fi** – Wi-Fi is a facility that allows computers, smartphones, or other devices to connect to the Internet or communicate with one another wirelessly within a particular area.
- **Zero-Day** – Zero-Day refers to a recently discovered vulnerability that hackers can use to attack systems.

Online Glossaries:

International Association of Chiefs of Police: https://www.iacpcybercenter.org/resources-2/glossary/

Global Knowledge: https://www.globalknowledge.com/us-en/topics/cybersecurity/glossary-of-terms/

Ohio State University: https://cybersecurity.osu.edu/about/glossaries/cyber-dictionary