Basic Terminologies

**Adware** – Adware refers to any piece of software or application that displays advertisements on your computer.

**Anti-Virus Software** – Anti-virus software is a computer program used to prevent, detect, and remove malware.

**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.

**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.

**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.

**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 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.

**DDoS Attack** – A distributed denial-of-service (DDoS) attack is 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.

**Domain name** – The part of a network address which identifies it as belonging to a particular domain.

**Domain Name Server –** A server that converts recognisable domain names into their unique IP address

**Download** – To copy (data) from one computer system to another, typically over the Internet.

**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.

**Hacking** – Hacking refers to an unauthorised intrusion into a computer or a network.

**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 in order to impersonate someone else.

**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 an 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.

**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.

**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.

**Ransomware**– A type of malicious software designed to block access to a computer system until a sum of money is paid.

**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.

**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 give up 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 programme that secretly records what you do on your computer

**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

**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.

**Worm –** A computer worm is a malware computer program that replicates itself in order to spread to other computers.

**Bot** − A bot is a program that automates an action so that it can be done repeatedly at a much higher rate for a more sustained period than a human operator could do it. For example, sending HTTP, FTP or Telnet at a higher rate or calling script to create objects at a higher rate.

**Botnet** − A botnet, also known as zombie army, is a group of computers controlled without their owners’ knowledge. Botnets are used to send spam or make denial of service attacks.

**Brute force attack** − A brute force attack is an automated and the simplest kind of method to gain access to a system or website. It tries different combination of usernames and passwords, over and over again, until it gets in.

**Buffer Overflow** − Buffer Overflow is a flaw that occurs when more data is written to a block of memory, or buffer, than the buffer is allocated to hold.

**Clone phishing** − Clone phishing is the modification of an existing, legitimate email with a false link to trick the recipient into providing personal information.

**Cracker** − A cracker is one who modifies the software to access the features which are considered undesirable by the person cracking the software, especially copy protection features.

**Denial of service attack (DoS)** − A denial of service (DoS) attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet.

**DDoS** − A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example, a botnet) flooding the targeted system with traffic.

**Exploit Kit** − An exploit kit is software system designed to run on web servers, with the purpose of identifying software vulnerabilities in client machines communicating with it and exploiting discovered vulnerabilities to upload and execute malicious code on the client.

**Exploit**− Exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to compromise the security of a computer or network system.

**Firewall**− A firewall is a filter 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.

**Keystroke logging** − Keystroke logging is the process of tracking the keys which are pressed on a computer (and which touchscreen points are used). It is simply the map of a computer/human interface. It is used by gray and black hat hackers to record login IDs and passwords. Keyloggers are usually secreted onto a device using a Trojan delivered by a phishing email.

**Logic bomb** − A virus secreted into a system that triggers a malicious action when certain conditions are met. The most common version is the time bomb.

**Malware** − Malware is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.

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

**Phishing** − Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking emails, in an attempt to gather personal and financial information from recipients.

**Phreaker** − Phreakers are considered the original computer hackers and they are those who break into the telephone network illegally, typically to make free long distance phone calls or to tap phone lines.

**Rootkit** − Rootkit is a stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer.

**Shrink Wrap code** − A Shrink Wrap code attack is an act of exploiting holes in unpatched or poorly configured software.

**Social engineering** − Social engineering implies deceiving someone with the purpose of acquiring sensitive and personal information, like credit card details or user names and passwords.

**Spam** − A Spam is simply an unsolicited email, also known as junk email, sent to a large number of recipients without their consent.

**Spoofing** − Spoofing is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.

**Spyware**− Spyware is software that aims to gather information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.

**SQL Injection** − SQL injection is an SQL code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).

**Threat**− A threat is a possible danger that can exploit an existing bug or vulnerability to compromise the security of a computer or network system.

**Trojan** − 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 designed with an intention to destroy files, alter information, steal passwords or other information.

**Virus**− A virus is a malicious program or a piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.

**Vulnerability**− A vulnerability is a weakness which allows a hacker to compromise the security of a computer or network system.

**Worms**− A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself.

**Cross-site Scripting** − Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side script into web pages viewed by other users.

**Zombie Drone** − A Zombie Drone is defined as a hi-jacked computer that is being used anonymously as a soldier or 'drone' for malicious activity, for example, distributing unwanted spam e-mails.