**Attack:** An attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission. It happens to both individuals and organizations.

**Unauthorized Access:** A person gains logical or physical access without permission to a network, system, application, data, or other resource. Any access that violates the stated security policy.

**Hacker:** A Hacker is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.

**Threat:** Any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. Threats arise from human actions and natural events.

**Vulnerability:** A Security Vulnerability is a weakness, flaw, or error found within a security system that has the potential to be leveraged by a threat agent in order to compromise a secure network.

**Antivirus:** Antivirus software is a type of program designed and developed to protect computers from malware like viruses, computer worms, spyware, botnets, rootkits, keyloggers and such. Antivirus programs function to scan, detect and remove viruses from your computer.

**Social engineering:** is the act of exploiting human weaknesses to gain access to personal information and protected systems. Social engineering relies on manipulating individuals rather than hacking computer systems to penetrate a target's account.

**Virus:** A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk.

**Firewall:** A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.

**Phishing:** Phishing is a type of attack carried out to steal usernames, passwords, credit card information, Social Security numbers, and/or other sensitive data. Phishing is most often seen in the form of malicious emails pretending to be from credible sources like people, departments, or organizations related to the university.

**DOS:** A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor.

**DDOS:** DDoS (Distributed Denial of Service) is a category of malicious cyber-attacks that hackers or cybercriminals employ in order to make an online service, network resource or host machine unavailable to its intended users on the Internet.

**Botnet:** A botnet (short for “robot network”) is a network of computers infected by malware that are under the control of a single attacking party, known as the “bot-herder.” Each individual machine under the control of the bot-herder is known as a bot.

**Worm:** A computer worm is a type of malware that spreads copies of itself from computer to computer. A worm can replicate itself without any human interaction, and it does not need to attach itself to a software program in order to cause damage.

**Trojan:** A Trojan, or Trojan horse, is a type of malware that conceals its true content to fool a user into thinking it's a harmless file. Like the wooden horse used to sack Troy, the "payload" carried by a Trojan is unknown to the user, but it can act as a delivery vehicle for a variety of threats.

**Ransomware:** Ransom means money, Ransomware is a malware designed to deny a user or organization access to files on their computer. By encrypting these files and demanding a ransom payment for the decryption key, cyberattackers place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files.

**Breach**: A data breach is a security violation, in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Other terms are unintentional information disclosure, data leak, information leakage, and data spill.

**Exploit:** An exploit is a code that takes advantage of a software vulnerability or security flaw. It is written either by security researchers as a proof-of-concept threat or by malicious actors for use in their operations.

**Ip Address:** An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

**VPN:** VPN stands for "Virtual Private Network" and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data.

**Domain:** When we discuss data and information, we must consider the CIA triad. The CIA triad refers to an information security model made up of the three main components: confidentiality, integrity and availability. Each component represents a fundamental objective of information security.

A security domain is the list of objects a subject is allowed to access. More broadly defined, domains are groups of subjects and objects with similar security requirements. Confidential, Secret, and Top Secret are three security domains used by the U.S. Department of Defense (DoD)

**Adware:** adware is any piece of software, malicious or not, that displays advertisements on a computer. Most often, however, people use the word adware to refer to malicious software that shows deceptive ads, flashing pop-up windows, large banners, and full-screen auto-play commercials within their web browser.

**Attachment:** Attachments are files embedded within online communication channels such as emails, instant messages, or social networks. File attachments can come in any form, such as images, documents, or programs.

**Authentication:** The process of authentication in the context of computer systems means assurance and confirmation of a user's identity. Before a user attempts to access information stored on a network, he or she must prove their identity and permission to access the data.

**Backup:** A backup is a copy of the system or network's data for file restoration or archival purposes. Backups are an essential part of a continuity of operations plan as they allow for data protection and recovery.

**Backdoor:** An undocumented way of gaining access to computer system. A backdoor is a potential security risk.

**Bug:** A bug is a software-related problem. If something on a website or in an application does not work as intended, this “error” is called a bug

A security bug or security defect is a software bug that can be exploited to gain unauthorized access or privileges on a computer system. Security bugs introduce security vulnerabilities by compromising one or more of: Authentication of users and other entities. Authorization of access rights and privileges.

**Cookies:** What Are Cookies? Cookies are text files with small pieces of data — like a username and password — that are used to identify your computer as you use a computer network. Specific cookies known as HTTP cookies are used to identify specific users and improve your web browsing experience.

**DNS:** The Domain Name System (DNS) is the protocol that makes the Internet usable by allowing the use of domain names. DNS is widely trusted by organizations, and DNS traffic is typically allowed to pass freely through network firewalls.

**Hacking:** Hacking is an attempt to exploit a computer system or a private network inside a computer. Simply put, it is the unauthorised access to or control over computer network security systems for some illicit purpose.

**IOT:** In short, the Internet of Things refers to the rapidly growing network of connected objects that are able to collect and exchange data in real time using embedded sensors. Thermostats, cars, lights, refrigerators, and more appliances can all be connected to the IoT

**Patch:** In short, the Internet of Things refers to the rapidly growing network of connected objects that are able to collect and exchange data in real time using embedded sensors. Thermostats, cars, lights, refrigerators, and more appliances can all be connected to the IoT

**Crack:** Software cracking (known as "breaking" mostly in the 1980s) is the modification of software to remove or disable features which are considered undesirable by the person cracking the software, especially copy protection features (including protection against the manipulation of software, serial number, hardware key,

**Scam:** A scam is a term used to define a fraudulent business which takes money or other expensive good from an unsuspecting person. As everything s getting connected to the internet, online scam is increasing rapidly

**Spyware:** The defintion of spyware is a software program that secretly gathers personal information and sends it without the user's knowledge from a computer when it is online. An example of spyware is a adware software program that records a user's keystrokes on online advertisements and reports them to a research or ad firm.

**DMZ:** In computer security, a DMZ Network (sometimes referred to as a “demilitarized zone”) functions as a subnetwork containing an organization's exposed, outward-facing services. It acts as the exposed point to an untrusted networks, commonly the Internet.

**Gateway:** Security Gateway means a set of control mechanisms between two or more networks having different trust levels which filter and log traffic passing, or attempting to pass, between networks, and the associated administrative and management servers.

**Router:** A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. Data sent through the internet, such as a web page or email, is in the form of data packets.

**Hashing:** Hashing is an algorithm performed on data such as a file or message to produce a number called a hash (sometimes called a checksum). The hash is used to verify that data is not modified, tampered with, or corrupted. In other words, you can verify the data has maintained integrity.

**IDS:** An Intrusion Detection System (IDS) is a network security technology originally built for detecting vulnerability exploits against a target application or computer.

**IPS:** An intrusion prevention system (IPS) is a network security tool (which can be a hardware device or software) that continuously monitors a network for malicious activity and takes action to prevent it, including reporting, blocking, or dropping it, when it does occur.

**IP Spoofing:** IP spoofing, or IP address spoofing, refers to the creation of Internet Protocol (IP) packets with a false source IP address to impersonate another computer system. IP spoofing allows cybercriminals to carry out malicious actions, often without detection.

**Key Logger:** Keyloggers are activity-monitoring software programs that give hackers access to your personal data. The passwords and credit card numbers you type, the webpages you visit – all by logging your keyboard strokes. The software is installed on your computer, and records everything you type.

**Password Sniffing:** Password sniffing is an attack on the Internet that is used to steal user names and passwords from the network. Today, it is mostly of historical interest, as most protocols nowadays use strong encryption for passwords.

**Reverse engineering:** Reverse engineering (also known as backwards engineering or back engineering) is a process or method through which one attempts to understand through deductive reasoning how a previously made device, process, system, or piece of software accomplishes a task with very little (if any) insight into exactly how it does so.

**Malware:** Malware (short for “malicious software”) is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behavior an attacker wants. And because malware comes in so many variants, there are numerous methods to infect computer systems.

**Rootkit:** A rootkit allows someone to maintain command and control over a computer without the computer user/owner knowing about it. Once a rootkit has been installed, the controller of the rootkit has the ability to remotely execute files and change system configurations on the host machine.

**Macro Virus:** A macro virus is a small piece of code which is lodged into the macros of different documentation and software programs such as spreadsheets and word documents

**Exploit Kits:** Exploit Kits are basically the package of automated threats that are used by attackers to launch exploits against vulnerable programs