

### Bot

### This is a type of software application or script that performs tasks on command, allowing an attacker to take complete control remotely of an affected computer. A group of these infected computers is known as a “botnet” and is controlled by the hacker. E.g such as Amazon's Alexa, Apple's Siri and Google Assistant.

1. **Phishing**

This is a technique used by hackers to obtain sensitive information. For example, using hand-crafted email messages designed to trick people into divulging personal or confidential data such as passwords and bank account information.

1. **Encrypt key**

This is the process of encoding data to prevent theft by ensuring the data can only be accessed with a key.

1. **Pen-testing**

Short for “penetration testing,” is a means of evaluating security using hacker tools and techniques with the aim of discovering vulnerabilities and evaluating security flaws. E.g Using unencrypted passwords shared in the network to access sensitive databases.

1. **Clickjacking**

This is a form of hacking attack that tricks victims into clicking on an unintended link or button, usually disguised as a harmless element. E.g. Let’s say you clicked on a button that says “**Log In**," but instead of logging in, it's performing an entirely different action- like taking you to a YouTube link.

1. **White Hat**

This breaches a network to gain sensitive information with the owner’s consent – making it completely legal. This method is usually employed to test infrastructure vulnerabilities. E.g ethical hackers.

1. **Black hat**

These hackers break into networks to steal information that will be used to harm the owner or the users without consent. It’s entirely illegal. E.g None ethical

1. **Grey hat**

A self-appointed vigilante whose motivation is usually to do good, but his/her actions are not sanctioned by anyone, and thus, he violates the law. E.g None ethical

### Cloud

### This is a technology that allows us to access our files and/or services through the internet from anywhere in the world. Technically speaking, it’s a collection of computers with large storage capabilities that remotely serve requests. E.g One Driver and Dropbox.

### Software

A set of programs that tell a computer to perform a task. These instructions are compiled into a package that users can install and use. For example, Microsoft Office is an application software.

### Domain

A group of computers, printers and devices that are interconnected and governed as a whole. For example, your computer is usually part of a domain at your workplace. E.g .com (commercial), .net (network), gov (government), .edu (educational), .org (organization

### Virtual Private Network (VPN)

A tool that allows the user to remain anonymous while using the internet by masking the location and encrypting traffic. E.g ExpressVPN, OpenVPN and Private Internet Access is a personal VPN.

### IP Address

An internet version of a home address for your computer, which is identified when it communicates over a network; For example, connecting to the internet (a network of networks). E.g 506.457.14.512

### Exploit

A malicious application or script that can be used to take advantage of a computer’s vulnerability. E.g Hardware: Poor encryption and Network: Unencrypted communication lines.

### Breach

The moment a hacker successfully exploits a vulnerability in a computer or device, and gains access to its files and network. E.g Cyberattacks, Lost devices, and Human error.

### Firewall

A form of defensive technology designed to keep the bad guys out. Firewalls can be hardware or software-based. E.g packet filtering firewall, next-generation firewall, circuit-level gateway.

### Malware

An umbrella term that describes all forms of malicious software designed to wreak havoc on a computer. Common forms include: viruses, trojans, worms and ransomware.

### Virus

A type of malware aimed to destroy, erase or modify information on a computer before spreading to others. However, in more recent years, viruses like [Stuxnet](https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/) have caused physical damage. E.g SQL Slammer, CryptoLocker and Morris Worm.

### Ransomware

A form of malware that deliberately prevents you from accessing files on your computer – holding your data hostage. It will typically encrypt files and request that a ransom be paid in order to have them decrypted or recovered. For example, [WannaCry Ransomware](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack), Bad Rabbit, Locky.

**Trojan horse**

This is a type of malware that often allows a hacker to gain remote access to a computer through a “back door”. E.g DDS, Rootkit Trojans, Remote Access Trojans

### Worm

A type of malware that can replicate itself in order to spread the infection to other connected computers. E.g Morris Worm, ILOVEYOU worm.

### Spyware

A type of malware that functions by spying on user activity without their knowledge. The capabilities include activity monitoring, collecting keystrokes, data harvesting (account information, logins, financial data), and more. E.g HawkEye, Look2Me.

1. **Adware**

Adware bombards users with endless ads and pop-up windows and cause a nuisance to user experience. Adware can also pose a real danger to devices and the unwanted ads can include malware or redirect user searches to malicious websites that collect personal data about users. Adware programs are often built into freeware or shareware programs, where the adware operator collects an indirect fee for using the program. Adware programs usually do not show themselves in the system in any way. Adware programs seldom include a de-installation procedure, and attempts to remove them manually may cause the original carrier program to malfunction. E.g DeskAd.

### Rootkit

Another form of malware that allows cybercriminals to [remotely control](https://us.norton.com/internetsecurity-malware-what-is-a-rootkit-and-how-to-stop-them.html) your computer. Rootkits are especially damaging because they are hard to detect, making it likely that this type of malware could live on your computer for a long time. E.g NTRootkit

### DDoS

An acronym which stands for distributed denial of service – a form of cyber-attack. This attack aims to make a service such as a website unusable by “flooding” it with malicious traffic or data from multiple sources (often botnets).

1. **Authentication**

This is the process of verifying the identity of a user’s information and the legitimacy of information provided. In computing, it is the process of identifying a person or system with the username, password, etc. Authentication helps individuals and systems gain authorization based on their identity and prevent unauthorized access. E.g voice recognition, and fingerprints.

1. **Backdoor**

This is used by attackers to gain access to a computer or a network. A programmer may bypass security steps and gain access to a computer by trapdoor programs, in the event of an attack on the computer system or networks. Attackers may also use such mechanisms to enter computers or networks without proper permission. E.g PoisonTap

1. **Brute Force Attack**

This is a method for guessing a password (or the key used to encrypt a message) that involves systematically trying a high volume of possible combinations of characters until the correct one is found. One way to reduce the susceptibility to a Brute Force Attack is to limit the number of permitted attempts to enter a password – for example, by allowing only three failed attempts and then permitting further attempts only after 15 minutes.

1. **Business Continuity Plan**

A Business Continuity Plan is an organization’s playbook for how to operate in an emergency situation, like a massive cyberattack. The business continuity plan provides safeguards against a disaster, and outlines the strategies and action plan on how to continue business as usual in the event of any large-scale cyber event. E.g IT disruptions to networks, servers, personal computers and mobile devices.

1. **Business Disruption**

The term Business Disruption refers to any interruption in the usual way that a system, process, or event works. Cyberattacks cause disruption to business operations and the associated risk of losses to the organization. E.g e-commerce, online news sites.

1. **CAPTCHA**

A CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a challenge response to test commonly used websites to verify the user is a real human and not a bot or computer. They can include simple arithmetic and questions about images that bots have difficulty answering. E.g randomly generated sequence of letters and/or numbers

1. **Cyberbullying**

Cyberbullying is primarily messaging persons on social media platforms, to bully and harass them. Cyberbullying has become a major problem, especially affecting young people, as it allows bullies to magnify their aggressive behavior, publicly ridicule victims on a large scale, and carry out damaging activities in a way that is difficult for parents and teachers to detect.

1. **Cybersecurity**

Cybersecurity relates to processes employed to safeguard and secure assets used to carry information of an organization from being stolen or attacked. It requires extensive knowledge of the possible threats such as viruses or such other malicious objects. Identity management, risk management and incident management form the crux of cybersecurity strategies of an organization. E.g VPNs

1. **Dark Web**

The Dark Web is encrypted parts of the internet that are not indexed by search engines, most notoriously used by all types of criminals including; pedophiles, illicit human and contraband traffickers, and cybercriminals, to communicate and share information without being detected or identified by law enforcement. Malware of all types can be purchased on the dark web. A subset of the deep web, which can be accessed by anyone with the correct URL, dark web pages need special software (ex. Tor) with the correct decryption key and access rights and knowledge to find content. Users of the dark web remain almost completely anonymous due to its P2P network connections which makes network

1. **Data Breach**

A Data Breach is the event of a hacker successfully exploiting a network or device vulnerability and gaining access to its files and data.activity very difficult to trace.

1. **Data Integrity**

Data Integrity is a broad term that refers to the maintenance and assurance of data quality. This includes the accuracy and consistency of data over its entire lifecycle. Data Integrity is an important part of the design, implementation and use of any data system which stores, processes, or retrieves information. The term is broad in scope and may have widely different meanings depending on the specific context. E.g database on servers

1. **Data Loss Prevention (DLP)**

Data Loss Prevention (DLP) is an umbrella term for a collection of security tools, processes and procedures that aim to prevent sensitive data from falling into unauthorized or malicious hands. DLP aims at preventing such occurrences through various techniques such as strict access controls on resources, blocking or monitoring email attachments, preventing network file exchange to external systems, blocking cut-and-paste, disabling use of social networks and encrypting stored data.

1. **Data Theft**

Data Theft is the deliberate theft of sensitive data by nefarious persons.

1. **Decryption**

Decryption is the process of decoding cipher text to plain text, so it is readable by humans. It is the reverse of encryption, the process of converting plaintext to cipher text. Cybercriminals use decryption software and techniques to ‘break’ security encryption and gain access to protected information.

1. **Detection and Response**

Network Detection and Response is a security solution category used by organizations to detect malicious network activity, perform forensic investigation to determine root cause, and then respond and mitigate the threat.

1. **Digital Forensics**

Digital Forensics is the process of procuring, analyzing, and interpreting electronic data for the purpose of presenting it as legal evidence in a court of law.

1. **Digital Transformation**

Digital Transformation is the process of using digital technologies to create or modify business processes and customer experiences to keep up-to-date with current business and market requirements. E.g 5G

1. **Domain Name Systems (DNS) Exfiltration**

Domain Name System (DNS) Exfiltration is a lower level attack on DNS servers to gain unauthorized access. Such attacks are difficult to detect and can lead to loss of data.

1. **Endpoint Protection**

Endpoint Protection refers to a system for network security management that monitors network endpoints, hardware devices such as workstations and mobile devices from which a network is accessed.

1. **Endpoint Detection and Response (EDR)**

Endpoint Detection and Response (EDR) are tools for protecting computer endpoints from potential threats. EDR platforms comprise software and networking tools for detecting suspicious endpoint activities, usually via continuous monitoring.

1. **Fast Identity Online (FIDO)**

Fast Identity Online (FIDO) is a set of open authentication standards that enable a service provider to leverage existing technologies for passwordless authentication.

1. **Fileless Malware**

Fileless Malware (FM), aka “non-malware,” or “fileless infection,” is a form of malicious computer attack that exists exclusively within the realm of volatile data storage components such as RAM, in memory processes, and service areas. This differentiates this form of malware from the classic memory-resident virus which requires some contact with non-volatile storage media, such as a hard disk drive or a thumb drive. Normally picked up following visits to malicious websites, fileless malware does not exist as a file that can be detected by standard antivirus programs. It lurks within a computer’s working memory and is exceptionally difficult to identify. However, this type of malware rarely survives a computer reboot, after which the computer should work as it did prior to infection.

1. **Honeypot**

Honeypots are computer security programs that simulate network resources that hackers are likely to look for to lure them in and trap them. An attacker may assume that you’re running weak services that can be used to break into the machine. A honeypot provides you advanced warning of a more concerted attack. Two or more honeypots on a network form a honeynet.

1. **Identity and Access Management (IAM)**

Identity and Access Management (IAM) is the process used by an organization to grant or deny access to a secure system. IAM is an integration of work flow systems that involves organizational think tanks who analyze and make security systems work effectively.

1. **Identity theft**

Theft Identity Theft occurs when a malicious actor gathers enough personal information from the victim (name, address, date of birth, etc.) to enable him to commit identity fraud – i.e., the use of stolen credentials to obtain goods or services by deception. Stolen data can be used to create a new account in the victim’s name (e.g., a bank account), to take over an existing account held by the victim (e.g., a social network account), or to masquerade as the victim while carrying out criminal activities.

1. **IoT**

The term Internet of Things (IoT) is used to describe everyday objects that are connected to the internet and are able to collect and transfer data automatically, without the need for human interaction. The Internet of Things encompasses any physical object (not just traditional computers) that can be assigned an IP address and can transfer data: this includes household appliances, utility meters, cars, CCTV cameras, and even people (e.g., heart implants).

1. **Cyberspace**

cyberspace, an amorphous, supposedly “virtual” world created by links between computers, Internet-enabled devices, servers, routers, and other components of the Internet’s infrastructure.

1. A **man-in-the-middle attack (MITM)**

is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other. For example, a victim believes he’s connected to his bank’s web site and the flow of traffic to and from the real bank site remains unchanged, so the victim sees nothing suspicious. However, the traffic is redirected through the attacker’s site, allowing the attacker to gather any personal data entered by the victim (login, password, PIN, etc.).

1. **Sandbox**

A sandbox is an isolated environment on a network that mimics end-user operating environments. Sandboxes are used to safely execute suspicious code without risking harm to the host device or network.

1. **Spam**

Is the name commonly given to unsolicited email. Essentially unwanted advertising, it’s the email equivalent of physical junk mail delivered through the post.

1. **Spoofing**

A Spoof is an attack attempt by an unauthorized entity or attacker to gain illegitimate access to a system by posing as an authorized user. Spoofing includes any act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address.

1. **Spyware**

Is software that is secretly installed on a user’s device to gather sensitive data. Spyware quietly collects information such as credentials and sends it outside the network to bad actors. Spyware often comes in the form of a free download and is installed automatically, with or without user consent.

1. **Threat Assessment**

Is a structured process used to identify and evaluate various risks or threats that an organization might be exposed. Cyber threat assessment is a crucial part of any organization’s risk management strategy and data protection efforts.

1. **Zero-day Exploit**

This term is used to describe exploit code that has been written to take advantage of a vulnerability before the software vendor knows about it and can publish a patch for it. The result is that would-be attackers are free to exploit the vulnerability, unless proactive exploit prevention technologies have been implemented to defend the computer being targeted by the attacker.

1. **Cookies**

Are little pieces of plain text shipped to your browser by a website you visit. This is sent by a server to the browser and is returned to the server every time it accesses the website. This is utilized to identify the user or track their access to the server.

1. **Intellectual Property**

IP short for Intellectual Property is intangible property that is the result of creativity, such as patents, copyrights, etc. Cyber theft of Intellectual Property (IP) is also one threat. Cyber theft of IP means stealing copyrights, trade secrets, patents, etc., using the internet and computers.

1. **Internet fraud**

is a type of cybercrime that makes use of the internet and it can be considered a general term that groups all of the crimes that happen over the internet like spam, banking frauds, theft of service, etc.

1. **ARPANET**

The first internet that was born this network took advantage of a new idea at the time called packet switching.

1. **TCP Transmission Control Protocol**

TCP stands for Transmission Control Protocol, a communications standard that enables application programs and computing devices to exchange messages over a network. It is designed to send packets across the internet and ensure the successful delivery of data and messages over networks.

64. **IP address stands**

For internet protocol address; it is an identifying number that is associated with a specific computer or computer network. When connected to the internet, the IP address allows the computers to send and receive information.

66. The dot-com boom started in 1995

67. **SSL protocol (Secure Sockets Layer)**

was developed and introduced by Netscape in February 1995.

68. **Voice over Internet protocol**

Voice-over-Internet protocol (VoIP) is communications technology that allows users to interact by audio through an Internet connection, rather than through an analog connection. Voice-over-Internet Protocol converts the voice signal used in traditional phone technology into a digital signal that travels through the Internet instead of through analog telephone lines.

69. **HTML (Hypertext Markup Language)**

HTML provides the basic structure for web pages. It consists of a series of commands, known as tags, that instruct a browser on how to interpret content. For example, specific HTML tags indicate a page’s headline, where a new paragraph begins, when text should be boldfaced or italicized and when to link to another document.

70. **XML (extensible markup language)**

Extensible Markup Language, or "XML," is a computer programming language designed to transmit both data and the meaning of the data. XML accomplishes this by being a markup language, a mechanism that identifies different structures within a document. Structured information contains both content (such as words, pictures, or video) and an indication of what role content plays, or its meaning. XML identifies different structures by assigning data "tags" to define both the name of a data element and the format of the data within that element. Elements are combined to form objects.

71.**Ethical**  
Ethics in cyber security is about what decisions are aligned with our values and what is morally acceptable for both the data owner and the organization. Ethical standards should also describe how to implement processes for ensuring ethical decision-making.

72. **Internet privacy**

This are general practices and strategies to keep one’s information safe from public view.

73. **Net**

This is the abbreviated form of the internet

74**. Network**

This is a series of interconnected computers, devices and or servers.\

75. **E-commerce**

This is business and commercial processes that take place over the internet with the use of a debit or credit card.

76. **Browser**

This is an application or software installed on a device designed to allow access to the internet and also to allow navigation between multiple webpages.

77. Biometrics

This is the use of biological identification factors to distinguish and identify a user. For example, this could be the use of fingerprints or the scanning of the retina.

78. **Cryptography**

This is the protection of information or hiding its meaning by converting it into a secret code before sending it out over a public network to guard the owner or organization information.

79. **Back** **door**

A type of vulnerability intentionally left behind by developers as an alternative means of accessing a programme or application.

80. **Privacy Policy**

This is a legal documentation that informs a user how their data is collected and managed.