UNIT -1

INTRODUCTION TO CYBER CRIME

Cyber Security

The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cybersecurity. We can divide cybersecurity into two parts one is cyber, and the other is security. Cyber refers to the technology that includes systems, networks, programs, and data. And security is concerned with the protection of systems, networks, applications, and information. In some cases, it is also called **electronic information security** or **information technology security**.

Some other definitions of cybersecurity are:

"Cyber Security is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access."

"Cyber Security is the set of principles and practices designed to protect our computing resources and online information against threats."

Types of Cyber Security

- **Network Security:** It involves implementing the hardware and software to secure a computer network from unauthorized access, intruders, attacks, disruption, and misuse. This security helps an organization to protect its assets against external and internal threats.
- **Application Security:** It involves protecting the software and devices from unwanted threats. This protection can be done by constantly updating the apps to ensure they are secure from attacks. Successful security begins in the design stage, writing source code, validation, threat modeling, etc., before a program or device is deployed.
- **Information or Data Security:** It involves implementing a strong data storage mechanism to maintain the integrity and privacy of data, both in storage and in transit.
- **Identity management:** It deals with the procedure for determining the level of access that each individual has within an organization.
- **Operational Security:** It involves processing and making decisions on handling and securing data assets.
- **Mobile Security:** It involves securing the organizational and personal data stored on mobile devices such as cell phones, computers, tablets, and other similar devices against

various malicious threats. These threats are unauthorized access, device loss or theft, malware, etc.

- **Cloud Security:** It involves in protecting the information stored in the digital environment or cloud architectures for the organization. It uses various cloud service providers such as AWS, Azure, Google, etc., to ensure security against multiple threats.
- **Disaster Recovery and Business Continuity Planning:** It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the same operating capacity as before the event.
- **User Education:** It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the same operating capacity as before the event.

Cyber Security Goals

Cyber Security's main **objective is to ensure data protection**. The security community provides a triangle of three related principles to protect the data from cyber-attacks. This principle is called the **CIA triad**. The CIA model is designed to guide policies for an organization's information security infrastructure. When any security breaches are found, one or more of these principles has been violated.

We can break the **CIA model into three parts**: Confidentiality, Integrity, and Availability. It is actually a security model that helps people to think about various parts of IT security. Let us discuss each part in detail.

1. **Confidentiality:** Confidentiality is equivalent to privacy that avoids unauthorized access of information. It involves ensuring the data is accessible by those who are allowed to use it and blocking access to others. It prevents essential information from reaching the wrong people. **Data encryption** is an excellent example of ensuring confidentiality.
2. **Integrity:** This principle ensures that the data is authentic, accurate, and safeguarded from unauthorized modification by threat actors or accidental user modification. If any modifications occur, certain measures should be taken to protect the sensitive data from corruption or loss and speedily recover from such an event. In addition, it indicates to make the source of information genuine.
3. **Availability:** This principle makes the information to be available and useful for its authorized people always. It ensures that these accesses are not hindered by system malfunction or cyber-attacks.

Cyber Crime

Cybercrime or a computer-oriented crime is a crime that includes a computer and a network. The computer may have been used in the execution of a crime or it may be the target. Cybercrime is the use of a computer as a weapon for committing crimes such as committing fraud, identity theft, or breaching privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to every field like commerce, entertainment, and government. Cybercrime may endanger a person or a nation's security and financial health. Cybercrime encloses a wide range of activities, but these can generally be divided into two categories:

1. Crimes that aim at computer networks or devices. These types of crimes involve different threats (like virus, bugs etc.) and denial-of-service (DoS) attacks.
2. Crimes that use computer networks to commit other criminal activities. These types of crimes include cyber stalking, financial fraud or identity theft.

Classification of Cyber Crime:

1. **Cyber Terrorism –**
   Cyber terrorism is the use of the computer and internet to perform violent acts that result in loss of life. This may include different type of activities either by software or hardware for threatening life of citizens.
   In general, Cyber terrorism can be defined as an act of terrorism committed through the use of cyberspace or computer resources.

2. **Cyber Extortion –**
   Cyber extortion occurs when a website, e-mail server or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand huge money in return for assurance to stop the attacks and to offer protection.

3. **Cyber Warfare –**
   Cyber warfare is the use or targeting in a battle space or warfare context of computers, online control systems and networks. It involves both offensive and defensive operations concerning to the threat of cyber attacks, espionage and sabotage.

4. **Internet Fraud –**
   Internet fraud is a type of fraud or deceit which makes use of the Internet and could include hiding of information or providing incorrect information for the purpose of deceiving victims for money or property. Internet fraud is not considered a single, distinctive crime but covers a range of illegal and illicit actions that are committed in cyberspace.

5. **Cyber Stalking –**
   This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. In this case, these stalkers know their victims and instead of offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.

Challenges of Cyber Crime:

1. **People are unaware of their cyber rights-** The Cybercrime usually happen with illiterate people around the world who are unaware about their cyber rights implemented by the government of that particular country.

2. **Anonymity-** Those who Commit cybercrime are **anonymous** for us so we cannot do anything to that person.

3. **Less numbers of case registered-** Every country in the world faces the challenge of cybercrime and the rate of cybercrime is increasing day by day because the people who even don't register a case of cybercrime and this is major challenge for us as well as for authorities as well.

4. **Mostly committed by well educated people-** Committing a cybercrime is not a cup of tea for every individual. The person who commits cybercrime is a very **technical** person so he knows how to commit the crime and not get caught by the authorities.

5. **No harsh punishment-** In Cybercrime there is no harsh punishment in every cases. But there is harsh punishment in some cases like when somebody commits cyber terrorism in that case there is harsh punishment for that individual. But in other cases there is no harsh punishment so this factor also gives encouragement to that person who commits cybercrime.

Prevention of Cyber Crime:
Below are some points by means of which we can prevent cybercrime:

1. **Use strong password –** Maintain different password and username combinations for each account and resist the temptation to write them down. Weak passwords can be easily cracked using certain attacking methods like Brute force attack, Rainbow table attack etc, So make them complex. That means combination of letters, numbers and special characters.

2. **Use trusted antivirus in devices –** Always use trustworthy and highly advanced antivirus software in mobile and personal computers. This leads to the prevention of different virus attack on devices.

3. **Keep social media private –**Always keep your social media accounts data privacy only to your friends. Also make sure only to make friends who are known to you.

4. **Keep your device software updated –**Whenever you get the updates of the system software update it at the same time because sometimes the previous version can be easily attacked.

5. **Use secure network –**Public Wi-Fi are vulnerable. Avoid conducting financial or corporate transactions on these networks.

6. **Never open attachments in spam emails –**A computer get infected by malware attacks and other forms of cybercrime is via email attachments in spam emails. Never open an attachment from a sender you do not know.

7. **Software should be updated –** Operating system should be updated regularly when it comes to internet security. This can become a potential threat when cybercriminals exploit flaws in the system.

Cyber Criminals

Cybercrime is taken very seriously by law enforcement. In the early long periods of the cyber security world, the standard cyber criminals were teenagers or hobbyists in operation from a home laptop, with attacks principally restricted to pranks and malicious mischief. Today, the planet of the cyber criminals has become a lot of dangerous. Attackers are individuals or teams who attempt to exploit vulnerabilities for personal or financial gain.

Types of Cyber Criminals:

1. Hackers: The term hacker may refer to anyone with technical skills, however, it typically refers to an individual who uses his or her skills to achieve unauthorized access to systems or networks so as to commit crimes. The intent of the burglary determines the classification of those attackers as white, grey, or black hats. White hat attackers burgled networks or PC systems to get weaknesses so as to boost the protection of those systems. The owners of the system offer permission to perform the burglary, and they receive the results of the take a look at. On the opposite hand, black hat attackers make the most of any vulnerability for embezzled personal, monetary or political gain. Grey hat attackers are somewhere between white and black hat attackers. Grey hat attackers could notice a vulnerability and report it to the owners of the system if that action coincides with their agenda.

- **(a). White Hat Hackers –** These hackers utilize their programming aptitudes for a good and lawful reason. These hackers may perform network penetration tests in an attempt to compromise networks to discover network vulnerabilities. Security vulnerabilities are then reported to developers to fix them and these hackers can also work together as a blue team. They always use the limited amount of resources which are ethical and provided by the company, they basically perform pentesting only to check the security of the company from external sources.
- **(b). Gray Hat Hackers –** These hackers carry out violations and do seemingly deceptive things however not for individual addition or to cause harm. These hackers may disclose a vulnerability to the affected organization after having compromised their network and they may exploit it .
- **(c). Black Hat Hackers –** These hackers are unethical criminals who violate network security for personal gain. They misuse vulnerabilities to bargain PC frameworks. theses hackers always exploit the information or any data they got from the unethical pentesting of the network.

2. Organized Hackers: These criminals embody organizations of cyber criminals, hacktivists, terrorists, and state-sponsored hackers. Cyber criminals are typically teams of skilled criminals targeted on control, power, and wealth. These criminals are extremely subtle and organized, and should even give crime as a service. These attackers are usually profoundly prepared and well-funded.

3. Internet stalkers: Internet stalkers are people who maliciously monitor the web activity of their victims to acquire personal data. This type of cyber crime is conducted through the

use of social networking platforms and malware, that are able to track an individual's PC activity with little or no detection.

4. Disgruntled Employees: Disgruntled employees become hackers with a particular motive and also commit cybercrimes. It is hard to believe that dissatisfied employees can become such malicious hackers. In the previous time, they had the only option of going on strike against employers. But with the advancement of technology there is increased in work on computers and the automation of processes, it is simple for disgruntled employees to do more damage to their employers and organization by committing cybercrimes.

Cyber-crime: A Global Perspective

Cybersecurity constitutes one of the top five risks of most firms, especially in Big Tech and Banking & Financial Services. A weekend reading led to some interesting data points from various sources such as AV-Test and Coveware, among others, and that further led to me pondering over the mitigating actions that we can take as individuals and as organisations for some, if not all, of these cybercrime risks. I extend my thanks to the respective experts who shared their knowledge, enabling me to piece together some parts of the larger jigsaw puzzle.

Global cybercrime damage costs this year are expected to breach US $6 trillion an annum. That is almost one-fourth of the US GDP or twice the GDP of India. This is expected to scale up to US $10.5 trillion an annum by 2025. Cyber attackers are disrupting critical supply chains, at least 4 times more than in 2019.

Yet, approximately 4 of every 5 organisations don't consider themselves having proper responses to cyber-attacks which creates a need for a cybersecurity risk management team for them. Let's have a look at the individual components

Malware - Total Malware expected to exceed 1.2 billion samples in 2021 and is averaging approx. 18 million new malware samples every month (Source AV-Test). Approximately 94 % of this malware is polymorphic, i.e., can constantly change its identifiable features to evade detection.

Ransomware - Average ransom payment peaked in Q3 2020 at ~US $234k but decreased to ~US $154k in Q4 2020. The threat to leak exfiltrated data was up 43% during this period. (Source: Coveware). Sodinokibi, Egregor, Ryuk, Netwalker and Maze are the top-ranked ransomware by market share.

Data Breach - In 2020, the average cost of a data breach was ~US $3.9 million. Data privacy and cybersecurity risk are major concerns that are seeing more regulation created, for example, GDPR (EU), PDP(India) etc. Unfortunately, data breaches take time to be detected.

Phishing - More than 80% of reported security incidents were in the form of phishing attempts.

Cybercrime Era: Survival Mantra for the Netizens.

The term "Netizen" was coined by Michael Hauben. Quite simply, "Netizens" are the Internet users.

"Netizen" is someone who spends considerable time online and also has a considerable presence online (through websites about the person, through his/her active blogc ontribute and/or also his/her participation in the online chat rooms).

The 5P Netizen mantra for online security is:

- **Precaution**
- **Prevention**
- **Protection**
- **Preservation**
- **Perseverance.**

- For ensuring the motto for the "Netizen" should be "Stranger is Danger!" If you protect your customer's our employee's privacy and your own company.
- Then you are doing your job in the grander scheme of the things to regulate and enforce rules on the Net through our community.
- NASSCOM urges that cybercrime awareness is important, and any matter should bere ported at once.
- This is the reason they have established cyber labs across major cities in India.
- More importantly, users must try and save any electronic information trail on their computers.
- That is all one can do until laws become more stringent or technology more advanced.
- There are agencies that are trying to provide guidance to innocent victims of cybercrimes. However, these NGO like efforts cannot provide complete support to the victims of cybercrimes and are unable to get the necessary support from the Police.

The need for a statutorily empowered agency to protect abuse of ITA 2000 in India was, therefore, a felt need for quite some time.

Cyber offenses: how criminals plan the attacks

Criminals use many methods and tools to locate the vulnerabilities of their target. The target can be an individual and/or an organization. Criminals plan passive and active attacks. Active attacks are usually used to alter the system, whereas passive attacks attempt to gain information

about the target. Active attacks may affect the availability, integrity and authenticity of data whereas passive attacks lead to breaches of confidentiality.

In addition to the active and passive categories, attacks can be categorized as either inside or outside. An attack originating and/or attempted within the security, perimeter of an organization is an inside attack. it is usually attempted by an "insider" who gains access to more resources. than expected. An outside attack is attempted by a source outside the security perimeter, maybe attempted by an insider and/or an outsider, who is indirectly associated with the organization, it is attempted through the Internet or a remote access connection.

The following phases are involved in planning cybercrime:

1. Reconnaissance (information gathering) is the first phase and is treated as passive attacks.
2. Scanning and scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities.
3. Launching an attack (gaining and maintaining the system access).

1. Reconnaissance

The literal meaning of "Reconnaissance" is an act of reconnoitering- explore, often with the goal of finding something or somebody (especially to gain information about an enemy or potential enemy).

In the world of "hacking," reconnaissance phase begins with "Footprinting" - this is the preparation toward preattack phase, and involves accumulating data about the target's environment and computer architecture to find ways to intrude into that environment. Footprinting gives an overview about system vulnerabilities and provides a judgment about possible exploitation of those vulnerabilities. The objective of this preparatory phase is to understand the system, its networking ports and services, and any other aspects of its security that are needful for launching the attack.Thus, an attacker attempts to gather information in two phases: passive and active attacks.

2. Passive Attacks

A passive attack involves gathering information about a target without his/her (individual's or company's) knowledge. It can be as simple as watching a building to identify what time employees enter the building's premises. However, it is usually done using Internet searches or by Googling (i,e., searching the required information with the help of search engine Google) an individual or company to gain information.

1. Google or Yahoo search: People search to locate information about employees.
2. Surfing online community groups like Orkut/Facebook will prove useful to gain the information about an individual.
3. Organization's website may provide a personnel directory or information about key employees, for example, contact details, E-Mail address, etc. These can be used in a social engineering attack to reach the target.
4. Blogs, newsgroups, press releases, etc. are generally used as the mediums to gain information about the company or employees.
5. Going through the job postings in particular job profiles for technical persons can provide information about type of technology, that is, servers or infrastructure devices a company maybe using on its network.

3. Active Attacks

An active attack involves probing the network to discover individual hosts to confirm the information (IP addresses, operating system type and version, and services on the network) gathered in the passive attack, phase. It involves the risk of detection and is also called "Rattling the doorknobs" or "Active reconnaissance."

Active reconnaissance can provide confirmation to an attacker about security measures in place,, but the process can also increase the chance of being caught or raise suspicion.

4. Scanning and Scrutinizing Gathered Information

Scanning is a key step to examine intelligently while gathering information about the target. The objectives of scanning are as follows:

1. **Port scanning:** Identify open/close ports and services.
2. **Network scanning:** Understand IP Addresses and related information about the computer network systems.
3. **Vulnerability scanning:** Understand the existing weaknesses in the system.

The scrutinizing phase is always called "enumeration" in the hacking world. The objective behind this step is to identify:

1. The valid user accounts or groups;
2. Network resources and/or shared resources
3. OS and different applications that are running on the OS.

5. Attack (Gaining and Maintaining the System Access)

After the scanning and enumeration, the attack is launched using the following steps:

1. Crack the password
2. Exploit he password
3. Execute the malicious command/applications;
4. Hide the files (if required);
5. Cover the tracks - delete the access logs, so that there is no trail illicit activity.

Social Engineering

Social engineering is a manipulation technique that exploits human error to obtain private information or valuable data. In cybercrime, the human hacking scams entice unsuspecting users to disclose data, spread malware infections, or give them access to restricted systems. Attacks can occur online, in-person, and by other interactions. Social engineering scams are based on how people think and act.

Hackers try to exploit the user's knowledge. Thanks to technology's speed, many consumers and employees are not aware of specific threats such as drive-by downloads. Users cannot realize the value of personal data like phone number. Many users are unsure of how best to protect themselves and their confidential information. Social engineering attackers have two goals:

1. Subversion: Interrupting or corrupting data due to loss or inconvenience.
2. Theft: Obtaining valuable items such as information, access or

How does social engineering work?

Most social engineering attacks depend on real communication between attackers and victims. Instead of using brute force methods to breach the data, the attacker prompts the user to compromise.

The attack cycle gives the criminals a reliable process to deceive you. The stages of the social engineering attack cycle are below:

- Prepare by gathering background information on a large group.
- Infiltrate by building trust, establishing a relationship or starting a conversation.
- Establish the victim once more to confront the attack with confidence and weakness.
- Once the user takes the desired action, release it.

Many employees and consumers are unaware that certain information can give hackers access to multiple networks and accounts.

By sending messages for IT support personnel as legitimate users, they grab your details - such as name, date of birth or address. It is a simple matter to reset the password and get almost unlimited access. They can steal money, spread social engineering malware, and many more.

Cyberstalking

Cyberstalking does not always include face-to-face contact, and some victims may not even be aware that they are being followed online. Numerous techniques can be employed to keep tabs on the victims, and the data acquired may then be utilised to commit crimes like identity theft. Some stalkers even contact the victims' acquaintances and continue their harassment offline.

What is the Meaning of Cyberstalking?

Cyberstalking is a type of online crime. Internet-related terms like "cyber" and "stalking" refer to the practise of looking into someone's online activity on social media or through other online techniques. In other words, it means simply keeping eyes on other’s activities with the help of computer and internet.

Purpose of Cyberstalking

Purpose of cyber staking may be positive or negative. If someone stalking someone to cheat, to scam, or with the intention to harm by any means, covered under negative purpose. On the other hand, if someone stalking (usually, government agency or family members/friends) with the intention to provide security, then it is covered under positive purpose. Furthermore, some of the government agencies (through cyber stalking) keep eyes on suspected people so that they can protect the national security.

Examples of Cyberstalking

Cyberstalking can take many different forms, such as harassing, embarrassing, and humiliating the victim, draining bank accounts, or exercising other forms of financial control, such damaging the victim's credit, pestering the victim's family, friends, and employers to isolate them through fear-mongering techniques, and more

Types of Cyberstalking

Major types of cyber stalking are −

Direct Cyberstalking

Offenders may send their victims emails directly or deluge their inboxes with emails. Or, they might bother them through IM, voicemail, texts, or other electronic means of communication. They may employ technology to watch over, track, or constantly browse the pages of their victims – frequently without their awareness.

Indirect Cyberstalking

Attacks involving indirect cyberstalking could result in device damage for the victim. They might accomplish this by infecting it with ransomware, which would lock its files and demand payment to unlock them. Alternately, they might put in a virus or key logger that keeps track of the victim's online activities and/or takes information from the target device.

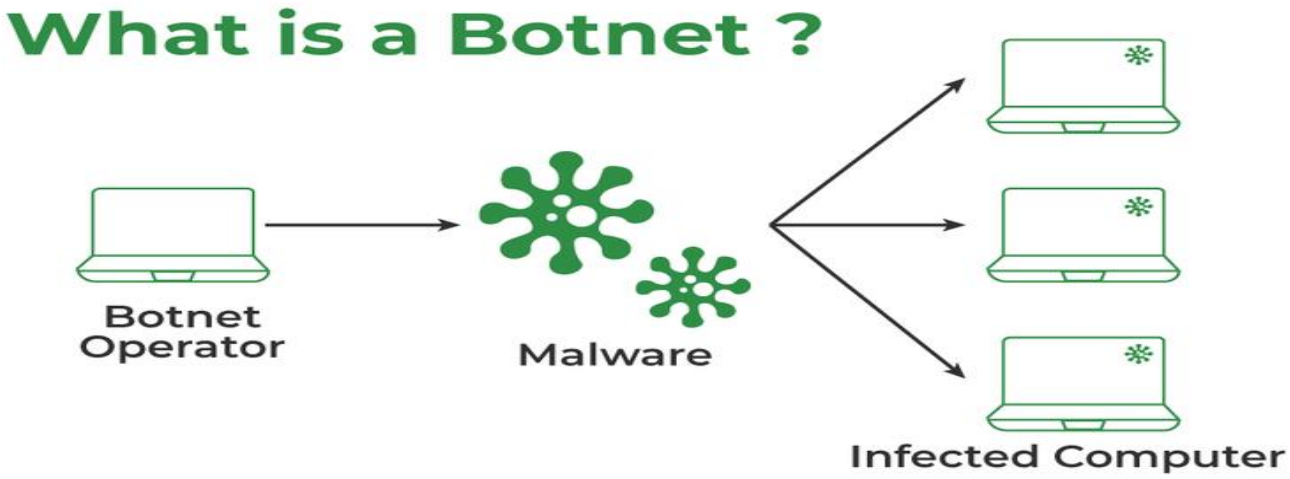
Effects of Cyberstalking

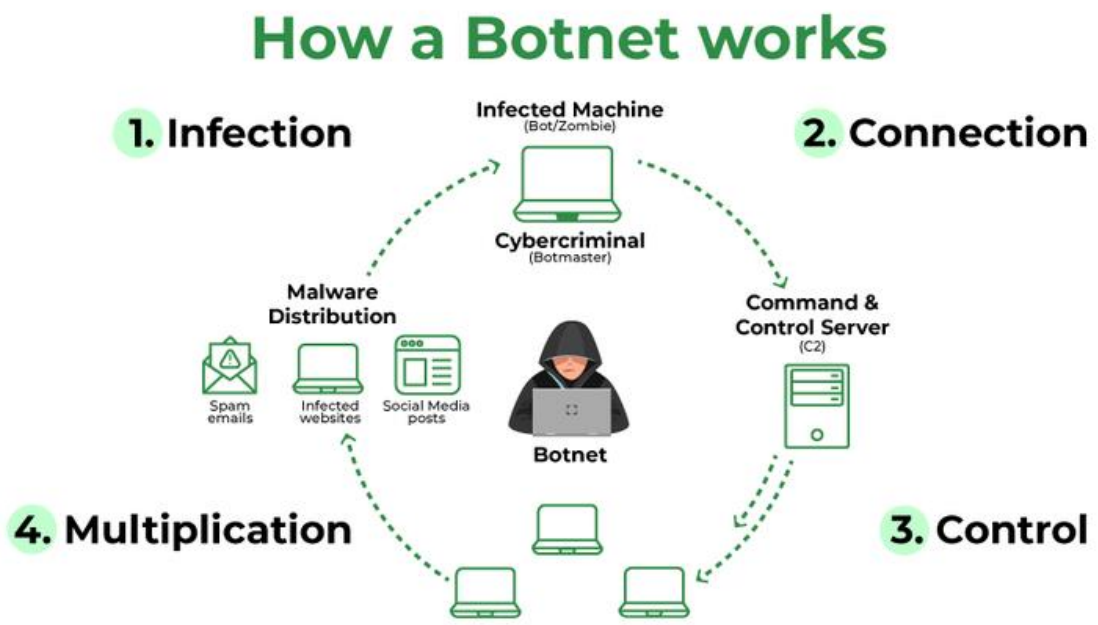
Its victims may experience a wide range of physical, mental, and emotional repercussions. These negative impacts can have an impact on their current relationships with those close to them and include anxiety, despair, the onset of PTSD, panic attacks, sleeping and eating

disorders, among others. A victim of anxiety or PTSD may experience vivid flashbacks of the occurrence, which may set off severe and incapacitating anxiety or panic attacks. Even PTSD and suicidal thoughts have been linked to cyberstalking victims, according to some research.

BOTNET:

A botnet is a collection of independent computers that have each been hacked by a cybercriminal who uses them as a group to carry out many malicious attacks over the Internet. In a botnet, each computer is remotely controlled by a hacker.





Types of Botnet Attacks

Below mentioned are the attacks performed by the Botnets.

- **Phishing:** Botnets help in distributing malware and suspicious activities via Phishing emails. These include a multiple number of bots and the whole process is automated and it is difficult to shut down.
- **Distributed Denial-of-Service(DDoS) Attack:** DDoS Attack is a type of attack performed by the Botnets in which multiple requests are sent that leads to the crash of a particular application or server. DDoS Attacks by Network Layer use SYN Floods, UDP Floods, etc to grasp the target's bandwidth and let them protect from being attacked.
- **Spambots:** Spambots are a type of Botnet Attack, where they take emails from websites, guestbooks, or anywhere an email id is required to log in. This section covers more than 80 percent of spam.
- **Targeted Intrusion:** This is one of the most dangerous attacks as they attack the most valuable thing or data, valuable property, etc.

How to Protect Against Botnets?

- The most important way to protect from Botnets is to give training to users about identifying suspicious links.
- Keep the system software always updated to become safe from the Botnets.
- Using two-factor authentication is a way to be safe from the Botnet.
- There are several antiviruses present in the market which keeps you protected from Botnets.
- Try to change passwords on a regular basis for better protection from Botnets.