

UNIT I

Introduction to Cyber Security

Contents

- Introduction and Overview of Cyber Crime
- Nature and Scope of Cyber Crime
- Types of Cyber Crime: crime against an individual , Crime against property
- Cyber extortion
- Drug trafficking
- cyber terrorism
- Need for Information security

Contents

- Threats to Information Systems
- Information Assurance
- Cyber Security, and Security Risk Analysis

Introduction and Overview of Cyber Crime,

What is Cyber security?

- Cybersecurity is all about protecting your computer, phone, or any digital device from hackers and online threats. It keeps your personal information, bank details, files, and online activity safe from being stolen, damaged, or misused. By acquiring knowledge of cyber attacks and cyber security we can secure and defend ourselves from various cyber attacks like phishing and DDoS attacks.

OR

- Cyber security is the protection of Internet-connected systems, including hardware, software, and data from cyber attacks.
- It is made up of two words one is cyber and other is security.

Cyber is related to the technology which contains systems, network and programs or data.

- Whereas security related to the protection which includes systems security, network security and application and information security.

Need of Cybersecurity

- Cybersecurity is crucial as it significantly impacts both individuals and organizations across various sectors. Some of the main reasons why it is so important are listed below.

1. Protection of Sensitive Data:

Cybersecurity is imperative for protecting sensitive data such as personal details, health records, financial information, and intellectual property. Without strong cybersecurity measures, organizations and individuals are vulnerable to data breaches that could lead to identity theft or financial fraud.

2. Business Continuity and Reputation

For businesses, cybersecurity protection helps ensure operational continuity and protects their reputation. Cyberattacks can cause substantial disruptions, resulting in financial losses, operational downtime, and reputational damage. A well-known incident involves Target.

3. Economic and Regulatory Implications

Ignoring cybersecurity can have severe economic repercussions. Businesses may face financial losses due to theft, the cost of system repairs, and compensation for affected parties. In addition, failure to protect sensitive data can also attract regulatory fines under laws like the General Data Protection Regulation (GDPR) in Europe or the Health Insurance Portability and Accountability Act (HIPAA) in the United States.

4. National Security and Critical Infrastructure

- Cybersecurity has become extremely important for national security. The reason for this is that cyberattacks can target essential services like water systems, power grids, and government agencies—all important assets. An example of an attack of this kind was the Stuxnet attack, which targeted nuclear facilities. Such incidents underscore the importance of protecting critical infrastructure to prevent potential catastrophes.

- 5. Trust and Reputation

Good cybersecurity practices help keep customers' and stakeholders' trust. A company known for protecting its own data and its customer data is usually more respected than one that has had many security breaches. For example, a bank that uses strong cybersecurity measures can assure its customers that their financial information is safe. This builds trust and strengthens the bank's reputation as a reliable place to do business.

Introduction of Cyber Crime

- Cybercrime encompasses a wide range of criminal activities that are carried out using digital devices and/or networks. It has been variously defined as "a crime committed on a computer network, especially the Internet"; Cybercriminals may exploit vulnerabilities in computer systems and networks to gain unauthorized access, steal sensitive information, disrupt services, and cause financial or reputational harm to individuals, organizations, and governments. [

Introduction of Cyber Crime

Cybercrime encompasses a wide range of criminal activities that are carried out using digital devices and/or networks. It has been variously defined as "a crime committed on a computer network, especially the Internet"; Cybercriminals may exploit vulnerabilities in computer systems and networks to gain unauthorized access, steal sensitive information, disrupt services, and cause financial or reputational harm to individuals, organizations, and governments.["

What is Cyber Crime?

Cybercrime refers to illegal activities involving computers, networks, or the internet as a tool to commit offenses.

These crimes include:

Identity Theft – Stealing personal information to commit fraud.

Financial Fraud – Online scams, fake transactions, and credit card fraud.

Cyberbullying – Harassment or threats through digital platforms.

Phishing Attacks – Deceptive emails or websites tricking users into revealing sensitive data.

Hacking – Unauthorized access to systems and data breaches.

Malware Attacks – Spreading viruses, ransomware, and trojans to damage or steal data.

Types of Cyber Crime

1. Crime Against an Individual

I) E-mail spoofing and other online frauds

E-mail spoofing is the creation of email messages with a forged sender address.[1] The term applies to email purporting to be from an address which is not actually the sender's; mail sent in reply to that address may bounce or be delivered to an unrelated party whose identity has been faked.

II) Phishing, Spear phishing

Phishing is a type of cybercrime where attackers deceive individuals into revealing sensitive information, such as passwords, credit card details, or other personal data, by disguising themselves as a trustworthy entity

III) Spamming'

IV) Cyber Defamation

V) Cyberstalking and harassment

VI) Computer Sabotage

VII) Pornographic offenses

a.Publication

b.Transmission

c. Password sniffing

2. Crime Against Property

I)Credit Card Frauds

II) Intellectual Property Crimes

III) Internet time theft.

Types of Cyber Crime

1. Cyber Crimes Targeting Computer Networks or Devices

These crimes involve direct attacks on computers, servers, or digital infrastructure to steal data, cause disruption, or damage systems. It involves different threats like-viruses, bugs, etc. and (DoS) denial-of-service attacks.

Malware Attacks: This kind of cyber threat relates to malware viruses, worms, Trojans, etc. for interfering, damaging, or unauthorized access to computer systems.

For example:ransomware encrypts files and then later demands ransom for decryption.

Denial-of-Service (DoS) Attacks: Here, the attackers focus on a system and flood it with high traffic, hence making it inaccessible to the users. Another dangerous variant of DoS is DDoS, wherein many compromised systems target one, thus, much difficult to defend against.

Phishing Attacks: These are masqueraded e-mails or messages claiming to be from a formal web but only request that the user grant access to sensitive information like password points for an account or credit card numbers. Phishing can be described as an outstanding one of the most common cyber threats.

Botnets (Zombie Networks): A number of hijacked computers can become a "botnet" of malware that can be used by an attacker for coordinated attacks or spamming.

Exploits and Vulnerabilities: The typical area through which cyber-thieves exploit software weakness is the application or operating system vulnerability in order to access it illegally.

2. Crimes Using Computer Networks to Commit Other Criminal Activities

Cyberstalking: This is considered as that crime in the nature of threatening or frightening a person on-line and spreading fear and emotional distress. This can be termed as involving threats, constant monitoring, or receiving repeated unwanted messages.

Financial Fraud: This is an example of a cybercrook manipulating the victim online to proceed with stealing money, such as fake investment opportunities, hacking a business email, and using someone else's credit card details.

Identity Theft: It is normally the identity of people whose information is stolen with the intention of only acting like them either to misuse their cash or money from their account or even to do malicious reasons. It always lowers the credit score of the victim and in the worst case scenario, misused the account/loan financially with incorrect transactions.

Online Harassment and Hate Crimes:

When people use the internet to discriminate against a particular person based on his or her racial background, gender, religion, or whatever, which can psychologically disturb the harassed person.

Nature of cyber crime

Cybercrime refers to criminal activities that are carried out using computers, digital devices, or networks. These crimes often target systems, data, individuals, organizations, or governments.

1. Technology-Based

Cybercrimes are facilitated through the internet, mobile networks, or digital platforms. This includes hacking, phishing, identity theft, and more.

2. Global and Borderless

Unlike traditional crimes, cybercrime can originate from anywhere in the world, making it difficult to trace and prosecute.

.

3. Invisible and Anonymous

Cybercriminals often hide their identities using tools like VPNs, proxy servers, or the dark web, making it hard to detect and stop them

4. Targeted or Random

Some cyberattacks are specifically targeted (e.g., corporate espionage), while others are broad-based (e.g., spam emails or ransomware attacks).

5. High Impact, Low Cost

With minimal investment, cybercriminals can launch attacks that result in huge financial, reputational, and operational damages.

Cyber Extortion