INTRODUCTION TO CYBER CRIME

Dr.R.SUGANYA

DEPARTMENT OF COMPUTER SCIENCE
WITH CYBER SECURITY

- Cybercrime is a rapidly growing threat, witn criminals using technology to commit various crimes. This presentation will explore different types of cybercrime, their impact, and ways to protect yourself.

Introduction to Cyber Crime

Cybercrime is a rapidly growing threat, with criminals using technology to commit various crimes. This presentation will explore different types of cybercrime, their impact, and ways to protect yourself.

Types of Cybercrime

1 Malware

Malware, like viruses, worms, and ransomware, can steal data, damage systems, or lock files for ransom.

2 Phishing

Phishing attacks use fake emails or websites to trick victims into revealing personal information, such as passwords or credit card details.

3 Social Engineering

Social engineering uses psychological manipulation to convince people to reveal sensitive information or grant access to systems.

4 Denial-of-Service (DoS) Attacks

DoS attacks overwhelm a website or network with traffic, making it unavailable to legitimate users.

Cybercrime Targets

Individuals

Cybercriminals can target individuals for financial gain, identity theft, or personal harassment.

1. Phishing emails
2. Social media scams
3. Identity theft

Businesses

Cybercriminals can target businesses for financial gain, disruption of operations, or theft of sensitive information.

1. Ransomware attacks
2. Data breaches
3. Espionage

Government Agencies

Cybercriminals can target government agencies to disrupt critical infrastructure, steal classified information, or influence elections.

1. Cyber espionage
2. Sabotage
3. Disinformation campaigns

Impact of Cybercrime

Financial Loss

Cybercrime can result in significant financial losses for individuals, businesses, and governments.

Reputation Damage

Data breaches and other cyberattacks can damage the reputation of individuals and organizations.

Disruption of Services

Cyberattacks can disrupt essential services, such as healthcare, transportation, and communication.

National Security Threats

Cybercrime can pose significant national security threats, particularly with the increasing reliance on technology.

Cybercrime Prevention

1

Strong Passwords

Use strong, unique passwords for all your online accounts.

2

Multi-Factor Authentication (MFA)

Enable MFA on your accounts to add an extra layer of security.

3

Security Software

Install antivirus and anti-malware software to protect your devices.

4

Regular Updates

Keep your operating systems, software, and apps up to date with the latest security patches.

5

Awareness

Be aware of common cyber threats and how to protect yourself.

Cybercrime Investigation & Prosecution

1 Evidence Collection

Law enforcement agencies collect evidence from digital devices, network logs, and other sources.

2 Forensics Analysis

Forensic experts analyze digital evidence to identify the perpetrators and their methods.

3 Prosecution

Suspects are arrested and prosecuted for their cybercrimes.

Cybersecurity Best Practices

Use Strong Passwords

Create strong and unique passwords for all online accounts.

Enable MFA

Activate multi-factor authentication on accounts for added security.

Update Software Regularly

Install security updates promptly to patch vulnerabilities.

Be Vigilant

Be cautious of suspicious emails, websites, or messages, and never reveal personal information without verification.

The Future of Cybercrime

As technology evolves, cybercrime will likely become more sophisticated. New threats will emerge, requiring ongoing vigilance and adaptation of cybersecurity measures. This means staying informed about new vulnerabilities and threats, and constantly updating security measures.

THANK YOU