**Introduction**

* Title: **Cybercrime: The Hidden Threat**
  + Image: A computer screen with a padlock symbol
* What is Cybercrime?
  + Definition: Illegal activities that take place over the internet
  + Examples: Hacking, identity theft, online fraud

## Types Of cyber crime:

* Financial Cybercrime
  + Types: Credit card fraud, online banking scams, phishing
  + Examples: Phishing emails, fake websites
* Identity Theft Crimes
  + Stolen Identities: How personal information can be obtained and misused
  + Data Breaches: Large-scale leaks of sensitive data
  + Legal Consequences: The potential legal repercussions of identity theft
* Cyberbullying
  + Definition: Using technology to harass or threaten others
  + Impact: Emotional and psychological harm
* Hacking
  + Definition: Unauthorized access to computer systems
  + Types: Black hat hacking, white hat hacking
  + Consequences: Data loss, financial damage, disruption of services

**Cyber Security Fundamentals**

* Understanding Threats
  + Identifying potential risks and vulnerabilities
  + Staying informed about emerging cyber threats
* Implementing Robust Security Measures
  + Strong passwords, antivirus software, firewalls
  + Regular software updates and security patches
* Fostering Security Awareness
  + Educating individuals about safe online practices
  + Promoting a culture of security within organizations
* Protecting Sensitive Data
  + Secure storage and transmission of personal information
  + Data encryption and access controls

**Cyber Security Best Practices**

* Enable Two-Factor Authentication
  + Adding an extra layer of security to accounts
* Use Strong and Unique Passwords
  + Creating complex and different passwords for each account
* Keep Software Up-to-Date
  + Ensuring that software has the latest security patches
* Be Cautious of Phishing Attempts
  + Recognizing and avoiding fraudulent emails or websites