**Title: Cybercrime: The Hidden Threat**

**Slide Image:** A computer screen with a padlock symbol.

**What is Cybercrime?**

* **Definition:** Cybercrime means doing something illegal on the internet. It's like breaking the law, but online.
* **Examples:**
  + **Hacking:** When someone breaks into a computer without permission.
  + **Identity Theft:** When someone pretends to be you online and uses your personal information.
  + **Online Fraud:** Tricking people into giving money or personal details online.

**Types of Cybercrime**

**1. Financial Cybercrime**

* **Types:**
  + **Credit Card Fraud:** Stealing credit card information to buy things without permission.
  + **Online Banking Scams:** Tricking people to give away their bank details.
  + **Phishing:** Sending fake emails to steal personal information.
* **Examples:**
  + **Phishing Emails:** Emails that look real but are actually traps to steal your information.
  + **Fake Websites:** Websites that look like real ones but are made to steal your information.

**2. Identity Theft Crimes**

* **Stolen Identities:** This happens when someone takes your personal information (like your name or address) and pretends to be you.
* **Data Breaches:** Sometimes, big companies lose lots of personal information, and criminals use that data for bad purposes.
* **Legal Consequences:** If someone steals an identity, they can face serious legal trouble.

**3. Cyberbullying**

* **Definition:** Cyberbullying is when someone uses the internet or a phone to hurt or threaten others.
* **Impact:** It can cause a lot of emotional pain and stress for the victim.

**4. Hacking**

* **Definition:** Hacking is when someone gets into a computer system without permission.
* **Types:**
  + **Black Hat Hacking:** Hacking to do bad things, like stealing information.
  + **White Hat Hacking:** Hacking to help protect systems and find weaknesses.
* **Consequences:** Hacking can lead to loss of data, financial problems, and disruptions in services.

**Cyber Security Fundamentals**

**1. Understanding Threats**

* **Identifying Risks:** Knowing what could be dangerous online and being aware of things that might harm your computer.
* **Staying Informed:** Keeping up with new cyber threats, like viruses or new tricks that hackers use.

**2. Implementing Robust Security Measures**

* **Strong Passwords:** Use passwords that are hard to guess.
* **Antivirus Software:** Protects your computer from viruses and other harmful software.
* **Firewalls:** Helps block unauthorized access to your computer.
* **Regular Updates:** Keep your computer’s software updated to protect it from new threats.

**3. Fostering Security Awareness**

* **Educating:** Teach people how to stay safe online.
* **Promoting a Security Culture:** Encouraging everyone, especially in schools or workplaces, to practice good online security.

**4. Protecting Sensitive Data**

* **Secure Storage:** Keep your personal information safe and private.
* **Data Encryption:** Scramble your data so that only authorized people can read it.
* **Access Controls:** Make sure only trusted people can access important information.

**Cyber Security Best Practices**

**1. Enable Two-Factor Authentication**

* **Extra Security:** This adds another step when logging into your accounts to make sure only you can get in.

**2. Use Strong and Unique Passwords**

* **Complex Passwords:** Use different, strong passwords for each account so they are harder to guess.

**3. Keep Software Up-to-Date**

* **Stay Updated:** Make sure your software has the latest security features to protect against new threats.

**4. Be Cautious of Phishing Attempts**

* **Avoiding Scams:** Learn to recognize and avoid fake emails or websites that try to steal your information.