UNIT I

Introduction of Cybercrime:

The internet has brought about a new type of crime called cybercrime, involving computers, the internet, and the worldwide web.

- In Australia, a 2008 survey depicted a rising trend in cybercrime, and the situation in India is no different.
- From February 2000 to December 2002, Indian corporate and government websites experienced over 780 attacks or defacements.
- In just five months, from January to June 2009, a staggering 3,286 Indian websites were hacked.
- This highlights the global and local challenges posed by cyber threats, emphasizing the need for effective cybersecurity measures.

Definition and Origins of the Word:

Cybercrime involves illegal activities with computer technology, spans traditional crimes with a digital twist, from theft to financial dishonesty.

- This includes threats like hardware/software theft, sabotage, and ransom demands.
- Also known as computer-related, internet, or e-crime, it encompasses techno-crime (planned attacks for copying or damaging systems) and techno-vandalism (opportunistic defacement).
- Different from traditional crimes, cybercrimes are easier to learn, require fewer resources, can be done remotely, and aren't always clearly illegal.
- Cyberterrorism employs computers for terrorist acts, while planning involves tactics like phishing and spoofing.
- Targets range from individuals to companies, leading to issues like intellectual property theft and the spread of illegal content.

Cybercrime and Information Security:

The Indian Information Technology Act of 2008 places a strong emphasis on "Information Security in India," defining cybersecurity as safeguarding information, devices, computers, and communication tools from unauthorized access.

- However, estimating financial losses from insider crimes is challenging due to difficulties in detecting impacts, hindering the quantification of losses.
- Compiling data on the business impact of cybercrime faces obstacles, as organizations often do not include the costs of security incidents in their accounting, struggle to assign a monetary value to stolen corporate data, and are reluctant to disclose information about security incidents, including cybercrime.
- Common network misuses, including internet radio, streaming audio and video, file sharing, instant messaging, online gaming, and online gambling, present additional challenges to information security in the digital realm.

Who are Cybercriminals:

Cybercriminals encompass individuals engaging in various illicit activities within the digital realm, including child pornography, credit card fraud, cyberstalking, online defamation, unauthorized access to computer systems, copyright infringement, software piracy, and identity theft for criminal purposes. They can be categorized into three types:

- Type I, driven by a desire for recognition.
- Type II, not interested in recognition but involved in cybercrimes.
- Type III, insiders who exploit their access to commit cybercrimes.

These individuals pose a diverse range of threats in the digital landscape, requiring comprehensive strategies for cybersecurity and law enforcement to combat their activities effectively.

Classification of Cybercrimes:

Cybercrimes are classified as follows:

- **Cybercrime against Individuals:** This involves crimes that directly target people. For example, hacking personal accounts, stealing sensitive information, or spreading false information about an individual online.
- **Cybercrime against Property:** Here, the focus is on crimes that damage or interfere with digital property. This could include things like hacking into computer systems, spreading malware that harms devices, or disrupting online services.
- **Cybercrime against Organizations:** Organizations, such as companies or government bodies, can be targets too. Cybercrimes against organizations may involve hacking into their systems for information or causing disruptions to their operations.
- **Cybercrime against Society:** This category covers crimes that have a broader impact on society. This could include activities like spreading fake news or engaging in cyberterrorism that affects the public.
- **Crimes emanating from Usenet Newsgroups:** Usenet newsgroups are online discussion forums. Crimes emanating from these could involve illegal activities discussed or coordinated within these forums. This might include the planning of cybercrimes or the exchange of illegal content.

Email Spoofing:

Description: Sending emails that appear to come from a different source than they do.
Impact: Misleading recipients, often used for phishing or spreading malware.

Spamming:

Description: Sending unsolicited and often irrelevant messages to many users, typically for advertising purposes.
Impact: Overloading email or messaging systems, causing inconvenience to users.

Internet Time Theft:

Description: Unauthorized use of internet resources during work hours.
Impact: Reduces productivity and wastes company resources.

Salami Attack/Salami Technique:

Description: Stealing tiny amounts of money from many transactions to avoid detection.
Impact: Financial losses that may go unnoticed for a long time.

Data Diddling:

Description: Illegally modifying data before or during entry into a computer system.
Impact: Distorted information leading to incorrect decisions.

Forgery:
Description: Creating fake documents, signatures, or data with the intent to deceive.
Impact: Undermining trust in documents and systems.

Web Jacking:
Description: Taking control of someone else's website without their permission.
Impact: Disrupting or defacing websites, damaging reputation.

Newsgroup Spam:
Description: Posting irrelevant or inappropriate messages in online discussion forums.
Impact: Cluttering forums, making it difficult for users to find useful information.

Industrial Espionage:
Description: Illegally gathering confidential business information for competitive advantage.
Impact: Undermining competitiveness and intellectual property theft.

Hacking:
Description: Unauthorized access and manipulation of computer systems or networks.
Impact: Compromised security, potential data breaches.

Online Frauds:
Description: Deceptive practices to gain financial benefits over the internet.
Impact: Financial losses for individuals or businesses.

Pornographic Offenses:
Description: Illegally distributing or creating explicit adult content.
Impact: Legal consequences, harm to individuals involved.

Software Piracy:
Description: Illegally copying, distributing, or using software without permission.
Impact: Financial losses for software developers, potential security risks.

Computer Sabotage:
Description: Deliberate actions to disrupt or damage computer systems.
Impact: System downtime, data loss, financial damage.

E-Mail Bombing:
Description: Flooding someone's email inbox with a massive number of emails.
Impact: Overloading email systems, disrupting communication.

Computer Network Intrusions:
Description: Unauthorized access and manipulation of an entire computer network.
Impact: Compromised security, potential data breaches.

Password Sniffing:
Description: Illegally capturing and decoding passwords.
Impact: Unauthorized access to accounts, potential data breaches.

Credit Card Frauds:

Description: Unauthorized use of credit card information for financial gain.
Impact: Financial losses for individuals and businesses.

Identity Theft:

Description: Stealing someone's personal information to commit fraud or other crimes.
Impact: Financial losses, damage to the victim's reputation.