CSE332

Unit 6:- Ethical and Professional issues in Information Security

Ethical and Professional issues in Information Security

Cyber Crime ,Cyber-crime on the rise, Need for cyber law in India

Cyber crime

- Cybercrime refers to any illegal activity that involves computers, networks, or digital devices.

- These crimes are committed using technology to steal, manipulate, or destroy data, systems, or personal information.

- Cybercrimes can target individuals, businesses, or even governments, leading to financial losses, security breaches, and privacy violations.

Types of Cyber Crimes

- Cyber Fraud - Any fraudulent activity conducted online to deceive individuals or businesses for financial gain.

- Hacking & Data Breaches - Gaining unauthorized access to computer systems or networks to steal, modify, or delete data.

- Cyberbullying & Harassment - The use of digital platforms to harass, threaten, or abuse someone. This includes sending offensive messages, spreading false rumors, or sharing private photos without consent.

- Intellectual Property Theft - The unauthorized use, reproduction, or distribution of copyrighted material, trademarks, or patented content.

- Cyber Terrorism - The use of cyber attacks to spoil critical infrastructures, government systems, or spread fear among the public.

Cyber-Crime on the Rise

- Cybercrime has been increasing at an alarming rate worldwide.

- With the rapid growth of digital transactions, cloud computing, and social media.

- The rise in cybercrime can be attributed to greater internet usage, lack of cybersecurity awareness, and evolving hacking techniques.

Statistics and Reports on Rising Cybercrime

- Cybercrime is expected to cost the world $10.5 trillion annually by 2025 (Cybersecurity Ventures report).

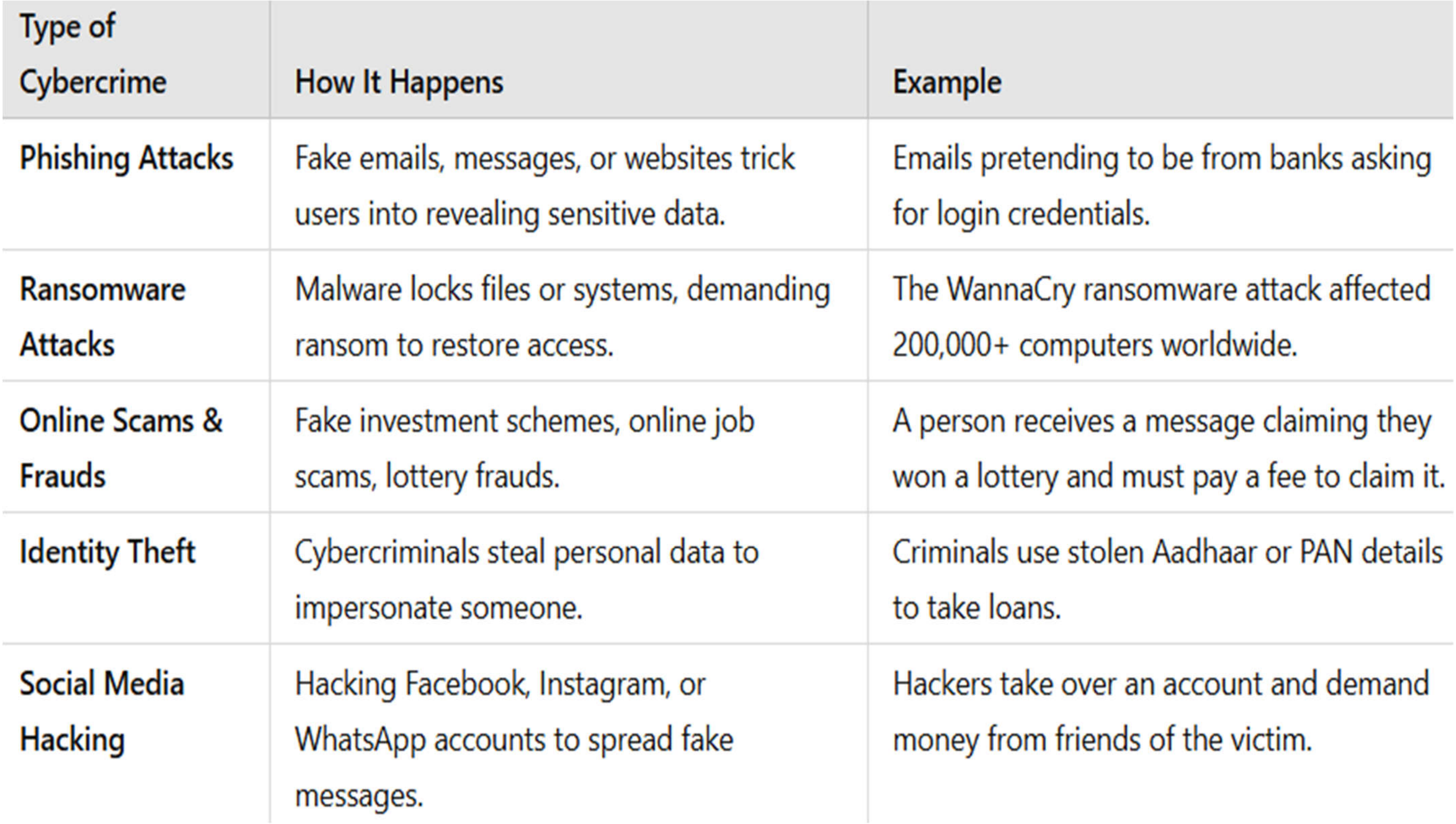
- A cyberattack occurs every 39 seconds worldwide.

- In 2023, more than 800 million ransomware attacks were reported globally.

- Over **50,000 cybercrime cases** were registered in India in 2023.

Major Reasons Behind the Rise in Cybercrime

1. Increased Digital Dependence
2. Lack of Cybersecurity Awareness
3. Advanced Hacking Techniques
4. Rise of Mobile & IoT Devices (**43% of cyberattacks** are now directed at mobile devices.)
5. Financial Motivation



Type of Cybercrime	How It Happens	Example
Phishing Attacks	Fake emails, messages, or websites trick users into revealing sensitive data.	Emails pretending to be from banks asking for login credentials.
Ransomware Attacks	Malware locks files or systems, demanding ransom to restore access.	The WannaCry ransomware attack affected 200,000+ computers worldwide.
Online Scams & Frauds	Fake investment schemes, online job scams, lottery frauds.	A person receives a message claiming they won a lottery and must pay a fee to claim it.
Identity Theft	Cybercriminals steal personal data to impersonate someone.	Criminals use stolen Aadhaar or PAN details to take loans.
Social Media Hacking	Hacking Facebook, Instagram, or WhatsApp accounts to spread fake messages.	Hackers take over an account and demand money from friends of the victim.

Need for Cyber Law in India

Cyber law refers to the legal framework that governs **cybercrime, digital transactions, data protection, and online activities.**

It defines the rights, responsibilities, and punishments related to crimes committed in cyberspace.

Objectives of Cyber Law:

✅ Prevent cybercrimes and punish offenders.

✅ Protect individuals, businesses, and government entities from cyber threats.

✅ Establish guidelines for e-commerce, digital payments, and IT security.

✅ Safeguard data privacy and prevent unauthorized access.

Key Cyber Laws in India

Information Technology (IT) Act, 2000

- India’s primary cyber law that governs cybercrimes, digital transactions, and electronic evidence.

- Covers: Hacking, identity theft, phishing, cyberstalking, and data protection.

- Punishments: Up to 10 years of jail and fines for serious cyber offenses.

Indian Penal Code (IPC) – Sections Related to Cybercrime

- **Section 419 & 420:** Punishment for cheating and online fraud.
- **Section 500:** Punishment for cyber defamation.
- **Section 354D:** Covers cyberstalking and online harassment.

Digital Personal Data Protection (DPDP) Act, 2023

- Protects **personal data privacy** and regulates how companies collect and use user information.

- Ensures strict penalties for **data breaches and misuse of private data.**

National Cyber Security Policy, 2013

- Strengthens India’s cybersecurity infrastructure.

- Focuses on protecting **critical sectors like banking, defense, and telecom.**

Challenges in Implementing Cyber Laws

⚠ **Lack of Awareness** – Many people are unaware of cyber laws and their rights.

⚠ **Slow Legal Proceedings** – Cybercrime cases take time to resolve due to technical complexities.

⚠ **Cybercriminals Using Advanced Technologies** – AI-powered malware and the **dark web** make it harder to track criminals.