SNS COLLEGE OF TECHNOLOGY

(An Autonomous Institution)

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A+' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER APPLICATIONS

ETHICS IN COMPUTING

I YEAR - II SEM

UNIT – II: ASPECTS OF COMPUTER CRIME AND INTELLECTUAL PROPERTY RIGHTS

TOPIC 1: ASPECTS OF COMPUTER CRIME – INTRODUCTION – WHAT IS COMPUTER CRIME?

INTRODUCTION TO COMPUTER CRIME:

Computer crime, also known as cybercrime, refers to criminal activities that are committed using computers, computer networks, or electronic devices. With the rapid advancement of technology and the widespread use of the internet, computer crime has become a significant concern for individuals, businesses, and governments worldwide. It encompasses a wide range of illegal activities that exploit vulnerabilities in computer systems, compromise data security, and cause financial losses or harm to individuals and organizations.

Computer criminals, often referred to as hackers or cybercriminals, employ various techniques and tools to carry out their illicit activities. They take advantage of weaknesses in software, networks, or human behavior to gain unauthorized access to sensitive information, disrupt systems, commit fraud, or engage in other malicious actions.

Some common types of computer crime include hacking, malware attacks, phishing, identity theft, denial of service attacks, data breaches, cyber fraud, intellectual property theft, cyberstalking, and online child exploitation. These crimes can have severe consequences, ranging from financial losses and reputational damage to compromised privacy, compromised national security, and even physical harm.

Computer crime poses significant challenges due to its transnational nature, making it difficult to track down and prosecute offenders. The anonymity provided by the internet and the global reach of cybercriminals make it crucial for international cooperation and the development of robust cybersecurity measures and laws.

To combat computer crime, governments and law enforcement agencies work alongside cybersecurity experts, computer forensic investigators, and technology companies to develop preventive measures, strengthen security infrastructure, and raise awareness about safe online practices. This includes implementing strong encryption protocols, conducting regular security audits, educating users about password hygiene and phishing scams, and promoting responsible online behavior.

As technology continues to advance, computer criminals evolve their techniques and exploit emerging vulnerabilities. Therefore, ongoing research, information sharing, and collaboration between public and private sectors are essential to stay one step ahead of cybercriminals and protect individuals, organizations, and critical infrastructure from the devastating effects of computer crime.

ASPECTS OF COMPUTER CRIME

Computer crime, also known as cybercrime, refers to criminal activities that are committed using computers or targeted at computer systems, networks, or electronic devices. Here are some key aspects of computer crime:

Hacking: Unauthorized access or intrusion into computer systems or networks with the intent to gain information, disrupt operations, or commit other illegal activities.

Malware: The creation, distribution, or use of malicious software such as viruses, worms, Trojans, ransomware, spyware, or botnets to compromise computer systems, steal data, or cause harm.

Phishing: A form of social engineering where attackers attempt to deceive individuals or organizations into providing sensitive information like passwords, credit card details, or personal data by posing as a trustworthy entity.

Identity theft: The fraudulent acquisition and use of someone else's personal information, such as their name, social security number, or financial details, to commit financial fraud, make unauthorized purchases, or engage in other illegal activities.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks: Overloading computer systems, networks, or websites with excessive traffic or requests, rendering them inaccessible to legitimate users.

Cyberstalking and harassment: Using electronic means, such as email, social media, or instant messaging, to stalk, intimidate, or harass individuals.

Data breaches: Unauthorized access, disclosure, or theft of sensitive or confidential information stored in computer systems or databases, often resulting in financial loss, identity theft, or reputational damage.

Cyber fraud: Various forms of fraud committed online, including online scams, fake websites, credit card fraud, investment fraud, and online auction fraud.

Intellectual property theft: Unauthorized copying, distribution, or use of copyrighted materials, trademarks, patents, or trade secrets, often for financial gain.

Cyberterrorism: The use of computer systems or networks to launch attacks intended to cause widespread disruption, fear, or harm, with political or ideological motivations.

Online child exploitation: The production, distribution, or possession of child pornography, grooming minors for sexual exploitation, or engaging in other illegal activities involving children through online platforms.

These are just a few examples of the different aspects of computer crime. With the ever-evolving nature of technology, new forms of computer crime continue to emerge, making it necessary for individuals, organizations, and law enforcement agencies to stay vigilant and adapt to the evolving threat landscape.

MOTIVE BEHIND COMPUTER CRIME

The motives behind computer crime can vary depending on the individuals or groups involved. Here are some common motives:

Financial gain: Many computer criminals engage in cybercrime with the primary objective of financial profit. They may attempt to steal sensitive financial information, such as credit card details or online banking credentials, to commit fraud, make unauthorized purchases, or conduct identity theft. Others may target businesses or organizations to extort money through ransomware attacks or by selling stolen data on the black market.

Espionage and intellectual property theft: Nation-states, corporate spies, or competitors may engage in computer crime to gain unauthorized access to valuable intellectual property, trade secrets, or classified information. They may target research institutions, government agencies, or businesses to gather intelligence, gain a competitive advantage, or disrupt rivals.

Hacktivism: Some individuals or groups engage in computer crime as a form of activism or protest. They may target organizations, government agencies, or websites to promote a particular social or political cause, expose corruption, or raise awareness about perceived injustices. Their actions may include website defacement, distributed denial of service (DDoS) attacks, or leaking sensitive information.

Cyberterrorism: In rare cases, computer crime is driven by political or ideological motives, with the intention to cause fear, disruption, or harm to individuals, organizations, or critical infrastructure. Cyberterrorists may target government systems, public utilities, or financial institutions with the goal of destabilizing societies or advancing their extremist agenda.

Personal vendettas or revenge: In some instances, individuals may engage in computer crime out of personal grievances or a desire for revenge. They may use hacking techniques to compromise the privacy, reputation, or financial well-being of specific individuals or organizations they perceive as having wronged them.

Thrill-seeking and notoriety: Some computer criminals engage in cybercrime for the thrill of the challenge and the desire to gain recognition among their peers. They may target high-profile organizations, government systems, or prominent individuals to showcase their skills or achieve a sense of notoriety.

Information gathering or surveillance: State-sponsored actors or intelligence agencies may engage in computer crime to gather intelligence, monitor communication networks,

or conduct surveillance on specific individuals or groups. Their motivations are often related to national security, political control, or defense strategies.

It's important to note that the motives behind computer crime are diverse and can overlap. Additionally, the evolving landscape of technology and the internet can give rise to new motives and opportunities for cybercriminals. Understanding these motives helps in developing effective cybersecurity strategies and implementing preventive measures to mitigate the risks associated with computer crime.