CYBERCRIME- Questions and Answers

1.Explain in brief the concept of Cybercrime.

Ans: Cybercrime refers to illegal activities carried out using computers, digital devices, or the Internet. Unlike the stereotypical image of a hacker in a dark hoodie, cybercrime today is highly organized and professional, often involving criminal groups or even state-sponsored actors. Cybercriminals use various techniques such as phishing, social engineering, malware, and ransomware to steal data, disrupt systems, or extort money. They operate in hidden online markets where malware, hacking tools, and even technical support services are bought and sold.

The impact of cybercrime is immense, causing trillions of dollars in financial damages each year to individuals, businesses, and governments. With the growth of the Internet of Things (IoT) and widespread smart devices, cybercriminals now have more opportunities to exploit security weaknesses. Cybercrimes can take many forms, including identity theft, fraud, cyberbullying, cryptojacking, and cyber extortion. Famous cases such as virus attacks on NASA or ransomware incidents highlight its serious consequences.

Protecting against cybercrime requires safe Internet practices—avoiding suspicious links, using strong passwords, updating software, and relying on antivirus programs. In short, cybercrime is a modern threat that misuses technology for illegal gain, making digital security essential in today's connected world.

2. Name any five types of online threats. What signs can indicate whether you have been a victim of these threats?

Ans: Five common types of online threats are malware, phishing, keylogging, botnets, and cryptojacking. Each of these cybercrimes has certain warning signs that can help victims identify if they have been attacked.

Malware is malicious software such as viruses or ransomware that damages files or locks data until a ransom is paid. A malware infection can be detected if a computer slows down, crashes frequently, or displays repeated error messages.

Phishing attacks trick victims into sharing personal information by luring them to fake websites through fraudulent messages. Signs of phishing include suspicious charges on bank or credit card accounts.

Keylogging involves spyware that secretly records everything typed on a keyboard. Victims may notice strange symbols appearing, duplicate text in their messages, or unusual account activity.

Botnets occur when cybercriminals take control of a computer and use it as part of a larger network for criminal purposes, such as launching attacks. Botnet infections are often hard to detect but may cause unusual system performance issues.

Cryptojacking hijacks a device's processing power to mine cryptocurrency without the user's consent. Victims may see increased electricity bills, overheating devices, or slower performance.

Recognizing these warning signs early and reporting them can prevent further damage and protect sensitive information.

3. With proper examples, write a short note on any two types of common cybercrimes.

Ans: Two common types of cybercrimes are malware attacks and identity theft.

Malware is one of the most widespread forms of cybercrime. It includes malicious software such as viruses, worms, ransomware, and adware, which are designed to damage systems, steal information, or make money for the attacker. For example, ransomware locks files on a victim's computer and demands payment to unlock them, while adware floods the user with unwanted advertisements. Malware infections can slow down computers, cause frequent crashes, and even spread to other devices on the same network. The virus attack on NASA in 1989 by the "Wank worm" is a famous example, where hackers used malware to disrupt NASA's operations for political reasons.

Identity theft and fraud are another serious category of cybercrime. Cybercriminals steal personal information such as names, bank details, or passwords and use it for fraudulent purposes like financial theft. Techniques like phishing, pharming, and keylogging are often used to gather this sensitive data. For instance, in January 2000, a Russian hacker accessed the credit card details of 300,000 customers of Cduniverse.com and attempted to extort money from the company. This case highlights how stolen personal data can be exploited for blackmail or fraud.

Both examples show that cybercrime not only disrupts technology but also causes huge financial and emotional damage to individuals and organizations.

4. List any two instances of cybercrimes that happened in the 20th century. How were they executed and for what reason?

Ans: Two significant instances of cybercrimes in the 20th century highlight how technology was exploited for personal gain and political motives.

The first case occurred in the 1970s at the Union's Dime Savings Bank in New York. A bank teller, despite having little technical knowledge, regularly stole portions of customers' deposits. To hide his theft, he altered customer receipts in the bank's central computer after working hours. This manipulation ensured that both account

holders and his supervisors remained unaware of the fraud. His motivation was purely personal enrichment, as he used the stolen money for sports betting, spending far beyond his modest annual salary of $11,000. He was eventually caught by chance during a police investigation.

The second notable incident happened in October 1989, when anonymous hackers released the Wank worm (Worms Against Nuclear Killers) into NASA's computer systems. This politically motivated cyberattack targeted the U.S. space agency's Greenbelt, Maryland center. Once the worm infiltrated the network, NASA employees found anti-nuclear messages displayed on their screens, criticizing the launch of a plutonium-powered Jupiter probe. The hackers' goal was not monetary but ideological, aiming to protest nuclear armament.

Both cases illustrate how cybercrime can be driven by greed or activism, using computers as powerful tools for deception and disruption.

5. Explain in brief the types of video forgery that is prevalent in the present day.

Ans: Video forgery, popularly known as deepfakes, has become a serious form of cybercrime in today's digital world. It uses advanced artificial intelligence and machine learning techniques to manipulate videos, making it appear as though people said or did things they never actually did. From the given text, five major types of video forgery are prevalent.

The first type Is face-swapping, where the face of a victim is replaced with that of another person, creating highly convincing fake videos. The second is lip syncing, in which the victim's lip movements are synchronized with a fake audio track, similar to dubbing, making the video appear real. The puppet master technique goes further by transplanting all of the donor's facial traits onto the victim's face, resembling movie-style facial recreation. Another form is face synthesis and attribute editing, where a single face is altered — it can be aged, rejuvenated, recolored, or accessorized with items like glasses, hats, or hairstyles. Finally, audio deepfakes forge voices through voice distortion, synthesizers, or cloning, making someone sound like they said something they never did.

These types of video forgery pose significant risks, as they can spread misinformation, damage reputations, and even be used in cyber extortion or political manipulation.

6. How can we protect ourselves from falling victim to cybercrimes?

Ans: To protect ourselves from falling victim to cybercrimes, it is important to adopt safe digital habits and use security tools effectively. Cybercriminals rely on phishing, malware, keylogging, and other techniques to steal data or cause harm. Therefore, one of the first steps is to be cautious online—never click on suspicious links, open unexpected attachments, or download files from untrusted sources. Always verify the

authenticity of websites before entering personal details, especially for banking or shopping. Using strong, unique passwords for different accounts and enabling two-factor authentication adds an extra layer of protection. Regularly updating software and applications is equally important, as updates fix vulnerabilities that attackers could exploit.

When using public Wi-Fi in places like airports or cafes, avoid accessing sensitive accounts unless connected through a VPN, since hackers can “sniff” unencrypted traffic. Strengthening the security of your home network, such as setting a strong router password, also helps. Installing a trusted antivirus program can defend against malware, ransomware, and other threats. Lastly, one should remain alert for unusual device behaviour, such as slow performance or strange error messages, which may indicate an attack. By combining cautious behaviour with technical safeguards, individuals can greatly reduce the risk of cybercrime.

7. “The internet is a boon as well as bane.” Explain.

Ans: The internet is truly a double-edged sword, serving as both a boon and a bane in modern life. On one hand, it has revolutionized the way people communicate, learn, and work. With a single click, we can access limitless information, connect with people across the globe, conduct business, and even enjoy entertainment. Online education, e-commerce, telemedicine, and digital banking have made life more convenient, efficient, and interconnected than ever before. The internet has also opened doors for innovation, creativity, and global collaboration.

On the other hand, the internet has also given rise to serious challenges, particularly in the form of cybercrime. Criminals exploit the web for malicious activities such as identity theft, phishing, malware attacks, cyber extortion, and even political hacking. These crimes can cause immense financial and emotional damage to individuals, organizations, and governments. Cyberbullying and misuse of social media have also negatively affected mental health and personal safety. Moreover, with the rise of deep fakes and online fraud, distinguishing truth from falsehood is becoming increasingly difficult.

Thus, while the internet is a powerful boon that enhances human progress, it also poses dangers when misused. The key lies in using it responsibly and adopting strong cybersecurity measures to minimize its risks.

8. With the help of your teacher, write short introductions about

a. Cookies

b. Firewall

c. Hacking

d. Keylogger

e. Big Data Analysis

f. Internet of Things

g. Social Engineering

h. Artificial Intelligence and Machine Learning

Ans: Cookies are small text files stored by websites on a user's computer. They remember login details, preferences, and browsing activities, making internet use more convenient but sometimes posing privacy risks.

Firewall is a security system—hardware or software—that monitors and controls network traffic. It acts as a barrier between trusted and untrusted networks to block unauthorized access.

Hacking refers to unauthorized access to computer systems or networks. While some hacking is ethical and used for security testing, malicious hacking aims to steal, disrupt, or damage data.

Keylogger is spyware that secretly records everything typed on a keyboard. Cybercriminals use it to capture passwords, banking information, or personal data.

Big Data Analysis involves examining vast amounts of structured and unstructured data to find useful patterns, trends, and insights. It supports decision-making in business, healthcare, and government.

Internet of Things (IoT) connects smart devices—like home appliances, cars, and wearables—to the internet. While it improves convenience, it also increases the attack surface for cybercriminals.

Social Engineering is the manipulation of people into revealing confidential information. Common methods include phishing and impersonation.

Artificial Intelligence (AI) and Machine Learning (ML) enable machines to mimic human intelligence, learn from data, and improve performance automatically. They power modern tools like chatbots, fraud detection, and autonomous vehicles.

9. What are some infamous cases of cybercrimes reported in the last decade? Use the internet to find out the *modus operandi* and damage caused by them. Concentrate on instances involving innocent children and youth. Eg: Blue Whale Challenge, Cinnamon Challenge etc.

Ans: In recent years, several cybercrime incidents have tragically targeted children and youth, often exploiting their vulnerability through online challenges. Two notorious examples are the Blue Whale Challenge and the Cinnamon Challenge.

Blue Whale Challenge

Originating in Russia in 2013, the Blue Whale Challenge is a purported online game that allegedly involves a series of tasks culminating in suicide. While the existence of the game itself is debated, its impact has been devastating. In 2016, Russian authorities arrested Philipp Budeikin, who claimed to have created the game to “cleanse society” by encouraging vulnerable teens to end their lives. He was convicted of inciting at least 16 teenage girls to commit suicide . Similar cases have been reported globally, including in Armenia, Spain, and India, where media coverage and online discussions have led to a moral panic and, in some cases, imitative self-harming behaviours .

Cinnamon Challenge

The Cinnamon Challenge is a dare that gained popularity on social media, where participants attempt to swallow a spoonful of ground cinnamon without drinking water. This seemingly harmless challenge has led to serious health risks, including choking, throat irritation, and even collapsed lungs. In 2013, a report indicated that at least 30 teens nationwide required medical attention after attempting the challenge . Tragically, in 2015, a 4-year-old boy in Kentucky died after ingesting cinnamon, underscoring the potential dangers of such online trends .

These incidents highlight the critical need for awareness and vigilance among parents, educators, and communities to protect young individuals from harmful online influences.

10. From the reading of the text and your text and your experience of using the internet on computers and phones, list ten good practices that will help you stay away and safe from the threats of cybercrimes.

Ans: Good Practices to Stay Safe from Cybercrime:

From the reading and my experience using the internet, here are ten good practices to stay safe from cybercrime:

1.Be careful with emails – Avoid clicking on suspicious links or attachments from unknown senders.

2. Verify websites – Check if the website is real before entering personal information like passwords or bank details.

3. Update software regularly – Software updates fix security gaps and protect against new threats.

4.Avoid public Wi-Fi without protection – Use a VPN if you need to connect to free networks at cafes or airports.

5.Use strong passwords – Create unique passwords for each account and change them regularly.

6.Enable two-factor authentication – It adds an extra layer of protection beyond the password.

7.Secure your home network – Change default settings on your router and use strong passwords.

8.Install antivirus software – A good antivirus program helps detect and remove malware.

9.Avoid downloading from untrusted sources – Only download apps or files from verified websites or app stores.

10.Report cybercrime – If you suspect you've been attacked, inform the authorities or a trusted adult.

By following these habits, we can enjoy the internet while staying safe from hackers and fraudsters.