

## **TOPIC-Cybercrime**

### **Fill-in-the-blank questions :-**

1. \_\_\_\_\_ is the unauthorized access to computer systems or networks with malicious intent.

Answer: Hacking

2. Phishing is a type of \_\_\_\_\_ attack where attackers trick individuals into revealing sensitive information.

Answer: Social engineering

3. \_\_\_\_\_ is a form of malware that can spread from one computer to another without user intervention.

Answer: Worm

4. The practice of sending fraudulent emails that appear to be from reputable sources to deceive individuals into revealing personal information is known as \_\_\_\_\_.

Answer: Email spoofing

5. A program that appears legitimate but is designed to carry out harmful activities on a computer system is called a \_\_\_\_\_.

Answer: Trojan horse

6. The process of converting information into an unreadable format to prevent unauthorized access is called \_\_\_\_\_.

Answer: Encryption

7. \_\_\_\_\_ is a cyber attack where a large number of compromised computers are used to flood a target system with traffic, causing it to become unavailable.

Answer: DDoS (Distributed Denial of Service)

8. The term \_\_\_\_\_ refers to the practice of securing information by verifying the identity of individuals or systems.

Answer: Authentication

9. \_\_\_\_\_ is a set of security practices, policies, and technologies designed to protect computer systems and data from unauthorized access.

Answer: Cybersecurity

10. A piece of code that is capable of replicating itself and spreading to other programs or files is known as a \_\_\_\_\_.

Answer: Virus

1. What does HTTPS stand for, and why is it important for safe browsing?

Answer: HTTPS stands for Hypertext Transfer Protocol Secure. It encrypts the data exchanged between your browser and the website, ensuring a secure and private connection.\*

2. Why should you regularly update your web browser?

Answer: Regular updates include security patches that fix vulnerabilities, protecting users from potential threats and ensuring a safer browsing experience.\*

3. What is the purpose of a browser extension, and how can it impact online security?

Answer: Browser extensions provide additional functionalities but can pose security risks. Users should only install extensions from reputable sources to avoid potential malware or privacy issues.\*

4. How can you recognize a phishing website, and why is it crucial for safe browsing?

\*Answer: Phishing websites often have suspicious URLs, incorrect spelling, and may request sensitive information. Recognizing these signs is crucial to avoid falling victim to scams and protecting personal data.\*

5. Explain the significance of using a strong, unique password for your browser accounts.

Answer: A strong, unique password enhances account security, reducing the risk of unauthorized access and potential data breaches.\*

6. What is incognito or private browsing, and how does it contribute to safe browsing?

Answer: Incognito or private browsing mode doesn't save browsing history, cookies, or site data, offering a more private and secure online session. However, it doesn't make users completely anonymous.\*

7. How can you ensure that a website is secure before entering sensitive information, such as passwords or credit card details?

Answer: Look for the padlock icon in the address bar and ensure the URL starts with "https://". These indicate a secure, encrypted connection.\*

8. Explain the concept of cookie management and why it is important for safe browsing.

Answer: Cookies store information about user preferences. Managing cookies helps control what data websites can access, enhancing privacy and security.\*

9. What is two-factor authentication (2FA), and how does it enhance the security of online accounts?

Answer: Two-factor authentication adds an extra layer of security by requiring a second verification step, such as a code sent to your mobile device, in addition to your password.\*

10. How can you protect your browser from malicious software, and why is this essential for safe browsing?

Answer: Installing reputable antivirus and anti-malware software can help protect browsers from malicious software, ensuring a safer online experience by preventing infections and unauthorized access.