1. Define the terms Virus, Malware, and Ransomware.

* Virus: A program that replicates itself and spreads to other files or systems, often causing harm.
* Malware: A broader term encompassing any malicious software that disrupts or gains unauthorized access to computer systems.
* Ransomware: A malicious software encrypting files or computer systems and requesting a ransom for their decryption.

2. Explain the difference between a Threat, Vulnerability, and Risk in cybersecurity.

* Threat: Any potential danger or harmful event that can exploit vulnerabilities and negatively impact security.
* Vulnerability: Weaknesses or gaps in security measures that threats can exploit.
* Risk: The probability of a threat capitalizing on a vulnerability and the potential consequences or damage it may inflict.

3. What is Phishing? Provide an example.

* [Phishing](https://www.simplilearn.com/tutorials/cryptography-tutorial/what-is-phishing-attack): A cyberattack in which malicious actors employ deceptive emails or messages to deceive individuals into disclosing sensitive information.
* Example: An email claiming to be from a bank, requesting the recipient to provide their login credentials by clicking a link that leads to a fake website.

4. How do firewalls protect network security?

* Firewalls serve as protective barriers, overseeing and screening both inbound and outbound network traffic in accordance with established security regulations.
* They block unauthorized access and help prevent malicious data from entering or leaving a network.

5. What is a VPN and why is it used?

* A Virtual Private Network encrypts and secures internet connections, ensuring privacy and anonymity.
* It protects data from eavesdropping, accesses restricted content, and enhances public Wi-Fi security.

6. Explain the concept of a secure Password.

* A secure password is complex, lengthy, and difficult to guess.
* It comprises a combination of uppercase and lowercase letters, numbers, and special characters, with the requirement that this combination should be distinct for every individual account.

7. What are the common techniques for securing a computer network?

Techniques include using strong passwords, regular updates and patch management, implementing firewalls, using intrusion detection systems, and conducting security audits.

8. What is two-factor authentication, and why is it important?

* Two-factor authentication enhances security by necessitating users to furnish two distinct forms of verification, typically a password and a temporary code, thereby bolstering protection.
* It's important because even if a password is compromised, unauthorized access is prevented without the second factor.

9. Define the terms Encryption and Decryption.

* Encryption: Converting plaintext data into a coded format to protect it from unauthorized access.
* Decryption: Converting encrypted data back into its original, readable form.

10. What is SSL encryption?

[SSL](https://www.simplilearn.com/tutorials/cyber-securiy-tutorial/ssl-handshake) (Secure Sockets Layer) encryption is a protocol that ensures secure data transmission between a user's web browser and a website server, protecting data during transit.

11. What is the difference between IDS and IPS?

* IDS (Intrusion Detection System): Monitors network traffic and generates alerts when suspicious activity is detected.
* IPS (Intrusion Prevention System): Not only detects but also actively blocks or prevents suspicious network activity.

12. Explain what a security audit Is.

A security audit systematically evaluates an organization's information systems and security policies to assess their effectiveness, identify vulnerabilities, and recommend improvements.

13. What steps would you take if you discovered a security breach?

Isolate affected systems, contain the breach, notify relevant parties, investigate the incident, remediate vulnerabilities, and implement measures to prevent future breaches.

14. What is social engineering? Give an example.

* Social engineering manipulates individuals to disclose confidential information or perform actions for malicious purposes.
* Example: Pretending to be a trusted colleague and asking for login credentials over the phone.

15. What are cookies in a web browser?

Cookies are stored by websites on a user's device. They are used to track user preferences, session information, and provide a personalized browsing experience.

16. What is a DDoS attack and how does it work?

A Distributed Denial of Service (DDoS) attack inundates a target server or network with excessive traffic originating from numerous sources, making it inaccessible to genuine users.

17. Explain what a security policy is.

A security policy comprises a collection of formally documented regulations, recommendations, and protocols that delineate an organization's methods to safeguard its information, assets, and technological resources.

18. What is the difference between symmetric and asymmetric encryption?

* Symmetric Encryption uses a similar key for encryption and decryption.
* Asymmetric Encryption employs a pair of keys, one public and one private. Data that is encrypted with one key can only be deciphered using the complementary key.

### 19. Explain the concept of a digital signature.

A [digital signature](https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-are-digital-signatures) employs cryptographic methods to confirm the genuineness and unaltered state of a digital document or message, assuring both the sender's authenticity and the content's integrity.

### 20. What is a brute force attack?

It involves attackers employing a trial-and-error approach to find a password or encryption key by systematically testing every conceivable combination until they discover the correct one.

### 21. What are the common cyber threats today?

Common threats include malware, ransomware, phishing, DDoS attacks, insider threats, and zero-day vulnerabilities.

### 22. What is the role of patch management in maintaining security?

Patch management regularly applies updates and patches to software and systems to fix security vulnerabilities. It's crucial for preventing the exploitation of known weaknesses by attackers.

### 23. What are the key elements of a strong security policy?

A strong security policy includes elements like access control, encryption, regular updates, user training, incident response plans, and compliance with relevant regulations.

### 24. How does Secure Socket Layer (SSL) work?

SSL protocol ensures secure data transmission between web browsers and servers using encryption, authentication, and data integrity checks.

### 25. What is network sniffing?

Network sniffing is the practice of intercepting and analyzing network traffic to gather information, potentially for malicious purposes. It can be used for monitoring or attacks.

### 26. Discuss the role of artificial intelligence in cybersecurity.

AI is used for threat detection, pattern recognition, and anomaly detection to improve cybersecurity defenses and automate incident response.

### 27. What are the challenges in cloud security?

Challenges include data breaches, compliance, data loss prevention, and securing shared responsibility models in cloud environments.