1. What is phishing, and how does it work?
2. What are some common tactics used in SMS phishing (smishing)?
3. What is the difference between a virus, a worm, and a Trojan horse?
4. How can I detect if my computer is infected with malware?
5. What are botnets, and how do they operate in cyberattacks?
6. What is fileless malware, and why is it harder to detect?
7. How can a business secure its wireless network, and why is WPA2 or WPA3 encryption important?
8. What are the characteristics of a strong password?
9. What are the common types of direct attacks used to steal passwords?
10. How can removable devices like USBs pose security risks?
11. What are best practices for encrypting sensitive files?
12. What measures can improve smartphone security against cyber threats?
13. What steps should businesses take to secure their wireless networks?
14. What is multi-factor authentication, and why is it essential for cybersecurity?
15. What is malware, and how does it threaten computer systems?
16. Explain the concept of polymorphic viruses and their impact on antivirus systems
17. How do ransomware attacks typically occur, and what steps can mitigate their impact on businesses?
18. How does email spoofing work, and what measures can organizations take to prevent it?
19. What are some common characteristics of phishing emails that users should be aware of?
20. How does the "zero trust" security model differ from traditional network security approaches?
21. Why is it important for organizations to maintain an up-to-date inventory of hardware and software assets?
22. How can email authentication technology prevent phishing scams?
23. How can organizations effectively back up data to ensure recovery after cyber incidents?
24. What are the main risks of using public Wi-Fi networks, and what precautions should employees take when connecting to them?
25. What are the primary security risks associated with removable devices like USBs, and how can these risks be minimized?
26. What are the key considerations for organizations when implementing a bring your own device (BYOD) policy?
27. Describe the Entry Point Obscuring (EPO) technique used by some viruses and why it's effective against antivirus systems.
28. How do logic bombs operate, and what typically triggers their activation?
29. What role does employee training play in preventing phishing attacks and other social engineering threats?
30. What is the purpose of the insertion code in a virus, and what strategies do virus designers use for code placement?
31. What are rootkits, and how do they allow attackers to maintain control over infected systems?
32. How do botnets function, and what types of malicious activities can they be used for?
33. What are the risks associated with using default credentials, and how can they be mitigated?