Malware and Cyber Threats

1. What types of malicious software can disguise themselves as legitimate applications or hide within a system?
2. How do sophisticated attackers maintain long-term access to target systems?
3. What techniques do cybercriminals use to manipulate people into divulging sensitive information?

Authentication and Access Control

1. What protocols are used to securely verify user identities across networks?
2. How do different access control models determine who can access specific resources?
3. What methods can enhance login security beyond just using passwords?
4. How can organizations manage user access across multiple systems or domains?
5. What factors can be considered when granting or restricting access to resources?

Network Security

1. Which protocols ensure secure communication and data transfer over networks?
2. How can network design improve security by isolating different parts of a system?
3. What tools can detect and prevent unauthorized access attempts on networks and individual devices?
4. How do load balancers maintain consistent user experiences across multiple servers?
5. What technology securely connects remote users to a private network?
6. How do modern wireless security standards protect against unauthorized access?

7. What systems are used to monitor and control industrial processes from a central location?

Security Best Practices

1. How does limiting user privileges contribute to overall system security?
2. What are the three core principles of cybersecurity?
3. What strategies can organizations employ to prevent or mitigate cyber-attacks?
4. How can organizations protect their users from deceptive emails and websites?
5. How can attackers intercept or redirect network traffic to gain unauthorized access?