

CYBERSECURITY

DISCUSSION QUESTIONS



A2

1. What is cybersecurity?
2. Why is it important to have passwords?
3. What is a computer virus?
4. How can you keep your computer safe?
5. What should you do if you see something strange on your computer?
6. Why shouldn't you share your password with others?
7. What is a hacker?
8. How can you protect your personal information online?
9. What does a firewall do?
10. Why is it important to update your computer?
11. What are some safe websites you know?
12. How do you know if an email is safe to open?
13. What can happen if your computer is not secure?
14. Why is it important to log out of websites?
15. What are some rules you should follow when using the internet?
16. How can you make a strong password?
17. Why should you be careful when downloading files?
18. What does it mean to encrypt data?
19. How do professionals protect computer systems?
20. What should you do if you lose your device?

B1

1. Discuss the different types of cyber threats.
2. How do firewalls protect your computer?
3. What are the dangers of using public Wi-Fi?
4. How can you recognize a phishing attack?
5. Discuss the importance of data encryption.
6. What are the consequences of a data breach?
7. How can you secure your mobile device?
8. What are some common cybersecurity myths?
9. Discuss the role of antivirus software.
10. How can businesses protect themselves from cyber attacks?
11. What is two-factor authentication and how does it work?
12. How does social engineering work in cyber attacks?
13. Discuss the impact of cybersecurity on online privacy.
14. What should you do if your personal information is compromised?
15. How can you safely use social media?
16. Discuss the importance of backing up your data.
17. What are some signs that your computer might be infected?
18. How do governments protect against cyber attacks?
19. What is the role of cybersecurity professionals?
20. Discuss the future challenges in cybersecurity.

B2

1. Analyze the impact of cybersecurity on global business.
2. Debate the balance between cybersecurity and user convenience.
3. Discuss the ethical implications of cyber surveillance.
4. Evaluate the effectiveness of current cybersecurity measures.
5. Analyze the role of artificial intelligence in cybersecurity.
6. Discuss the challenges in protecting against zero-day attacks.
7. Evaluate the impact of cybersecurity laws on personal freedoms.
8. Discuss the role of encryption in protecting sensitive information.
9. Analyze the impact of cyber warfare on international relations.
10. Debate the responsibilities of companies in protecting customer data.
11. Discuss the impact of cybersecurity on the Internet of Things (IoT).
12. Analyze the role of human error in cybersecurity breaches.
13. Evaluate the role of cybersecurity in critical infrastructure.
14. Discuss the challenges of securing cloud-based systems.
15. How does cybersecurity affect e-commerce?
16. Analyze the impact of ransomware attacks on organizations.
17. Discuss the role of cybersecurity in healthcare data protection.
18. Evaluate the challenges of securing mobile applications.
19. Analyze the role of international cooperation in cybersecurity.
20. Debate the future of cybersecurity in an increasingly connected world.

C1

1. Critique the role of cybersecurity in protecting digital rights.
2. Analyze the impact of quantum computing on cybersecurity.
3. Evaluate the challenges of cybersecurity in a remote work environment.
4. Discuss the implications of machine learning in cyber defense strategies.
5. Examine the role of cybersecurity in financial services.
6. Analyze the challenges of cybersecurity in emerging technologies.
7. Evaluate the role of ethical hacking in strengthening security.
8. Discuss the implications of biometric security measures.
9. Examine the challenges in regulating international cyber crime.
10. Critically assess the role of public awareness in cybersecurity.

C2

1. Debate the philosophical aspects of cybersecurity in a digital age.
2. Analyze the long-term impacts of cybersecurity policies on society.
3. Critically evaluate the role of cybersecurity in national defense strategies.
4. Examine the ethical implications of autonomous cyber defense systems.
5. Discuss the implications of cybersecurity on global digital inequality.
6. Analyze the impact of cybersecurity on the future of democracy.
7. Evaluate the role of blockchain technology in enhancing cybersecurity.
8. Debate the impact of international cybersecurity treaties on sovereignty.
9. Examine the role of cybersecurity in shaping future tech developments.
10. Critically assess the balance between cybersecurity and digital innovation.