

The history of cybersecurity

The eight CISSP security domains

Review: The evolution of cybersecurity

Video: Wrap-up

1 min

Reading: Glossary terms from week 2

10 min

Quiz: Weekly challenge 2

10 questions

🎉 Congratulations! You passed!

Grade received: 95%

Latest Submission

Weekly challenge 2

Quiz • 10 min

To pass 80% or higher

Go to next item

Review Learning Objectives

1. What is the term for software that is designed to harm devices or networks?

1 / 1 point

👉 Malware

Submit your assignment

🕒 11:59 PM +03

Attempts: 3 every 24 hours

🔄 Try again

2. What historical event used a malware attachment to steal user information and passwords?

1 / 1 point

👉 LoveLetter attack

🕒 11:59 PM +03

🔍 Report an issue

3. Fill in the blank: Social engineering is a _____ that exploits human error to gain private information, access, or valuables.

1 / 1 point

👉 manipulation technique

🕒 11:59 PM +03

4. Which of the following threats are most likely to occur in the event of a phishing attack? Select all that apply.

0.5 / 1 point

👉 Theft of the organization's hardware

👉 This should not be selected

Please review, [🔗the video on attacks in the digital age](#) 17.

👉 Employees inadvertently revealing sensitive data

👉 Malicious software being deployed

👉 Overloading systems with too many internal emails

👉 This should not be selected

Please review, [🔗the video on attacks in the digital age](#) 17.

5. Which domain involves defining security goals and objectives, risk mitigation, compliance, business continuity, and the law?

1 / 1 point

👉 Security architecture and engineering

👉 Identity and access management

👉 Security and risk management

👉 Security assessment and testing

👉 Correct

6. Which of the following tasks may be part of the security architecture and engineering domain? Select all that apply.

0.5 / 1 point

👉 Securing hardware

👉 This should not be selected

Please review, [🔗the video on security domains](#) 17.

👉 Ensuring that effective systems and processes are in place

👉 Validating the identities of employees

👉 This should not be selected

Please review, [🔗the video on security domains](#) 17.

👉 Configuring a firewall

👉 Correct

7. Which of the following tasks may be part of the asset security domain? Select all that apply.

0.75 / 1 point

👉 Securing digital and physical assets

👉 Proper disposal of digital assets

👉 Ensuring users follow established policies

👉 This should not be selected

Please review [the video on security domains](#) 17.

👉 Data storage and maintenance

👉 Correct

8. A security professional is auditing user permissions at their organization in order to ensure employees have the correct access levels. Which domain does this scenario describe?

0 / 1 point

👉 Security assessment and testing

👉 Security and risk management

👉 Communication and network security

👉 Asset security

👉 Incorrect

Please review [the video on security domains](#) 17.

9. Which of the following tasks may be part of the identity and access management domain? Select all that apply.

0.75 / 1 point

👉 Ensuring users follow established policies

👉 Conducting security control testing

👉 This should not be selected

Please review, [🔗the video on security domains](#) 17.

👉 Setting up an employee's access keycard

👉 Controlling physical assets

👉 Correct

10. Which of the following tasks may be part of the security operations domain? Select all that apply.

0.75 / 1 point

👉 Conducting investigations

👉 Investigating an unknown device that has connected to an internal network

👉 Implementing preventive measures

👉 Using coding practices to create secure applications

👉 This should not be selected

Please review, [🔗the video on security domains](#) 17.