1. Introduction to Security

Weeks 1–4

安全导论

They should be able to

1. Identify common indicators of social engineering tactics.
2. Explain how social engineering tactics influence victims to perform a desired action.
3. Describe possible impacts for victims of social engineering attacks.
4. Identify common signs of a password attack.
5. Explain how adversaries take advantage of weak authentication.
6. Explain how to make authentication stronger.
7. Identify the type of adversary conducting a cyberattack.
8. Identify types of wireless cyberattacks.
9. Describe actions individuals can take to increase protection of sensitive data when using the internet and Wi-Fi.
10. Explain how adversaries use AI-powered tools to augment cyberattacks.
11. Explain how to protect against some AI-augmented cyberattacks.
12. Explain how cyber defenders can leverage AI-powered tools to protect networks, applications, and data.
13. Explain how AI-powered tools are enabling faster and more accurate threat detection and response.

Stage	Use	Your notes
Starter 10 min · retrieval practice	Topic quiz 01 (10 questions, answers on sheet 2)	
Teach the new content	Handout 01 Slide deck 01 Vocabulary list 01	
Practice guided then independent	Exercise sheets 1.1, 1.2, 1.3, 1.4, 1.5 Past-paper sheets 1.1	
Check before they leave	*nothing in the Library for this stage yet*	
Homework set from the Library	Any unused exercise sheet above Holiday homework pack	

2. Securing Spaces

Weeks 5–11

保护物理空间

They should be able to

1. Identify social engineering attacks.
2. Identify types of adversaries.
3. Describe the phases of a cyberattack.
4. Describe the risk assessment process.
5. Identify strategies for managing risk.
6. Identify types of security controls.
7. Explain why a defense-in-depth security strategy is necessary to optimally protect an organization.
8. Identify common physical attacks.
9. Explain how threats can exploit common physical vulnerabilities to cause loss, damage, disruption, or destruction to assets.
10. Assess and document risks from physical vulnerabilities.
11. Identify managerial controls related to physical security.
12. Determine mitigation strategies for risks from physical vulnerabilities.
13. Identify ways security controls can detect physical attacks.
14. Determine effective placement of security controls for detecting physical attacks.
15. Apply detection techniques to identify physical attacks.

Stage	Use	Your notes
Starter 10 min · retrieval practice	Topic quiz 02 (10 questions, answers on sheet 2)	
Teach the new content	Handout 02 Slide deck 02 Vocabulary list 02	
Practice guided then independent	Exercise sheets 2.1, 2.2, 2.3, 2.4 Past-paper sheets 2.1, 2.2	
Check before they leave	*nothing in the Library for this stage yet*	
Homework set from the Library	Any unused exercise sheet above Holiday homework pack	

3. Securing Networks

Weeks 12–17

保护网络

They should be able to

1. Identify common network attacks.
2. Explain how adversaries can exploit network vulnerabilities to steal, disrupt, or destroy network communication.
3. Assess and document risks from network vulnerabilities.
4. Identify managerial controls related to network security.
5. Configure wireless network security features.
6. Identify techniques for segmenting a network.
7. Explain why network segmentation can increase network security.
8. Identify types of network-based firewalls.
9. Explain how a firewall uses an access control list to allow or deny traffic entering or leaving a network.
10. Determine the effective placement of firewalls in a network.
11. Configure a firewall to manage the flow of network traffic.
12. Identify types of automated security tools used to detect network attacks.
13. Explain how organizations can leverage artificial intelligence (AI) to enhance threat detection and response.
14. Determine a network detection method.
15. Evaluate the impact of a network detection method.
16. Apply detection techniques to identify indicators of network attacks by analyzing log files.

Stage	Use	Your notes
Starter 10 min · retrieval practice	Topic quiz 03 (10 questions, answers on sheet 2) Starter quiz 3 – past-paper questions	
Teach the new content	Handout 03 Slide deck 03 Vocabulary list 03	
Practice guided then independent	Exercise sheets 3.1, 3.2, 3.3, 3.4, 3.5 Past-paper sheets 3.1, 3.4, 3.5	
Check before they leave	Unit test 3 (with mark scheme)	
Homework set from the Library	Any unused exercise sheet above Holiday homework pack	

4. Securing Devices

Weeks 18–23

保护设备

They should be able to

1. Identify types of computing devices.
2. Identify the type of malware used in a cyberattack.
3. Explain how adversaries can exploit common device vulnerabilities to cause loss, damage, disruption, or destruction.
4. Assess and document risks from device vulnerabilities.
5. Explain why hashes (also called hash outputs, checksums, message digests, or digests) are used to store passwords.
6. Explain how password attacks exploit vulnerabilities.
7. Determine the type of authentication used to verify the identity of a user.
8. Configure login settings to make a device more secure.
9. Identify managerial controls related to device security.
10. Explain how anti-malware software can make a device more secure.
11. Explain why keeping a device's operating system and software updated makes it more secure.
12. Configure a host-based firewall.
13. Explain how to detect attacks against devices.
14. Determine controls for detecting attacks against a device.
15. Evaluate the impact of a device detection method.
16. Apply detection techniques to identify indicators of password attacks by analyzing log files.

Stage	Use	Your notes
Starter 10 min · retrieval practice	Topic quiz 04 (10 questions, answers on sheet 2) Starter quiz 4 – past-paper questions	
Teach the new content	Handout 04 Slide deck 04 Vocabulary list 04	
Practice guided then independent	Exercise sheets 4.1, 4.2, 4.3, 4.4 Past-paper sheets 4.2, 4.4	
Check before they leave	Unit test 4 (with mark scheme)	
Homework set from the Library	Any unused exercise sheet above Holiday homework pack	

5. Securing Applications and Data

Weeks 24–30

保护应用与数据

They should be able to

1. Explain how adversaries can exploit application and file vulnerabilities to cause loss, damage, disruption, or destruction.
2. Explain how application attacks exploit vulnerabilities.
3. Assess and document risks from application and data vulnerabilities.
4. Explain how the state or classification of data impacts the type and degree of security applied to that data.
5. Identify managerial controls related to application and data security.
6. Determine an appropriate access control model to protect applications and data.
7. Configure access control settings on a Linux-based system.
8. Explain how encryption can be used to protect files.
9. Apply symmetric encryption algorithms to encrypt and decrypt data.
10. Determine the appropriate asymmetric key to use when sending or receiving encrypted data.
11. Explain why the length of a key impacts the security of encrypted data.
12. Apply asymmetric encryption algorithms to encrypt and decrypt data.
13. Identify the application security principles of secure by design and security by default.
14. Explain how user input sanitization protects applications.
15. Explain how to detect attacks on data.
16. Determine controls for detecting attacks against applications or data.
17. Evaluate the impact of a method for detecting attacks against an application or data.
18. Identify whether a file has been altered by verifying its hash.
19. Apply detection techniques to identify and report indicators of application attacks by analyzing log files.

Stage	Use	Your notes
Starter 10 min · retrieval practice	Topic quiz 05 (10 questions, answers on sheet 2) Starter quiz 5 – past-paper questions	
Teach the new content	Handout 05 Slide deck 05 Vocabulary list 05	
Practice guided then independent	Exercise sheets 5.1, 5.2, 5.3, 5.4, 5.5, 5.6 Past-paper sheets 5.1, 5.2, 5.5, 5.6	
Check before they leave	Unit test 5 (with mark scheme)	
Homework set from the Library	Any unused exercise sheet above Holiday homework pack	