Y10 - HT5 – Principles of Computer Science

High Tunstall College of Science Curriculum Intent

Topic:	Principles of Computer Science Topic 3: Computers Topic 5: Issues and Impact ***Vulnerabilities and Malware***	Year:	10	Half Term:	5

	Progress		
Key Ideas	**R**	**A**	**G**
I can define what is meant by the term ‘cyberattack’			
I can describe the financial, reputational and legal damage that a cyberattack can cause			
I can describe the characteristics of and threats posed by different types of malware			
I can describe how anti-malware software works			
I can explain why it is important to keep anti-malware software up to date			
I can define what is meant by the term ‘hacker’			
I can explain why unpatched software is a target for hackers			
I can explain the function of a firewall			
I can explain how ethical hacking and penetration testing help identify vulnerabilities			
Define what is meant by the term ‘social engineering’			
I can describe some commonly used social engineering tactics (phishing, pretexting, baiting, quid pro quo) used by hackers			
I can explain the purpose of an Acceptable Use Policy (AUP) and what it typically includes			
I can explain how data is protected by encryption			
I can describe how backup and recovery procedures protect against data loss			
I can explain how access control helps to protect systems and data			
I can define what is meant by the term ‘robust software’			
I can explain how a hacker can exploit a code vulnerability			
I can describe examples of bad coding practices and secure coding practices			
I can explain how code reviews and audit trails help to identify vulnerabilities			

Lesson	**Learning Focus**	**Assessment**	**Key words**
1 **(P25)**	Define what is meant by the term ‘cyberattack’ Describe the financial, reputational and legal damage that a cyberattack can cause Describe the characteristics of and threats posed by different types of malware Describe how anti-malware software works Explain why it is important to keep anti-malware software up to date	Evidence in Teams End of topic assessment	Adware, Anti-malware, Bots, Cyberattack, Keyloggers, Malware, Ransomware, Trojans, Virus, Worms
2 **(P26)**	Define what is meant by the term ‘hacker’ Explain why unpatched software is a target for hackers	Evidence in Teams End of topic assessment	Ethical hacking, Firewall, Hacker, Patches, Penetration testing, Social Skills,

	Explain the function of a firewall Explain how ethical hacking and penetration testing help identify vulnerabilities		Unauthorised access,
3 **(P27)**	Define what is meant by the term ‘social engineering’ Describe some commonly used social engineering tactics (phishing, pretexting, baiting, quid pro quo) used by hackers Explain the purpose of an Acceptable Use Policy (AUP) and what it typically includes	Evidence in Teams End of topic assessment	Acceptable Use Policy (AUP), Baiting, Phishing, Pretexting (blagging), Quid pro quo, Social Engineering,
4 **(P28)**	Explain how data is protected by encryption Describe how backup and recovery procedures protect against data loss Explain how access control helps to protect systems and data	Evidence in Teams End of topic assessment	Access control, Backup, Data, Encryption, Physical security, Protecting data, Recovery
5 **(P29)**	Define what is meant by the term ‘robust software’ Explain how a hacker can exploit a code vulnerability Describe examples of bad coding practices and secure coding practices Explain how code reviews and audit trails help to identify vulnerabilities	Evidence in Teams End of topic assessment	Audit trails, Code reviews, Hackers, Robust software, Security, Vulnerabilities
6 **(P30)**	Revision lesson All of the above	Evidence in Teams End of topic assessment	All of the above
7 **(P30)**	End of topic Assessment	End of topic assessment	All of the above
8 **(P30)**	Assessment feedback lesson	Evidence in Teams	All of the above