Topic: Unit 1.4 Network Security

Key vocabulary:	**Core knowledge questions**	**Powerful knowledge crucial to commit to long term memory**	**Links to previous and future topics**

Malware
Virus
Worm
Trojan Horse
Phishing
Social Engineering
Data Interception
Network Policies
Brute Force Attacks
DDoS
Botnet
Exploit
SQL Injection
Network Forensics
Penetration Testing
Anti-Malware / Virus
Firewall
Legislation
Packet Sniffing
User Access Levels
Passwords
Encryption
Cipher
Key
	1. What are the main forms of attack?
	2. What is Malware?
	3. What is Social Engineering? (eg phishing, people as the weak point)
	4. What is a Brute-Force Attack?
	5. What are Denial of Service Attacks?
	6. What is Data interception and Theft?
	7. Explain the concept of SQL Injection
	8. What are common prevention methods?
	9. What is penetration testing?
	10. What is Anti-Malware software
	11. What is a Firewall
	12. What are User Access Levels?
	13. Explain the secure use of Passwords
	14. What is Encryption?
	15. What is Physical Security?
		• Know and describe the threats posed to devices/systems
		• Understand the principles and have knowledge of each form of attack including:
		  ○ How the attack is used
		  ○ The purpose of the attack
		• Understanding of how to limit the threats posed
		• Understanding of methods to remove vulnerabilities
		• Understand the principles and have knowledge of each prevention method including:
		  ○ What each prevention method may limit/prevent
		  ○ How it limits the attack
			• Network Security is covered in Y7 and Y8
			• Security is fundamental to Computer Science and will be revisited throughout the course.
			• The previous topics 1.3 is Computer Networks, Connections and Protocols, which appropriately leads into this network security theme

We will develop these skills:

Impressive reading	**Impressive speaking**	**Impressive writing**	**Resilience**	**Numeracy via:**	**Digital Literacy via:**	**Employability via:**
Research using the Internet to find relevant and appropriate information about threats posed and how they can be limited. Interpreting scenarios to recommend appropriate preventions	Discussion of research findings. Discussion in groups of threats and preventions	Recording research findings appropriately. Writing definitions for each threat and methods of prevention. Answering exam questions	Developing ability to consistently amend and refine work. Listen to others' opinions	Encryption, Caesar Cipher, using left and right shifts, deciphering encrypted text	Use of the Internet Use of MS Office Suite	Teamwork – working in groups Flexibility – taking on opinions of others Problem Solving – using information to decipher encrypted text

SEND

- Peer Support - Some students may be more aware of Networking Security and associated issues – use these students as Lead Students
- Differentiated Activities and Tasks, choice of tasks for certain activities, support sheets
- Questioning
- Flipped Learning resources for students to study either prior to or after lesson
- Peer Assessment / Support on labelling tasks
- Provision of scaffolded writing schemes to allow learners to complete appropriate and accurate definitions