Scheme of Learning: Year 9 Computing

Topic Sequence:

1	2
Cyber Security	Animations

Topic Overview:

This unit takes learners on a journey of discovery of techniques that cybercriminals use to steal data, disrupt systems, and infiltrate networks. The learners will start by considering the value their data holds and what organisations might use it for. They will then learn about social engineering and other common cybercrimes, and finally look at methods to protect against these attacks.

Links
Year 7: Networks, GCSE computing Unit 4 Networks

Lesson Sequence:

Lesson 1: You and your data - Learners are introduced to the unit to help them understand the value of data to companies. The focus will be on what data companies collect from their users and how they use it. They will be introduced briefly to the law regarding data protection and will reflect on why cybercriminals might want to gain access to data.
Lesson 2: Social engineering - The aim of this lesson is for learners to become aware of how humans can be a weak point in the system, as well as looking at the social engineering tactics deployed by cybercriminals to dupe users into giving away data that could lead to further crime. Learners will be taken through the common social engineering techniques, completing exercises through the lesson to encourage them to think more deeply about the consequences of the scams and how to avoid becoming a victim.
Lesson 3: Script kiddies - Learners explore the concept of hacking and the techniques used by hackers to exploit computer systems. They look at terms such as brute force attacks, hacktivists, script kiddies, and DDoS attacks. The lesson will conclude with the learners exploring the Computer Misuse Act and the consequences of hacking.
Lesson 4: Rise of the bots - The purpose of this lesson is to make learners aware of malware and the different categories of malware, as well as understanding how they work and the potential damage they can do. They will then be introduced to the key terms before being instructed to do a research task to create a fact-based quick read on one type of malware they have learnt about. Learners will be introduced to web bots and what task they perform on the internet. They will then be shown how bots are used in conjunction with malware and will be given a scenario that allows them to understand the hidden role of bots and what potential influence they could have on societal issues.
Lesson 5: There's no place like 127.0.0.1 - The aim of this lesson is for learners to develop their understanding of the risks that cyberthreats pose to a network, followed by an exploration of some of the more common methods of defending a network against attacks, such as firewalls and anti-malware. The learners will look at the more common threats that exist globally before thinking of the threats at the level of a school network.
Lesson 6: Under Attack - the learners are encouraged to reflect on the learning that has taken place throughout the unit before taking an end-of-unit assessment. The learners will be prompted to reflect through a game called Under Attack. Learners will work in groups to plan their defence strategy on a tight budget before cyberattacks start to happen

National curriculum links

- Understand a range of ways to use technology safely, respectfully, responsibly, and securely, including protecting their online identity and privacy; recognise inappropriate content, contact, and conduct, and know how to report concerns

Education for a Connected World links

- I can explain how contributors to social media may be 'social bots'
- I can explain what malware is and give some examples of how it operates and what its impact could be on a device or user (e.g. viruses, trojans, ransomware)
- I can explain how to manage security software (e.g. anti-virus, security patches, adware blockers) on my devices and understand why regular updates are important
- I can explain how and assess when more secure use may require more advanced password management (e.g. dual-factor authentication, regular rolling, security questions, CAPTCHA, biometrics)

Sequence of Lessons:

1	Lesson 1: You and your data
2	Lesson 2: Social engineering
3	Lesson 3: Script kiddies
4	Lesson 4: Rise of the bots
5	Lesson 5: There's no place like 127.0.0.1
6	Lesson 6: Under Attack

Topic Resources:

Knowledge Map:	9.1 Cyber Security	**Any other Resources:**	

Assessment:

Knowledge:	15 Multiple Choice questions
Application of Knowledge:	Classwork and Strategy in the game

Supportive Reading:

BBC Bitesize	Malware and security - eSafety - KS3 ICT Revision - BBC Bitesize
KS3 Computing Complete Revision &	Chapter 2 Available from: KS3 Computing Complete Revision