Year 9 – Cybersecurity

Unit introduction

This unit takes the learners on an eye-opening journey of discovery about techniques used by cybercriminals to steal data, disrupt systems, and infiltrate networks. The learners will start by considering the value of their data to organisations and what they might use it for. They will then look at social engineering techniques used by cybercriminals to try to trick users into giving away their personal data. The unit will look at the more common cybercrimes such as hacking, DDoS attacks, and malware, as well as looking at methods to protect ourselves and our networks against these attacks.

Overview of lessons

Lesson	**Brief overview**	**Learning objectives**
Lesson 1: You and your data	The aim of this lesson is to introduce the learners to the unit and 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. Learners will explore this topic through scenarios as well as by looking at the privacy policies of some tech companies that they may already be giving data to. They will be introduced briefly to the law regarding data protection and will reflect on why cybercriminals might want to gain access to data.	● Explain the difference between data and information ● Critique online services in relation to data privacy ● Identify what happens to data entered online ● Explain the need for the Data Protection Act
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. The lesson starts with the learners using a Scratch program aimed	● Recognise how human errors pose security risks to data ● Implement strategies to minimise the risk of data being

	at tricking them into giving away personal information. Learners will then 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.	compromised through human error
Lesson 3: Script kiddies	This lesson allows the learners to explore the concept of hacking and the techniques used by hackers to exploit computer systems. The lesson starts with the learners looking for clues to hack into a friend's account to help his parents find out where he is. They will then be forced to think about the ethics behind their actions. The rest of the lesson looks at terms such as brute force attacks, hacktivists, script kiddies, and DDoS attacks. Some of the key terminology is introduced around the real-life example of the Dyn attack that disabled DNS servers (mostly in the USA) for a time. The lesson will conclude with the learners exploring the Computer Misuse Act and the consequences of hacking.	● Define hacking in the context of cyber security ● Explain how a DDoS attack can impact users of online services ● Identify strategies to reduce the chance of a brute force attack being successful ● Explain the need for the Computer Misuse Act
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. This lesson focuses more on the technical side than on prevention methods, which will be covered in Lesson 5 of this unit. This lesson will start with a pretend scenario of the network having been infected by ransomware; the learners have to decide what action to take. 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. Towards the end of the lesson, the 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.	● List the common malware threats ● Examine how different types of malware causes problems for computer systems ● Question how malicious bots can have an impact 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. Learners will discuss methods used by network managers to reduce risk. The homework for this lesson is to write a short report to the head teacher on how to manage the most significant risk to the school network.	● Compare security threats against probability and the potential impact to organisations ● Explain how networks can be protected from common security threats
Lesson 6: Under Attack	This is the final lesson in the unit, and 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. The use of their budget will be key in determining whether or not they were able to defend the organisation against the attack. Learners will then take their end-of-unit assessment and if there is time they will be directed to research the available career choices in cyber-defence.	● Identify the most effective methods to prevent cyberattacks

Progression

Curriculum links

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)