# KS4 – Cybersecurity

## Unit introduction

This unit enables GCSE students to gain knowledge and understanding of the range of cybersecurity threats that impact the world, our organisations, and us as individuals. The learners start by defining fundamental terms, such as cybersecurity and network security. They then progress to understanding different forms of attack, both non-automated and automated. Examining the different techniques used by social engineers (perpetrating non-automated attacks) enables the learners to protect themselves against tactics such as blagging, phishing, and pharming. They also learn about automated cybercrime, including denial-of-service (DoS) attacks and SQL injection.

The learners then take this further by examining how organisations design and use networks and software to reduce the likelihood of a cyberattack, for example by using firewalls, MAC address filtering, automatic software upgrades, and modular testing. They also learn about the policy side of organisations, understanding how levels of access and network policies can protect an organisation.

Once they have understood the impact of cybercrime, they learn about how companies identify and reduce vulnerability through penetration testing. Lastly, the unit encourages learners to be inspired to be part of the solution, as they find out about the potential for lucrative and fulfilling careers in cybersecurity.

##

## Overview of lessons

|  |  |  |
| --- | --- | --- |
| **Lesson** | **Brief overview** | **Learning objectives** |
| Lesson 1: The cost of cybercrime and hacker motivation | This lesson introduces the subject of cybersecurity to your learners. They begin to understand the difference between cybersecurity and network security and learn that although networks are wonderful inventions, they can make an organisation vulnerable to attack. Learners get a sense of the size of the problem as they learn how important it is to understand a hacker’s motivation and take the subject seriously. | * Describe the impact of cybercrime on businesses and individuals
* Analyse an attack on a company and identify what motivated the hackers
* Define the terms cybersecurity and network security, explain their importance, and distinguish between the two concepts
* Describe the features of a network that make it vulnerable to attack
 |
| Lesson 2: Non-automated cybercrime | This lesson enables the learners to distinguish between non-automated and automated cybercrime. The lesson focuses on social engineering and introduces the idea that humans are the weakest link in the security chain. Learners find out how to recognise and categorise different types of social engineering. | * Identify and describe non-automated forms of cyberattacks, and learn how humans can be the weak links in an organisation
* Demonstrate knowledge of social engineering through role playing activities and case studies
 |
| Lesson 3: Automated cybercrime | This lesson builds on the last lesson, which was about non-automated cybercrime, to enable learners to distinguish between non-automated and automated cybercrime. Learners are given terms and techniques related to automated cybercrime to help them understand the vulnerabilities of a network or software that can expose companies or individuals to such attacks. | * Describe automated forms of cyberattacks
* Analyse a real cyberattack and identify the network or software weaknesses that enabled it to happen
 |
| Lesson 4: Protecting systems with software | In the previous lessons, learners have developed their understanding of cyberattacks and identified the network and software weaknesses that can enable them to happen. In this lesson, they discover the ways to protect software systems, all the way from design to access. It leads on to Lesson 5, in which the learners find out how businesses secure their existing networks. | * Identify how software can be used to protect from cyberattacks
* Describe how organisations use software to protect against cyberattacks
 |
| Lesson 5: Network design as defence | This lesson builds on the previous one, which taught learners how companies design software that discourages cybercrime and how they use software to avoid cybercrime. Learners are introduced to the key concepts for the lesson and given an activity and descriptions to help them unpack the meanings. They then put their knowledge together to create a Network Access Control plan for the school. This lesson leads on to Lesson 6, in which the learners discover how businesses investigate themselves to ensure that the steps they have taken to stay safe are effective. | * Explain the need for, and the importance of, network security
* Explain a number of methods of achieving network security
 |
| Lesson 6: Where is the danger? | In this lesson, learners explore the steps that companies can take to discover where their vulnerabilities are with regards to a cyberattack. The lesson focuses on the role that penetration testers can play in helping with this process. The learners are given a role play scenario where they have to plan a penetration test for a social media company.  | * Describe different methods of identifying cybersecurity vulnerabilities, such as:
	+ Penetration testing
	+ Ethical hacking
	+ Network forensics
	+ Commercial analysis tools
	+ Review of network and user policies
 |
| Lesson 7: Being part of the solution | This lesson enables the learners to engage in a comprehensive end of unit assessment that covers aspects from each of the preceding six lessons. In addition, it provides some inspiration for the learners to get involved with cybersecurity for themselves, for the benefit of their careers and wider society. | * Evaluate the potential for cybersecurity careers
* Apply your knowledge of cybersecurity to GCSE-style questions
 |

## Progression

This unit progresses learners’ knowledge and understanding of the dangers that threaten IT systems, as well as methods of protection against such threats. View the learning graphs to see clear progression routes.

## Curriculum links

[**National curriculum links**](https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study/national-curriculum-in-england-computing-programmes-of-study)

* Develop their capability, creativity, and knowledge in computer science, digital media, and information technology
* Understand how changes in technology affect safety, including new ways to protect their online privacy and identity, and how to report a range of concerns

[**Education for a Connected World links**](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/683895/Education_for_a_connected_world_PDF.PDF)

### Privacy and security (age 11 to 14)

* I can explain what malware is and give some examples of how it operates and what the impact could be on a device or user (e.g. viruses, trojans, ransomware)
* I can explain how to manage security software (e.g. antivirus, 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)

### Privacy and security (age 14 to 18)

* I can explain how the security of data in a network can be compromised internally or externally and give examples of how this might occur (e.g. DDoS, proxy-bypass, distro, hacking); I can describe actions that can minimise risks
* I can explain why networks require secure management and can give examples of services that support this (e.g. firewalls, VPN, user monitoring)
* I can explain the value of regular data backup in system recovery, and can give examples of and demonstrate effective practice in how this might be achieved (e.g. removable media, cloud)
* I can identify and assess when data needs to be transferred securely and can describe strategies to achieve this (e.g. encryption, secure services)
* I can explain why it is essential to recognise and follow my future employer’s online security policy and protocols

## Assessment

### Summative assessment

* Please see the assessment question and answer documents for this unit

## Subject knowledge

This unit focuses on the following key areas of cybersecurity, cybercrime, and the laws in place surrounding these issues:

* Profiling
* Data Protection Act
* Computer Misuse Act
* Hacking
* Malware
* Protection methods such as firewalls, anti-malware, and password authentication

Enhance your subject knowledge to teach this unit through the following training opportunities:

### Online training courses

* [Introduction to Cybersecurity for Teachers](https://www.futurelearn.com/courses/teaching-cybersecurity)

### Face-to-face and remote courses

* [Introduction of computer systems, networks and cyber security in computer science (face to face)](https://teachcomputing.org/courses/CP238/an-introduction-to-computer-systems-networking-and-security-in-gcse-computer-science-face-to-face)
* [Introduction of computer systems, networks and cyber security in computer science (remote)](https://teachcomputing.org/courses/CP438/an-introduction-to-computer-systems-networking-and-security-in-computer-science-remote)
* [The internet and cyber security (face to face)](https://teachcomputing.org/courses/CP232/the-internet-and-cyber-security-face-to-face)
* [The internet and cyber security (remote)](https://teachcomputing.org/courses/CP432/the-internet-and-cyber-security-remote)

Resources are updated regularly — the latest version is available at: [ncce.io/tcc](http://ncce.io/tcc).

This resource is licensed under the Open Government Licence, version 3. For more information on this licence, see [ncce.io/ogl](http://ncce.io/ogl).