




System security

	Age group	11 and above
	Time	30 mins
	Subject	Computing



National Curriculum links

This activity would suit KS3 and KS4 students.

The national curriculum for computing for key stages 3 and 4 aims to ensure that all pupils “*can analyse problems in computational terms*” and “*are responsible, competent, confident and creative users of information and communication technology.*”

England Key stage 3 subject content

Pupils should be taught to:

- understand the hardware and software components that make up computer systems, and how they communicate with one another and with other systems
- design, use and evaluate computational abstractions that model the state and behaviour of real-world problems and physical systems
- 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

England Key stage 4 subject content

Pupils should be taught to:

- understand how changes in technology affect safety, including new ways to protect their online privacy and identity, and how to identify and report a range of concerns

Learning outcomes

Pupils should be able to:

- List the main areas covered by the Computer Misuse act.
- Explain the terms: phishing and ransomware.
- Describe how a company can keep its computer system secure.

Skills developed

- **Decomposition:** Breaking a bigger problem down into smaller more manageable sections.
- **Abstraction:** Removing unnecessary details to focus on the key parts.
- **Communication:** Sharing thoughts with others on how they arrived at their solution.

Prior Learning

Learners would benefit from understanding networks in a company to appreciate the implications of a hacker gaining access to a company's computer systems.

Requirements

Students will need access to computers and the internet to complete this task.

Overview of 'System security'

This activity gives learners the opportunity to consider the wider implications of unauthorised access to a company's computer systems. Pupils will look at the impact of hacking on a company and an individual as well as how individuals can act to keep a company's computer systems secure.

When any company utilises technology, it must consider the security of its systems to prevent criminals from hacking into the system to steal information or disrupt the company's business. There are different types of attacks from hackers, ones from inside the company and ones from outside. Both require a person or people to gain unauthorised access to a computer system. Hacking is gaining unauthorised access to a computer system and is an illegal act under the Computer Misuse Act. A system where all the devices are connected can give a hacker more options as they only need access to one device to gain access to many.

Resource Overview

This resource includes these items:

- Teacher notes.
- Student activity sheet setting out the task and giving the information required for the students.
- Exemplar responses which teachers may use to support groups of students who need some scaffolding to get started.
- Presentation slides to help explain the tasks.

The context

Emma, as part of her role as a trainer in a logistics company, has been asked to research and write a report highlighting the information needed for a new training session to staff on the importance of keeping the company safe from cybercriminals.

Her first step is to research the Computer Misuse Act, the threats from cybercriminals and how company staff can keep a company's computer systems secure from unauthorised access. She must then write a report highlighting the content that needs to be included in the training session which will help staff understand:

- why system security is important
- their role in keeping the company's computer system safe

The task

Students have to research the Computer Misuse Act, the potential risks from hackers and what actions can be taken by employees to prevent cybercriminals accessing a company's computer systems. Using this research pupils write a report highlighting the relevant information.

Supporting notes

This task could be completed in class or as homework.

Useful websites

Malicious software and emails:

- [Isaac Computer Science – Malicious software](#)
- [BBC Bitesize – Malware and security](#)
- [BBC Bitesize – Spam email and phishing](#)

Network Security:

- [Isaac Computer Science – Network security](#)
- [BBC Bitesize – Network security](#)
- [BBC Bitesize - Network security - Forms of attack](#)

(Please note - to use the free Isaac Computer science website, users need to register:
<https://isaaccomputerscience.org>)

Generation Logistics Education Hub

This resource is one of the many engaging resources available from Generation Logistics on their Education Hub. For more details go to: <https://educationhub.generationlogistics.org>