

How can employees stop hackers?

Background information

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 employees understand:

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

Your task - Possible responses

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.

Write a report highlighting the information to include in a new training session covering the following sections:

- What are the main areas covered by the Computer Misuse Act?

3 offences covered by the Computer Misuse Act:

1. *Unauthorised access – access a computer or its contents without authorisation*
2. *Unauthorised access with intent - access a network or device with the intent of committing further criminal activity.*
3. *Unauthorised modification - intent to modify or destroy a computer system, software or data without authorisation.*

- Why would someone hack into a logistics company's computer systems?
- *Find out the location of high-end goods with the intention of stealing them.*
- *Obtain financial details of customers, companies and employees to commit fraud.*
- *Obtain customer details for some sort of financial gain such as approaching them for business or fraud.*
- *Obtain employee details to gain access to them for marketing or fraud.*
- *Location of lorries to steal goods or the lorry.*
- *A competitor may want the plans for the company to find out that company's secrets.*
- *Lock the company's computer systems and demand payment before unblocking them.*
- What is phishing?
Phishing is an email received that looks legitimate with a request to click a link and enter personal information. This is not a legitimate email and is used to gather personal information usually for an unscrupulous purpose.
- What is ransomware?
Ransomware is malicious code used to stop you gaining access to your computer system. It then tells you to pay a sum of money for access to be granted again.

- What measures can the company's digital team take to keep the computer system secure?
- *Strong password management.*
- *Install a firewall.*
- *Install anti-malware software.*
- *Control user access rights dependent on level in the company.*
- *Ensure there is good physical security of system area – CCTV, card or key access.*
- *Train staff so they understand the risks from hackers and how to keep the company's computer systems safe.*
- *Employ a penetration tester to ethically hack into the system to highlight vulnerabilities and then rectify these.*
- What measures can all employees take to ensure that they keep the company's computer system safe?
- *Ensure they change their password regularly.*
- *Not use a password more than once.*
- *Use 2 factor authentication.*
- *Ensure strong passwords used and not shared.*
- *Computers locked when away from desk.*
- *Watch out for phishing emails by looking for common signs that an email is not legitimate such as poor spelling and grammar.*
- *Report any suspicious activity immediately.*