Explain **one** reason why software should be patched regularly.

(2)

Explain **one** reason why an employee who is logged on to the company network should not click on a link in an email from an unknown source.

(2)

Identify the **two** types of malware that replicate their code.

(2)

A Key logger **B** Ransomware **C** Trojan **D** Virus **E** Worm

Identify the type of malware that is disguised as a legitimate software and can give unauthorized access to a user's computer system? **(1)**

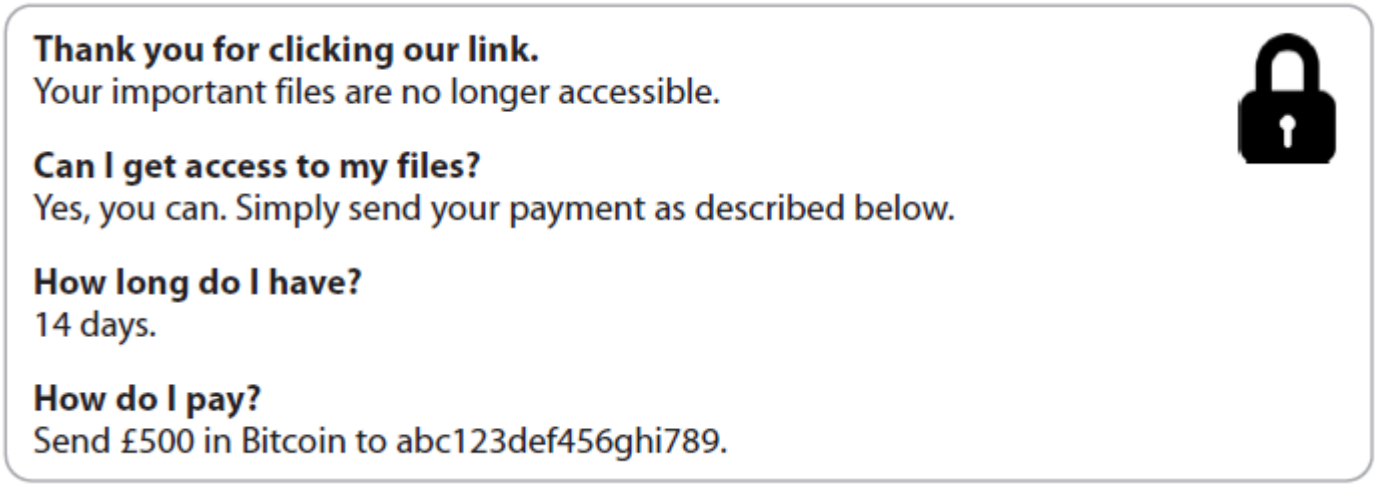
A) Worm **B**) Trojan **C**) Virus **D**) Adware

What can a Trojan do once it has infected a computer system?

A) Delete files or corrupt data **B**) Steal sensitive information, such as passwords and financial data

C) Turn the computer into a zombie or bot that can be controlled remotely **D)** All of the above **(1)**

Q4.
Issues and impact
This notification appears on a computer screen.



Name the type of malware used in this cyberattack.

(1)

Explain **one** way that digital systems may be vulnerable to cyberattacks when users do not properly maintain their software. **(1)**

How does anti-malware software detect and remove malicious software? **(1)**
A By encrypting sensitive files and hiding them from attackers **B**) By blocking access to known malicious websites
C) By scanning the computer system for known signatures and patterns of malware **D**) By preventing users from downloading any software from the internet

ANSWERS

1. **Regular software patching** is crucial because it **fixes security vulnerabilities**. These patches address weaknesses that could be exploited by hackers or allow malware to enter, ensuring better protection for systems and data.

   A **security vulnerability** is a weakness or flaw in software, hardware, or a system that could be exploited by attackers to compromise its integrity, confidentiality, or availability
2. **One crucial reason** why an employee should **avoid clicking on links** in emails from unknown sources is to **prevent phishing attacks**. These emails often contain malicious links that can lead to unauthorized access, data breaches, or the installation of harmful software. Any of these could compromise the company's network, potentially stopping the company's operation or putting customer's data at risk.

3. **D and E.** Both worms and viruses replicate their code and spread themselves quickly through connected devices. A worm doesn't need human action to install it but a virus does. **A keylogger** is a type of spyware that records keystrokes, stores them in a text file and sends this file back to the criminal who analyses it looking for personal data and usernames and passwords. **Ransomware** is a cyber attack where files are encrypted and the attacker demands a ransom to give the user access to their files again. A **Trojan** is a type of **malware** that disguises itself as legitimate software but actually carries out harmful actions without the user's knowledge or consent.

4. **B.** A **Trojan** disguises itself as harmless software but carries out malicious actions without the user's knowledge. It doesn't replicate like a virus.
   On the other hand, A **virus** attaches itself to legitimate programs or files and spreads by infecting other files. It can replicate and spread across systems.

5. **D** all of the above.

6. Ransomware

7. **C.** Anti malware software works by scanning the computer system for known signatures and patterns of malware.