Types of malware:

Malware:

- Software with a purpose to infect and cause harm to the computer or user

- Exploits vulnerabilities in the operating system

- Commit crimes such as fraud and identity theft

Types of viruses:

- Standard virus:

  Hide in files/programs

  Replicate themselves to spread into other programs/files

  Aim is to damage/delete data

- Worms virus:

  Does not damage/delete data
  Replicates themselves

  Uses computer resources to slow down computer and make it useless

- Trojan virus:

  Programs disguised as games or other things

  Causes harm in the background like deleting files or making changes to settings to annoy you

  It may create a portal for other users to gain access to your system

Types of malware:

- Spyware:

Aim is to spy on the user and send back as much information about them such as passwords and usernames etc. to the attacker

Common piece is a key logger which runs in the background and records every key that you press and can be used to steal your passwords and sensitive information

Collecting the data by the senders of the spyware can be sold to third party companies for advertising or identification theft

- Adware:

  Aim is to download and display unwanted adverts

  Collects marketing information about online habits

  Directs you to unwanted websites

- Scareware:

  Pop ups telling you that you have a virus
  Pop up advertises software to help get rid of this fake virus that they are promoting to make money

- Ransomware:

  Malware which encrypts files and demands money in exchange for the master/encryption key to decrypt files

- Rootkits:

  Contains tools which can allow criminals or users to access the computer at administrator level

  Allows them to do anything

Forms of attack:

Phishing – Cyber criminals impersonating trusted companies and uses communication methods such as email, messages or a website and tries to gain sensitive information (bank details or passwords)

Brute force – Trial and error method automated by a piece of software to find the correct password and goes through millions of combinations until successful in breaking to the account

Denial Of Service attack (DOS) – Attack sends requests increasing traffic to the server which can overload it and slow it down or crash it causing the network to fail

Distribution Denial Of Service attack (DDOS) – Compromised computers (zombies) are used by the attacker to flood the server by sending millions and millions of request and a lot of traffic crashing the server and is scheduled at certain times and can go on for days, weeks, months etc.

Data interception and theft – Attacker monitors traffic and sniffs data packets to get sensitive information

SQL injection – Code entered into input fields of a website such as a login page to gain access to database and damage the database

Pharming – A cyber attack which changes the IP address of the websites in the domain name server (DNS) and sends the user to a fake website or to a website which contains malware

Threats posed to networks:

Threats of viruses:

- Gather personal information and damage/delete files/programs and ruin computers
- On a client server network, viruses can spread to all other computers on the network causing harm to data and may potentially cause a company to go bankrupt

Phishing:

- Gain victims personal information such as passwords and bank credentials
- Purchase things on the victims card or commit fraud
- Blacklist brand by banks which damages reputation

Brute force:

- Access to systems and data

- Theft of data

Denial Of Service:

- Loss of access to customers on the website
- Lower productivity (workers are stopped because of attack)
- Lost revenue
- Damage to reputation

Data interception and theft:

- Theft of data
- Sensitive information can be compromised and can be used to commit fraud

SQL injection:

- Reveals private data from a database such as usernames and passwords of users registered
- Allows new entries or removal of entries in the database

- Danger of database being completely destroyed or being sold on the black market or third party companies

Humans are referred to as the weakest point in the system

Social engineering:

This refers to an attack which involves people giving away information by deceiving an individual

Phishing:

- Sent in the form of an email/message
- Impersonate a trusted company

Baiting:

- Offers user something valuable in exchange for login details or data
- Intentions to exploit them

Quid Pro Quo:

- Hacker offers a service in exchange for the user’s data or login details

Pretexting:

- Impersonating worker and creating trust with user
- Gain access to data and information

Piggybacking/tailgating:

- Unauthorised person physically follows worker through the door
- Also could involve borrowing the workers laptop for a few minutes to install malware

Shoulder surfing:

- Looking over a person’s shoulder while they are putting in details
- Could be done at an ATM or watching their computer while they password and username in

Preventing vulnerabilities:

Protecting against malware:

- Firewalls (filters traffic and quarantine viruses and asks for permission to allow viruses)
- Spam filter which can reduce phishing
- Anti-virus to protect against viruses
- Anti-spyware to protect against spyware
- Enable security and OS updates to maximise security
- Staff training to be cautious when opening emails/attachments and downloading software
- Backup files frequently so you have copies of files if anything happens to originals

Phishing:

- Security
- Staff training
- Email filter

Brute force attack:

- Network lockout policy
- Progressive delays
- Stronger passwords
- Challenge response (reCAPTCHA)

DDoS:

- Strong firewalls
- Packet filters on routers
- Configuring webserver
- Monitor traffic and data streams which reduces it

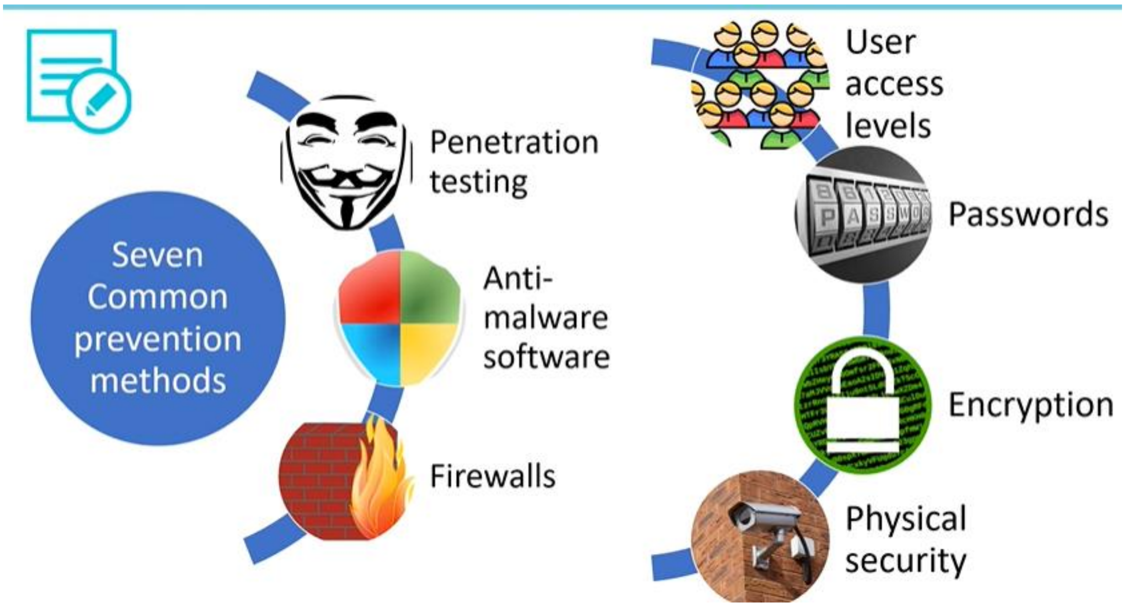
Data interception and theft:

- Encryption of data
- Using virtual networks
- Staff training (Strong passwords, logging of computers, closing doors)
- Penetration testing

SQL injection:

- Input validation/santization
- Using parameter queries

- Database permissions
- Pen testing



Seven Common prevention methods

Penetration testing

Anti-malware software

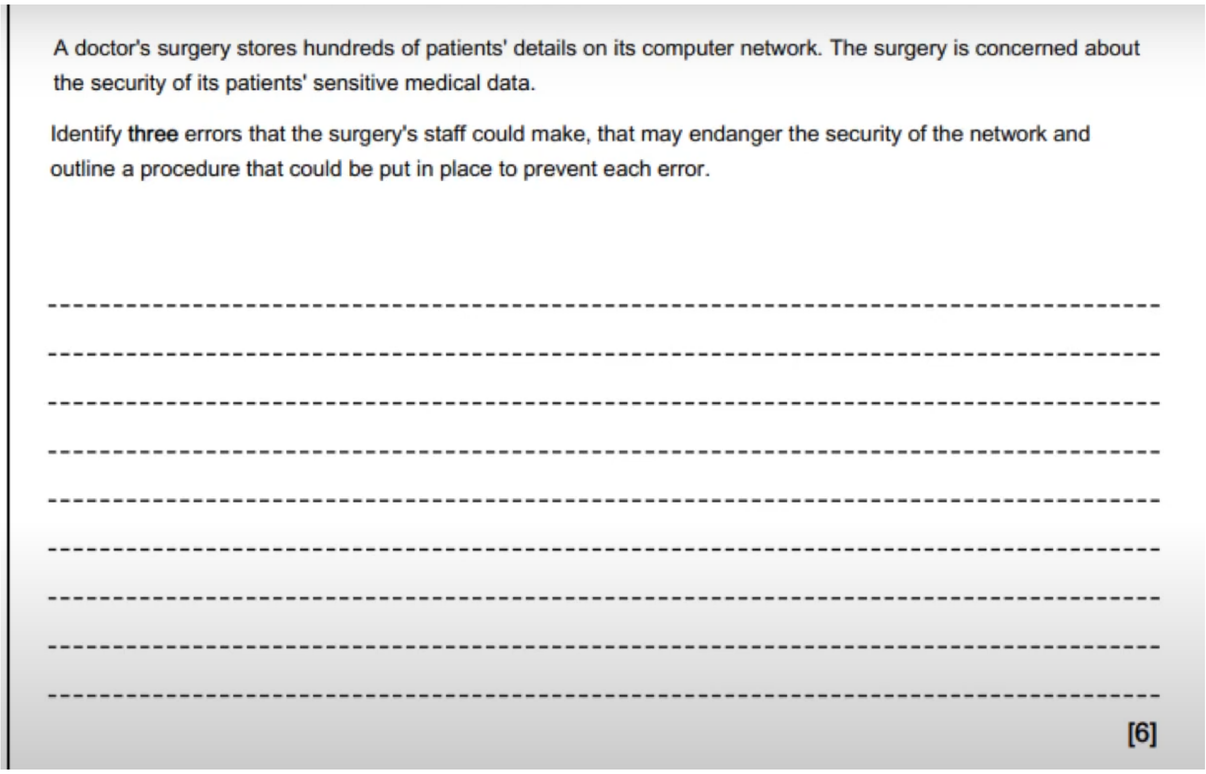
Firewalls

User access levels

Passwords

Encryption

Physical security



A doctor's surgery stores hundreds of patients' details on its computer network. The surgery is concerned about the security of its patients' sensitive medical data.

Identify **three** errors that the surgery's staff could make, that may endanger the security of the network and outline a procedure that could be put in place to prevent each error.

[6]

• Brings in files via any medium (1- AO2 1a)… • …not allowing/stopping external devices being used on the network (1-AO2 1b) • Downloading infected files from the internet (1 - AO2 1a)… • …blocking/restricting access tinsecure websites (1 - AO2 1b) • Allowing physical access to the surgery's network (1 - AO2 1a)… • …locking of doors/key cards/any physical security procedure (1 - AO2 1b) • Sending/sharing sensitive data with third parties (1- AO2 1a)… • … blocking/restricting access to USB ports/email/internet/printing (1 - AO2 1b)	6	1 mark to be awarded for each correct identification to a maximum of 3 marks. (AO2 1b) 1 mark to be awarded for each correct outlining of a procedure to a maximum of 3 marks. (AO2 1b) Allow any reasonable combination of error and reasonable procedure to mitigate the risk.

A hospital stores patients' details on its computer network. The hospital is concerned about the security of its patients' details.

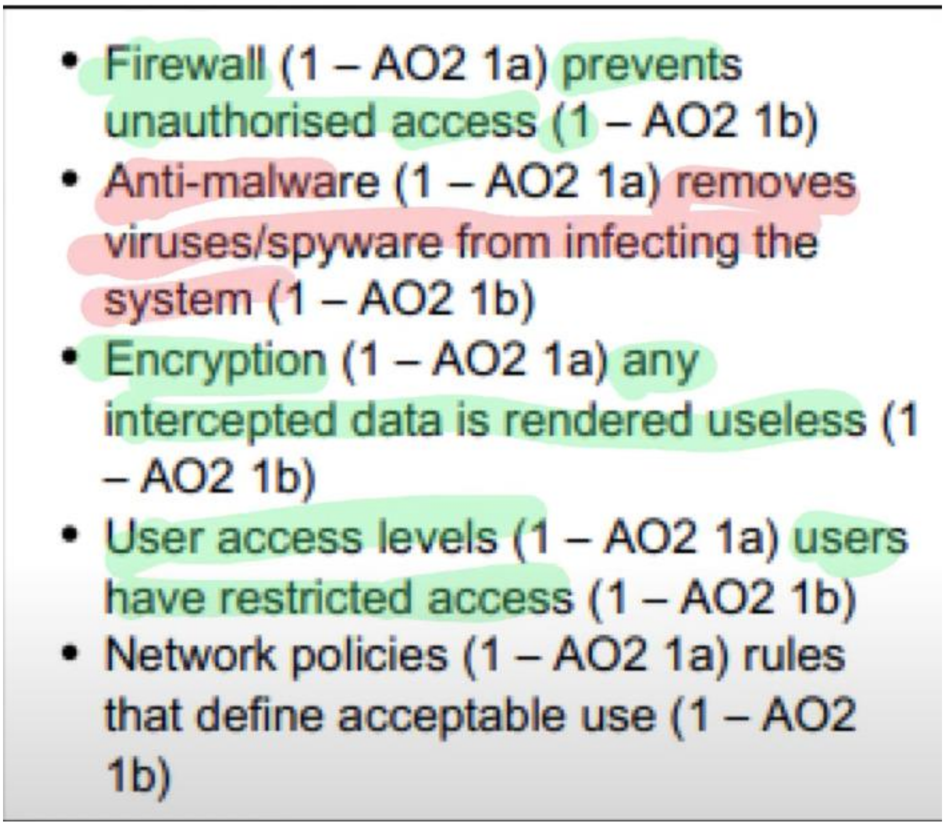
Staff already use strong passwords to protect systems. Explain, with reference to system security, **three** other ways that the hospital could protect the network system.

1

2

3

[6]



- Firewall (1 – AO2 1a) prevents unauthorised access (1 – AO2 1b)
- Anti-malware (1 – AO2 1a) removes viruses/spyware from infecting the system (1 – AO2 1b)
- Encryption (1 – AO2 1a) any intercepted data is rendered useless (1 – AO2 1b)
- User access levels (1 – AO2 1a) users have restricted access (1 – AO2 1b)
- Network policies (1 – AO2 1a) rules that define acceptable use (1 – AO2 1b)