

4.2.1 Security of Data Transfer

Syllabus 2026 - 2028

WHAT YOU NEED TO KNOW

- The privacy and confidentiality of data when it is transferred
- Security issues when data is sent across a network
- How to avoid password interception: up-to-date anti-spyware and regularly changing passwords

Privacy and confidentiality

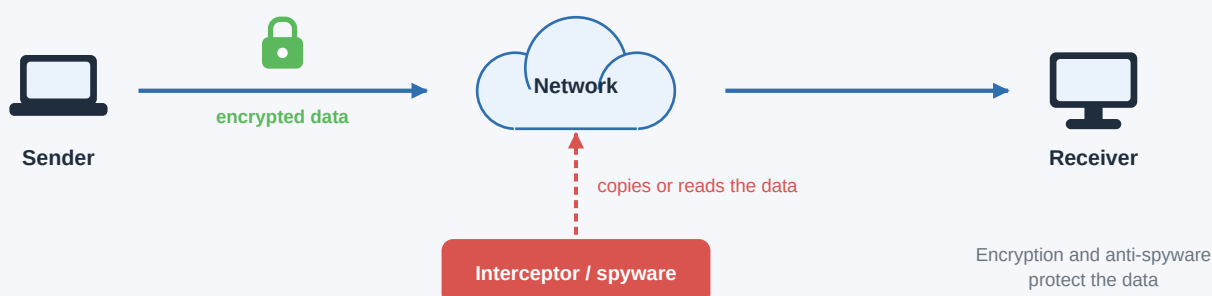
Term	Meaning	Example
Privacy	A person's right to control who can see and use their personal information.	A learner's home address and phone number are not shared without permission.
Confidentiality	Keeping data secret so that only authorised people can see it.	Exam results sent from a school to the examinations council can be read only by the intended receiver.

When data is transferred over a network, it passes through many devices and can be seen, copied or changed by people who should not have access. Data sent over public Wi-Fi or the internet is at most risk.

Security issues when data is sent

Issue	What it is	How to reduce the risk
Interception	Someone reads or copies data while it travels, for example on an unsecured Wi-Fi network (eavesdropping).	Use encryption, use secure websites (https and padlock), avoid public Wi-Fi for private data.
Spyware	Malware that secretly records what the user does, such as key presses, and sends it to an attacker. It can capture passwords as they are typed.	Install anti-spyware software and keep it up to date; scan regularly; do not install unknown software.
Password theft	Passwords are guessed, stolen by spyware or tricked out of users by fake messages (phishing).	Use strong passwords, change them regularly, never share them, and do not follow links in unexpected messages.
Hacking	Unauthorised access to a network or computer to see or change data.	Use a firewall, passwords and user access levels.
Data theft or loss in transit	Data is lost, copied or changed before it reaches the receiver.	Encrypt data, keep backups, and send only to verified recipients.

Figure 7: Data can be intercepted while it travels across a network



Avoiding password interception

- **Use up-to-date anti-spyware:** it detects and removes spyware that records key presses, and its list of known threats must be updated so that new spyware is found
- **Change passwords regularly:** a password that has been stolen quietly becomes useless when it is changed
- **Do not type passwords on shared or public computers,** which may hold spyware
- **Do not use public Wi-Fi** for logging in to private accounts, unless it is a secure connection
- **Use encryption:** data is scrambled so that if it is intercepted it cannot be read without the key

EXAM TIP

Spyware is **not** the same as a virus. A virus copies itself and damages files, while spyware **secretly watches** and reports what the user does. Keep the two ideas separate in your answers.

Key terms

Term	Meaning
Privacy	The right to control who sees your personal data.
Confidentiality	Keeping data secret from unauthorised people.
Interception	Reading or copying data while it is being sent.
Spyware	Malware that secretly records and reports a user's activity.
Key logger	Spyware that records key presses.
Encryption	Scrambling data so it cannot be read without a key.
Phishing	Fake messages that trick users into giving away data.
Anti-spyware	Software that detects and removes spyware.

Practice questions

Answer each question in full sentences. Command words used: State (give a short answer), Describe (say what it is like), Explain (give reasons), Analyse (break it down and examine it), Suggest (apply your knowledge to a situation), Compare and contrast (similarities and differences), Evaluate (weigh up and reach a judgement).

No.	Question	Marks
1	State two examples of data that should be kept confidential when it is sent over a network.	[2]
2	Explain the difference between the privacy and the confidentiality of data.	[2]
3	Describe how spyware can be used to find out a user's password.	[3]
4	Suggest three steps a school could take to keep data safe when it is sent between computers.	[3]

Total: 10 marks