

4.2.2 Passwords

Syllabus 2026 - 2028

WHAT YOU NEED TO KNOW

- The differences between strong and weak passwords
- How to avoid password interception using up-to-date anti-spyware and regular changes

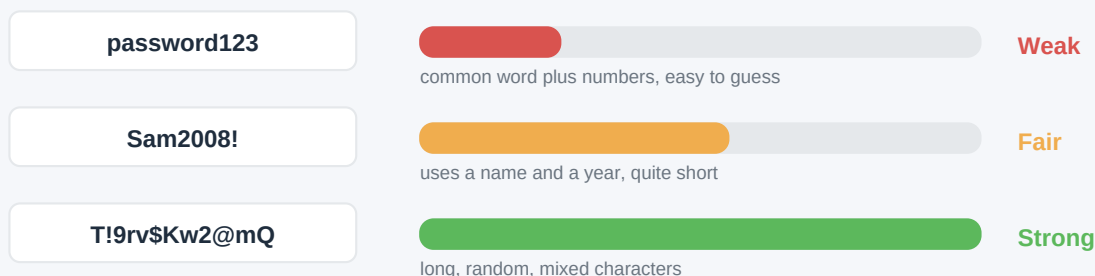
What a password does

A **password** is a secret string of characters that a user types, with a username, to prove who they are and gain access to a system. It protects accounts, files and personal data from unauthorised users.

Strong and weak passwords

	Weak password	Strong password
Length	Short (under 8 characters)	Long (12 or more characters)
Characters	Only letters or only numbers	A mix of upper and lower case letters, numbers and symbols
Content	A word, name, date of birth or common pattern such as 'password' or '123456'	Random, or a long phrase of unrelated words, with no personal information
Use	The same password on many accounts	A different password for each account
Result	Quickly guessed or cracked	Takes far too long to guess

Figure 8: Weak and strong passwords



How passwords are attacked

- **Guessing:** trying likely passwords such as names and birth years
- **Brute force:** a program tries every possible combination until one works. Short passwords fall quickly
- **Dictionary attack:** a program tries a list of common words and passwords
- **Spyware or key logger:** secretly records what is typed
- **Phishing:** a fake website or message tricks the user into entering the password
- **Shoulder surfing:** watching someone type their password

Good password practice

- Choose a strong password and a different one for each account
- **Change passwords regularly** and immediately if you think someone knows it
- Keep **anti-spyware up to date** and scan regularly, so passwords are not intercepted as they are typed
- Never share passwords or write them where others can see them
- Use a password manager or a long passphrase that is easy to remember but hard to guess

- Add a second check, such as a code sent to your phone (two-factor authentication)

EXAM TIP

'Longer' is the key idea. A password that is both **long** and **unpredictable** is stronger than a short one with a few symbols. Do not say a strong password is 'hard to remember'; say it is 'hard to guess'.

Key terms

Term	Meaning
Password	A secret set of characters used to prove identity.
Strong password	Long, random and mixed, so it is hard to guess.
Weak password	Short or predictable, so it is easy to guess.
Brute force attack	Trying every possible combination.
Dictionary attack	Trying a list of common words and passwords.
Two-factor authentication	Using two different checks to prove identity.
Password manager	A program that stores passwords securely.
Shoulder surfing	Watching someone enter their password.

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 features of a strong password.	[2]
2	Describe two weaknesses of the password 'sam2008'.	[2]
3	Explain why a user should change their passwords regularly.	[2]
4	Analyse why it is risky to use the same password for every online account.	[3]
5	Suggest a strong password for an online account and explain why it is strong.	[3]
6	Evaluate the use of passwords alone as a method of protecting a user account.	[5]

Total: 17 marks