COMPUTING AND DIGITAL LITERACY

Password Security

Difficulty level: Easy

Computing and Digital Literacy

This document was made by AI and there may be mistakes. If a question or answer looks wrong, use the Flag a mistake button to let Brett know so he can fix it.

Overview of the concept

This is how you keep strangers out of your email, bank, and social accounts, like locking your front door and never leaving the same key under every mat. A password that is reused everywhere is like one key that opens every door you own, so a single leak opens them all. A strong password is long and different for each account, and a password manager remembers them so you do not have to. The few minutes it takes to set that up is the cheapest protection your accounts will ever get.



© 2026 Brett Robbins. All Rights Reserved.

Worked examples

EXAMPLE 1

Q Make a strong password from the four random words cloud, tiger, pencil, river.

SOLUTION

Length is what makes a password strong, and four random words are long and easy to remember. Join them with hyphens, in any order.

cloud-tiger-pencil-river

EXAMPLE 2

Q Someone has your password, but not your phone. Can they get into your account?

SOLUTION

Not if two-factor authentication is on. The password is only the first check. The second check is a code sent to your phone, and they do not have it.

No, they do not have the code from your phone.

© 2026 Brett Robbins. All Rights Reserved.

Practice questions

1 Which password is stronger: fluffy or ocean-brick-guitar-lemon?

- A fluffy
- B ocean-brick-guitar-lemon
- C password123
- D qwerty

Understand It with Pulse | Flag a mistake

2 Build a passphrase from these four random words: apple, mountain, zebra, candle.

Understand It with Pulse | Flag a mistake

© 2026 Brett Robbins. All Rights Reserved.

3 Why is password123 a weak password?

- A It is too long to remember
- B It is common and easy to guess
- C It has too many symbols
- D It changes every month

Understand It with Pulse | Flag a mistake

4 What makes a passphrase strong: its length, or the words being related to each other?

- A Its length
- B The words being related to each other
- C Using the same password everywhere
- D Making it short so it is easy to remember

Understand It with Pulse | Flag a mistake

© 2026 Brett Robbins. All Rights Reserved.

5 Why is reusing one password on many sites dangerous?

- **A** It makes passwords too long
- **B** It makes passwords hard to remember
- **C** One breach unlocks every account
- **D** It changes your password every month

Understand It with Pulse | Flag a mistake

6 What does two-factor authentication add after your password?

- **A** A longer password
- **B** A new username
- **C** A password manager
- **D** A second check, such as a code from your phone

Understand It with Pulse | Flag a mistake

© 2026 Brett Robbins. All Rights Reserved.

7 **You lose your phone with your two-factor codes on it. What should you use instead?**

- **A** A backup code kept somewhere safe
- **B** Your old password
- **C** A new phone number
- **D** Your email password

Understand It with Pulse | Flag a mistake

8 **What is the one password you must remember when you use a password manager?**

- **A** Your email password
- **B** Your master password
- **C** Your bank password
- **D** Your Wi-Fi password

Understand It with Pulse | Flag a mistake

© 2026 Brett Robbins. All Rights Reserved.

9 Your password was in a data breach. What should you do first?

- **A** Keep using it until it stops working
- **B** Delete your account
- **C** Change it, and change it anywhere you reused it
- **D** Change your username

Understand It with Pulse | Flag a mistake

10 Which is safer: a long passphrase you can remember, or a short password with symbols that you forget?

- **A** The short password with symbols
- **B** The long passphrase

Understand It with Pulse | Flag a mistake

© 2026 Brett Robbins. All Rights Reserved.

ANSWER KEY

1. ocean-brick-guitar-lemon

2. apple-mountain-zebra-candle

3. It is common and easy to guess

4. Its length

5. One breach unlocks every account

6. A second check, such as a code from your phone

7. A backup code kept somewhere safe

8. Your master password

9. Change it, and change it anywhere you reused it

10. The long passphrase

© 2026 Brett Robbins. All Rights Reserved.