Share:

How to choose a strong password

Print this guide

The passwords you use online are intended to protect your personal data, so it’s important to choose ones that are difficult for other people to guess.

How do cybercriminals gain access to your accounts?

One method that hackers use to access your accounts is to try and guess your password based off personal information gained from your security questions. Another way a hacker can attempt to gain access to your account is through a password cracker which uses multiple combinations of characters to repeatedly guess a password until it gains access to the account. The longer and more complex a password is, the harder it will be to crack the password.

Be clever with your passwords by following these simple pointers:

- **Don’t use anything that’s easy for someone else to find out** . For instance, you shouldn’t use any part of your name, address or birth date or those of close family members, or your pet’s name.
- **Don’t use common words**. One of the most common passwords is the word ‘password’ and it’s one that any criminal will try first. Criminals will use dictionary-based systems to crack solitary words.
- Try thinking of a **short sentence or phrase and use the first letter of each word.** You could use a line of, say, a poem or song – for example, ‘I wandered lonely as a cloud’ becomes ‘iwlaac’. You could write down ‘daffodils’ as a reminder for this. Similarly, a short phrase could be ‘My teacher’s name was Miss Clarke’. The password would be ‘mtnwmc’ and ‘teacher’ could be your reminder.
- Many websites require you to use capital letters and numbers in your password as these make them more secure. A good way to incorporate numbers is to substitute numbers for letters that look similar – for instance: ’1′ for ‘i’ or '0′ (zero) for ‘o’.
- **Use a password that is at least 8 characters long**, the more characters there are in a password the more difficult it will be to guess.
- **Don't use the same password across all your online accounts.**
- **Change your passwords regularly.**
- **Don't click on 'yes' when prompted by browsers to save your password.**
- **Consider using a password manager.** These store your passwords, and generate secure ones for you. This article from SoftWareHow will help to reassure you about the safety of password managers.
- For sites that have access to your payment cards (if not all passwords) consider turning on Two-Factor Authentication (2FA). This adds a second second step to the log in process on a site, thereby making it harder for hackers to break into your account.

Finally, if you do ever suspect that on our your accounts has been hacked, the first thing to do is to change your password and notify the service provider.

Last updated January 2023

Next steps

How to stay safe online

- ▶ Email safety tips
- ▶ How to get an email account
- ▶ A guide to internet security
- ▶ 10 top tips for smartphone security
- ▶ 2 Step Verification for Gmail
- ▶ What is identity theft?

How do digital skills change lives?

Find out about Digital Inclusion