Passwords

Here are a few simple principles to follow when you're setting up passwords for your accounts

Don't use the same password on different websites

If a website is "hacked" (has its security breached), those that breached the security will use the combination of your username and password on other websites, i.e. if one account is compromised, other accounts could be at risk.

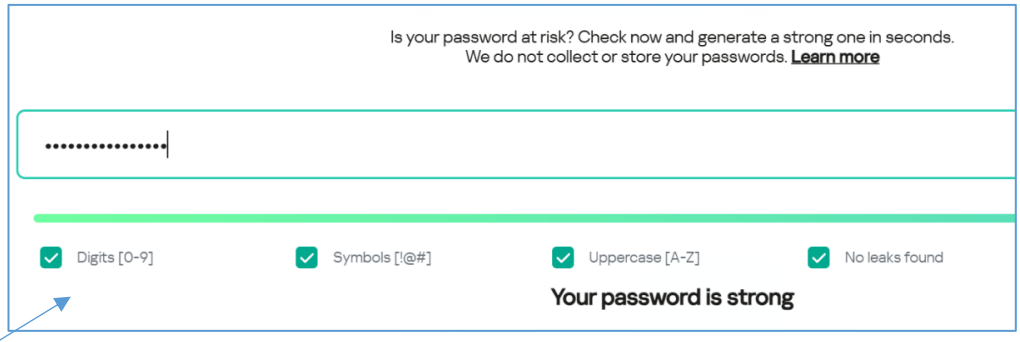
Don't use passwords that are easily guessed

We share a lot of information about ourselves without realising it, birthdays, names of friends, family and pets. You may think using Fido as a password is a good idea but his personalised dog bowl in the photo you posted may just give it away.

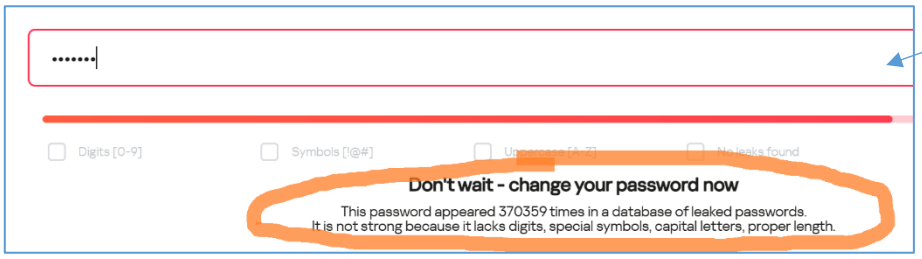
Below is a selection from "Most common corporate passwords" in 2024 Top 200 Most Common Passwords | NordPass. These are still used by people despite being easily guessed – all of these took less than 1 second to crack.

123456	12345678	123456789	secret	chelsea	qwerty123
qwerty1	111111	123123	Arsenal1	qwerty	1234567
11111111	abc123	iloveyou	123123123	000000	rangers
a123456	password1	654321	1q2w3e4r5t	123456a	charlie
P@ssw0rd	princess	1qaz2wsx3edc	asdfghjkl	88888888	1234561
football	dragon	ashley	baseball	sunshine	soccer

You can check the strength of your password by entering it on the Kapersky website https://password.kaspersky.com/



This is a strong password because it is long, contains upper- and lower-case letters, digits and symbols.



This is a weak password – it is a short common word, all lower case, with no letters, digits or special characters

Ideally, your password should be at least 20 characters long and include a mix of uppercase and lowercase letters, numbers, and special symbols. Steer clear of easily guessable information like birthdays, names, or common words.

Change your passwords regularly

Make sure to regularly check the health of your passwords. Identify any weak, old, or reused ones, and upgrade them to new, complex passwords for a safer online experience.

Password Managers

These are examples of secure passwords, but they are difficult to remember. Some people prefer to use a password manager to store passwords safely. This means you can have unique passwords for each service, and you won't need to remember them. Password managers often have other features to help your security such as autofill, synchronising passwords across devices, and compromise warnings. You can save passwords on your own device, but you need to make sure that it is secure. You could also choose to use a third-party password manager – normally an app that you download to your device. If you choose to use a password manager, you need to remember your primary password in order to access it.

Passkeys

Passkeys are created, saved, stored and managed for you on your trusted device(s) such as your smartphone, tablet or computer. This is done by your chosen credential manager. This will most likely be the default one built into your device - for example Apple Passwords, Google Password Manager - unless you have specifically chosen to install and use another one.
The technology consists of two keys – your passkey and its verifier. Both pieces of information are required to sign into an account – like 2-step verification:

Your device creates an account-unique passkey and saves it to your credential manager for you, so you don't have to worry about this.

Your device shares the accompanying verifier (not your passkey) with the online service

Passkeys are regarded as more secure than passwords. You can find more information on the National Cyber Security website:

Managing your passwords - NCSC.GOV.UK

Passkeys: the promise of a simpler and safer alternative... - NCSC.GOV.UK