National Cyber Security Centre

Using passwords

To protect your devices & data

Passwords are an effective way to control access to your data, the devices you store it on, and the online services you use.This page contains tips about how to create strong passwords, how to look after them, and what to do if you think they've been stolen. For more information, please refer to www.cyberaware.gov.uk .

How can your passwords be stolen?

Criminals will use the most common passwords to try and access your accounts, or use information from your social media profiles to guess them. If successful, they will use this same **password** to try and access your **other accounts**.

Criminals also try and trick people into revealing their passwords by creating fake 'phishing' emails that link to **dodgy websites**, or by using **persuasive techniques** through social media.

Even if you create strong passwords (and look after them), they can still be **stolen** if an organisation containing your details suffers a **data breach**. Criminals will use these stolen customer details (such as user names and passwords) to try and access other systems and accounts.

Create strong passwords

Create a strong and memorable password for your email account (and other important accounts).

Avoid using predictable passwords (such as dates, family and pet names). Avoid the most common passwords that criminals can easily guess (like 'passw0rd').

Don't re-use the same password across important accounts. If one of your passwords is stolen, you don't want the criminal to also get access to (for example) your banking account.

To create a memorable password that's also hard for someone else to guess, you can combine three random words to create a single password (for example cupfishbiro).

Look after your passwords

If you store your passwords somewhere safe, you won't have to remember them. This allows you to use unique, strong passwords for all your important accounts.

You can write your password down to remember it, but keep it somewhere safe, out of sight, and (most importantly) away from your computer.

Store your passwords in your browser when prompted; it's quick, convenient and safer than re-using the same password. Browsers can also detect 'dodgy' websites that phishing emails try and trick you into visiting.

You can also use a standalone password manager app to help you create and store strong passwords.

Use 2FA to protect your account

Many companies allow you to set up two-factor authentication (also known as 2FA) on your accounts. It's called 2FA because it involves signing into your account using two passwords or codes; one that you know, and the other usually sent to your phone.

The most common form of 2FA is when a code is sent to your smartphone that you must enter in order to proceed. You should set up 2FA for important websites like banking and email.

Even if a criminal knows your passwords, they will struggle to access any accounts that you've protected by turning on 2FA.

Visit www.ncsc.gov.uk/2fa for up-to-date instructions on how to set up 2FA across popular online services such as Gmail, Facebook, Twitter, LinkedIn, Outlook and Instagram.

What to do if your password is stolen?

If you suspect your password has been stolen, you should change it as soon as possible.

If you have used the same password on any other accounts, change these as well.

';--have i been pwned?

You can use the website www.haveibeenpwned.com to check if your information has ever been made public in a major data breach.

www.ncsc.gov.uk @NCSC National Cyber Security Centre @cyberhq