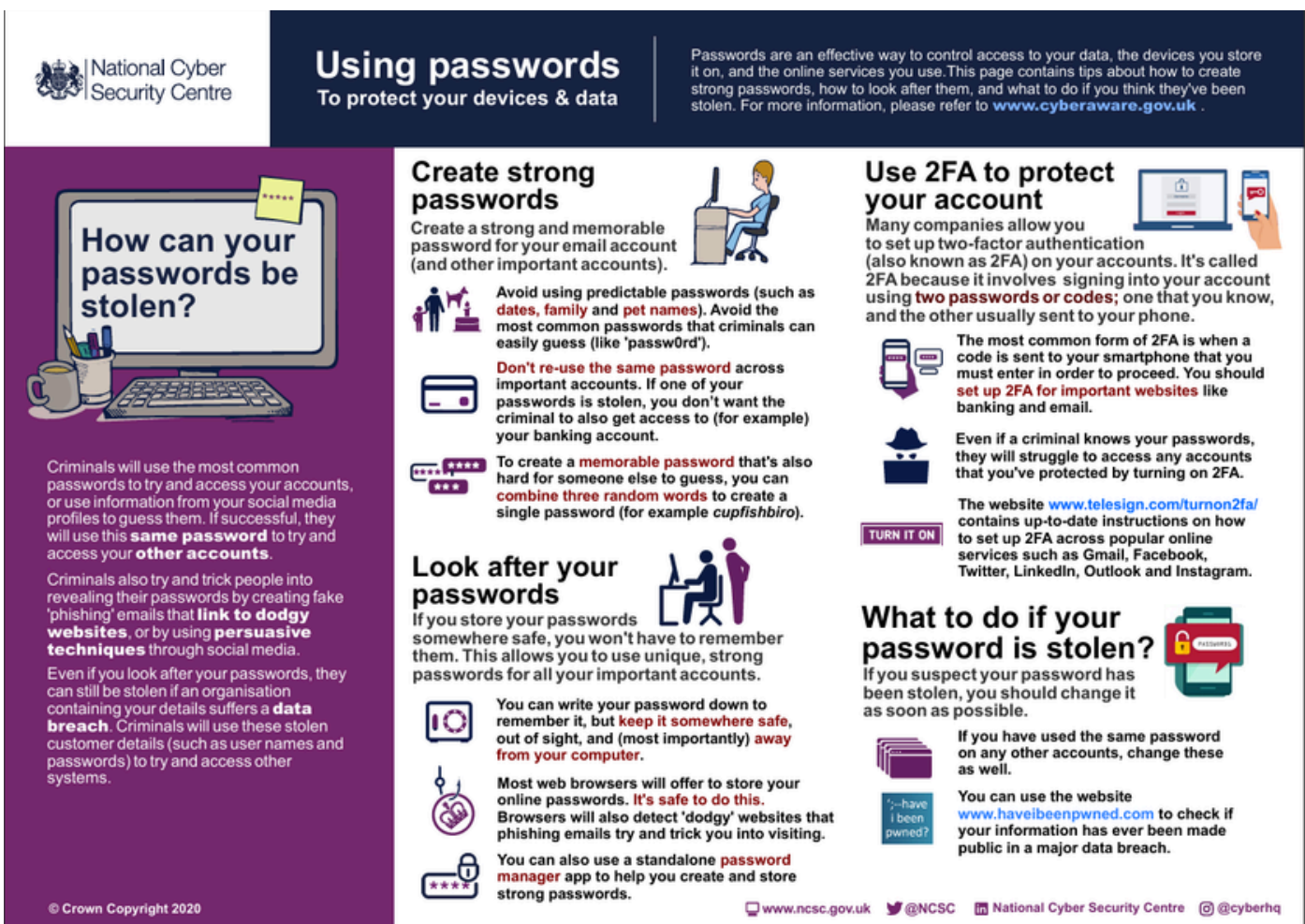


## Passwords - An Everyday Essential

Passwords are a part of everyday life, yet creating, remembering, and using them can feel like a chore. With so much of our personal and professional activity now happening online, understanding how to use passwords effectively is essential for protecting your information.

The National Cyber Security Centre has created an excellent infographic that explains how to choose and manage strong passwords. It's a practical resource worth printing and displaying at work, in school, or anywhere people might benefit from quick, reliable guidance on staying secure.



**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](http://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 look after your passwords, 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.

#### 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**).

#### 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.

The website [www.telesign.com/turmon2fa/](http://www.telesign.com/turmon2fa/) contains up-to-date instructions on how to set up 2FA across popular online services such as Gmail, Facebook, Twitter, LinkedIn, Outlook and Instagram.

**TURN IT ON**

#### 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**.
- Most web browsers will offer to store your online passwords. **It's safe to do this**. Browsers will 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.

#### 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.

You can use the website [www.haveibeenpwned.com](http://www.haveibeenpwned.com) to check if your information has ever been made public in a major data breach.

© Crown Copyright 2020

[www.nccsc.gov.uk](http://www.nccsc.gov.uk) @NCSCL National Cyber Security Centre @cyberhq