Crime prevention advice for

Passwords

Protect your email by using a strong and separate password

Cyber criminals can use your email to access many of your personal accounts and find out vital personal information, such as your bank details, address or date of birth, leaving you vulnerable to identity theft.

Having a strong, separate password for your email means that if cyber criminals steal the password for one of your less important accounts, they can’t use it to access your email account.

Use three random words to create a strong password

A good way to create a strong and memorable password is to use three random words. Numbers and symbols can still be used if needed, for example CyberS@feWarks24!

Be creative and use words memorable to you, so that people can’t guess your password. Your social media accounts can give away vital clues about yourself so don’t use words such as your child’s name or favourite sports team which are easy for people to guess.

Cyber criminals are very smart and know many of the simple substitutions we use such as ‘Pa55word!” which utilises symbols to replace letters.

Never use the following personal details for your password:

- Current partner’s name
- Child’s name
- Other family members’ name
- Pet’s name
- Place of birth
- Favourite holiday
- Something related to your favourite sports team

Password managers: how they help you secure passwords

What is a password manager?

A password manager is an app on your phone, tablet or computer that stores your passwords securely, so you don’t need to remember them all. Some password managers can synchronise your passwords across your different devices, making it easier to log on, wherever you are. Some can also create random, unique passwords for you, when you need to create a new password (or change an existing one).

What types of password manager are available?

You may be already using a password manager without knowing it. Many are **built into** your internet browser (such as Google Chrome, Microsoft Edge or Firefox), or are part of the operating system on your smartphone or tablet. You may have noticed when you sign into an account, a box appears asking you if you want the browser (or device) to remember your password. If you are **not** sharing the device with anyone else, then it is safe to tick the box. If it doesn't offer to save your password, you may need to turn this option on in your device settings.

Standalone password manager apps are also available to download, many of which can be installed on different types of device, and with extra features like the ability to create good passwords for you. It's worth finding online reviews of the password managers you're considering and deciding on the features you need (and the support the vendor provides) before choosing one that's right for you**.**

How do I protect my password manager?

Whether you're using a standalone password manager or a built-in one, it is important to keep the password manager account secure because if a criminal accesses this, they'll potentially have access to all your passwords and associated accounts. You also need to take steps to make sure you can always get in yourself, so you don't lose access to all your passwords. It is recommended that you set up two-factor authentication on your password manager, always update when prompted, and chose a strong password for the password manager.