Passwords

Keep your systems safe

Passwords are an important part of your online security. As computers get more advanced, passwords become easier to crack and care must be taken to ensure they are as secure as possible.

Simple steps can be taken to create and maintain strong passwords to keep your systems and data safe.

How long should my password be?

Any password of less than 9 characters is vulnerable to what is called ‘brute force cracking’. This is where a computer tries every possible combination of letters to match a given password. For good security, passwords should be over 12 characters long.

What is 2-factor-authentication (2FA)?

2-factor authentication (or 2-step-verification) adds an additional layer of security to the authentication process by making it harder to gain access to devices and accounts. It significantly decreases the risk of a hacker accessing your online accounts by combining your password (something you know) with a second factor, like your mobile phone (something you have). After inputting your username and password, a message is sent via text or an app to confirm you are the rightful user.

2FA significantly enhances the security of online accounts and many e-mail providers, social media platforms, banks and shopping sites offer this service.

Visit **www.telesign.com/turnon2fa** for more information.

Can I use a single word for my password?

Using a single word for a password makes it more vulnerable to a ‘dictionary attack’ – another form of brute force cracking where long lists of previously used passwords are used to try and match the password. Even long, single words are vulnerable so creating more complex passwords can help prevent them being compromised.

How do I create a strong password?

Strong passwords will consist of at least 3 random words, be longer than 12 characters and include numbers, symbols and capital letters.

For example:

GOOD

DurbanPalmMountain

BETTER

DurbanPa1mM0unTa1n

BEST

~DurbanPa1mM0unTa1n!

Can I reuse my password?

Every password should be different – especially your e-mail account password. When account information is lost in a data breach, criminals will try and crack the associated passwords, and then use the credentials to try and log into other accounts. Having different passwords will prevent them from being successful.

How do I remember lots of passwords?

Many people have multiple online accounts, so remembering all the associated passwords can be difficult.

Password manager software can be used to store all your passwords across all your devices, meaning you only need to remember the password to get into your password manager. Create a strong password based on this guidance to maximise the chances of keeping it safe. 2-factor authentication can also be used for extra security.

Research reputable security software and choose the best option for your needs.

How do I know if my password has been compromised?

You may not know if your password has been compromised, meaning it can be too late to take action. It is therefore important to make sure your passwords are strong when you create them.

Data breaches happen regularly, so it is important to check if you have been affected. A website called **haveibeenpwned.com** provides information about breaches and could advise you if your username and password has been compromised.

Is there anything else I need to know?

Many devices such as routers or IP cameras have a default username and password. As soon as you install these on to your network, make sure you change the default password to prevent anyone else accessing them.

For further advice and information on a range of cyber security topics, visit the following sites:

www.ncsc.gov.uk

www.cyberaware.gov.uk

www.takefive-stopfraud.org.uk

www.actionfraud.police.uk

www.serocu.police.uk/individuals

Report online at **www.sussex.police.uk**
or **www.surrey.police.uk** or **call 101**.
In an emergency always **call 999**.

Find us on social media

Produced by Sussex Police Corporate Communications 2019