Passwords

With cybercrime on the increase, it's more important than ever to use strong passwords to protect your online accounts - ideally, a strong password should be hard to guess but easy to remember!

Passwords are the most common way to prove your identity when using online sites and services such as email, social media, and banking.

Often used in conjunction with other methods of authentication – such as a one-time verification code sent to your mobile phone – passwords are your first line of defence against cyber criminals.

But weak passwords – such as 'abc123' or 'letmein' – are easily cracked, allowing hackers to access confidential and sensitive information, and putting you, your colleagues, family and friends at risk of losing money, data, or reputation.

It is your responsibility to make sure the passwords you use are as strong as possible and – when it comes to University systems and services – that they meet University policy.

Follow our tips to help you create strong passwords and protect your data.

Don't

- Share your passwords with work colleagues, friends, or family.
- Give out your password to anyone who asks for it. Digital and Information Services will NEVER ask for your password. Neither will any trustworthy organisation.
- Use the same password for all your accounts – if one is compromised, they all are!
- Use names, common sequences (e.g. '12345abc'), a dictionary word, or a word with obvious substitutions (e.g. 'p@55w0rd'). The sophisticated software used by hackers can crack these quickly and easily.
- Add a suffix to an existing password.

Do

- Use a mix of characters – upper and lower case letters, numbers, and symbols.
- Use long passwords where possible – the longer the password, the longer it takes to crack. A minimum of 10 characters is a good rule of thumb.
- Use three or more random words together. And by using a mix of upper and lowercase letters and substituting some letters with numbers and special characters, you can make your password even harder to guess.
- Use different passwords for all your accounts – work and personal
- Use a Password Manager to store and manage your passwords – see PC Magazine's independent product review for 2020
- Reset your password when necessary – after a security incident for example – and tell the Service Desk if you have any doubts whether your password might have been compromised.

Useful links

- The Little Guide to Passwords, from Get Safe Online
- Find out if your account has been compromised in a data breach at https://haveibeenpwned.com/
- Most hacked passwords as revealed in the NCSC's first 'UK cyber security survey' https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security

Still unsure?

If you're still unsure, or if you would like advice, contact the Service Desk – servicedesk@abdn.ac.uk or https://myit.abdn.ac.uk.