Password security

Top tips

Creating a password
• Make your password as long as possible – we recommend using at least 12 characters.
• Use a passphrase or a combination of unconnected words separated by another character, for example: Tango-Teakettle-Barbecue.
• Be discreet when typing in your password. Make sure others do not see you keying it in.
• Do not write passwords down, do not share passwords and do not use the same password for more than one thing – unless it is a Single Sign-On.

Check out this video for further guidance:

FAQs

How do I change the password on my account?
You can change your password by logging in to the Raven Password Management system.

If you have forgotten your Raven password you can reset your password by using the self-service password recovery. Action: sign-up to the self-service recovery as soon as possible, if you have not already done so!

How do I use a password manager?
A password manager is an application used to store and manage your passwords. Your passwords are stored in an encrypted format and the password information is accessed with a master password you set. There are lots of password managers available – UIS suggests reading the National Cyber Security Centre’s (NCSC) guidance and buyer’s guide.

What is Single Sign-On (SSO)?
The University’s Single Sign-On service allows you to access most of the University systems using your Raven password. You can find out further information and a list of the systems this includes on the UIS SSO guidance webpage.

Why not...
• Check if your account has been pwned (compromised in a data breach).
• Find out what the top 10,000 common passwords are so you know what not to use!

Jargon buster:
Pwned = A word that originated in video gaming when someone has been controlled or compromised. In the context of passwords it relates to personal information being compromised (or ‘hacked’) by a data breach.