# How to create strong passwords

**Set a smart password that's easy to remember but difficult for others to guess.**

## Make it longer

RMIT recommends passwords with at least 12 characters. Try using a passphrase, which is string of unrelated words that are long but easy to remember. For example, CIO Paul Oppenheimer joined RMIT in 2015 and has overall oversight of information technology. A memorable passphrase might be *Paul-2015-Sight-Technology*

## Make intentional, personal and memorable typos

Create harder to guess slang phrases and dictionary words by inserting intentional typos that are easy for you to remember.

## Use multi-factor authentication

Link your mobile number for verification with your RMIT Google mail. Set up the RMIT self service password reset tool so you can reset your password from anywhere on any device.

## Use a password manager

Create strong and unique passwords for all the sites you visit and store them in a password manager, such as lastpass, 1password, dashlane and keepass. Ensure the passwords are incomplete, eg leave a chain of three characters you can add to each of these passwords that is not stored in the password manager. Ensure the password you use for the password manager is strong and set up multi-factor authentication to avoid it being compromised.

## Keep it to yourself

Never share your passwords with anyone, including loved ones even temporarily. Change your password immediately if you think someone may know your details. And never write your password down -- especially on a post-it note near your device.

## Never use the same password

Keep different passwords for work, personal and social accounts. If one of the accounts is compromised, hackers can access accounts using the same loging details -- and it means your password is likely to be added to hacker databases.

## Never use remember password

Web browsers and applications may offer you the option to save a password -- set a memorable password instead.

## What to avoid

- **Default passwords** - Always change your password from the default
- **Number sequences** - Not just 0000 but also common sequences such as 1234, 911 and 90210
- **Common phrases** - Words or phrases in any language, including lines from films and verses from religious texts
- **Predictable patterns** - Patterns such as an uppercase character at the start and a number at the end
- **Oversharing personal details on social media** - Scammers will research to get specific details about you, so don't make it easy for them
- **Known facts** - Date of birth, pet names, family members and places of birth

RMIT passwords should be:

- 8-25 characters in length
- signficantly different to any previously used password
- nothing to do with your name or username
- mixed uppercase, lowercase, numeric characters and symbols
- changed every 180 days.