## Dos and Don'ts for creating strong passwords

Passwords are an extremely important feature when it comes to security and keeping your data and information safe - so why do most of us adopt a cavalier approach when it comes to creating the passwords which are so profoundly important to us?

It's hard to imagine anyone who does not use technology in some form today and that means having access to something on a corporate or personal scale which needs to be kept secure. It goes almost without saying, therefore, that this same access and information is of great value to others if only they can get at it.

## Toughening up your passwords

Passwords are a vital part of everyday life but the reason so many are easily breached is down to the simplicity of the password chosen - they just aren't tough enough to crack! We understand why people chose simple passwords, the main reason being they are easy to remember, but it's time to think again and act before it is too late!

Here is a list of vital Dos and Don'ts when it comes to making your passwords strong and secure.

## Password dos:

- Make your password long - it should be ten characters or more, but the longer the better
- Include upper and lower case letters, numbers and symbols
- Combine different unrelated words (but separate them with numbers, symbols or other complexity)
- Better still, use a phrase for your password which is pure gobbledygook and would make no sense to anyone
- Keep your password to yourself
- Steer clear of using personal information
- Use a different password for each device and each account you have
- Start using a password manager - these are services which auto-generate and store strong passwords on your behalf. These passwords are kept in an encrypted, centralised location you can access with a master password
- Change your password semi-regularly


## Password don'ts:

Don't. . .

- Use the word Password
- Share your password with another account or device
- Use your business name, username or actual name
- Choose family or pet names or family birthdays
- Choose personal information which can be easily accessed by other means, like social media which highlight your interests
- Use a single commonplace dictionary word which could be cracked by common hacking programs
- Use numerical sequences
- When choosing numerical passwords or PINs, do not use ascending or descending numbers, for example, 9876 or 45678 , duplicated numbers such as 4444 or easily recognisable keypad patterns such as 14789 or 2580.
- Share your password with another person
- Write down a complicated and difficult to remember password and leave it lying around


