# YOU SHALL NOT... CREATE WEAK ●●●●●●| PASSWORDS!

Having strong passwords may not be top of mind for most people.

But for most online accounts, it's the only thing that protects your information from an attacker.

Weak or reused (where you use the same password for more than one account) passwords could result in a data breach with impact on you, your business and your customers, stolen funds and even reputational damage to your business.

### INCREASE STRENGTH

Your different applications might already have rules and recommendations in place of how long a password should be. Strong passwords are usually made up of at least eight characters with a combination of numbers, uppercase and lower case letters and characters. Use a passphrase where you can.

### PASSPHRASES

Passphrases are unique to you, easy to remember and should be hard to guess to anyone else. They give you an opportunity to H@ves0mefunwithp@sswords!

### DON'T GET PERSONAL

Never include personal information, or information that could easily be taken from social media, in your passwords. This can include your birthday, children or pet's name.

### DON'T REUSE OR RECYCLE.

Passwords that are reused leave you at higher risk of multiple hacking incidents, should it ever get stolen or leaked.

### PASSWORD MANAGERS

Password managers can take away the headache that can be dealing with passwords. Not only do they create complicated passwords for you, they also remember and store them. Just make sure your master password is a really good one! Have a look at LastPass or KeePass.

mindshift