



# YOUR ONLINE SAFETY DEPENDS ON THE STRENGTH OF YOUR PASSWORD

PASSWORDS AND PIN CODES ARE THE GATEWAY TO OUR ELECTRONIC ACCOUNTS AND DEVICES. THEY PROTECT OUR INFORMATION, OUR HOMES AND OUR HARD EARNED MONEY. HAVING A STRONG PASSWORD IS VITAL TO SECURE YOUR ONLINE IDENTITY AND ASSETS.

A password should have a minimum of 8 characters.

 <h2>DO'S</h2> <ul style="list-style-type: none"> <li> Passphrases (sentence, song or joke)</li> <li> Symbols and numbers</li> <li> Two-factor authentication</li> </ul>	 <h2>DON'TS</h2> <ul style="list-style-type: none"> <li> Dictionary words</li> <li> Names (partner, middle, children, pets etc)</li> <li> Special dates (birthday, anniversary etc)</li> </ul>
--	--

## What is a passphrase?

Instead of using a dictionary word, a passphrase uses a sequence of words or other text. It is similar to a password in usage, but is generally longer for added security.

### The best way to come up with a passphrase is:

- 01 Think of a line from your favourite song or joke...  
**We will, we will, rock you!**  
From this your password could be  
**Ww,ww,ry!**
- 02 Once you have your core password established **add some numbers**  
(try to avoid birthdays, ID numbers or other easy to guess digits)
- 03 Then **add symbols**, we like to suggest text based emojis :D ;P ;)
- 04 For your critical accounts, add another layer of security by implementing **two-factor authentication (2FA)**



## What is two-factor authentication?

This is combining your password with something you own. So if a criminal were to get hold of your password they would also need the device which receives your two-factor authentication code. This is recommended for critical accounts such as email and banking.

### EXAMPLES OF TWO-FACTOR AUTHENTICATION

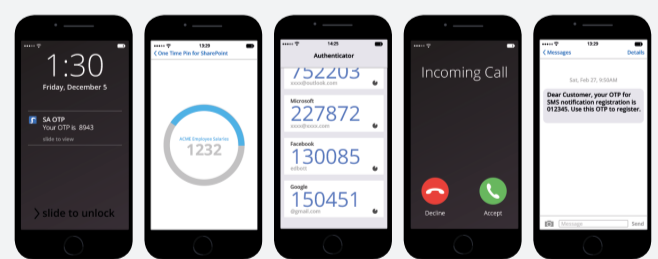
**One-time password (OTP)** – There are plenty of options available on your app store to download an app and link it to the account you wish to secure with 2FA.

**Call** – Some service providers such as Microsoft or your bank offer verification services whereby you receive a call with an OTP.

**SMS** – Think about when you pay for something online and you have to verify the payment by inputting a code you receive via SMS.


**Push notification** – The push notification is received via an app linked to an online platform. Some banks offer this option.

**Email** – When it comes to online payments you can have the option to receive the OTP via email instead of SMS.



EXAMPLES OF TWO-FACTOR AUTHENTICATION

To ensure that your password is difficult to guess, use the following tips:

	+		+		+		=	<b>A STRONG &amp; SECURE PASSWORD</b>
Ww,ww,ry!		5935		:p				Ww,ww,ry!5935:p