**CyberSecurity**

**HOW STRONG ARE YOUR PASSWORDS?**

Add up your points (see bottom) and get your score.

0 - 3
Pretty weak... Remember, passwords help protect your information and devices. Choose them wisely.

3 - 5
They’re ok, but there are a few more things you can do to strengthen your passwords.

6
Great, you have mastered creating strong passwords. Have you thought about MFA?

**1 What do you normally use as a password?**

A = Something personal – date of birth, family member’s name, city where I live, etc.
B = A passphrase or combination of three or more words
C = A random mix of numbers, letters and special characters

**2 How long are your passwords?**

A = Pretty short, 8 characters or less
B = Whatever is required, around 8 to 12 characters
C = Pretty long, at least 12 characters

**3 How many passwords do you have?**

A = A different one for each account or profile
B = The same one for everything
C = Variations of the same password

---

**Use passphrases**
These are passwords of 3 or more words, for example: “chickendogcatrabbit”. It will take several centuries to crack it, while “Ng3h7!a/” would be found in just three days. Remember that what makes a password strong is its length, not its complexity.

**Use multi-factor authentication (MFA)**
In addition to having a strong password, use multi-factor authentication (MFA) whenever possible. This method requires additional forms of identification that only you have, such as a code sent to your mobile, your fingerprint or facial recognition.

**Use a password manager**
Don’t write down your passwords on a piece of paper or in the notes on your mobile phone. Instead, use a password manager. These applications allow you to save all your passwords in one place and you only need to remember a master code to access them.

**Helping you have a more secure digital life**
Santander uses one time passcodes to make your transactions more secure. We will never ask you for your complete password, PIN number or one time passcodes. Don’t share them with anyone.

**REMEMBER, KEEP YOUR PASSWORDS SAFE.**

**POINTS**

1. A=0, B=2, C=1
2. A=0, B=1, C=2
3. A=2, B=0, C=1