5 Cyber rules for a healthy digital life

Now you can take control of your digital life with these simple tips:

1 Protect your information and equipment

- **Keep your software and apps up to date** on all your devices through reputable sources
- Make sure your device **locks automatically**

2 Be discreet online and in public

- **Google yourself** to find out what information is publicly available
- Check your **privacy settings** on social media

3 Think before you click or reply

- **Be careful when clicking on links,** opening attachments or downloading files from a suspicious email
- **If you are not sure, call/text/email** the sender using the contact details you have or are publicly available, not those on the suspicious message

4 Keep your passwords safe

- **Use passphrases** (3 or more words) as passwords, they are easier to remember
- When posible, use **Multi-Factor Authentication** to make your accounts even more secure

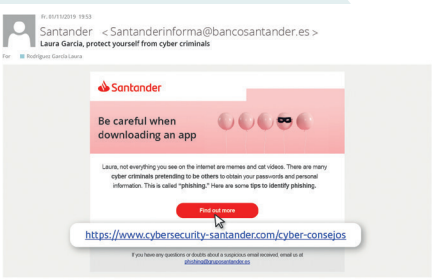
5 If you suspect it, report it

- Whenever you receive a call, message or email that you are not sure about, flag it and **report it to the company or individual**. They can verify its legitimacy
- When contacting the company or individual make sure you use the information you have or is publicly available, **not the details provided**

Stay safe online and share these tips with others so they can also have a healthy digital life

Remember,
every click counts!

Santander



Phishing

A fraudulent attempt to obtain personal information using social engineering techniques or pretending to be a trustworthy entity in an electronic communication.

Malware

A type of software that tries to affect and/or damage a device by accessing it without the user's knowledge.

Virus

A computer virus is a computer program used to alter the function of a device without the permission or knowledge of the user.

MFA

Multi-Factor Authentication (MFA) is a particulary secure way of logging in that not only queries a password but also one or more additional pieces of verification, like a confimation code or your fingerprint.

Secure website

HTTPS (Hypertext Transfer Protocol Secure) is a communication protocol that protects users' data when transmitted between their computers and a website. It has one more layer of security than the HTTP system.

Backup copy

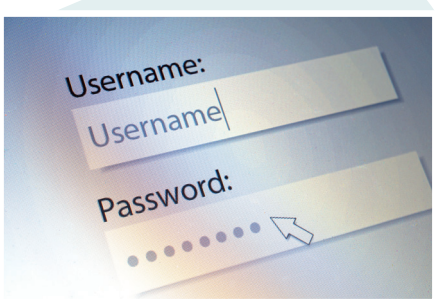
A copy of data created on a different device to the one in which said data is stored. The aim is to be able to restore the data if it is lost.

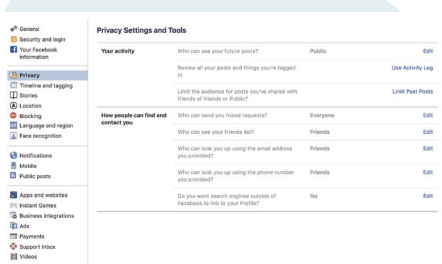
Social Engineering

The practice of obtaining confidential information by manipulating and impersonating the identity of legitimate users.

Passphrase

A password containing three or more words (like a sentence) that enhances security as it is more difficult to crack than a single-word password.





Privacy settings

A series of preferences that users can manage in order to control which information they share and with whom.

Encryption

Encrypting a message means transforming the contents of that message using an algorithm so that only authorised users that know the algorithm can access it.

Santander