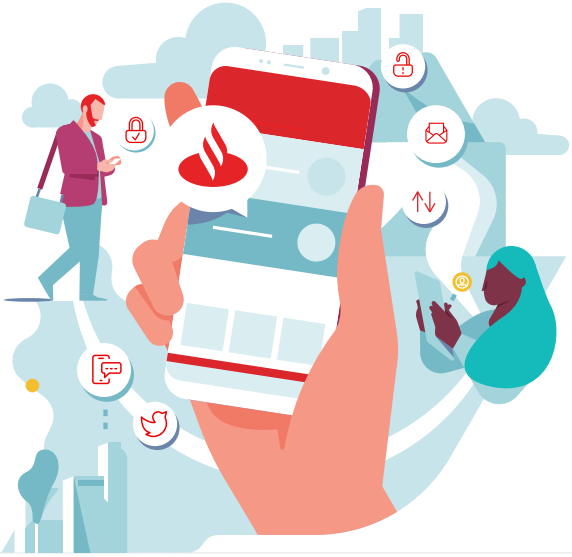
5 Cyber principles to secure your business

Practical advice to help protect your business in today's digital environment.



1 Protect your information and equipment

- **Keep software up to date:** Laptops, PCs, Smartphones... make sure their programmes, antivirus and applications are always up to date with the latest security patches. These updates can be automated so you don't miss out.
- **Secure your website with HTTPS:** The added 'S' stands for secure. This will automatically encrypt the information going to and from your website, protect the data within and generate trust with your customers.
- **Back-up regularly:** Safeguard your business by regularly backing up essential information needed for day-to-day operations. The more critical the data, the more often it should be backed up. Ensure you have one copy backed-up offline in case others are compromised.

2 Be discreet online and in public

- **Check your business' digital footprint:** Use search engines to see what information about the business you can Find on the web. Remember, don't reveal more than is necessary about yourself or the company. If sensitive information ends up in the wrong hands, it could be used for fraudulent purposes.
- **Define public vs. private:** Understanding what information can be shared externally will help everyone in the business manage and maintain security.
- **Raise awareness of staff responsibilities:** Employees are an asset to your organisation so you should help them understand the direct impact they could have when sharing information externally, whether on social media or to suppliers.

3

Think before you click or reply

- **Stay vigilant beyond email:** A phish can be delivered by email, phone call, SMS or instant message. Make sure all employees know how to spot the signs of a suspicious message.
- **Understand the threats:** There are specific attacks targeting businesses, such as CEO fraud (where someone poses as a superior to convince an employee to make a payment) or Business Email Compromise (which looks to steal specific pieces of information).
- **Protect others:** Make it harder to impersonate your business or deceive customers and suppliers. Keep your communications consistent and personalised, and if you are making any changes, let everyone know in advance.

4

Keep your password safe

- **Use Multi-Factor Authentication (MFA):** MFA adds an additional layer of security to your accounts. It could be a code sent to your mobile, your fingerprint or facial recognition. Use it whenever possible and try to offer it on your platforms.
- **Have a strong password culture:** Make sure employees use unique, unpredictable and memorable passwords. Passphrases using three or more words that are combined together are good options as they are easy to remember.
- **Change default passwords:** As part of the standard factory settings, some devices will have a default password - change these. This will make it harder for others to access them.

5

If you suspect it report it

- **Define reporting processes and channels:** Establish a simple and accessible way to report cyber incidents for colleagues, suppliers and customers.
- **Build a cyber culture:** It is important that all employees feel comfortable and know what to do in case of cyber incidents so building a culture where employees can report easily is key.
- **Think about your supply chain:** It could be the case that the victim business is not yours but a company you work with. Define a clear process for them to alert you, so you can act quickly.

Employees are your business's first line of defence. Share these principles with them.

Santander