Santander

CyberSecurity

HAVING A MORE SECURE ONLINE SHOPPING EXPERIENCE

Keep in mind these simple tips and help protect your information and devices in each step of your purchase

You receive an offer that interests you.

It can come by email, SMS, instant message, a phone call or a pop-up on your browser. It can be sent by someone you know or someone you don't.

This can be a real marketing promotion or a scam.

Verify the offer is legitimate

Before you click on any links, check the offer on the official website by typing the URL into the address bar.

Clicking directly on the links provided can lead you to a malicious site where malware could infect your device or your credentials could be stolen.

Can't find it? This may be a phishing message. **Report it!**

Let the company being impersonated know, so they can look into it and prevent others from falling into the trap.

If a friend sent it to you, warn them so they don't get tricked.

Check the URL starts with HTTPS

Before you proceed to make the purchase, check that the website address stars with https (vs. http) or has a padlock next to it.

This means that the information you enter is encrypted before it's shared with the company, which helps to keep it safe.

If the website is HTTP, it's fine to browse, but **don't enter any personal or payment information.**

The same applies to downloading software or files. Files from unsecured websites can contain malware, which can lead you to lose control of your device.

If you have entered your payment information into an HTTP website, keep an eye on your account just in case.

If you need to register, choose a strong unique password

Some shopping websites require users to register with them and create an account. If that's the case, make sure you choose a long strong password and you don't repeat it for other accounts.

Using the same password across multiple sites **could put your information at risk.**

If your credentials on one site get cracked or leaked, they may be used to gain access to other accounts and profiles.

You can find out if your account has been compromised on https://haveibeenpwned.com/.

Make your purchase and wait for your delivery!

Helping you have a more secure digital life

Set up alerts and notifications through online or mobile banking to know what happens on your account. If you notice any suspicious activity notify us immediately.

REMEMBER, PROTECT YOUR INFORMATION AND EQUIPMENT.