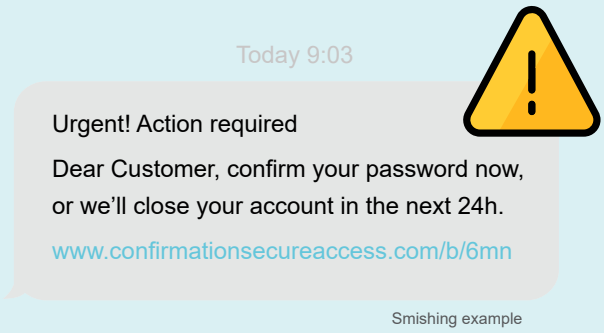
Santander

CyberSecurity

IF YOU SUSPECT IT, REPORT IT

If you receive a suspicious message urging you to share information, download a file or click on a link, report it!

Cyberattacks can appear in numerous ways: email, SMS, instant message, call..., so don't let your guard down.



Smishing example

Have you received a suspicious communication?

Pretending to be Santander

Please let us know.

Remember, Santander will never ask you for your full passwords, PIN numbers or One Time Pass codes.

telephone: 054 11 4345 2400 or 0800 999 2400

email: servicioalcliente@santander.com.co
telephone: +571 743 4222

telephone: 600 320 3000

email: phishing@gruposantander.es
telephone: 915 123 123

email: csirt@santander.pl
telephone: 19999 or +48 61 81 1 9999

telephone: 132

email: netbancoparticulares@santander.pt
telephone: +351 217 807 364

telephone: 55 5169 4300

email: reportabuse@Santander.us

email: phishing@santander.co.uk
telephone: 0800 9 123 123

email: ciberseguridad@santander.com.pe

email: suspeita@santander.com.br

Impersonating another company

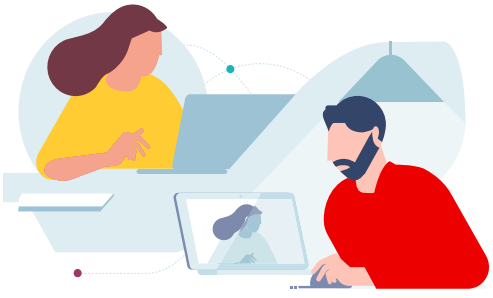
It's important you also let them know.

You can reach the impersonated company via their official channels, such as their website, telephone number or email address.

Never use the contact details included in the communication you have received.

Do the right thing

When you report you are helping others, as the affected companies will be able to investigate the cases and take action to prevent and stop similar attacks.



REMEMBER, IF YOU SUSPECT IT, REPORT IT.