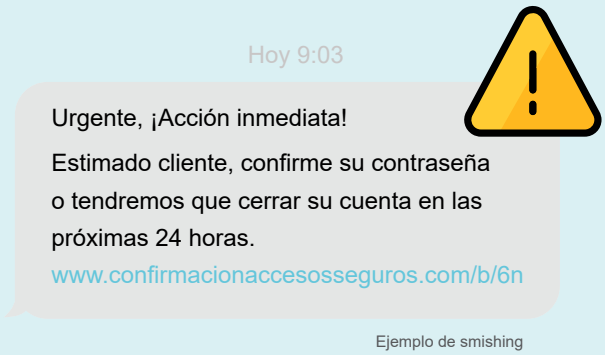
Santander

CyberSecurity

SI SOSPECHAS, REPÓRTALO

Si recibes un mensaje sospechoso, pidiendo que compartas información, descargues un archivo o hagas clic en un enlace, ¡repórtalo!

Los ciberataques pueden llegar por distintas vías: email, SMS, mensaje instantáneo, llamada...no bajes la guardia.



Ejemplo de smishing

¿Has recibido una comunicación sospechosa?

Haciéndose pasar por Santander

Por favor, comunícanoslo.

Recuerda, Santander nunca te pedirá tus contraseñas, números PIN o códigos de confirmación.

teléfono: 054 11 4345 2400 o 0800 999 2400

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

teléfono: 600 320 3000

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

email: csirt@santander.pl
teléfono: 19999 o +48 61 81 1 9999

teléfono: 132

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

teléfono: 55 5169 4300

email: reportabuse@Santander.us

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

email: ciberseguridad@santander.com.pe

email: suspeita@santander.com.br

Suplantando a otra empresa

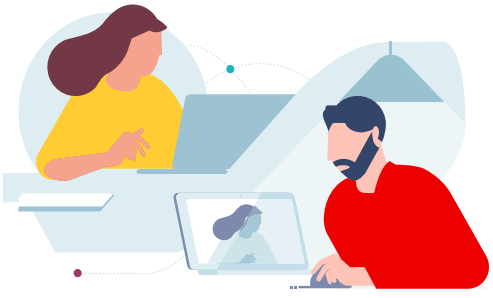
Es importante que también se lo hagas saber.

Puedes contactar a la empresa que está siendo suplantada a través de sus canales oficiales, como su página web, teléfono o email.

Nunca utilices la información de contacto incluida en la comunicación que hayas recibido.

Haz lo correcto

Cuando reportas estás ayudando a proteger a otros. La empresa afectada podrá investigar el caso y tomar las medidas necesarias para prevenir y evitar ataques similares.



RECUERDA, SI SOSPECHAS, REPÓRTALO.