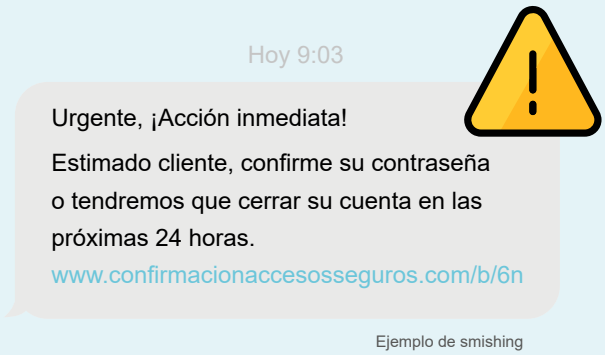
Santander

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 al completo, números PIN o códigos de confirmación.

delitosinformaticos@santander.com.ar	
mensajesospechosoclientes@santander.com.co	
fraudesinformaticos@santander.cl	
phishing@gruposantander.es	
csirt@santander.pl	
delitosinformaticos@santander.com.uy	
alertafraudes@santander.pt	
delitosinformaticos@santander.com.mx	
reportabuse@santander.us	
phishing@santander.co.uk	
ciberseguridad@santander.com.pe	
suspeita@santander.com.br	

Suplantando a otra empresa

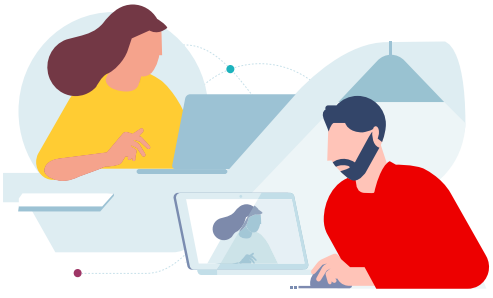
Es importante que también se lo hagas saber.

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.