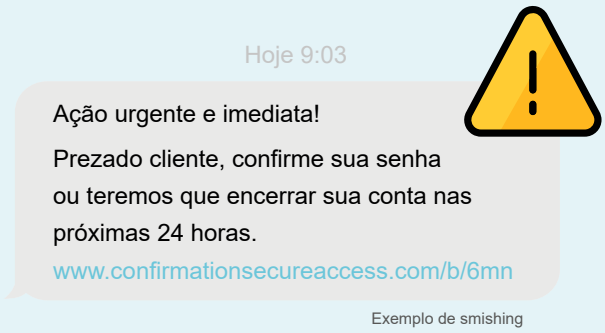
Santander

CyberSecurity

SE SUSPEITAR, REPORTE

Se você receber uma mensagem suspeita pedindo para compartilhar informações, baixar um arquivo ou clicar em um link, reporte!

Os ataques cibernéticos podem vir de diferentes maneiras: e-mail, SMS, mensagem instantânea, ligação ... não baixe a guarda.



Exemplo de smishing

Você recebeu uma comunicação suspeita?

Se passando pelo Santander

Por favor, nos informe.

Lembre-se de que o Santander nunca solicitará suas senhas, tokens ou código do ID Santander.

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	

Se passando por outra empresa

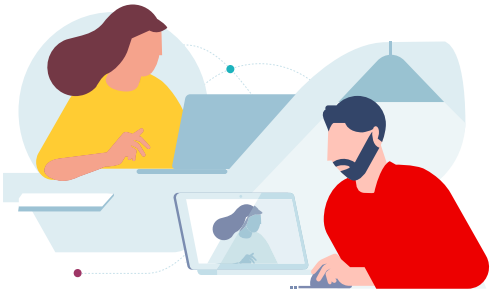
É importante que você também os informe.

Você pode entrar em contato com a empresa cuja identidade está sendo falsificada por meio de seus canais oficiais, como site, telefone ou e-mail.

Nunca use as informações de contato incluídas na comunicação que você recebeu.

Faça o certo

Quando você reporta, está ajudando a proteger outras pessoas. A empresa afetada pode investigar o caso e tomar as medidas necessárias para prevenir e evitar ataques semelhantes.



LEMBRE-SE, SE SUSPEITAR, REPORTE.