

Phishing

*El **phishing** es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como: nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.*

Esta técnica, generalmente está asociada con la capacidad de duplicar una página web para hacer creer al visitante que se encuentra en el sitio web original, en lugar del falso. El engaño suele llevarse a cabo a través de correo electrónico y a menudo estos correos contienen enlaces a un sitio web falso con una apariencia casi idéntica a un sitio legítimo. Una vez en el sitio falso, los usuarios incautos son engañados para que ingresen sus datos confidenciales, lo que les proporciona a los delincuentes un amplio margen para realizar estafas y fraudes con la información obtenida.

La principal manera de llevar adelante el engaño es a través del envío de spam (correo no deseado) e invitando al usuario a acceder a la página señuelo. El objetivo del engaño es adquirir información confidencial del usuario como: contraseñas, tarjetas de crédito o datos financieros y bancarios. A menudo, estos correos llegan a la bandeja de entrada disfrazados como procedentes de departamentos de Recursos Humanos o Tecnología o de áreas comerciales relacionadas con transacciones financieras.



Estimado Cliente,

Restringimos algunas funcionalidades de tu cuenta.

¿Por qué?

Esta es una medida preventiva para mantener la seguridad en todas las operaciones de la comunidad de .

¿Qué tengo que hacer?

1. Ingresar al link que figura al final del mensaje.

1. Llenar el formulario que se le solicitará a continuación con los datos correspondientemente solicitados. Una vez confirmado sus datos su cuenta quedará habilitada para operar.

.com/mla/accountSummary">https://www..com/mla/accountSummary



 .com/pagos.html">http://.com/pagos.html

Recomendaciones para evitar y prevenir este tipo de estafa

1. Toma por regla general: rechazar adjuntos y analizarlos, aun cuando estés esperando recibirlos.
2. Nunca hagas clic en un enlace incluido en un mensaje de correo. Siempre intenta ingresar manualmente a cualquier sitio web, especialmente cuando de entidades financieras se trata, o cuando se solicita información confidencial (como usuario, contraseña, tarjeta, PIN, etc.)

3. *La entidad, empresa, organización, etc., con la que tienes algún tipo de relación, sea cual sea, **nunca** te solicitará datos confidenciales por ningún medio (ni por teléfono, fax o correo electrónico) ni a través de ningún otro medio existente. En caso de recibir un correo de este tipo, es importante ignorarlo y/o eliminarlo.*
4. *Otra forma de verificar si realmente está ingresando al sitio web original, es asegurarse que la dirección web de la página inicia con https y no http. La **S** final, nos brinda un alto nivel de confianza, garantiza que se está navegando por una página web segura.*
5. *Es una buena costumbre verificar el certificado digital al que se accede haciendo doble clic sobre el candado de la barra de estado, en la parte inferior del explorador. (Actualmente, algunos navegadores también pueden mostrarlo en la barra de navegación superior).*
6. *No respondas solicitudes de información que lleguen por e-mail. Cuando las empresas reales necesitan contactar usan otros medios.
El correo electrónico nunca será el canal elegido, debido a sus riesgos inherentes de seguridad.*
7. *Si al recibir un correo tienes dudas sobre su legitimidad, contacta por teléfono a la compañía, a **un número nunca** los contactes a través de los números que indican los mensajes recibidos.*
8. *El correo electrónico es muy fácil de interceptar y puede ser recibido por terceros, por tal razón jamás se debe enviar contraseñas, números de tarjetas de crédito u otro tipo de información sensible.*

9. *Es recomendable tener el hábito de examinar los cargos que se hacen a las cuentas o tarjetas de crédito para detectar cualquier actividad inusual.*
10. *Usa antivirus y firewall; estas aplicaciones no se hacen cargo directamente del problema, pero pueden detectar correos con troyanos o conexiones entrantes/salientes no autorizadas o sospechosas.*
11. *También es importante, ante cualquier amenaza como las citadas, reportar a: soc@santander.com.co o comunicarse con la unidad de delitos informáticos de tu país.*

Algunas características comunes presentes en este tipo de mensajes de correo electrónico:

- *Uso de nombres de compañías ya existentes. En lugar de crear desde cero el sitio web de una compañía ficticia, los emisores de correos con intenciones fraudulentas adoptan la imagen corporativa y funcionalidad del sitio de web de una empresa existente, con el fin de confundir aún más al receptor del mensaje.*
- *Uso del nombre de un empleado real de una empresa como remitente del correo falso. De esta manera, si el receptor intenta confirmar la veracidad del correo llamando a la compañía, desde ésta le podrán confirmar que la persona que dice hablar en nombre de la empresa trabaja en la misma.*
- *Direcciones web con apariencia correcta. Como hemos visto, el correo fraudulento suele conducir al lector hacia sitios web que replican el aspecto de*



la empresa que está siendo utilizada para robar la información. En realidad, tanto los contenidos como la dirección web (URL) son falsos y se limitan a imitar los contenidos reales. Incluso la información legal y otros enlaces no vitales pueden redirigir al confiado usuario a la página web real.

- *Factor miedo. La ventana de oportunidad de los defraudadores es muy breve. Una vez se informa a la compañía que sus clientes están siendo objeto de este tipo de prácticas, el servidor que aloja el sitio web fraudulento y sirve para la recepción de información se cierra en pocos días. Por lo tanto, es fundamental para el estafador conseguir una respuesta inmediata por parte del usuario. En muchos casos, el mejor incentivo es amenazar con una pérdida, ya sea económica o de la propia cuenta existente, si no se siguen las instrucciones indicadas en el correo recibido, y que usualmente están relacionadas con nuevas medidas de seguridad recomendadas por la entidad.*

Fuentes:

- Phishing – www.segu-info.com.ar
- Ransomware - <https://www.bancosantander.es>
- Contraseñas seguras - <https://www.bancosantander.es>