¿Qué es Phishing, Smishing y Vishing? ¿Cómo protegerse?

1. Phishing

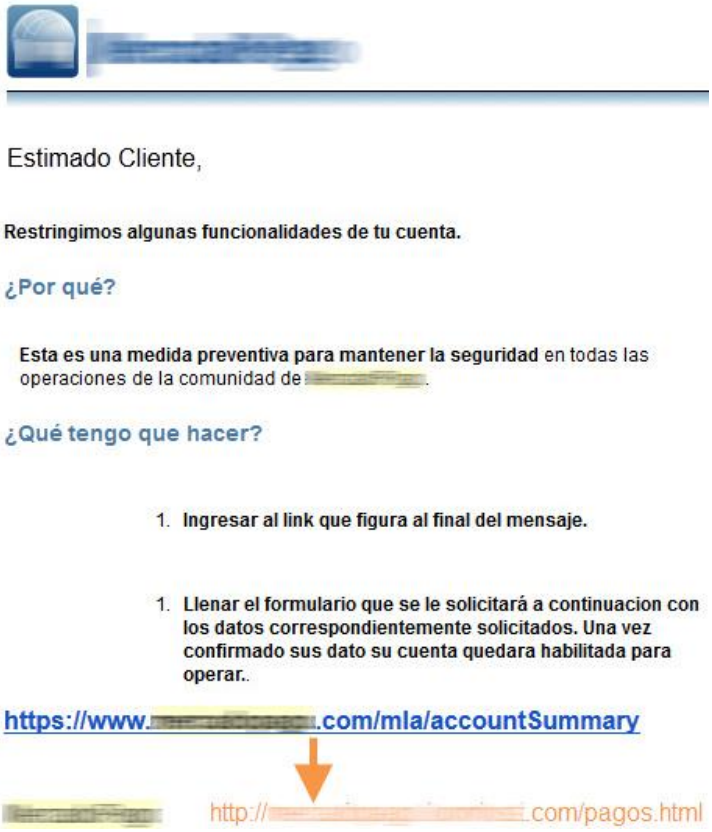
Es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como: nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.

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.

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA

Santander



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 [redacted].

¿Qué tengo que hacer?

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

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

https://www.[redacted].com/mla/accountSummary

[redacted] http://[redacted].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 des 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.)*

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA

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 ignóralo 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.*

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA

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*

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA

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.*

Fuente:
www.segu-info.com.ar

2. Smishing

Se trata de un tipo de delito que utiliza mensajes de texto dirigidos a usuarios de telefonía móvil con intención de estafar, mediante reclamos atractivos con alertas urgentes, ofertas interesantes o grandes premios; los delincuentes tratan de engañar

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA

al usuario aprovechando las funcionalidades de navegación web que incorporan los dispositivos móviles actuales.

El Smishing es una variante del Phishing, un fraude común en Internet, consiste en el envío de correos electrónicos que simulan ser de empresas importantes como bancos, financieras, negocios donde se realizan pagos y compras en línea, etc. Estos correos incluyen supuestas promociones o beneficios en nombre de una empresa con el fin de cometer delitos como robo de identidad, extracción de dinero, entre otros.

Así como el Phishing, el Smishing pretende redirigir al usuario a un sitio web fraudulento, intentando obtener su información personal, robar sus datos bancarios o infectar su dispositivo con algún virus; así como obtener otro tipo de beneficio como la recarga de saldo, muy común en nuestro país.

En otras ocasiones los delincuentes tratan de convencer al usuario para que llame a un número con tarificación especial, se suscriba a un servicio SMS premium de forma ilícita o simplemente tratar de venderle algún servicio o producto inexistente pagando cierta cantidad por ello.

Mensajes atractivos como "FELICIDADES, ha sido seleccionado entre millones de usuarios con un [auto]. Para obtener su premio envía al [número] la palabra COCHE", son contenidos comunes que los ciberdelincuentes utilizan para estafar a sus víctimas con una suscripción a un servicio SMS premium.

Fuente:
http://www.protecciononline.com/que-es-el-smishing/

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA

Cómo evitar ser víctima de Smishing

En general, no debes responder mensajes de texto de personas que no conoces, es la mejor forma de permanecer protegido.

Adopta precauciones básicas para el momento de usar tu teléfono, como:

- *No hacer clic en vínculos que aparezcan en tu móvil a menos que conozcas a la persona que lo envía. Incluso si recibes un mensaje de texto de un amigo con un vínculo, antes de hacer clic, verifica si fue su intención enviártelo.*
- *Nunca instales aplicaciones desde mensajes de texto. Cualquier aplicación que instales en tu dispositivo debe provenir de la tienda de aplicaciones oficial. Es preferible ser demasiado precavido.*
- *Si tienes alguna duda sobre la seguridad de un mensaje de texto, ni siquiera lo abras.*

Fuente:
https://co.norton.com/internetsecurity-emerging-threats-what-is-smishing.html

Vishing

El vishing o voice phishing ocurre cuando un estafador crea un sistema de voz automatizado para hacer llamadas a los usuarios y pedirles información privada, el término es una combinación del inglés "voice" (voz) y phishing.

El propósito es el mismo que el del Phishing por correo electrónico o por SMS, pues la llamada produce un sentido de urgencia en el usuario que lo lleva a tomar acción y a proporcionar información personal.

Cómo evitar ser víctima del Vishing

- *No proporciones ningún número de identificación personal, números de tarjeta, códigos de seguridad o contraseñas bancarias.*

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA

- *Confirma con tu banco que la llamada recibida es legítima.*

- *Sé cuidadoso sobre cómo y con quién compartes información personal o financiera.*

- *Si en definitiva algún aspecto de la llamada te parece sospechosa, no respondas y suspende la llamada.*

Fuente:
https://ayuda.homeaway.es/articles/Que-es-el-smishing-y-el-vishing

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA