





fiduciaria popular

FILIAL DEL BANCO POPULAR

Tips de Seguridad en Internet

El siguiente es un documento con algunos de los métodos de captura de información mós comunes en internet y los cuidados que debe tener para proteger su información personal en internet.

Ingeniería Social

Hace referencia al arte de manipular personas para eludir los sistemas de seguridad. Esta técnica consiste en obtener información de los usuarios por teléfono, correo electrónico, correo tradicional o contacto directo.

Los atacantes de la ingeniería social usan la fuerza persuasiva y se aprovechan de la inocencia del usuario haciéndose pasar por un compañero de trabajo, un técnico o un administrador, entre otros.

En general, los métodos de la ingeniería social están organizados de la siguiente manera:

- Una fase de acercamiento para ganarse la confianza del usuario, haciéndose pasar por un integrante de la administración, de la compañía o del círculo o un cliente, proveedor, etc.
- Una fase de alerta, para desestabilizar al usuario y observar la velocidad de su respuesta. Por ejemplo, éste podría ser un pretexto de seguridad o una situación de emergencia.
- Una distracción, es decir, una frase o una situación que tranquiliza al usuario y evita que se concentre en el alerta. Ésta podría ser un agradecimiento que indique que todo ha vuelto a la normalidad, una frase hecha o, en caso de que sea mediante correo electrónico o de una página Web, la redirección a la página Web de la compañía.

La ingeniería social puede llevarse a cabo a través de medios como son: por teléfono, por correo electrónico, por correo tradicional, por mensajería instantánea, por redes sociales, por formularios web, por abuso de confianza, por espionaje, entre otros.

¿Cómo puede protegerse?

La mejor manera de protegerse contra las técnicas de ingeniería social es utilizando el sentido común y no divulgando información que podría poner en peligro su seguridad.

Sin importar el tipo de información solicitada, se aconseja que:

- Averigüe la identidad de la otra persona al solicitar información precisa (apellido, nombre, compañía, número telefónico).
- Si es posible, verifique la información proporcionada.
- Pregúntese qué importancia tiene la información requerida.
- No proporcione datos a través de redes sociales.
- Evite diligenciar formatos en sitio web para participar en rifas o suscribirse a boletines en línea.
- Evite diligenciar formularios físicos donde le invitan a actualizar datos a cambio de premios.

Phishing (captura ilícita de datos)

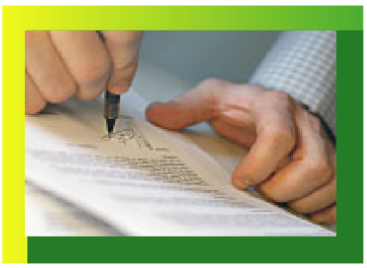
El Phishing (pesca de información) es una modalidad de fraude de Internet, que utiliza mensajes de correo electrónico "engañosos" y sitios Web fraudulentos, diseñados para confundir a los destinatarios para que divulguen información financiera personal, como nuestros números de Tarjeta de Crédito, o Débito, contraseñas, nombre de usuario u otros datos personales como cédula o Nit.

¿Cómo detectarlo?

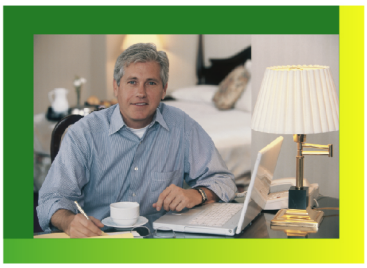
Los ciberdelincuentes envían un correo electrónico a nombre de entidades financieras de confianza, incluyendo situaciones de urgencia para que las personas reaccionen de manera inmediata y respondan con la información que ellos desean.

Generalmente, incluyen un vínculo falso que parece llevarlo al sitio Web legítimo que están suplantando, pero en realidad lleva a un sitio falso o incluso a una ventana emergente con el mismo aspecto del sitio web oficial de la entidad financiera.

¿Cómo puede protegerse?



- No utilice la opción de almacenar las contraseñas que ofrece el navegador, memorícelas.
- Teclee siempre usted mismo la dirección de la página Web de la página de la Fiduciaria. No siga enlaces que se encuentren en correos electrónicos, mensajería instantánea o banners, que le podrían conducir a páginas falsas de la Fiduciaria Popular.



- Siempre que finalice su actividad en el portal transaccional, cierre la sesión según las especificaciones de seguridad que allí se le indican.
- Evite realizar transacciones en lugares de concesión pública a Internet.
- Nunca responda a ninguna solicitud de información personal a través de un correo electrónico. La Fiduciaria Popular no solicita información confidencial para la actualización de datos por este medio.
- El único sitio autorizado para ingresar a la página Web de la Fiduciaria, en Internet es **www.fidupopular.com.co**

- Actualice las opciones de seguridad de su computador y antivirus utilizando herramientas de seguridad adecuadas (antivirus, antyspyware, firewall, etc).
- Nunca preste su número de inversión en Cartera Colectiva o Fondo de Pensión Voluntaria para recibir fondos cuyo origen usted desconoce, delincuentes utilizan este método para la transferencia de dinero de procedencia ilícita.

- Realice sus transacciones personalmente, no delegue esta responsabilidad en familiares y/o amigos.
- No diligencie formularios que vienen dentro de los correos electrónicos.
- Consulte frecuentemente los saldos de sus productos.
- Comunique los posibles delitos relacionados con su información personal a las autoridades competentes.

Recuerde:

- Ningún funcionario de Fiducia Popular está autorizado para solicitar información de autenticación (nombre de usuarios y contraseñas).
- NO es política del Fiduciaria Popular enviar correos electrónicos solicitando actualización de información confidencial (documento de identidad o claves).
- Si usted recibe un correo electrónico donde se solicite información confidencial como claves, número de tarjetas o usuario, por favor informe inmediatamente a Fiduciaria Popular, e-mail **servicioalcliente@fidupopular.com.co,** anexando el correo recibido.

Pharming (instalación de software malicioso)

El pharming es una nueva modalidad de fraude en línea que consiste en sustituir el sistema de resolución de nombres de dominio (DNS) o el archivo hosts del sistema operativo para conducir al usuario a una página web falsa, mediante la implantación de un virus o un troyano en el sistema.

¿Cómo ocurre?

Para llevar a cabo el pharming se requiere que alguna aplicación se instale en el sistema del usuario a atacar, a través de e-mail, descargas por Internet, copias desde un disco o CD, etc. Una delas fuentes que se ha detectado es el envío de un e-mail a los clientes en el que se les invita a descargar una tarjeta animada del sitio de **Gusanito.com** cuando en realidad es una liga falsa para descargar el virus o troyano en su equipo.

El pharming modifica el sistema de resolución de nombres, de manera que cuando el usuario piensa que está accediendo a su banco en Internet, realmente está ingresando a la IP de una página web falsa. Aunque es una amenaza creciente y peligrosa, la solución inicia con la prevención mediante un antivirus eficaz.

¿Cómo puede protegerse?

- Nunca responda a ninguna solicitud de información personal a través de un correo electrónico. La Fiduciaria Popular no solicita información confidencial para la actualización de datos por este medio.
- Evite abrir mensajes de destinatarios desconocidos porque se podrían activar programas informáticos malignos son previo aviso.
- No abra correos de destinatarios que no conoce.

- Instale y active el firewall en su computador para bloquear comunicaciones que los troyanos establecen para robar la información.
- Trabaje en su computador configurándolo con privilegios mínimos para su usuario, de tal forma que los troyanos.
- Evite visitar sitios para instalar programas gratuitos, descargar videos, archivos o música, porque son reconocidos como fuentes de infección de virus y troyanos.

Recuerde:

- Ningún funcionario de Fiducia Popular está autorizado para solicitar información de autenticación (nombre de usuarios y contraseñas)
- NO es política del Fiduciaria Popular enviar correos electrónicos solicitando actualización de información confidencial (documento de identidad o claves).
- Si usted recibe un correo electrónico donde se solicite información confidencial como claves, número de tarjetas o usuario, por favor informe inmediatamente a Fiduciaria Popular, e-mail **servicioalcliente@fiduppopular.com.co,** anexando el correo recibido.

Whaling (ataques informáticos focalizados)

Es un ataque enfocado y repetitivo a personas de alto perfil, que combina modalidades de fraude y técnicas de ingeniería social para obtener información confidencial de los clientes.

El ataque comienza con el bloqueo de la cuenta en la web, el cliente recibe un correo electrónico donde lo invitan a abrir un enlace a un sitio web falso para desbloquear la cuenta, el cliente ingresa la información confidencial sin darse cuenta que está en un sitio falso. El delincuente captura la información del cliente para cometer los delitos.

¿Cómo puede protegerse?

- Mantenga actualizado el computador con los últimos parches de seguridad del fabricante; actualice el software antivirus y los programas anti espía, active el firewall y las medidas de protección contra ventanas emergentes.
- No abra correos de destinatarios que no conoce.

Keylogger / Clicklogger (captura de información de teclado y mouse)

Programa informático que captura la información del cliente, al descargar software gratuito normalmente se descarga, a través de correo electrónico o enlaces de redes sociales. Igualmente se puede adaptar al computador por medio de una USB.

¿Cómo ocurre?

- Keylogger hace referencia a la captura de datos que se van digitando a través del teclado.
- Clicklogger toma imágenes de las pantallas cuando se hace clic con el mouse.

¿Cómo puede protegerse?

- Active el firewall en su computador con el fin de bloquear las comunicaciones que los troyanos establecen para robar información.
- Revise periódicamente las aplicaciones instaladas en su computador.
- No instale programas de fuentes desconocidas.
- Instale antivirus y software de prevención de Anti-Spyware y manténgalos actualizados.