Consejos para Evitar las

Estafas de Phishing

Verifique la Fuente:
Compruebe siempre la dirección de correo electrónico o el número de teléfono del remitente. Los estafadores suelen utilizar direcciones o números similares a los legítimos.

Tenga Cuidado con los Enlaces:
Deslice el cursor por encima de los enlaces antes de hacer clic para ver la URL real. Si parece sospechosa, ¡no haga clic!

No Comparta Información Sensible:
Las organizaciones legítimas nunca le pedirán una contraseña, un número de la Seguro Social o los datos de una tarjeta de crédito por mensaje de correo electrónico o de texto.

Tarjetas Regalo = Señal de Alerta:
Siempre que un mensaje le solicite a un consumidor que envíe una tarjeta regalo como forma de pago, es más que probable que se trate de una estafa y la comunicación con la entidad debe interrumpirse de inmediato.

Habilite la Autenticación Multifactor:
Habilite la autenticación multifactor en todas las cuentas disponibles para añadir una capa de seguridad en caso de que ocurra una filtración de la información.

Mantenga el Software Actualizado:
Actualice de manera periódica los sistemas operativos, los navegadores y los programas antivirus para protegerse de las amenazas más recientes.

Oficina de la Fiscal General
Estafas a Simple Vista:

Una Estafa de Phishing, Dos Estafas de Phishing

Denuncie las estafas de phishing ante el Centro de Denuncias de Delitos en Internet del FBI en
IC3.gov

Visite **MyFloridaLegal.com** para obtener consejos para los consumidores o para presentar un reclamo.

Denuncie el fraude llamando al
1-866-9-NO-SCAM
(1-866-966-7226)

Consulte otros recursos de Estafas a Simple Vista en:
MyFloridaLegal.com/ScamsAtAGlance

Oficina de la Fiscal General
PL-01 The Capitol
Tallahassee, FL 32399-1050
MyFloridaLegal.com

03/2025

Estafas a Simple Vista:

Una Estafa de Phishing, Dos Estafas de Phishing

OFFICE OF ATTORNEY GENERAL

JAMES UTHMEIER

SAFE ★ STRONG ★ FREE

¿Qué son las Estafas de Phishing?

Las estafas de phishing son intentos fraudulentos de ciberdelincuentes quienes se hacen pasar por entidades de confianza para obtener información sensible, como nombres de usuario, contraseñas y datos financieros. Estas estafas suelen producirse a través de mensajes de correo electrónico, mensajes de texto o llamadas telefónicas, en las que el estafador se hace pasar por una organización o persona de confianza.

¿Cuán Frecuentes son las Estafas de Phishing?

Las estafas de phishing son la forma más frecuente de ciberdelitos, con unos 3,400 millones de mensajes de correo electrónico basura que se envían cada día. Los informes muestran que más del 83 % de las empresas sufrieron ataques de phishing. El aumento del trabajo a distancia y de la actividad en línea no hace más que ampliar las oportunidades de estas estafas.

ALERTA DE ESTAFA

Ejemplos de

Estafas de Phishing

Phishing de Correo Electrónico

Un mensaje de correo electrónico que parece proceder de un banco y en el que se le pide al consumidor que actualice la información de su cuenta a través de un enlace proporcionado. El enlace conduce a un sitio web falso diseñado para imitar el sitio web del banco legítimo y robar las credenciales del usuario.

Spear Phishing

Un ataque más selectivo, en el que un estafador envía un mensaje personalizado en el cual se hace pasar por un colega o amigo e insta a la víctima a hacer clic en un enlace o descargar un archivo adjunto que contiene malware.

Smishing

Un mensaje de texto fraudulento en el que se afirma que la entrega de un paquete se ha retrasado y se le pide al consumidor que haga clic en un enlace para resolver el problema. El enlace puede llevar a un sitio web falso o descargar malware en un dispositivo.

Quishing

Los estafadores utilizan códigos QR falsos que llevan a sitios web maliciosos o roban datos confidenciales. Los códigos QR falsos podrían colocarse en surtidores de gasolineras, parquímetros o incluso menús de restaurantes y tomar desprevenidos a los consumidores.