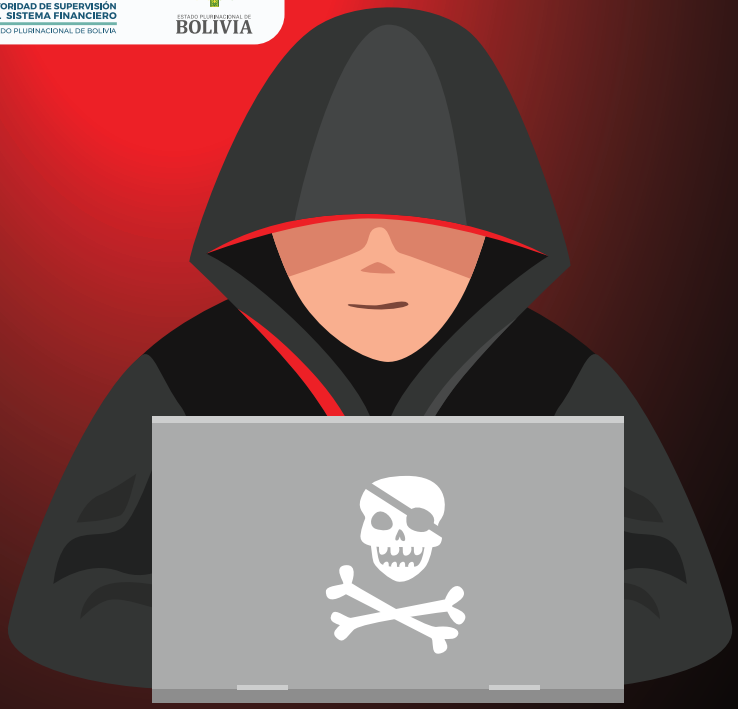
BICENTENARIO DE BOLIVIA

ASFI
AUTORIDAD DE SUPERVISIÓN DEL SISTEMA FINANCIERO
ESTADO PLURINACIONAL DE BOLIVIA
desde 1928

ESTADO PLURINACIONAL DE BOLIVIA



CIBERDELINCUENCIA

"2025 BICENTENARIO DE BOLIVIA"

CIBERDELINCUENCIA

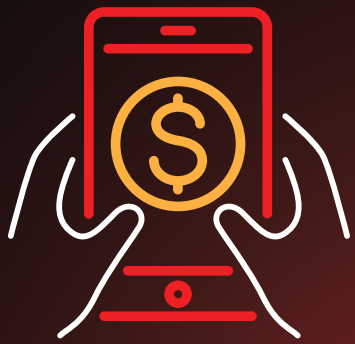
Es una actividad delictiva realizada a través de internet y tecnologías digitales con el objetivo de obtener ganancias ilegales o causar daño a las Entidades Financieras (EF) u otras organizaciones, sustrayendo información estratégica, robando datos de los clientes financieros, obteniendo claves de tarjetas de crédito o débito, entre otros actos delictivos.

Los ataques cibernéticos pueden tener un impacto negativo en la economía y las finanzas de la entidad afectada y de los clientes financieros.

TIPOS DE ATAQUES

SMISHING:

Es un tipo de estafa que involucra mensajes de texto fraudulentos o engañosos al móvil o llamadas, que intentarán suplantar la identidad de alguna persona entre los contactos del usuario del teléfono con el fin de solicitar dinero.

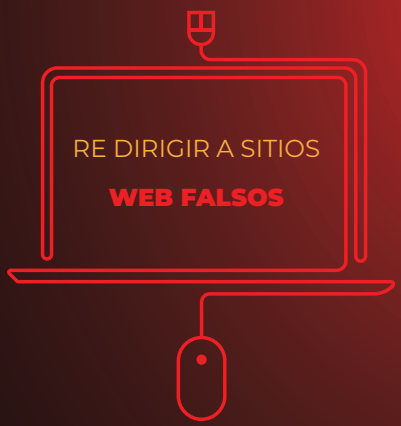


PHISHING:

Es un tipo de ataque cibernético en el que los estafadores intentan engañarte para que reveles información personal, como contraseñas o datos financieros. Suelen hacerlo a través de correos electrónicos, mensajes o sitios web falsos que imitan a empresas o instituciones legítimas.

PHARMING

Es una técnica cibernética en la que los atacantes redirigen el tráfico de Internet de los usuarios a sitios web falsos o maliciosos sin su conocimiento ni consentimiento. A diferencia del phishing, que se basa en engañar a las personas para que revelen información personal, el pharming manipula el sistema para dirigir a los usuarios a sitios falsos.

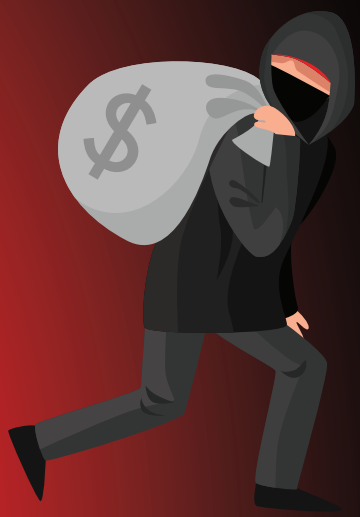


VISHING

Es una forma de estafa telefónica en la que los estafadores se hacen pasar por personas o instituciones legítimas para obtener información personal o financiera. Utilizan tácticas de persuasión y engaño para convencer a las víctimas de que compartan datos confidenciales, como números de tarjetas de crédito, contraseñas o información personal.

MALWARE

A través de correos electrónicos, o accesos a páginas web infectadas, el usuario contamina su computador con algún código malicioso generando daño en el equipo y robando información personal.



¿CÓMO PROTEGERSE DE LOS CIBERATAQUES?

En todo lo relacionado al tema financiero; tarjetas, contraseñas, páginas web y sitios de las EF, funcionan con internet y tecnologías digitales siendo que la seguridad de éstos depende en gran medida del usuario, por lo tanto es importante :

1. Cuidar la información personal

No compartir información personal vinculada a sus aplicaciones móviles o por internet (principalmente contraseñas, pin de tarjetas de débito o crédito, claves de acceso a los token digitales).

Es importante que el usuario cierre las sesiones que haya iniciado en cualquier dispositivo para realizar sus transacciones por banca por internet y banca móvil.

No compartir información personal a través de mensajes de texto o llamadas.

No escribir la clave o pin en la misma tarjeta de crédito o débito.

No guardar contraseñas en computadoras porque no se almacenan cifradas.

Evitar contraseñas fáciles de adivinar en las computadoras personales.

El uso de la contraseña es vital, por lo que deben ser cambiadas periódicamente cada dos o tres meses.

Los consumidores financieros también deben asegurarse de que la EF de la cual son clientes tenga un sistema de validación doble, en el que además de la primera contraseña se necesite de un segundo mecanismo para validar.

2. No confiar en mensajes dudosos

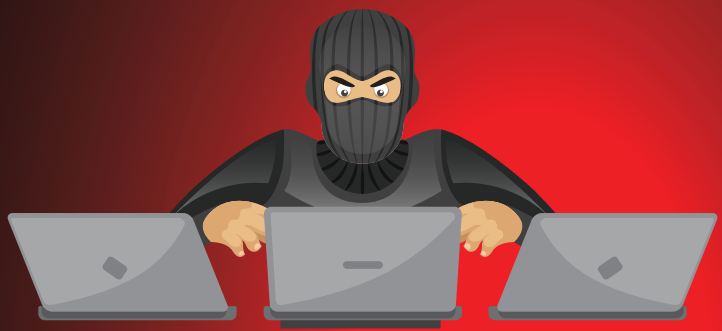
Los ciberdelincuentes utilizan la suplantación de identidad para obtener información y es una de las técnicas más utilizadas para efectuar ciberataques, por lo que no se deben tomar en cuenta falsas invitaciones de promociones o premios, ya que una EF nunca pide contraseña ni datos de cuentas mediante mensajes.

3. No caer en engaños de ingeniería social

La ingeniería social es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos, valiéndose principalmente de información difundida en redes sociales, haciéndose pasar por familiares para solicitar favores económicos mediante transferencias o depósitos.

ASFI te recomienda

Evitar realizar cualquier transacción financiera ante la duda del destino de los recursos. No dejarse sorprender por ciberdelincuentes con mensajes y llamadas telefónicas que solicitan estos datos e información con el único propósito de ocasionar algún tipo de afectación a las cuentas de los clientes financieros.



Línea Gratuita
800 103 103

www.asfi.gob.bo

@asfibolivia

ASFI Bolivia

ASFI Bolivia

asfibolivia

asfibolivia