CARTILLA DE PREVENCIÓN DEL PHISHING: FRAUDE POR INTERNET

José Eduardo Rojas

(**Coordinador en*reD*omino**)

El phishing es un fraude que consiste en la obtención ilegal de datos personales y bancarios por Internet para realizar transacciones económicas **suplantando SU identidad** para realizar **Transacciones Económicas Ilícitas** en línea.

Primero obtienen ilícitamente sus datos personales	**Después realizan transacciones económicas utilizando SUS datos**
Nombres y apellidos, dirección, Número de Identificación, seguro social, etc.	Compras por Internet
Sus números de tarjetas de crédito	Transferencias bancarias
Sus contraseñas o números PIN	Pagos por Internet
Su información de cuentas bancarias	

Recuerde que los ciber-delincuentes obtienen sus datos a través de las siguientes artimañas:

Falsos correos electrónicos	**Falsas páginas Web en ventanas emergentes o enlaces (link).**
Le envían un mail solicitando información personal con cualquier pretexto. Generalmente utilizan **formularios o enlaces falsos (links)** idénticos a los de su Empresa.	Ya sea por correo electrónico o a través de ventanas emergentes (Pop Up) le aparece una **falsa página Web idéntica a la de su EMPRESA** y le piden información personal.
Precaución: Si recibe estos correos NO ABRA NINGÚN ENLACE y contáctese inmediatamente con su EMPRESA.	**Precaución:** NUNCA BRINDE SU INFORMACION en sitios Web que provienen de ventanas emergentes o links dudosos.

Falsas llamadas telefónicas

También puede recibir llamadas telefónicas engañosas que le piden **SU** información personal, haciéndose pasar por funcionarios de su EMPRESA o de otros servicios.

Precaución: NO BRINDE SU INFORMACIÓN y solicite un número fijo de referencia para verificar la veracidad de la llamada.

COMUNÍQUESE INMEDIATAMENTE con su empresa.

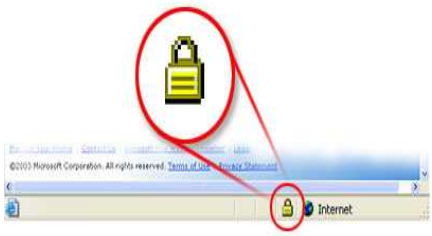
Falsos SMS

Usted recibe mensajes de texto en su teléfono celular solicitándole información personal.

Precaución: NO RESPONDA ESOS MENSAJES y comuníquese inmediatamente con su empresa.

Usted puede protegerse del fraude por Internet o **Phishing** tomando las siguientes precauciones:

- Cuando le pidan información personal por páginas Web, e-mail o teléfono, NO BRINDE SU INFORMACIÖN. Primero **verifique directamente con su empresa si la solicitud de información es confiable** y contáctese con las líneas de atención al cliente.
- **No utilice hipervínculos (link) o ventanas emergentes para ingresar al sitio Web** de su empresa. Escriba personalmente la dirección de su empresa en el navegador de Internet.
- Refuerce su seguridad y **utilice software de detección y eliminación de virus y espías**, siempre actualizados y confiables.
- **Compruebe que la página Web en la que ha entrado es segura**: debe empezar con **https://** y un pequeño candado cerrado debe aparecer en la barra de estado de su navegador de Internet. Haga doble clic sobre dicho candado para tener acceso al certificado digital que confirma que la web se corresponde con la que está visitando.



- **Revise periódicamente sus cuentas bancarias**. Los extractos mensuales son especialmente útiles para detectar transferencias o transacciones irregulares, tanto operaciones que no haya realizado y se vean reflejadas en el extracto, como operaciones realizadas online y que no aparezcan en el extracto.

¡NUNCA BRINDE SU INFORMACIÓN PERSONAL PROVENIENTE DE CORREOS, ENLACES, LLAMADAS TELEFÓNICAS O MENSAJES DE DUDOSA PROVENIENCIA!

Advertencia: La Fundación REDES y la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB), recomiendan tomar éstas precauciones debido al incremento de estafas electrónicas. Por favor divulgue esta información.