RECOMENDACIONES DE SEGURIDAD

Técnicas de fraude

ALGUNAS DE LAS SIGUIENTES DEFINICIONES SON PRÁCTICAS QUE DERIVAN FRECUENTEMENTE EN FRAUDES A TRAVÉS DE INTERNET

Phishing

El estafador (o phisher) se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica (mail) o telefónica, e intenta adquirir información confidencial de forma fraudulenta (como puede ser una contraseña, PIN o información detallada sobre sus tarjetas de crédito u otra información bancaria).
Protégete contra el fraude: la recomendación más efectiva es saber que el banco NUNCA solicitará el ingreso de contraseñas o números de tarjetas para revalidar datos ni para ningún otro trámite.

Vishing

Esta práctica tiene por objeto obtener información personal y financiera, para usos fraudulentos, a través de llamadas telefónicas.
Evite brindar información sensible en este tipo de comunicaciones. Siempre tomate un minuto antes de actuar. Quienes realizan este tipo de estafas apelan a las emociones, descuidos y urgencias.
El Banco NUNCA solicitará el ingreso de contraseñas o números de tarjetas para revalidar datos ni para ningún otro trámite.

Skimming

Es un método de robo de información de tarjetas de crédito/débito con la finalidad de reproducir o clonar la tarjeta para su posterior uso fraudulento. Consiste en el copiado de la banda magnética de una tarjeta.
Nunca pierdas de vista tu tarjeta. Al realizar compras exigí que el POSNET esté en un lugar visible.

Malware

Es un software malicioso que tiene como objeto infiltrarse o dañar una PC sin el conocimiento de su dueño y con finalidades muy diversas. Entran en esta categoría los troyanos, los spyware y los keyloggers entre otros. Pueden llegar mediante mails que aparentan ser de una entidad Bancaria o de Tarjetas.

Banco del **Chubut**

MÁS QUE UN BANCO, **NUESTRO BANCO.**

RECOMENDACIONES DE SEGURIDAD

Técnicas de fraude

Mantené actualizado el navegador, el sistema operativo y las aplicaciones. NUNCA clickees los links que traen estos mail y chequeá que el dominio sea oficial (@visa.com, @bancochubut.-com.ar, etc.)

Smishing

Se trata de una versión del phishing que se realiza a través de los servicios de mensajería de los teléfonos móviles. Con esta modalidad de fraude online pretenden capturar tus datos personales haciéndose pasar por un tercero. Para evitarlo, no accedas a los enlaces que te envíen por SMS.

Pharming

Es una técnica que permite a un atacante redirigir un nombre de dominio a otra máquina distinta. De esta forma, un usuario que introduzca una determinada dirección de internet, accederá en su explorador de internet a la página web que el atacante especificó para esa dirección.

Rootkit

Consiste en un programa que permite al intruso el acceso a distintos sistemas operativos con el objetivo de extraer en forma remota información crítica.

"Secuestro" de sesión

Es el apoderamiento no autorizado de una sesión válida en un equipo, de esta manera el atacante puede "tomar el control" de su sesión, o bien monitorear su actividad en la PC, de este modo puede hacerse de información valiosa que Ud. ingresa en las aplicaciones, páginas web y correos electrónicos.

Banco del **Chubut**

MÁS QUE UN BANCO, **NUESTRO BANCO.**