ASOCIACION DE BANCOS DE PUERTO RICO

CÓMO EVITAR SER VÍCTIMA DE FRAUDE CIBERNÉTICO Y/O MÓVIL

En la era del Internet y las comunicaciones móviles, el fraude por email o mediante mensajes de texto es muy común hoy día y su objetivo es tener acceso a información clave como tus contraseñas, números de cuenta bancaria o de tarjetas de crédito. A continuación te ofrecemos información sobre algunos de los esquemas de fraude más comunes y recomendaciones para evitar ser víctima de estos.

Fraude por e-mail

El fraude cibernético o por email ha evolucionado con el pasar de los años, hasta desarrollar mensajes tan sofisticados que parecen comunicaciones oficiales provenientes de instituciones reconocidas y fidedignas. Un ejemplo de estos son los emails que supuestamente te envía tu banco o empresa de tarjeta de crédito pidiéndote que accedas a un enlace provisto para actualizar tu información. Estos son conocidos como *Phishing Scams*. Al acceder al enlace, entras a un portal falso desde donde los estafadores retiran la información de sus víctimas.

Para evitar ser víctima del fraude por email recuerda:

- Nunca respondas a correos electrónicos de fuentes desconocidas, o aquellos que te pidan dinero, datos personales o financieros.
- No accedas (hagas click) a enlaces enviados para actualizar tu información financiera o personal.
- Si recibes un email de tu banco que requiere alguna acción de tu parte, por precaución, ingresa directamente la dirección en la barra del navegador para no acceder posibles enlaces fraudulentos.
- Nunca contestes correos de personas que te piden ayuda para sacar dinero –desde países lejanos- a cambio de una recompensa.
- No reenvíes (forward) mensajes de cadenas. Por más inofensivos que parezcan pueden ser utilizados para instalar virus o *spyware* en tu computadora.
- Toma medidas de prevención e instala sistemas de protección anti-virus y *anti-spyware* en tu computadora y actualízalos con regularidad.

Fraude Móvil

Una de las nuevas modalidades de fraude es el "*SMiShing*". Estos son mensajes de texto que parecen provenir de fuentes legítimas. Usualmente, estos mensajes

208 AVE. PONCE DE LEON
SUITE 1014
SAN JUAN PR 00918-1002

POPULAR CENTER BUILDING
SUITE 1014
HATO REY · PUERTO RICO

TEL. (787) 753-8630
FAX (787) 754-6022
www.abpr.com
info@abpr.com

incluyen un enlace que te lleva a un *website* fraudulento o te piden que llames a un número particular. La mayoría de estos mensajes recurren a notificaciones urgentes, como notificaciones de vencimiento de servicios que necesitas renovar inmediatamente o mensajes de cobro por algún servicio automático y te indican que debes llamar o enviar un mensaje a un número provisto para desactivar el cobro automático.

¿Qué debes hacer si recibes mensajes de textos sospechosos?

- No contestes mensajes de números desconocidos. Bórralos inmediatamente.
- No accedas a enlaces incluidos en mensajes de fuentes desconocidas.
- Coteja con tu compañía de servicio celular si cuentan con opciones para bloquear este tipo de mensajes de texto.
- Instala aplicaciones o *software* solo de compañías o proveedores reconocidos y confiables.
- Registra tu número de celular en la lista nacional de "No Llamar" a través de www.donotcall.gov o llamando al 1-888-382-1222.
- Si entiendes que has recibido un mensaje sospechoso o has sido víctima de "*SMiShing*", reenvía el mensaje de texto a la Federal Trade Commission a: spam@uce.gov o accede www.consumer.gov/idtheft.

Para obtener más información sobre cómo puedes protegerte del fraude, accede www.abpr.com/fraude/ o comunícate con el Grupo Especializado en Prevención de Fraude de la Asociación de Bancos de Puerto Rico al 787-753-8630.

Síguenos en Facebook® y Twitter®.