3. Cambia frecuentemente tus contraseñas, no compartas esta información con ninguna otra persona, el uso de las mismas es personal.
4. Las entidades financieras ya tienen tu información personal y no te contactarán por teléfono, correo electrónico o SMS, para que les proporciones la misma.
5. Instala una barra de herramientas anti-phishing. La mayoría de los navegadores más conocidos de Internet pueden ser personalizados con barras de herramientas anti-phishing. Dichas barras de herramientas ejecutan comprobaciones rápidas en los sitios que visitas y los compara con listas de sitios conocidos de Phishing. Si identifica un sitio malicioso, la barra de herramientas te alertará al respecto. Esta es sólo una capa más de protección contra las estafas de Phishing, y son completamente gratis.
6. Revisa el estado de tus cuentas regularmente, para asegurarte de que no se hayan realizado transacciones fraudulentas sin tu conocimiento.
7. Ten cuidado con Pop-Ups, las ventanas emergentes a menudo se disfrazan como componentes legítimos de un sitio web, sin embargo, son intentos de Phishing. Muchos navegadores populares te permiten bloquear ventanas emergentes; pudiendo habilitarlas caso por caso.
8. Mantén actualizado tu equipo y todas las aplicaciones, sobre todo el antivirus y anti-spam. Aplica los parches de seguridad facilitados por los fabricantes.

Aplicar estos consejos es tu responsabilidad.

Medidas para usar adecuadamente los servicios bancarios por Internet

Tal como se repasó en el capítulo 11 del programa Aprendiendo con el BNB: "Banca Electrónica", los bancos tienen plataformas transaccionales que brindan servicios bancarios por Internet. Para utilizarlas debes tener en cuenta las siguientes medidas de seguridad:

- Para ingresar al sitio web de tu banco escribe en el navegador la dirección del mismo, por ejemplo: **www.tubanco.com.bo**, no lo hagas a través de enlaces (links) desde otras páginas, y verifica que se trata de una página segura y que corresponda al portal verdadero de tu banco, verificando las siguientes características:
- La dirección (URL) de la página donde te encuentras se inicie con **"https://".** La letra **"s"** indica que se trata de un sitio seguro.
- Al lado de la dirección (URL) de la página donde te encuentras, verifica la presencia de la imagen del Candado de Seguridad.
- Evita acceder a los sitios web de banca electrónica desde sitios y/o redes de uso público (cabinas de Internet, wifi y otros). Si lo hiciste, te recomendamos que cambies inmediatamente tus contraseñas.
- Una vez que concluyas con tus transacciones, cerciórate de cerrar la sesión en el sitio web de banca electrónica así como el navegador.
- Mantén actualizado tu equipo y todas las aplicaciones, sobre todo el antivirus y anti-spam. Aplica los parches de seguridad facilitados por los fabricantes.

La dirección (URL) de la página donde te encuentras tiene que iniciar con **"https://"**, la letra **"s"** te indica que se trata de un sitio seguro.

Al lado de la dirección (URL) de la página donde te encuentras tiene que aparecer la imagen del **Candado de Seguridad.**

Aprende mucho más ingresando a:
www.descubre.bo

Aprendiendo con el BNB

Acerca del Programa

En el marco de la Responsabilidad Social Empresarial y en virtud al fuerte compromiso con sus clientes y la comunidad en general, el Banco Nacional de Bolivia S.A. ha estructurado el programa "Aprendiendo con el BNB", con el objetivo de mejorar la cultura financiera de los bolivianos, dotándoles de los conocimientos básicos y las herramientas necesarias para que administren sus finanzas de forma responsable e informada, promoviendo de esta manera el uso efectivo y provechoso de todos los productos bancarios que se ofrecen en el sistema financiero.

Datos de contacto

Para más información acerca del programa ingresa a www.bnb.com.bo o escribe a bnbrse@bnb.com.bo.

BNB | Banco Nacional de Bolivia

16

Aprendiendo con el BNB

Programa de Educación Financiera

Protección y Prevención Financiera

SEGURIDAD EN MEDIOS ELECTRÓNICOS - I

.RESPONSABILIDAD SOCIAL

¿Qué es el fraude electrónico?

El fraude electrónico es una modalidad delictiva utilizando medios electrónicos —bancarios en muchos casos— en beneficio económico del delincuente.

Especialistas en materia jurídica definen el delito informático o electrónico, como toda conducta que revista características antijurídicas y culpables que atentan contra el soporte lógico de un sistema de procesamiento de información, sea sobre programas o datos relevantes, o a través del empleo de las tecnologías de la información y que afectan a terceras personas.

En nuestro país este tipo de delitos se ha hecho cada vez más común, motivado fundamentalmente por la masificación del uso de Internet y la facilidad del envío de información a través de páginas web. Esta situación ha obligado al sistema bancario a mantener una actualización constante de sus sistemas de seguridad en los diferentes medios electrónicos, a fin de resguardar la seguridad de las transacciones de sus clientes.

Existen varias modalidades de fraude electrónico, así como también métodos de prevención y seguridad, por ello dedicaremos este y el próximo capítulo del programa "Aprendiendo con el BNB" a conocer los tipos de fraude electrónico más importantes y cómo combatirlos.

¿Qué es el Phishing?

El término Phishing proviene de la palabra inglesa "fishing" (pesca) y hace alusión al intento de hacer que los usuarios "muerdan el anzuelo". Algunos expertos del país lo han calificado como "el cuento del tío electrónico".

El Phishing es una forma de ingeniería social en la cual un atacante intenta de forma fraudulenta adquirir información confidencial de una víctima, haciéndose pasar por un "tercero de confianza".

Los métodos utilizados para la realización del Phishing no se limitan exclusivamente al correo electrónico, sino que también utilizan SMS (smishing), telefonía (vishing), redes sociales, mensajería instantánea a través del móvil, etc.

Cuando el contacto se realiza vía correo electrónico, es usual que se inserten formularios para que el afectado proporcione sus datos de forma directa. Otras veces los delincuentes incluyen un enlace a una página web falsa, que simula la página oficial de una empresa (entidad financiera, por ejemplo). Si el afectado hace clic en el enlace, se abre un portal que en su apariencia puede ser idéntico al de la entidad financiera con su nombre, logotipo, colores, etc., suplantando el sitio original de la empresa. Al introducir datos personales como el nombre de usuario, la contraseña y otros, se está proporcionando información personal a los delincuentes para que puedan utilizarla para acceder a la cuenta bancaria y a la información personal relacionada a ésta para cometer algún tipo de fraude.

Riesgos

Los riesgos derivados de estas técnicas son el robo de identidad y de datos confidenciales.

Ejemplo de Phishing

A continuación te presentamos un ejemplo de un correo electrónico tipificado como Phishing. El mismo aparenta ser de un remitente conocido y el asunto capta tu interés:

Banco Ayuda - Activasión de SERVICIOS

De: Tu Banco S.A (mailto:info@tvbanco.com)
Para: victima@gmail.com
Fecha: viernes, 15 de septiembre de 2018
Asunto: Banco Ayuda – Activasion de SERVICIOS

Estimado cliente:
El Tu Banco S.A. le informa que, de acuerdo a resolución 20234, todas las cuentas bancarias debían ser actualizadas antes del antes del 14-09-2018 aplicando un nuevo sistema de seguridad.

Su cuenta no fue actualizada en el plazo indicado motivo por cual nos vimos obligados a suspender temporalmente el acceso al portal del banco. Para poder activar nuevamente este servicio y contar con mayor seguridad bancaria, por favor haga clic en el siguiente enlace:

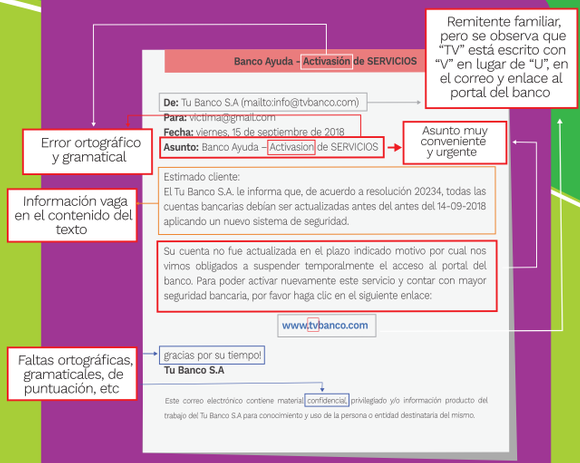
www.tvbanco.com

gracias por su tiempo!
Tu Banco S.A

Este correo electrónico contiene material confidencial, privilegiado y/o información producto del trabajo del Tu Banco S.A para conocimiento y uso de la persona o entidad destinataria del mismo.

¿Cómo combatir el Phishing?

Volviendo al ejemplo anterior, identifiquemos las partes del correo que debes verificar cuando recibas correos electrónicos de remitentes desconocidos, e incluso si vienen de remitentes conocidos.



Adicionalmente, toma en cuenta las siguientes recomendaciones:

1. Elimina todos los mensajes de email y texto que te pidan que confirmes o suministres tu información personal, tales como:
   - El número de PIN de la tarjeta de crédito o débito.
   - El PAN o número de la tarjeta de crédito o débito.
   - El número de seguridad de la tarjeta de crédito o débito (CVV).
   - El número de cuenta bancaria (CCC).
   - El nombre, apellidos, fecha de nacimiento y, número de cedula de identidad.
   - Los datos de acceso (usuario, contraseña, tarjetas de coordenadas) a los servicios de Banca por Internet.
2. Desconfía de los mensajes provenientes de remitentes desconocidos e incluso conocidos como entidades financieras, cuyo texto te amenaza con cerrarte la cuenta o tomar alguna otra medida, y no hagas clic en los enlaces (links) contenidos en el mismo.