.RESPONSABILIDAD SOCIAL

# Otros tipos de fraudes electrónicos

En el capítulo 16 del programa Aprendiendo con el BNB – Seguridad en Medios Electrónicos - I, hablamos principalmente del Phishing y cómo combatirlo (si quieres repasar el capítulo 16 ingresa a www.bnb.com.bo). En esta ocasión, y como parte complementaria, dedicaremos este capítulo a conocer otros tipos de ataques cibernéticos y las medidas de seguridad para prevenirlos.

## Malware o programa malicioso

Malware o programa malicioso, es cualquier programa o archivo que es perjudicial para un usuario de la computadora. El malware incluye virus informáticos, gusanos, caballos de Troya y spyware. Estos programas maliciosos pueden realizar una variedad de funciones, incluido el robo, el cifrado o la eliminación de datos confidenciales, la alteración o el secuestro de funciones informáticas básicas y la supervisión de la actividad informática de los usuarios sin su permiso.
A continuación explicamos cada uno de ellos:

**Virus:** Programas que infectan a otros programas, añadiendo su código para tomar el control después de la ejecución de los archivos infectados.
**Worms o Gusanos:** Su nombre implica que pueden propagarse de un equipo a otro como un gusano. Lo hacen por medio de correo electrónico, sistemas de mensajes instantáneos, redes de archivos compartidos P2P, chats, redes locales, redes globales, etc. Su velocidad de propagación es muy alta.
**Troyanos:** Un troyano es un pequeño programa generalmente alojado dentro de otra aplicación (un archivo) normal. Su objetivo es pasar inadvertido al usuario e instalarse en el sistema cuando este ejecuta el archivo "huésped". Luego de instalarse, pueden realizar las más diversas tareas ocultas al usuario. La similitud con el "caballo de Troya" de los griegos es evidente y debido a esa característica recibieron su nombre.
**Spyware o Programa Espía:** Estos programas se instalan en nuestros equipos o dispositivos con la finalidad de robar nuestros datos y espiar nuestros movimientos por la red para, posteriormente, lucrar con los mismos.

### ¿Cómo uno se infecta con un malware o programa malicioso?

A continuación te mostramos los medios por los cuales se propagan los programas maliciosos:

- Correos electrónicos.
- Archivos o imágenes adjuntas a correos electrónicos.
- Chat.
- Pop Ups o ventanas emergentes.
- Actualizaciones o parches falsos.
- Redes públicas o wifi gratuito.
- Dispositivos externos: CD, DVD, USB, cable USB (USBHarpoon), etc.
- Mensajes de texto.

**Riesgos del malware o programa malicioso**

Robo de identidad y datos confidenciales, pérdida de productividad y consumo de recursos de las redes corporativas.

# ¿Cómo combatir el malware o programa malicioso?

Para evitar que el malware haga estragos en tu equipo y/o en tus dispositivos, toma en cuenta las siguientes medidas de seguridad:

- Mantén actualizado tu equipo y todas las aplicaciones, sobre todo el antivirus. Aplica los parches de seguridad facilitados por los fabricantes.
- Evita descargar e instalar programas desconocidos, y mucho menos hacer clic en enlaces provenientes de correos electrónicos sospechosos.
- No compres ningún programa sin licencia (programa pirata). No hagas clic sobre mensajes pop-up, especialmente si te informan que han escaneado tu computadora y que detectaron malware. Los estafadores envían este tipo de mensajes para comprometer tu computadora y tomar control de ella y de la información que resguarda.
- No abras archivos adjuntos de correos electrónicos que te parezcan sospechosos hasta que confirmes la identidad del remitente.

### ¿Cómo identificar que tu computadora fue infectada con un malware o programa malicioso?

Si tu computadora presenta alguna de las siguientes características, podría estar infectada con malware y debes llevarla a un técnico para que la repare:

- Disminuye su capacidad de procesamiento, funciona mal o te aparecen mensajes de error con frecuencia.
- Recibes anuncios molestos mediante ventanas emergentes o pop-up.
- Te aparecen páginas web que no tenías intención de visitar.
- Aparecen barras de herramientas nuevas e imprevistas en los navegadores.
- El antivirus de tu computador se desactiva inesperadamente.

# Clonación de tarjetas de crédito y débito

Este delito se presenta cuando, mediante el uso de distintos dispositivos electrónicos, se reproducen los datos y elementos de seguridad de las tarjetas, ya sea de crédito o débito, sin la autorización del titular de las mismas.

Una tarjeta puede ser clonada cuando se realiza un pago en un punto de venta (point of sale – POS) o cuando la usamos para hacer alguna transacción en un cajero automático. En el primer caso se utiliza un dispositivo conocido como skimming que permite copiar la banda magnética de la tarjeta bancaria. En cajeros automáticos la clonación se da mediante la colocación de un lector falso, que transmite la información de la tarjeta por vía inalámbrica, así como una cámara oculta dirigida al teclado del cajero, para captar la información adicional del cuentahabiente.

Una vez clonada tu tarjeta puede ser utilizada para hacer compras sin tu autorización en comercios o bien por Internet, ocasionando serios inconvenientes para ti y la entidad financiera que emitió la tarjeta.

Para evitar la clonación de tus tarjetas de crédito o débito debes tener en cuenta las siguientes medidas de seguridad:

En un cajero automático:

- Procura utilizar cajeros automáticos que se encuentren dentro de establecimientos.
- Revisa que los cajeros automáticos no tengan elementos que parezcan ajenos.
- Cuando tengas que digitar el PIN cubre el teclado con la otra mano.
- Nunca aceptes ayuda o sugerencias de extraños al usar el cajero automático.
- Al finalizar la operación en el cajero automático recoge el recibo y guárdalo.
- Si el cajero automático retiene tu tarjeta sin razón aparente, notifica de inmediato al banco.
- Si el problema se presenta por la noche, llama al banco o a la empresa procesadora y pide el bloqueo inmediato de la tarjeta.

## En compras o establecimientos:

- Si es posible, solicita la terminal Punto de Venta (POS) para hacer el cargo a tu tarjeta en tu presencia.
- Si tienes que entregarle la tarjeta al empleado para que realice el cargo, no la pierdas de vista y considera que debe regresártela en un tiempo razonable.
- Cerciórate de que tu tarjeta no sea pasada por ningún artefacto diferente al destinado para realizar pagos con la misma.
- Observa las manos del empleado y la manipulación de la tarjeta, si notas algo extraño repórtalo al supervisor del establecimiento y comunícate inmediatamente con el banco o con la administradora de tarjetas de crédito (ATC).
- No divulgues tu número de PIN al cajero o vendedor del establecimiento donde utilices tu tarjeta.
- Verifica que el importe del ticket o "voucher" de compra corresponda al monto de tu transacción.

## En todo momento:

- Cuando recibas tu tarjeta fírmala en el reverso.
- Cambia tu número de PIN de forma periódica.
- Nunca lleves o portes juntos tu tarjeta y el número de PIN anotado. Memorízalo.
- Conserva los tickets y recibos de tus gastos para que puedas cotejarlos con tu estado de cuenta bancario.
- Nunca des información sobre tu tarjeta a quien lo solicite por teléfono, aun cuando aseguren que llaman de tu banco.

# Tarjetas bancarias inteligentes

El sistema EMV, que lleva el nombre de las tres compañías que han desarrollado el proyecto (Europay, MasterCard, Visa), consiste en un microcircuito incorporado a las tarjetas de crédito y débito para utilizarlas con mayores niveles de seguridad, reduciendo los riesgos asociados a fraudes electrónicos.

En otras palabras, es un nuevo estándar de medios de pago (tanto de crédito como débito) que se caracteriza principalmente por estar basado en la tecnología "chip". A diferencia de la banda magnética, el chip es un elemento activo de seguridad, ya que es la propia tarjeta la encargada de evitar su manipulación garantizando su autenticidad, por lo tanto, esta tarjeta no puede ser clonada.

¡Alerta! Las tarjetas inteligentes incorporan el chip pero no dejan de tener banda magnética, por lo tanto, son aceptadas en todos los comercios y cajeros automáticos a nivel mundial, independientemente de que éstos tengan incorporada la tecnología para leer las tarjetas con "chip".

## ¿Cómo realizar una compra con las tarjetas de crédito con chip?

1. Entrega la tarjeta de crédito con chip y el documento de identificación al cajero del establecimiento comercial al momento de realizar el pago de la compra.
2. Verifica que el cajero inserte la tarjeta de crédito en la parte frontal inferior del dispositivo Punto Electrónico de Venta (POS) y que la mantenga dentro mientras dure la transacción.
3. Ingresa tu PIN y espera a que el cajero termine la transacción.
4. Firma el comprobante de pago y entrégalo al cajero.
5. Asegúrate que el cajero retire tu tarjeta de crédito del POS y junto con ésta te devuelva el documento de identificación y una copia del comprobante de venta.

## ¿Cómo realizar una transacción en cajero automático?

Como siempre se hace, el proceso es el mismo.

Si quieres más información acerca de estas tarjetas visita las oficinas de tu banco o ingresa a la página web del mismo.

# ¿Cómo crear una contraseña?

1. Cuanto más extensa sea tu contraseña más difícil será descifrarla. Usa como mínimo diez (10) caracteres aunque lo ideal son doce (12).

2. Combina letras, números y símbolos. Trata de no crear contraseñas obvias, no uses tu nombre, fecha de nacimiento, o palabras de uso corriente.

3. No uses la misma contraseña para varias cuentas. Si te la roban, o se la roban a alguna de las compañías que tiene tu contraseña, podrían usarla para tratar de acceder a todas tus cuentas.

4. No facilites tus contraseñas por teléfono, en mensajes de texto o por email. Las empresas que operan legítimamente no envían mensajes para pedir contraseñas. Si recibes un mensaje solicitando el número de tus contraseñas, lo más probable es que sea un intento de fraude.

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

17

Aprendiendo con el BNB

Programa de Educación Financiera

Protección y Prevención Financiera

# SEGURIDAD EN MEDIOS ELECTRÓNICOS - II