Universidad Veracruzana

Protégete de los Fraudes Bancarios

Ciberseguridad
UV-CSIRT

Información segura... ¡es cultura!®

Protégete de los fraudes bancarios

Hoy en día la tendencia a los fraudes bancarios es cada vez mayor, es por ello que, ante las recientes o recurrentes formas utilizadas por los ciberdelincuentes para realizar estafas, es indispensable que todos, a nivel personal e institucional, conozcan los distintos tipos de ataques usados, así como algunas recomendaciones que es importante considerar para protegerte y no caer en estos fraudes.

Principales ciberataques bancarios

Vishing y Smishing: Son llamadas o SMS falsos que imitan la comunicación de los canales oficiales del banco o a ejecutivos bancarios.

Phishing: Son correos falsos que solicitan datos personales o bancarios y que invitan a acceder a un sitio falso o a descargar un archivo con código malicioso (malware).

Malware: Es un software malicioso que infecta dispositivos mediante descargas no autorizadas y realiza funciones en el sistema que perjudican al usuario y/o sistema o roban información. Por ejemplo: spyware, virus, ransomware, etc.

Pharming: Es un tipo de ciberataque con el que se intenta redirigir el tráfico a sitios web falsos que copian el diseño de los canales oficiales y tienen como finalidad recopilar tu información personal o descargar software malicioso (malware).

Spear Phishing: Es una variación del Phishing donde los atacantes investigan a la víctima mediante sus perfiles en redes sociales y de esta manera poder dirigir correos o llamadas personalizadas y convincentes para que proporciones información o realices alguna acción.

¿Información que solicitan en un fraude?

- Ponerse en contacto con números nuevos o inusuales
- Proporcionar contraseñas, fecha de vigencia o el NIP de tu tarjeta
- Recibir o actuar según instrucciones no solicitadas
- Hacer clic en enlaces inesperados o innecesarios en un correo electrónico
- Transferir la mayoría o la totalidad del saldo de la cuenta
- Aprobar transacciones desconocidas
- Transferir fondos antes o durante un día festivo

¿Cómo protegerte?

1. Si recibes una alerta vía SMS o por email, ¡Verifica quien te contacta!

Protégete de los fraudes bancarios

2. No des clic a links sospechosos, ni descargues archivos adjuntos cuando el remitente es desconocido o tienes sospechas que el sitio web es falso.
3. Nunca respondas con tus datos personales o bancarios, no proporciones tus contraseñas y elimina los mensajes o cuelga las llamadas que te solicitan datos personales o realizar transferencias.
4. Actualiza tus datos de contacto en sucursal y/o Banca Movil.
5. Activa alertas y notificaciones, para que vía SMS o correo electrónico recibas confirmación sobre las compras.
6. Activa tu firma electrónica en cajeros, ya que ayudará a reducir las posibilidades de un cargo no reconocido.
7. Es importante que siempre que utilices la banca en línea, utilices computadoras con software de detección de antivirus, antispyware y malware.
8. Cambia tu clave de acceso para ingresar a la banca en línea con frecuencia, por lo menos cada 3 meses.

Mantente alerta:

- Cuando vayas al cajero verifica que no tenga dispositivos extraños en el lector de tarjetas. Además protege tu NIP y la pantalla. No aceptes ayuda, ni te dejes distraer por alguien más.
- Cuando pagues con tu tarjeta, no la pierdas de vista y pide que lleven la terminal a tu lugar e inserta tú mismo la tarjeta.
- Al recibir tu estado de cuenta, revisa que no tenga ningún movimiento inusual.
- Activa el servicio de alertas y notificaciones para tus transacciones con tarjetas y cuentas.
- Si robaron o extraviaste tu tarjeta de crédito o débito, repórtala de inmediato al Centro de Ayuda del banco.

Recuerda:

Las instituciones bancarias nunca solicitan información personal o de su cuenta a través de mensajes de texto, llamadas o correo electrónico.

¡Ante la duda, la respuesta es NO!

Referencia:
https://www.banamex.com/centro-de-seguridad/index.html