Recomendaciones de Seguridad de la Información

Contra el fraude y robo de identidad

Los fraudes pueden ocurrir vía telefónica, a través de mensajes de texto (SMS), correos electrónicos y enlaces. Sin importar el medio, los delincuentes usarán pretextos como los siguientes, con el fin de que la víctima se familiarice con el engaño y los defraudadores puedan obtener su información:

- Usted cuenta con depósitos retenidos.
- Su tarjeta ha sido bloqueada.
- Su cuenta y/o contraseña ha sido bloqueada.
- Debemos actualizar sus datos de contacto.
- Encontramos un cargo no reconocido.

Recuerde que la Caja San José de Tlajomulco no le contactará a través de correo, SMS o llamadas para solicitar datos confidenciales como: acceso, contraseña, token, NIP o CVV.

Proteja su identidad

Cuide su información y su identidad

Las personas cuya identidad ha sido robada, pueden tardar meses, incluso años, y gastar parte de su patrimonio limpiando el problema que los ladrones han hecho de su buen nombre y registro en el buró de crédito.

- Los defraudadores le tratarán de engañar para obtener tanta información como les sea posible, misma que utilizarán para robar su identidad o su dinero.
- Los delincuentes buscan información personal (nombres, direcciones, números telefónicos, RFC, etc.) e información financiera (números de cuentas bancarias, números de tarjetas, claves de acceso, NIPs, etc.).
- No proporcione nunca datos personales o bancarios por teléfono a menos que usted haya comenzado la llamada y asegúrese de la identidad de su interlocutor.
- Ponga especial cuidado cuando cambie de domicilio, asegúrese que el correo llegue a su nueva dirección y no a la anterior.
- Si sale de vacaciones o no se va a encontrar en casa por un tiempo, solicite a algún vecino o familiar de confianza que recoja su correspondencia.
- Destruya cualquier documentación que contenga datos personales antes de tirarla.
- Revise su historial crediticio en el Buró de Crédito por lo menos 1 vez al año y levante una aclaración en cuanto detecte créditos no solicitados. Recuerde que tiene derecho a una consulta gratuita por año.
- Denuncie a la autoridad cualquier robo en sus cuentas inmediatamente.

Cuide su información y su identidad

- Rechace ofertas de tarjetas comerciales, descuentos o pagos de servicios en vía pública, no entregue copia de su tarjeta.

- Implemente con su familia la norma de no proporcionar ninguna información por teléfono a personas desconocidas.
- Eventualmente podría recibir llamadas de su banco para verificar si realizó transacciones diferentes a su patrón de comportamiento, atienda las mismas tan pronto le sea posible.
- Las instituciones financieras pueden solicitar datos personales como: nombre completo, fecha de nacimiento, RFC y dirección, para realizar la autenticación necesaria.
- Recuerde que las instituciones financieras NO piden información como el NIP de la tarjeta, claves del dispositivo TOKEN o contraseña.

Autenticación

Si se comunica a su banco es normal que soliciten algunos datos para confirmar que sea usted. Recuerde que no debe compartir su: acceso, contraseña, NIP, token o CVV.

Si su banco llama primero, no le pedirá información confidencial como accesos y contraseñas.

El banco puede pedir para autenticación:

- Nombre completo
- Fecha de nacimiento
- RFC
- Dirección
- Correo electrónico
- Número de teléfono

No lo compartas:

- Acceso
- Contraseña completa
- CVV: número al reverso de tu tarjeta
- Dirección
- NIP: clave de cuatro dígitos de tu tarjeta
- Token: contraseña dinámica

Fraude telefónico

Los fraudes telefónicos se pueden realizar a través de: llamadas directas, llamadas con mensajes pregrabados (vishing) y mensajes de texto (smishing).

Llamadas

- Si recibe llamadas relativas a ofertas para la contratación o adquisición de productos o servicios, desconfíe y no se deje presionar. Una compañía seria entenderá que quiera decidir con calma la compra o contratación.
- Resulta más sencillo descartar un correo electrónico que decirle ¡no! a una persona por teléfono; sin embargo, rechace las ofertas o promociones que le parezcan sospechosas.
- **Recuerde que su banco no llama para solicitar datos confidenciales como:** el código de verificación de la tarjeta (CVV), que son los tres números al reverso del plástico; tampoco el número de identificación personal (NIP), o los códigos del token, ni los datos para acceder a la cuenta (usuarios o contraseñas).

Vishing

¿Qué es el vishing?

Es un fraude que se realiza mediante una llamada telefónica, generalmente con una voz automatizada, que simula ser tu banco. La finalidad es conseguir los datos personales y/o bancarios de una persona.

Ocurre bajo dos circunstancias:

1. La víctima recibe un mensaje de texto (SMS) que dice ser su banco y le alerta de alguna anomalía en su cuenta. Dicho SMS, indica comunicarse al

teléfono que se proporciona. Cuando la víctima se comunica, la operadora pide ingresar datos con el fin de “autenticar” al cliente: número de cuenta, dígitos de seguridad, fecha de expedición, correo electrónico, NIP de cajero automático y hasta número de celular. Al proporcionar el último dato, la llamada se corta.

2. La víctima recibe una llamada en la que escucha una voz pregrabada que solicita su información confidencial con el pretexto de ayudarla con alguna actividad sospechosa referente a su cuenta.

¿Cómo identificarlo?

1. Compare el remitente del mensaje de texto con el remitente de los mensajes que ha recibido de tu banco.

2. Al llamar por teléfono, el primer filtro es un sistema de voz automatizada que le pide proporcionar información confidencial.

3. Si contesta una persona que no puede identificarse de manera rápida y válida.

¿Cómo evitarlo?

- Nunca entregue información confidencial, recuerde que su banco no llama para solicitar datos como: el código de verificación de la tarjeta (CVV), tampoco el número de identificación personal (NIP), código token, ni los datos para acceder a la cuenta (usuarios o contraseñas).
- Comuníquese a la línea oficial de su banco o acuda a la sucursal.
- Cambie sus contraseñas periódicamente (ver contraseñas).

Smishing

¿Qué es el smishing?

Es un fraude telefónico que se comete a través de un mensaje de texto (SMS) que afirma ser su banco y que le pide información personal o financiera.

¿Cómo evitarlo?

Si le llega un mensaje a su celular informándole que ha ganado un premio o que necesita proporcionar datos personales para resolver algún problema con su cuenta, no conteste (ver pretextos que usan los delincuentes).

Números confiables

La mejor forma de prevenir los fraudes por teléfono es no permitir el contacto con el estafador. Se recomienda no contestar llamada de números privados o fuera de sus contactos. La mayoría de los estafadores o vendedores colgarán sin dejar mensaje.

Si tiene duda que la llamada sea de su banco, cuelgue y comuníquese directamente al centro de atención de su banco.

Fraude por correos electrónicos (phishing)

Las estafas denominadas “phishing” llegan a través de un correo electrónico que parece ser de su banco o de otro servicio. El correo incluye un enlace peligroso que lleva a una página similar a la de la institución o empresa que dice ser. En esta página fraudulenta, la víctima introduce sus datos y el estafador logra obtenerlos.

Puede haber dos tipos de “anzuelo”, el primero, es un correo que le pedirá acceder a su cuenta con el pretexto que ha identificado una transacción o actividad sospechosa. Así le convence de dar clic al enlace adjunto, que le dirigirá a un sitio fraudulento similar al de su banco, que robará sus datos en cuanto los ingrese.

El segundo indica que debe actualizar sus datos de pago de algún servicio, para ello, le proporciona un enlace a una página que pedirá los datos de su tarjeta; sin embargo, en el momento que intenta entrar a su cuenta a través de este enlace, o que actualiza los datos que le solicitan, el estafador logra robar sus datos.

¿Cómo evitarlo?

- Si recibe correos electrónicos que contienen vínculos, revise primero que el remitente sea confiable antes de acceder al enlace (ver banca en línea).
- Recuerde que su banco no enviará vínculos a través de correo electrónico.
- Si recibe un correo electrónico supuestamente de su banco solicitándole que se ponga en contacto a un determinado teléfono, no lo haga, puede ser que sea falso (ver vishing). Llame directamente a su banco y compruebe que ellos le han enviado el correo.

Fraudes con remitente enmascarado (Spoofing)

Con este fraude, el delincuente “enmascara” o “disfraza” su número, para que aparezca el nombre del banco en el identificador y así solicitar sus datos confidenciales.

¿Cómo evitarlo?

Registre el número oficial en su teléfono y siempre compruebe que el teléfono del remitente coincida, aunque el identificador diga el nombre de su banco.

Cuidado, aunque su identificador diga el nombre de tu banco, NO comparta sus datos confidenciales.

Recuerde que su banco no llama para solicitar información sensible como accesos, contraseñas, NIPs o CVV.

Si tiene duda CUELGUE y comuníquese directamente con su banco.

Operaciones seguras

Cajeros automáticos (ATMs)

- Proteja y resguarde sus claves confidenciales (NIPs).
- Lleve en su cartera únicamente la tarjeta que utilizará.
- Al acceder o salir del área de cajeros automáticos, no es necesario digitar su NIP, insertar o deslizar su tarjeta en la puerta de entrada.
- Antes de introducir su tarjeta en el cajero automático, verifique que éste NO tenga aditamentos extraños.
- Al realizar una operación en un cajero, no acepte ayuda de personas ajenas al banco.
- Al teclear su número confidencial, asegúrese que nadie esté cerca.
- Al terminar, recuerde tomar su tarjeta y verifique que el lector de tarjetas esté en verde para garantizar que su sesión ha finalizado.
- No olvide su comprobante.
- Utilice cajeros automáticos que estén bien iluminados y preferentemente con vigilancia, como aquellos localizados en las sucursales bancarias o centros comerciales.
- Nunca realice transacciones en cajeros que hayan sido vandalizados; es decir, que tengan daños en su estructura.
- Reporte a su banco cualquier anomalía detectada en el cajero automático.
- Cuando el cajero no le devuelva su tarjeta, cancele su operación y repórtela de inmediato.

Sucursales bancarias.

Antes de retirarse de la ventanilla, asegúrese de tener su comprobante y revise que la impresión del sistema refleje correctamente el tipo de operación, depósito, retiro o pago y el número de cuenta o contrato, así como el monto correcto y la fecha de las operaciones realizadas.

¡Tenga cuidado! En una sucursal bancaria, ninguna persona le puede solicitar dinero para ayudarle con su operación. Si nota alguna irregularidad, repórtela de inmediato al personal de la sucursal.

Banca electrónica y banca en línea

La banca electrónica opera por cualquier medio electrónico como teléfonos, cajeros automáticos e internet, mientras que la banca en línea opera únicamente por internet.

Banca en línea

- Para acceder al sitio web de su banco, siempre teclee la dirección directamente en el navegador, no lo haga a través de hipervínculos o del buscador.
- Compruebe que la dirección de su banco sea correcta y que comience con "**HTTPS**" y no con "**HTTP**." Asimismo, podrá observar un candado junto a la dirección web que indica que es un sitio seguro.
- Nunca dé clic o responda a una ventana emergente (pop-up) o correo sospechoso, porque puede conducirlo a una imitación de página web y solicitarle información personal, financiera o datos de sus contraseñas (ver phishing).
- Evite almacenar información financiera (usuarios, contraseñas, NIPs, estados de cuenta, etc.) en su computadora personal.
- Si usa equipos que no le pertenecen, asegúrese de borrar todos los archivos temporales de internet y cierre todas sus sesiones.
- Revise periódicamente las cuentas que tiene registradas para hacer traspasos. Asegúrese de que no existan cuentas que usted no dio de alta.

Banca electrónica o digital

- Descargue la aplicación de su banco de sitios oficiales como App Store y Play Store o directamente en el portal de su banco.
- Actualice regularmente su dispositivo y su aplicación de banca electrónica.

- Configure **la opción de bloqueo automático en los dispositivos móviles**. Se puede hacer mediante el PIN, patrón de desbloqueo, huella digital o si el móvil dispone de la herramienta de reconocimiento facial, aún mejor.
- **Si utiliza una red wifi pública**, no capture sus datos confidenciales, ya que algunas se utilizan para robar información de los usuarios.

Dispositivos

- Instale en todos sus dispositivos (computadora, tableta, teléfono) un software de protección antivirus y antiespía.
- Actualice regularmente su software de protección antivirus, para evitar que algún hacker pueda acceder a su información.

Wifi seguro

- No acceda a su banca en línea o a la banca electrónica desde una red wifi pública o gratuita ya que pone en riesgo sus datos.
- Si utiliza una red wifi gratuita, asegúrese de mantener sus dispositivos actualizados y contar con antivirus y antiespía. También se recomienda usar una aplicación VPN para disfrazar su ubicación.
- Asegúrese de que la red wifi de su casa tenga contraseña.