TIPS DE SEGURIDAD

1. Uso de cajeros automáticos (ATM)

Al utilizar los cajeros automáticos los puntos críticos de seguridad a considerar son:

- Tu tarjeta de débito
- Tu clave de seguridad (PIN)
- Tu integridad física

Los fraudes más frecuentes con cajeros automáticos (ATM)

Retención de Tarjeta: La tarjeta queda retenida en una máquina lectora de un cajero automático previamente manipulado por un criminal, para posteriormente ser removida por el delincuente.

Captura de la Clave de Seguridad (PIN): Cuando un tercero copia la clave mientras se marca en el cajero automático, bien sea observando por encima de tu hombro, haciendo uso de un espejo, de una cámara escondida o de un teclado falso.

Precauciones que debes tener en cuenta al transaccionar en un cajero automático

Observa a tu alrededor detalladamente antes de acercarse a un cajero automático. Si observas individuos sospechosos en sus alrededores o, si el área se encuentra muy aislada o peligrosa, no uses el cajero automático.

No aceptes ayuda de desconocidos mientras se encuentra en el cajero automático.

Asegúrate que las otras personas en la fila de espera mantienen cierta distancia de ti. Ten cuidado que no te estén observando cuando ingresas tu clave.

Párate cerca del cajero automático y protege el teclado con tu mano cuando ingresas tu PIN.

No uses el cajero automático si tiene algún elemento adjunto a la abertura donde se inserta la tarjeta o teclado.

Evita usar cajeros automáticos que tengan mensajes o letreros fijados indicando que las instrucciones de la pantalla han sido cambiadas.

Si sospechas que ha ocurrido alguna situación inusual en un cajero automático, dirígete a otro cajero e infórmale al Banco.

Precauciones que debes tener en cuenta con las tarjetas de débito y claves de seguridad (PIN)

- Tu tarjeta de débito es personal e intransferible.
- Mantén tu tarjeta de débito siempre bajo tu resguardo
- Memoriza tu clave.
- NUNCA divulgues tu clave a nadie.
- No utilices claves de fácil deducción, tal como datos personales.
- Cambia tu clave periódicamente, y si sospechas que alguien la conoce, cámbiala inmediatamente.
- Verifica tus saldos y estados de cuenta regularmente y reporta cualquier discrepancia al Banco inmediatamente.

1. **Uso de puntos de venta (POS):**

Los puntos de venta son propensos a la clonación de claves de seguridad, sustitución fraudulenta de tarjetas de débito y doble facturación fraudulenta.

Los fraudes más frecuentes con puntos de venta (POS)

Captura de clave de seguridad (PIN): Cuando un tercero copia la clave del cliente mientras la marca en el teclado del punto de venta (PIN Pad).

Sustitución fraudulenta de tarjetas de débito: Se comete directamente en el establecimiento comercial cuando de manera intencional el cajero al cobrar un servicio o compra realiza el intercambio de tarjetas de débito entregando al cliente la tarjeta fraudulenta.

Doble facturación fraudulenta: Se comete directamente en el establecimiento comercial cuando de manera intencional el cajero al cobrar un servicio realiza dos veces la misma transacción de forma exitosa, pero le indica al cliente que la primera transacción tuvo problemas y no fue satisfactoria. Finalmente el cliente paga dos veces por el mismo servicio.

Precauciones que debes tener en cuenta al momento transaccionar por un punto de venta

- Revisa tu tarjeta después de hacer el pago en un punto de venta a fin de verificar que sea la tuya.
- No pierdas de vista tu tarjeta cuando estés realizando una transacción; asegúrate que el comerciante no pase la tarjeta por un dispositivo distinto a un punto de venta.
- Al introducir la clave secreta cerciórate que nadie te esté observando.
- No aceptes ayuda de terceras personas.
- Solicita siempre el comprobante de compra que emite el punto de venta, con más razón cuando tu transacción haya presentado problemas.
- Firma tu tarjeta para identificarla.
- No proporciones tu número de tarjeta de débito bajo ninguna circunstancia, a no ser que esté negociando con una empresa de buena reputación.

2. Uso cheques y chequeras:

Para la seguridad de cheques y chequeras es importante protegerse de la falsificación y estafa de cheques, lea nuestras recomendaciones.

Los fraudes más frecuentes con cheques y chequeras

Adulteración de cheques : El cliente emite un cheque y el delincuente una vez en posesión del mismo, modifica uno o más datos del cheque emitido, como por ejemplo cambiar el monto, el nombre del beneficiario o el número de cuenta del cliente, para posteriormente cobrar el cheque con los nuevos datos.

Sustracción de cheques: Cuando el delincuente roba uno o más cheques al cliente y falsificando la firma de este, emite cheques a su favor para cobrarlos por taquilla o los emite a favor de establecimientos comerciales para el pago de compras.

Duplicidad de cheques: Un cliente emite un cheque y el delincuente antes de que llegue a manos del beneficiario lo duplica y lo presenta al Banco antes que el beneficiario. El duplicado del cheque puede realizarse de dos maneras:

Se copian los datos del cheque original de manera manual y se transcriben e imprimen en papel valor original.

Se escanea el cheque y la imagen se imprime en papel convencional.

Precauciones que debes tener en cuenta al momento transaccionar con cheques

- Al recibir tu chequera verifica frente al personal del Banco tus datos y revise que la cantidad de cheques sea la correcta y que el número de los mismos sea consecutivo. Si tiene algún faltante no reciba la chequera y solicite de inmediato la presencia del Gerente.
- Custodia tus cheques en blanco, como si se tratara de dinero en efectivo, evitando que alguien más tenga acceso a éstos.
- Custodia tu chequera en un lugar seguro, de preferencia con llave, evitando dejarla en:
    - Gavetas sin el debido resguardo
    - Prendas de vestir
    - Maletines, carteras o bolsos

- Recuerda que los cheques son tu responsabilidad desde el momento que los recibes, incluyendo el mal uso que hagas de ellos.
- No dejes desatendida tu chequera sobre escritorios, mesas de restaurantes o mostradores de comercios.
- Evita dejar tu chequera en el carro para que la misma sea sustraída en servicios de auto-lavados, valet parking, estacionamientos, entre otros.
- No firmes cheques en blanco.

- Si perdiste o te robaron un cheque o chequera, notifícalo inmediatamente al Banco y ordena su cancelación.
- No elabores cheques con bolígrafos de otras personas.
- Verifica que los cheques que recibas no tengan tachaduras o alteraciones en sus datos.
- Antes de tirar a la basura, destruye perfectamente cheques cancelados o no utilizados. Hoy en día la basura es una fuente de información muy útil para la delincuencia.
- Lleva un registro de todos los cheques que emitas, con esto evitarás problemas de sobregiro.
- Si sospechas que ha ocurrido alguna situación inusual con tus cheques o chequeras, informa al Banco.

3. Uso de banca electrónica:

Los fraudes más frecuentes a través del uso de banca electrónica son:

- Phishing.
- Vishing o phishing telefónico.
- Pharming.
- Keylogger mejor conocido como capturador de teclas.

Phishing

Es una de las modalidades más utilizadas para generar fraude. Se trata una técnica de fraude financiero cuyo objetivo es engañar a los clientes para que suministren información de sus cuentas y datos personales por medio del envío de correos electrónicos falsos.

Características:

Te envían correos utilizando una página web ficticia con información o imagen de un Banco, entidad financiera o tienda de Internet, en el que se le explica que por motivos de seguridad, mantenimiento, mejora en el servicio, confirmación de identidad, advertencia de fraude o cualquier otro motivo, debe actualizar los datos de tu cuenta. Además, te informa que la misma será bloqueada si no realizas la actualización de datos en un tiempo determinado.

El mensaje imita exactamente el diseño (logotipo, firma, etc.) utilizado por la entidad para comunicarse con sus clientes.

El mensaje puede integrar un formulario para enviar los datos requeridos, aunque lo más habitual es que incluya un enlace a una página donde actualizar la información personal.

Precauciones que debes tener en cuenta para prevenir un phishing:

- No abras correos electrónicos de destinatarios desconocidos.
- Nunca ingreses a una página web a través de un enlace de correo electrónico.
- Evita suministrar información personal ni financiera mediante correos electrónicos.
- Escribe directamente la dirección www.bancrecer-ve.com

Vishing o phishing telefónico

Es una técnica de fraude financiero cuyo objetivo es engañar a los clientes para que suministren información de sus cuentas y datos personales a través de una llamada telefónica realizada a un número de atención al cliente falso.

Características:

Haciéndose pasar por representantes de tu Banco, se intenta persuadir a los usuarios/clientes para que llamen a un número falso de atención al cliente, donde te solicitan introducir tu número de cuenta bancaria, tarjeta de crédito, claves y números de cédula por medio de teléfono, a través del teclado del mismo.

Precauciones que debes tener en cuenta para prevenir Vishing o phishing telefónico:

No suministres ninguna información personal ni financiera a personas que lo contacten telefónicamente y de dudosa procedencia.

Pharming

Es una amenaza más sofisticada y peligrosa que consiste en conseguir que las páginas visitadas por los usuarios no sean las auténticas, sino con otras creadas para recabar datos confidenciales, sobre todo relacionadas con la banca online.

Características:

Una técnica muy utilizada para realizar éste tipo de ataque es a través del envío masivo de correos electrónicos. El correo electrónico puede provenir de distintas fuentes, las cuales, resultan llamativas para el usuario; algunos de los principales temas que se utilizan son los siguientes:

- Noticias falsas o amarillistas. En este tipo de correos los intrusos crean una noticia llamativa y, en la mayoría de las ocasiones, utilizan un tema actual y de interés general para la sociedad.

- Envío de tarjetas postales electrónicas. En este caso, el intruso enviará un correo invitando al usuario a abrir una postal que supuestamente le ha enviado un amigo, en la cual debas proporcionar tus datos personales.

- Supuesta obtención de algún premio. Estos correos intentan engañar al usuario diciéndole que ha sido ganador de algún premio: viaje, dinero en efectivo, autos, etcétera., solicitando que suministres información personal.

- Supuestos boletines informativos de una institución pública o privada, solicitando datos personales. Los intrusos que utilizan este tipo de temas invitan al usuario al usuario a descargar un archivo o visitar una página que supuestamente contiene un "boletín" o archivo elaborado por alguna institución reconocida y de confianza para la sociedad

Precauciones que debes tener en cuenta para prevenir un pharming:

- Instala un antivirus que filtre y controle las actividades de tu PC.
- Actualiza con frecuencia tu antivirus.
- Keylogger mejor conocido como capturador de teclas
- KeyLogger o captura de teclado, son todos aquellos programas o dispositivos que se instalan en tu computador para capturar la información que escribes en el teclado, frecuentemente utilizado por los estafadores.

Características:

- Existen dos tipos: El tipo hardware, se presenta como un dispositivo externos, que se conectan entre el PC y el teclado, a través de los puertos, y el tipo Software, son programas que se instalan y funcionan de manera invisible.
- Los keyloggers son detectados como programas espías o troyanos por los antivirus y otros mecanismos de defensa.

Actualmente los KeyLoggers monitorean:

- Las teclas que pulsan

- Pantallas que muestran al espía ventanas con las que ha trabajado.

- Información sobre la utilización de Internet y muchas otras actividades que se realizan en el computador.

- Es importante mencionar que el espía ni siquiera necesita tener acceso físico al PC, porque la mayoría de los keyloggers envían la información que capturan por correo electrónico.

- Es de fácil adquisición e instalación.

Precauciones que debes tener en cuenta para prevenir un keylogger:

- Abstente de realizar transacciones en línea desde lugares públicos o poco confiables.
- No abras link que no conozcas, tomando en cuenta que estos programas espías se presentan con regularidad de forma engañosa.
- Instala en tu computador programas antivirus y actualízalos regularmente.
- No utilices los dispositivos externos de terceros.

Precauciones generales que debes tener en cuenta al momento de transar por Internet

- No respondas ningún mensaje de correo que le solicite datos personales y confidenciales tales como: claves, contraseñas, números de tarjeta de crédito o débito, códigos de seguridad o de acceso.
- Nunca ingreses a Crecernet a través de vínculos enviados en correos electrónicos, ingrese siempre desde el acceso directo que se encuentra en la página Web de Crecernet.
- Escribe tu mismo la dirección electrónica del banco www.bancrecer-ve.com , en el espacio “Address” o “Dirección” de su explorador de Internet.
- Verifica que accediste de manera segura a la página auténtica de Crecernet. Al ingresar a haz click en la imagen del candado de seguridad.
- Cambia tu contraseña de Crecernet con regularidad y memorícela. Nunca la escribas ni la compartas con nadie.
- No utilices la misma contraseña con la cual ingresas a Crecernet para acceder a otros servicios que posees en Internet.
- Consulta frecuentemente los movimientos de tus cuentas y tarjetas.
- Al hacer uso de tu correo electrónico, no abras ni descargues archivos adjuntos sospechosos o llamativos de temas de actualidad (tipo PDF, videos, audio, texto) provenientes de remitentes conocidos, estos pueden ser virus encubiertos que luego de abrirlos se instalan en su computador, generalmente con el objeto de robar sus credenciales.
- Instala en tu computador personal un antivirus con capacidad antispyware y actualízalo periódicamente, para evitar que programas espías se alojen en tu computador.
- Elimina regularmente los archivos temporales de Internet y los “cookies” del navegador que están almacenados en tu computador.
- Nunca accedas a su sitio de Banca en Línea desde computadoras de acceso público (Eje: locales de cibercafé, oficinas de trabajo de uso compartido, etc.)