

Verifica la autenticidad de cualquier mensaje SMS o correo que recibas Si tienes la menor sospecha sobre la legitimidad del SMS o correo, evita dar clic en los enlaces que vengan adjuntos.

- Si notas que la señal de tu línea telefónica se ha perdido por un periodo inusual de tiempo, acércate a tu proveedor para notificarle la situación y llama a SuperLínea (55 5169 4300) para verificar el estado de tus cuentas.
- Recuerda, todos los SMS oficiales de Santander llegarán de números con dígitos cortos o del correo electrónico oficial de Santander. (terminación @santander.com.mx). Ante cualquier sospecha, marca inmediatamente a SuperLínea (55 5169 4300).



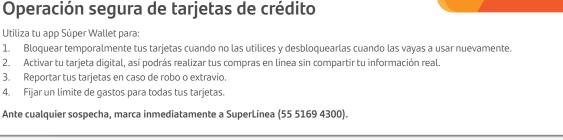
(SuperToken) o claves recibidas por mensajes de texto.

Llamadas telefónicas fraudulentas

Si tienes sospechas de la llamada, es posible que sea un fraude. Sigue estos pasos: No respondas a preguntas sospechosas o información sensible. Si te piden información sensible, cuelga inmediatamente.

Consulta el movimiento de tus cuentas desde SuperMóvil, SuperNet o SuperLínea. Ante cualquier sospecha, cuelga y marca inmediatamente a SuperLínea (55 5169 4300).

en el identificador de llamadas y estar atento ante solicitudes o comportamientos inusuales.



Ante cualquier sospecha, marca inmediatamente a SuperLínea (55 5169 4300).

Reportar tus tarjetas en caso de robo o extravío. Fijar un límite de gastos para todas tus tarjetas.

Operación segura de tarjetas de crédito

- Más consejos de seguridad

Utiliza tu app Súper Wallet para:

móviles, dentro de lo cual pueden robar tu información financiera, para evitar esto:

No abras y descargues contenido de correo electrónico de destinatarios desconocidos.

 Usa un antivirus actualizado y activado para proteger tus equipos. No descargues software de sitios no seguros y no instales software pirata.

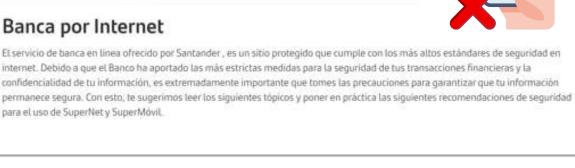
Manten tu sistema operativo y aplicaciones actualizadas

Malware

Ante cualquier sospecha llama a SuperLínea 55 5169 4300

Los delincuentes cibernéticos han desarrollado malware que les permite robar la información de tus equipos de cómputo y dispositivos

- Banca por Internet El servicio de banca en linea ofrecido por Santander, es un sitio protegido que cumple con los más altos estándares de seguridad en

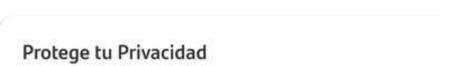


Compras por Internet

para el uso de SuperNet y SuperMóvil.

Protege tu identidad (clave de usuario), ya que son únicos y sin ellos, no se puede tener acceso a tu cuenta. Así como nunca se firmaria

1.-Verifica la autenticidad, reputación y puntaje de la pagina o vendedor al que pretendes realizar la compra, si tienes duda mejor evita la



Es importante que al realizar una compra por internet tomes en cuenta los siguientes pasos

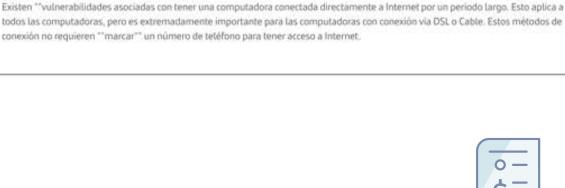
 La dirección electrónica sea la correcta y no tenga ninguna letra, símbolo, espacio o falta de ortografía 3.-La dirección electrónica siembre debe empezar con HTTPS; este es un certificado de seguridad



Protege tu Computadora

Siempre que uses tu computadora personal e Internet, existe un potencial de riesgo de contagiarse de un virus informático o la

posibilidad de infiltración de un software de intrusión, comúnmente conocido como ""Caballo de Troya" o Spyware.



Phishing Phishing: Como evitar ser pescado Hoy en día existen muchas practicas que tienen como finalidad engañar a los usuarios de Internet poniendo en riesgo su privacidad. Una

Spyware y software no deseado

telefonia IP, los defraudadores buscan obtener información financiera.

conexión no requieren ""marcar" un número de teléfono para tener acceso a Internet.

de estas prácticas es el phíshing, un tipo de spam que consiste en el envio masivo de mails cuyo objetivo es obtener información confidencial (número de cuentas, códigos de cliente, claves personales, entre otras) para después realizar actos ilícitos y/o fraudes.



de la computadora.

Vishing

El Vishing" es la nueva modalidad de fraude por Internet, su nombre proviene de sus siglas en ingles (Voice over Internet Protocol), es una nueva modalidad de Phishing; en los últimos meses han aparecido casos en Australia y Estados Unidos, donde por medio de la



SPAM

Pharming

conducir al usuario a una página web falsa.

Protege tu información

actualizado o tenga un anti-spyware.

Consejos para salvaguardar su información al utilizar Supernet

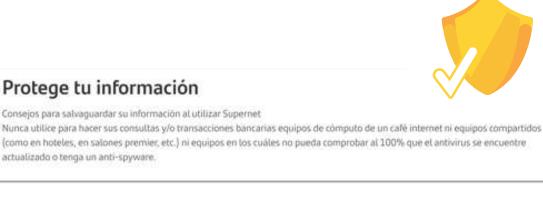
eliminación de información y en ocasiones fraudes millonarios.

Recomendaciones generales

Es muy importante cuidar tu información personal toma en cuenta las siguientes recomendaciones:

Es importante verificar los Billetes al recibirlos verificando los siguientes puntos:

Por SPAM se entiende todo mensaje de correo electrónico de carácter cornercial que invita o sugiere masivamente la compra de un bien o servicio, licito o llícito, generalmente siendo este un engaño para el usuario del correo electrónico. Por su naturaleza masiva y con la presencia de tantos SPAMMERS resulta sumamente molesto para los usuarios, pues satura sus buzones y dificulta la lectura del correo



Domicilio etc.)

Billetes

por ningún motivo los proporciones

Hackers

5.-Nunca abras correos electrónicos o des Clic en Links desconocidos o de dudosa procedencias 6.-Si recibes un mensaje SMS donde te indican que tu cuenta ha sido bloqueada por seguridad, comunicate al teléfono de atención a clientes, que se encuentra al reverso de la tarjeta y verifica esta información 7.- Si se presentan personas en tu domicilio y se identifican de Banco Santander, No entregues ningún tipo de documento ni tus tarjetas.

1- No entregues información personal por ningún medio a desconocidos (copias de INE/IFE, estados de Cuenta, Comprobantes de

3.-Revisa continuamente tu situación en el Buró de crédito si identificas alguna irregularidad, repórtala de inmediato

1. Textura. Revisa por medio del tacto, el papel, el grosor y los relieves de la tinta que tienen los billetes originales

5.-Más información en http://www.banxico.org.mx/billetes-y-monedas/disenos-actuales-circutacion-.html

4.- Elementos que cambian de color, se encuentran en todos los billetes y se observan contra luz y al mover los billetes

2.-Observa, los billetes dependiendo de la denominación que sean, como: hilo mícro impreso, ventana transparente e hilo de seguridad 3.-Marcas de Agua, estas se pueden observar a simple vista al mover los billetes de forma uniforme, y se encuentran en ambos lados de

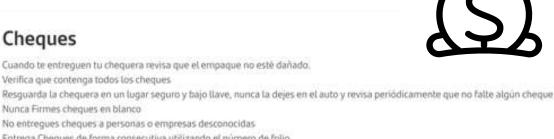
Al tlenar un cheque recarga de manera fuerte la mano, usando un boligrafo de tinta Azul o Negra, no dejes espacios en blanco al inicio

De preferencia expide tus cheques con la leyenda "No Negociable" y por ningún motivo cambies el cheque con un desconocido, dentro o

2- Si recibes una llamada y te solicitan los datos de tus tarjetas, Contraseñas de banca electrónica, cuentas bancarias o datos personales

4. - Todos los documentos que ya no serán utilizados y que poseen información privada, es necesario destruirlos antes de desecharlos.

Los hackers (Piratas informáticos) son aquellas personas que utilizan técnicas para penetrar en forma no autorizada a una computadora o sistema de computo. Los fines pueden ser varios, van desde probar la seguridad de los sistemas hasta el robo, sustitución, dañino o



Cheques Cuando te entreguen tu chequera revisa que el empaque no esté dañado. Verifica que contenga todos los cheques Nunca Firmes cheques en blanco

fuera de sucursal

No entregues cheques a personas o empresas desconocidas Entrega Cheques de forma consecutiva utilizando el número de folio

Si cancelas algún cheque se debe solicita la baja del documento en la sucursal.

del texto capturado en todos los campos.

Tarjeta de Crédito

cualquier otro medio.

estos son los tips que te recomendamos:

4.-Utiliza la Aplicación para activar o desactivar tu tarjeta 5 - En caso de Robo o extravio debes notificarlo de inmediato.

1.-Nunca descuides el resguardo de tu tarjeta, mantenta siempre en un lugar seguro 2.-Nunca compartas tu NIP, ya que este podría ser utilizado sin tu autorización

5.-En caso de que un cajero retenga la tarjeta debes reportarlo inmediatamente.

En caso de Robo o Extravío de la chequera o algún cheque, repórtalo de inmediato a tu sucursal

Las tarjetas de crédito posen sistemas de seguridad sin embargo es necesario tomas algunas medidas extras para prevenir un fraude, 3.-Al realizar compras, es importante que no pierdas de vista tu tarjeta y no permitas que capturen los datos en una cámara, pápel o

1.No concentres todo tu dinero en la cuenta de cheques, si es posible transfiere el exceso a una cuenta de inversión. 2. Nunca descuides el resguardo de tu tarjeta, mantenla siempre en un lugar seguro y asegúrate de firmarla. 3. Elije un NIP sin números consecutivos o repetidos y que sea fácil de recordar.

Tarjeta de Débito

Las tarjetas de débito posen sistemas de seguridad sin embargo es necesario tomas algunas medidas extras para



Cajeros Automáticos

Nunca aceptes ayuda de desconocidos

4. Nunca compartas tu NIP, ya que este podría ser utilizado sin tu autorización. 5. Al realizar compras, es importante que no pierdas de vista tu tarjeta y no permitas que capturen los datos en una cámara, papel o cualquier otro medic 6. Utiliza la Aplicación para activar o desactivar tu tarjeta. 7. En caso de Robo o extravío debes notificarlo de inmediato.

prevenir un fraude, estos son los tips que te recomendamos:

8.En caso de que un cajero retenga la tarjeta debes reportarlo inmediatamente.

Al acudir al cajero automático es importante que prestes atención a los siguientes puntos:

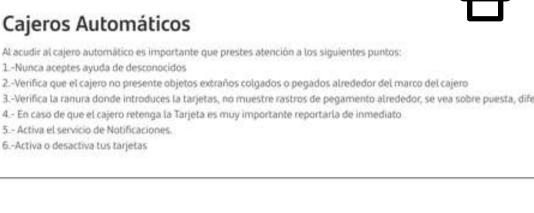
3.-Verifica la ranura donde introduces la tarjetas, no muestre rastros de pegamento alrededor, se vea sobre puesta, diferente color 4.- En caso de que el cajero retenga la Tarjeta es muy importante reportarla de inmediato 5.- Activa el servicio de Notificaciones. 6.-Activa o desactiva tus tarjetas

Sucursales Cuando acudas a una sucursal es importante tomes en cuenta los siguientes tips

 Todos los depósitos se deben realizar directamente en ventanilla. En caso de ser contactado por una fuente sospechosa

(vía telefónica, SMS o e-mail), marca inmediatamente a SuperLínea (55 5169 4300) y verifica el estado de tus

cuentas Santander.



1 - Ninguno de nuestros funcionarios está autorizado para realizar una operación de cambio de cheque en la fila, en los escritorios o fuera de la sucursal, por tu seguridad es mejor que personalmente cambies el cheque directamente en la ventanilla de la sucursal 2 - Al realizar cualquier operación es importante que te entreguen el recibo que respalde dicha operación, este será necesario para