Tips Antifraude

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).

Llamadas telefónicas fraudulentas

Los estafadores pueden suplantar la identidad de los números telefónicos del banco, por lo cual te recomendamos no confiar plenamente en el identificador de llamadas y estar atento ante solicitudes o comportamientos inusuales.
Recuerda que al contactarte por teléfono **nunca vamos a solicitar información sensible** como contraseñas, NIP, claves del NIP Dinámico (SuperToken) o claves recibidas por mensajes de texto.
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).

Operación segura de tarjetas de crédito

Utiliza tu app Súper Wallet para:

1. Bloquear temporalmente tus tarjetas cuando no las utilices y desbloquearlas cuando las vayas a usar nuevamente.
2. Activar tu tarjeta digital, así podrás realizar tus compras en línea sin compartir tu información real.
3. Reportar tus tarjetas en caso de robo o extravío.
4. Fijar un límite de gastos para todas tus tarjetas.

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

Más consejos de seguridad

Malware

Los delincuentes cibernéticos han desarrollado malware que les permite robar la información de tus equipos de cómputo y dispositivos móviles, dentro de lo cual pueden robar tu información financiera, para evitar esto:

- Usa un antivirus actualizado y activado para proteger tus equipos.
- No descargues software de sitios no seguros y no instales software pirata.
- Mantén tu sistema operativo y aplicaciones actualizadas.
- No abras y descargues contenido de correo electrónico de destinatarios desconocidos.

Ante cualquier sospecha llama a SuperLínea 55 5169 4300

Banca por Internet

El servicio de banca en línea ofrecido por Santander , es un sitio protegido que cumple con los más altos estándares de seguridad en internet. Debido a que el Banco ha aportado las más estrictas medidas para la seguridad de tus transacciones financieras y la confidencialidad de tu información, es extremadamente importante que tomes las precauciones para garantizar que tu información permanece segura. Con esto, te sugerimos leer los siguientes tópicos y poner en práctica las siguientes recomendaciones de seguridad para el uso de SuperNet y SuperMóvil.

Compras por Internet

Es importante que al realizar una compra por internet tomes en cuenta los siguientes pasos
1.-Verifica la autenticidad, reputación y puntaje de la pagina o vendedor al que pretendes realizar la compra, si tienes duda mejor evita la compra.
2.- 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 Privacidad

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 firmaría un cheque en blanco a un extraño, nunca divulgues tu usuario y contraseña, a fin de no correr el riesgo de que otras personas tengan acceso a tu cuenta de Supernet. Si sospechas que alguien conoce tu contraseñas, cámbiala inmediatamente.

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.

Protege tu conexión a internet

Existen ""vulnerabilidades asociadas con tener una computadora conectada directamente a Internet por un periodo largo. Esto aplica a todos las computadoras, pero es extremadamente importante para las computadoras con conexión vía DSL o Cable. Estos métodos de conexión no requieren ""marcar"" un número de teléfono para tener acceso a Internet.

Phishing

Phishing: Cómo 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 de estas prácticas es el phishing, un tipo de spam que consiste en el envío 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.

Spyware y software no deseado

Spyware es el término con el que se le conoce al tipo de software que invade los equipos de los usuarios de Internet y cuya característica principal es la de poner en ejecución ciertos programas sin previa autorización del usuario; por lo que se corre el riesgo de intercambiar y/o compartir información con usuarios desconocidos, estar en contacto con publicidad no deseada o sufrir cambios en la configuración 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 telefonía IP, los defraudadores buscan obtener información financiera.

Pharming

Pharming
El Pharming es una modalidad de fraude electrónico que consiste en manipular las direcciones DNS (Domain Name Server) para conducir al usuario a una página web falsa.

SPAM

SPAM
Por SPAM se entiende todo mensaje de correo electrónico de carácter comercial que invita o sugiere masivamente la compra de un bien o servicio, lícito o ilícito, 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 electrónico.

Protege tu información

Consejos para salvaguardar su información al utilizar Supernet
Nunca utilice para hacer sus consultas y/o transacciones bancarias equipos de cómputo de un café internet ni equipos compartidos (como en hoteles, en salones premier, etc.) ni equipos en los cuáles no pueda comprobar al 100% que el antivirus se encuentre actualizado o tenga un anti-spyware.

Hackers

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 eliminación de información y en ocasiones fraudes millonarios.

Recomendaciones generales

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

1- No entregues información personal por ningún medio a desconocidos (copias de INE/IFE, estados de Cuenta, Comprobantes de Domicilio etc.)
2- Si recibes una llamada y te solicitan los datos de tus tarjetas, Contraseñas de banca electrónica, cuentas bancarias o datos personales por ningún motivo los proporciones
3.-Revisa continuamente tu situación en el Buró de crédito si identificas alguna irregularidad, repórtala de inmediato
4.- Todos los documentos que ya no serán utilizados y que poseen información privada, es necesario destruirlos antes de desecharlos.
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, comunícate 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.

Billetes

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

1.-Textura. Revisa por medio del tacto, el papel, el grosor y los relieves de la tinta que tienen los billetes originales
2.-Observa, los billetes dependiendo de la denominación que sean, como: hilo micro 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 los billetes.
4.- Elementos que cambian de color, se encuentran en todos los billetes y se observan contra luz y al mover los billetes
5.-Más información en http://www.banxico.org.mx/billetes-y-monedas/disenos-actuales-circulacion-.html

Cheques

Cuando te entreguen tu chequera revisa que el empaque no esté dañado.
Verifica que contenga todos los cheques
Resguarda la chequera en un lugar seguro y bajo llave, nunca la dejes en el auto y revisa periódicamente que no falte algún cheque
Nunca Firmes cheques en blanco
No entregues cheques a personas o empresas desconocidas
Entrega Cheques de forma consecutiva utilizando el número de folio
Al llenar un cheque recarga de manera fuerte la mano, usando un bolígrafo de tinta Azul o Negra, no dejes espacios en blanco al inicio del texto capturado en todos los campos.
Si cancelas algún cheque se debe solicita la baja del documento en la sucursal.
En caso de Robo o Extravío de la chequera o algún cheque, repórtalo de inmediato a tu sucursal
De preferencia expide tus cheques con la leyenda "No Negociable" y por ningún motivo cambies el cheque con un desconocido, dentro o fuera de sucursal

Tarjeta de Crédito

Las tarjetas de crédito posen sistemas de seguridad sin embargo es necesario tomas algunas medidas extras para prevenir un fraude, estos son los tips que te recomendamos:
1.-Nunca descuides el resguardo de tu tarjeta, mantenla siempre en un lugar seguro
2.-Nunca compartas tu NIP, ya que este podría ser utilizado sin tu autorización
3.-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 medio.
4.-Utiliza la Aplicación para activar o desactivar tu tarjeta
5.- En caso de Robo o extravío debes notificarlo de inmediato.
6.-En caso de que un cajero retenga la tarjeta debes reportarlo inmediatamente.

Tarjeta de Débito

Las tarjetas de débito posen sistemas de seguridad sin embargo es necesario tomas algunas medidas extras para prevenir un fraude, estos son los tips que te recomendamos:

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.
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 medio.
6. Utiliza la Aplicación para activar o desactivar tu tarjeta.
7. En caso de Robo o extravío debes notificarlo de inmediato.
8.En caso de que un cajero retenga la tarjeta debes reportarlo inmediatamente.

Cajeros Automáticos

Al acudir al cajero automático es importante que prestes atención a los siguientes puntos:
1.-Nunca aceptes ayuda de desconocidos
2.-Verifica que el cajero no presente objetos extraños colgados o pegados alrededor del marco del cajero
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
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 cualquier aclaración.
3.-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.