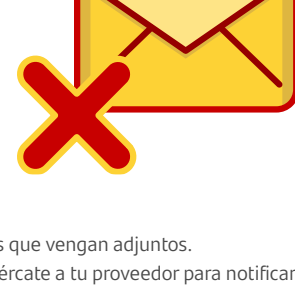


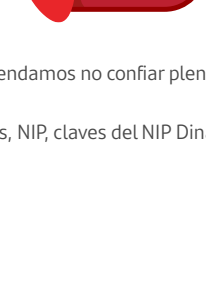
Tips Antifraude



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:

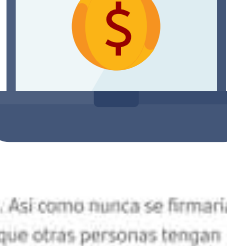
- Usa un antivirus actualizado y activado para proteger tus equipos.
- No descargues software de sitios no seguros y no instales software pirata.
- Mantén tu sistema operativo y aplicaciones actualizadas.
- No abras y descargues contenido de correo electrónico de destinatarios desconocidos.

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 permanezca 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.



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 contraseña, 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

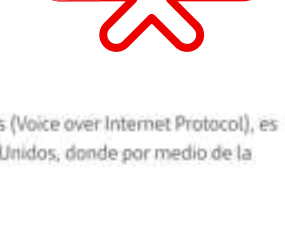
Existen "vulnerabilidades asociadas con tener una computadora conectada directamente a Internet por un periodo largo. Esto aplica a todos las computadoras, pero es extremadamente importante para las computadoras con conexión vía DSL o Cable. Estos métodos de conexión no requieren "marcar" un número de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



Phishing

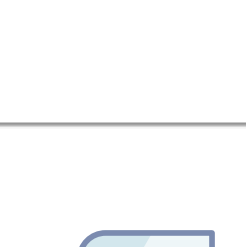
Phishing: Cómo evitar ser pescado

Hoy en día existen muchas prácticas 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.



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

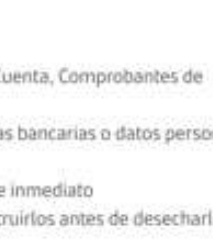
Por SPAM se entiende todo mensaje de correo electrónico de carácter comercial que invita o sugiere masivamente la compra de un bien o servicio, lícito o ilícito, generalmente siendo este un engaño para el usuario del correo electrónico. Por su naturaleza masiva y con la presencia de tantos SPAMMERS resulta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



Protege tu información

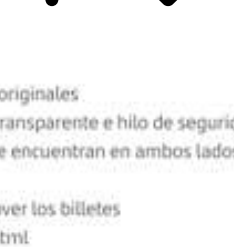
Consejos para salvaguardar su información al utilizar SuperNet

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 cuales 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 cómputo. Los fines pueden ser varios, van desde probar la seguridad de los sistemas hasta el robo, sustitución, dainio 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 las 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, comunícale 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.



Pharming

Pharming

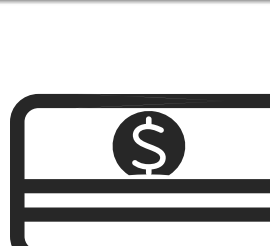
El Pharming es una modalidad de fraude electrónico que consiste en manipular las direcciones DNS (Domain Name Server) para conducir al usuario a una página web falsa.



Pharming

Pharming

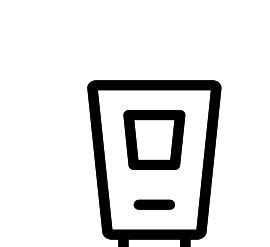
El Pharming es una modalidad de fraude electrónico que consiste en manipular las direcciones DNS (Domain Name Server) para conducir al usuario a una página web falsa.



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.



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.



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.



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.