Ministerio de Producción,
Ciencia y Tecnología

Santa Fe
Provincia

Guía práctica para la prevención de

Fraudes Bancarios por Medios Electrónicos y Digitales

Secretaría de Comercio Interior y Servicios -
Dirección Provincial de Promoción de la Competencia y Defensa del Consumidor

Santa Fe
Provincia

Pautas de Prevención y Cuidado en entornos digitales para transacciones bancarias y financieras

Existen ciertas pautas de cuidado que debemos tener en cuenta al manejarnos en el cyberespacio, con medios electrónicos, en todo lo referente a transacciones bancarias, al manejo de cuentas bancarias o de datos sensibles.

Esto es importante porque las herramientas que los bancos ponen a nuestra disposición para facilitar la operatoria pueden usarse por terceros para generarnos grandes daños.

- Acceder a cuentas bancarias, homebanking y aplicaciones de carácter personal o que contengan o requieran contraseñas o datos privados, como nombre, apellido, DNI, fecha de nacimiento o clave de la seguridad social, entre otras, desde redes seguras. Evitar hacerlo desde redes públicas de Wifi o redes de cortesía.
- Verificar los datos de autenticidad de las páginas por las que se navega. Chequear que la página sea segura, comenzando la dirección con https:// o posean el logo del candado de seguridad. Sobre todo verificar estas condiciones de seguridad antes de ingresar datos o claves en páginas de internet.
- No acceder a páginas ni aplicaciones a través de links o enlaces recibidos por correo electrónico, por whatsapp o publicados en redes sociales.
- Realizar las transacciones o cualquier operación de comercio electrónico en páginas confiables y operar con personas de identidad conocida o posible de identificar. Evitar la compra a desconocidos que ofrecen productos a precios extremadamente bajos a través de redes sociales mediante la transferencia directa o el depósito en una cuenta bancaria, sin pasar por una página web o medios de pago provistos por plataformas on line. Si se ofrecen los bienes en redes sociales, intentar chequear el producto y la identidad del vendedor antes de realizar cualquier pago.
- En general, se aconseja no realizar compras en redes sociales o sitios web que no garanticen la identidad de las personas que ofrecen los bienes y servicios. En caso de realizar estas contrataciones, se aconseja verificar que una persona con CUIT (Clave única de identificación tributaria otorgada por AFIP) aparezca claramente como el vendedor, que su domicilio exista en la realidad (se puede verificar en Google Maps, viendo el frente del local comercial a través de Google Street View), y evitar hacer transferencias por banco o billetera virtual. El medio de pago más aconsejable sería la tarjeta de crédito, que permite desconocer el consumo en caso de tratarse de un fraude.
- Mantener los equipos y dispositivos informáticos actualizados. Eliminar todas las aplicaciones que no se utilicen y mantener actualizados los sistemas operativos.
- Usar claves diferentes para las distintas aplicaciones o sitios. Lo mejor es que sean alfanuméricas, combinando letras mayúsculas y minúsculas con números. De esta forma se dificulta el acceso a las mismas por parte de terceros no autorizados.
- Cerrar todas las sesiones y sistemas al terminar la operatoria o transacción. Si la sesión queda abierta, un tercero puede seguir operando sin autorización y generar graves daños patrimoniales.
- No brindar datos sensibles a terceros. No revelar claves, PIN, Token, número o imagen del DNI, ni a terceros, ni telefónicamente, ni por mail o whatsapp. No publicar esta información en redes sociales.
- Verificar cuidadosamente y con tiempo los correos electrónicos, mensajes de texto o whatsapp antes de brindar cualquier tipo de dato personal. Ni las entidades bancarias y financieras, ni el Estado, ni las empresas prestadoras de servicios domiciliarios se contactan

con los clientes para solicitar claves, números de cuenta completos u otros datos sensibles.Tomarse siempre unos minutos para reflexionar antes de actuar.

- Si se recibe un llamado, y la persona que se contacta dice pertenecer a una entidad bancaria, es importante no responder ni brindar datos. Nunca abrir aplicaciones ni recurrir a cajeros automáticos y realizar operaciones guiadas telefónicamente por desconocidos.
- Actuar con cautela frente a los avisos de “beneficios” o “premios”, sobre todo cuando no se los ha solicitado. Muchas veces la aceptación de estos premios requiere que se brinden datos sensibles que luego permiten la comisión de fraudes o delitos bancarios o informáticos.
- Ser cuidadosos al operar en cajeros automáticos, no aceptar ayuda de extraños y tratar de verificar que no haya elementos extraños: cintas, ganchos, etc.
- Al operar con Billetera Santa Fe, es recomendable tener presente el usuario y contraseña, a los fines de evitar los bloqueos de cuentas, prestar atención al momento de consignar los montos a abonar para evitar pagos excesivos o sin causa y aguardar que el sistema arroje el comprobante de pago para evitar la duplicación de los mismos.
- Intentar no dejar abierta la aplicación de Billetera Santa Fe en el celular, ni dejar grabada la clave de la aplicación, para evitar fraudes y hackeos, o que, en general, terceras personas no autorizadas operen con la cuenta.
- Con Billetera Santa Fe, vincular de modo permanente y automático una cuenta bancaria, como la caja de ahorros, por ejemplo, implica la posibilidad de acceso a esta cuenta desde la aplicación en todo momento. Por ello, si se elige esta modalidad para operar con la aplicación, es recomendable redoblar los cuidados relativos a la guarda de los dispositivos, así como también aquellos relativos a las claves y contraseñas, para que terceras personas no autorizadas no accedan a nuestra cuenta.

De haber sido víctimas de un ilícito

En caso de ser víctimas de alguna de estas acciones, si nos has sustraído dinero o nos han endeudado, hay que actuar lo más rápido posible.

- 0800 555 6768 (opción 3);
- Presencialmente, en Santa Fe en Bv. Pellegrini 3100. En Rosario en Mitre 930 – 3º Piso, o en la Oficina Municipal ó Comunal de Información al Consumidor (OMIC u OCIC) más cercana.
- On line: Ventanilla Única Federal de Defensa del Consumidor (VUF) https://www.argentina.gob.ar/produccion/defensadelconsumidor/formulario

- Hacer la **denuncia penal en el Centro Territorial de Denuncias más cercano a tu domicilio. https://www.santafe.gov.ar/index.php/web/content/view/full/198373/(subtema)/199106**

- Hacer la denuncia en el banco, la compañía financiera o la empresa. Es recomendable utilizar la carta documento como medio fehaciente de notificación, para que se abstenga de efectuar descuentos o retenciones relacionadas al hecho ilícito.