Si recibiste una llamada, mensaje de texto o correo que no te da buena espina, consulta esta guía:

Correo electrónico o mensaje de texto

Si el texto o correo que recibiste cumple uno o más de los siguientes puntos, probablemente es un intento de fraude:

- Revisa los correos anteriores de tu banco. Si la dirección de correo electrónico que hace el envío es distinta a la habitual, no lo abras.
- El texto te quiere transmitir una sensación de urgencia, como dar datos de inmediato para evitar problemas con tu cuenta.
- Incluye un link para que proporciones información confidencial como número de cuenta, tarjeta, token, etc.
- La redacción es mala o tiene faltas de ortografía.
- La imagen del correo no corresponde a la que usa tu banco.
- Contiene datos adjuntos.

Recuerda:

- ✔ No des clic en los links
- ✔ No abras los documentos adjuntos
- ✔ Solo llama al número que está al reverso de tu tarjeta
- ✔ Repórtalo a tu banco
- ✔ Bórralo

Tú eres la primera línea de defensa en la prevención de fraudes electrónicos.

Página Web

La banca en línea es muy fácil y práctica, pero hay personas que hacen páginas muy parecidas a las de los bancos para tomar el control de tus cuentas.

Estás en riesgo si:

- No tienes instalado un programa antivirus, antiespía, anti malware, o los que tienes no están actualizados.
- Ingresaste a la página a través de un buscador como Google, Yahoo!, Bing, etc.
- Ingresaste a la página a través de una liga en un correo electrónico sospechoso.
- Al intentar ingresar, además de usuario y contraseña, te solicita otros datos como e-llave (token), número de tarjeta de débito, código de seguridad, correo electrónico, nombre y número telefónico, etc.
- La página muestra texto con faltas de ortografía.
- Aparece una pantalla de instalación de algún software.
- El diseño de la página no corresponde con la imagen del banco.

Recuerda:

- ✔ Instala Trusteer Rapport
- ✔ Entra a tu banca en línea tecleando la dirección en tu navegador.
- ✔ Guarda la página en los Favoritos de tu computadora para volver a ella fácilmente.
- ✔ Desconfía de los portales que te pidan mucha información.
- ✔ Llama al número que está al reverso de tu tarjeta para certificar o reportar la página.

Tú eres la primera línea de defensa en la prevención de fraudes electrónicos.

Llamadas

Prevenir fraudes mediante llamada telefónica es muy fácil:

- Si te notifican cargos que no reconoces y para cancelarlos te piden información como usuario y contraseña.
- Si te piden confirmar datos confidenciales como códigos de seguridad.

Cuelga y llama al número que está al reverso de tu tarjeta.

Tú eres la primera línea de defensa en la prevención de fraudes electrónicos.

Scotiabank®