8 CONSEJOS PARA LA BANCA SEGURA EN LÍNEA

1 Controle Sus Cuentas Regularmente.

Asegúrese de que todas las transacciones publicadas sean las que haya autorizado. Reporte inmediatamente a su banco cualquier sospecha de actividad fraudulenta o sospechosa.

2 Esté Atento a Correos Electrónicos Extraños.

No responda a correos electrónicos que dicen ser de su banco (o de cualquier otra compañía) solicitando los detalles o contraseñas de su cuenta. **Los bancos no se comunicarán con usted por correo electrónico pidiendo los detalles de su cuenta.**

3 Evite Hacer Clic en Enlaces Dentro del Correo Electrónico

Por lo general, es mucho más seguro iniciar sesión en el sitio web de su banco manualmente para asegurarse de que está ingresando a un sitio seguro.

4 Cambie la Contraseñas de su Banco Regularmente

Evite usar la misma contraseña en varios sitios y asegúrese de elegir una contraseña segura que sea una combinación de mayúsculas y minúsculas, números y caracteres especiales. Evite utilizar palabras o frases que contengan su nombre, sus iniciales o su fecha de nacimiento.

5 Habilitar la Autentificación de dos Factores

Muchas instituciones financieras han agregado una capa de seguridad para los titulares de cuentas. La autenticación de dos factores requiere que ingrese una credencial de verificación adicional antes de poder acceder a su cuenta.

6 Deshabilitar el Inicio de Sesión Automático

No permita que su navegador web almacene información privada de nombre de usuario y contraseña para sus sitios web de banca en línea.

7 Cuando Disponible Solo Use las Aplicaciones Móviles Oficiales de su Banco

Y asegúrese de descargar aplicaciones de fuentes acreditadas como Apple Store o Google Play Store.

8 ¿No Está Seguro si Algo es Legítimo?

¿Tiene preguntas sobre la tecnología de su banco? Llámalos, ¡estarán encantados de ayudarle!

Presentado en colaboración por:

THE STATE OF TEXAS DEPARTMENT OF BANKING

TexasBankers Association

8 CONSEJOS PARA TENER MAS CIBERSEGURIDAD

1 Fraude de Correo Electrónico

Si algo parece ser muy bueno para ser verdad, es probable que sea fraude. No crea que personal de la lotería ni príncipes de países foráneos harán contacto con usted por correo electrónico.

2 Pagos Fraudulentos

Mantenerse siempre alerto contra cheques fraudulentos, cheques de caja, órdenes de pago y traspasos de fondos electrónicamente enviados y pidiendo que usted electrónicamente regrese una parte del dinero.

3 Ofertas No Solicitadas

Sea cauteloso de ofertas no solicitadas que requieran que "ACTÚE RÁPIDAMENTE".

4 Manténgase Actualizado

Asegure que su aparato esté actualizado con todas las últimas actualizaciones de seguridad de su sistema de operación – Windows, Apple IOS, teléfono móvil IOS (Apple, Android, etc).

5 Advertencias y Errores

No confíe en los sitios web con advertencia y errores de certificados.

6 Cuidado Con Los Archivos Adjuntos al Correo Electrónico

Nunca es una buena idea hacer clic en un archivo adjunto a un correo electrónico o software gratuito de fuentes desconocidas. Puede exponer su sistema al fraude o robo en línea.

7 Compartiendo en Línea

Fíjese cuánto comparte en línea. Cuanto más publique sobre usted en los sitios de redes sociales, más fácil le resultará a alguien usar esa información para acceder a sus cuentas, robar su identidad y más.

8 Estafas Financieras

Esté al tanto de las estafas financieras relacionadas con el desastre. Los estafadores aprovechan a las personas después de eventos catastróficos afirmando ser de organizaciones caritativas legítimas cuando, de hecho, intentan robar dinero o información personal valiosa.

Recursos adicionales sobre seguridad en línea:

Departamento de Banca de Texas – www.dob.texas.gov
Asociación de Banqueros de Texas – www.texasbankers.com/BankingSafely
Better Business Bureau – www.bbb.org/council/for-businesses/cybersecurity