Seguridad

En Third Coast Bank SSB nos comprometemos a proteger la información de los clientes, la cual incluye tanto los datos financieros como la identidad. Tomamos medidas de seguridad conforme a las regulaciones federales y reforzamos la seguridad para las actividades de banca en línea.

Amenazas

Ingeniería social/Phishing

¿Qué es la ingeniería social?

Se trata de una técnica empleada para obtener o intentar obtener información confidencial mediante el engaño.

La meta básica es acceder sin autorización a datos personales o sistemas, con el fin de cometer fraudes, acceder a redes, robar identidades o simplemente afectar el funcionamiento de sistemas informáticos.

Llame al banco al 713.446.7000 si cree haber sido víctima de esta técnica.

Phishing es todo intento de robar información financiera personal, como números de tarjetas de crédito, nombres de usuario y contraseñas de cuentas o números de seguro social, mediante falsos mensajes de correo electrónico, llamadas (vishing), mensajes de texto (smishing) y sitios web.

Cómo funciona el phishing

- Usted recibe un mensaje de correo electrónico, una llamada o un mensaje de texto que parece ser de un banco, una institución financiera u otra entidad conocida o prestigiosa.
- En el mensaje se le presenta un enlace y la instrucción de visitar urgentemente un sitio web que parece legítimo y auténtico, o se le da un número al cual llamar para confirmar o actualizar datos personales que la organización verdadera ya posee, como contraseñas, datos de tarjetas de crédito, números de seguro social y números de cuentas bancarias.
- En realidad, el sitio web es falso y solo se creó para robar datos de usuarios.

Cómo protegerse del phishing

- No responda estos mensajes ni visite los sitios web allí mencionados a pesar de que se le advierta que le van a cerrar la cuenta si no lo hace.
- Nunca responda con datos confidenciales, como contraseñas, números de cuentas o números de seguro social, a mensajes de correo electrónico, mensajes de texto o llamadas telefónicas.
- No revele a nadie datos personales/financieros ni contraseñas.
- No haga clic en enlaces de mensajes de correo electrónico. Vaya directamente al sitio principal de la empresa para iniciar sesión.
- Para comunicarse con la empresa mencionada en el mensaje de correo electrónico, busque por otros medios el número telefónico o el sitio web verdadero.
- Antes de enviar datos personales/financieros mediante un sitio web, busque el ícono del "candado" en la barra de estado del navegador, para asegurarse de que se protejan los datos al transmitirlos.
- Reporte todos los hechos sospechosos a la Comisión Federal de Comercio en www.ftc.gov.

Robos de cuentas corporativas

Se trata de un tipo de robo de identidad mediante el cual delincuentes toman control de la cuenta bancaria de una empresa tras robar contraseñas de empleados y demás credenciales válidas. Luego los delincuentes pueden efectuar transferencias y transacciones de ACH fraudulentas.

Llame de inmediato al banco al 713.446.7000 si cree que su cuenta de Third Coast Bank SSB corre peligro.

Malware

Se trata de software que se instala en su dispositivo para efectuar tareas que usted no desea. Estos programas pueden generar desde molestias menores (publicidades emergentes) hasta intromisiones y daños graves en la computadora.

Las siguientes son algunas categorías de malware:

- **Virus**: Software capaz de replicarse a sí mismo y pasar a otras computadoras, o programado para dañar la computadora eliminando archivos, reformateando el disco duro o utilizando toda la memoria.
- **Adware**: Software que presenta publicidades emergentes o redirige el navegador a sitios determinados cuando usted se conecta a Internet.
- **Spyware**: Software que recopila información y la transmite a las partes interesadas. La información puede incluir los sitios web visitados, los datos del navegador/sistema y la dirección IP de la computadora.
- **Ransomware**: Software que restringe de algún modo el acceso al sistema informático infectado y exige al usuario que pague un rescate al delincuente.
- **Software de secuestro de navegador**: Software publicitario que modifica la configuración del navegador, crea accesos directos en el escritorio y presenta publicidades emergentes intermitentes. Una vez secuestrado el navegador, el software también puede redirigir a sitios determinados publicitarios o sitios que recopilan datos de uso de Internet e inicios de sesión.

Registrador de teclas (Keylogger)

Programa que captura y transmite las teclas presionadas en el teclado. Se suele instalar mediante malware transmitido a través de un mensaje de correo electrónico de phishing u otro tipo de ataque, con el proposito de espiar lo que escribe el usuario, como nombres de usuario y contraseñas.

Protección

Firewall y protección contra malware

Un firewall es una barrera entre el Internet y su red/computadora, para controlar el acceso a los recursos de la red. En general se utiliza para definir qué tipo de tráfico se permite en la red, y todos los demás tipos se rechazan. Se recomienda enfáticamente utilizar un firewall. Con el firewall no es suficiente para garantizar la seguridad; se trata solo de la primera línea defensiva.

Un firewall brinda muy poca o ninguna protección contra lo siguiente:

- Si da permiso a otras computadoras para conectarse a la suya
- Si se desactiva o tiene muchas excepciones o puertos abiertos
- La mayoría de los virus
- El correo no deseado
- Las instalaciones de software espía
- Cualquier tipo de estafa o actividad delictiva en línea
- Si usted o un virus ha creado una puerta trasera para atravesar el firewall
- Si un hacker conoce la contraseña del firewall
- Gente con acceso físico a la computadora o a los sistemas de la red
- Tráfico malintencionado que no pasa por el firewall, como en una red inalámbrica mal configurada
- Ataques a redes con problemas de seguridad

- Tráfico que parece legítimo
- Phishing

El software antivirus y antimalware permite prevenir, detectar y eliminar infecciones con virus/malware en sistemas informáticos.

Seguridad para redes Wi-Fi

Conéctese únicamente a redes Wi-Fi que merezcan su absoluta confianza. Desactive la función de conexión automática en su teléfono. Nunca acceda a servicios en línea desde redes Wi-Fi públicas, como las de restaurantes, bares, bibliotecas públicas, etc.

Seguridad para compras en línea

Las compras en línea son muy populares, ya que permiten adquirir artículos sin lidiar con el tráfico y las multitudes. No obstante, el Internet tiene sus riesgos, por lo cual es importante tomar las medidas adecuadas para protegerse al comprar en línea.

Consejos para las contraseñas

Todos sabemos lo que cuesta recordar las contraseñas, pero debemos agradecer que nos obliguen a utilizarlas. Existen muchos hackers malintencionados, por lo cual tener una contraseña complicada es un paso sencillo para dificultarles acceder a nuestros datos personales.

Estos son algunos consejos para que sus contraseñas lo protejan bien:

- Cree contraseñas seguras de al menos 8 caracteres y que combinen minúsculas, mayúsculas, números y caracteres especiales.
- Si puede introducir mayúsculas y minúsculas, use letras de los dos tipos.
- No emplee contraseñas genéricas, como la palabra "contraseña", 123456789, o cualquier parte de su nombre, domicilio, cumpleaños o número telefónico.
- Utilice una contraseña diferente para cada sitio web.
- Cambie las contraseñas al menos varias veces por año.
- Nunca comparta su nombre de usuario y contraseña con nadie.
- Nunca le diga su contraseña a nadie (ni siquiera al banco).
- No anote sus contraseñas en lugares donde se puedan ver fácilmente.

Prácticas recomendadas para proteger sus datos personales

- Sospeche de los mensajes de correo electrónico que digan ser de bancos, instituciones financieras o agencias gubernamentales y soliciten datos de cuentas o credenciales de acceso a la banca, como nombres de usuario, contraseñas, códigos de NIP e información similar. Al abrir adjuntos o hacer clic en enlaces de mensajes sospechosos, podría exponerse a código malintencionado que tome el control de su computadora o le robe sus credenciales. Third Coast Bank SSB nunca se comunicará con usted para solicitarle sus contraseñas.
- Instale un firewall exclusivo.
- Instale protección contra virus/malware en todos los sistemas informáticos y recuerde actualizarla con regularidad.
- Instale con regularidad las actualizaciones para computadoras y servidores.
- Considere la posibilidad de emplear programas de detección de software espía.
- Verifique en el navegador que se establezca una sesión segura (https, no http) en todos los sitios de banca en línea.
- No utilice en la banca en línea opciones de inicio de sesión automático que guarden nombres de usuario y contraseñas.
- Mientras utilice un servicio de banca en línea, nunca deje la computadora sola.

- Para las empresas que efectúan transacciones en línea, se recomienda realizar las actividades de banca en línea desde una computadora aislada, de seguridad reforzada y protección absoluta en la cual no se pueda utilizar correo electrónico ni navegar por Internet.
- Cree copias de seguridad de sus datos con frecuencia.
- La mejor manera de protegerse es nunca dar datos personales por Internet.
- Recuerde que **Third Coast Bank SSB** NUNCA le pedirá el NIP de su tarjeta de débito ni las contraseñas de sus cuentas en línea.
- Trate su dispositivo móvil con el mismo cuidado que su tarjeta de crédito. Si lo pierde o se lo roban y no lo tenía bien protegido, puede correr peligro.
- Proteja con una contraseña su dispositivo móvil.

Para obtener más información sobre las prácticas recomendadas para reforzar la seguridad de su experiencia y sus actividades en la banca en línea, consulte la información de la FDIC cuya página se presenta a continuación (tenga en cuenta que se han eliminado los enlaces, por lo cual deberá copiar y pegar la dirección en otra ventana de navegador para acceder a la página):

https://www.fdic.gov/consumers/consumer/news/cnwin18/

https://www.thatsmybank.com/images/blog-images/CyberBusiness.pdf