Guía de Prevención de Fraude Comercial

Una guía simple y sencilla para ayudarlo a mantener su negocio protegido.

business banking for good

1STBANK

Miembro FDIC

Tipos de Fraude

Reconocer los diferentes tipos de fraude puede ayudarlo a prepararse para evitar que sucedan.

Fraude con Cheques

El fraude con cheques es un problema grave y común. Asegúrese de verificar si el cheque tiene modificaciones en el nombre del beneficiario o el monto y si hay señales de que el cheque ha sido "alterado". Una práctica recomendada para proteger la información de su cuenta es que, al enviar cheques por correo, siempre use un punto de entrega seguro, como el buzón de USPS. Se recomienda realizar una revisión diaria de los cheques de la cuenta para asegurarse que no hayan alterados.

Apropiación de Cuenta

La apropiación de cuentas corporativas es un tipo de fraude en el que un tercero no autorizado obtiene acceso a las finanzas de una empresa. Esto puede incluir la apropiación de un perfil de servicios de banca en línea o el acceso a los sistemas de nómina. Muchas veces, los fondos que se envían son irrecuperables. Una práctica recomendada es asegurar que la información de su antivirus esté actualizada en su computadora. También, asegúrese de contar con la función de doble aprobación para que más de una persona verifique las transacciones.[1]

Fraude Impostor

Los estafadores pueden crear o manipular información de contacto y actuar como personas que usted conoce y en las que confía para parecer legítimos. Esto le permite al estafador solicitar pagos o cambiar las instrucciones de pago, como la información de la nómina o las facturas y puede incluir cambios en el tipo de pago, por ejemplo, el cambio de un pago a través de la Cámara de Compensación Automatizada (Automated Clearing House, ACH) a una transferencia bancaria. Esto se puede lograr a través de ataques al correo electrónico, llamadas telefónicas o mensajes de texto. Una práctica recomendada es nunca aceptar instrucciones de pago en formato de correo electrónico sin una verificación verbal. La mejor medida de seguridad al aceptar instrucciones de pago es solicitar que los pagos se realicen en persona siempre que sea posible. Si debe recibir un pago por correo electrónico, nunca acepte las instrucciones de pago sin haber realizado una verificación verbal.

[1] "Protect Your Small Biz Account." (Proteja la Cuenta de su Pequeña Empresa). ABA. Consultado el 5 de Junio del 2020. https://www.aba.com/advocacy/community-programs/consumer-resources/protect-your-money/protecting-small-biz-accounts

Ataque de Correo Electrónico Comercial (Business Email Compromise, BEC)

Un ataque de correo electrónico comercial es un delito en línea sofisticado en el que los delincuentes obtienen acceso a las redes de la empresa mediante de malware o falsificando una cuenta de correo electrónico o sitio web. El impostor luego enviará mensajes de correo electrónico que parezcan provenir de una fuente conocida y que realiza una solicitud legítima, a menudo en relación con facturación, facturas, títulos y bienes raíces. La información que se obtiene se utiliza para enviar una solicitud a través de una dirección de correo electrónico que puede tener ligeras variaciones de la dirección de correo electrónico legítima. El correo electrónico comprometido luego se utiliza para enviar una notificación para actualizar la información de pago. Una vez procesado el pago, los fondos se envían al estafador.

Para protegerse contra los BEC, asegúrese de verificar las solicitudes de pago y compra en persona, si es posible, o llamando a la persona para verificar la información a un número de teléfono conocido, que no esté incluido en la correspondencia por correo electrónico. Los impostores esperan ser más astutos que usted cuando recibe las instrucciones de pago por correo electrónico; están previendo a que usted no verifique de forma verbal las instrucciones de pago actualizadas. No haga clic en ningún enlace de un correo electrónico o mensaje de texto no solicitado. Asegúrese de examinar cuidadosamente la dirección de correo electrónico, URL y ortografía utilizada en la correspondencia. Tenga cuidado con lo que descarga y con cualquier archivo adjunto de correo electrónico que se le reenvíe. Si el solicitante lo presiona para que actúe con rapidez, tómese su tiempo y vuelva a verificar la situación y la información.

74% de las organizaciones fueron objeto de estafas de pago.[2]

62% de las empresas informaron que BEC es la principal fuente de intentos de fraude.[2]

66% de las organizaciones experimentaron fraude de cheques.[2]

[2] "Encuesta de Control y Fraude de Pagos AFP (Association for Financial Professionals) 2021." Último acceso: 21 de septiembre de 2021. https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud

Prevención del Fraude

Hay muchas acciones que puede tomar para disminuir la probabilidad de fraude. Puede empezar por aquí.

Herramientas de FirstBank

Alertas
Configurar alertas a través de los servicios en línea le permitirá realizar un mejor seguimiento de la actividad de su cuenta.

Servicio Positive Pay
El Servicio Positive Pay ofrece una rápida detección de cheques fraudulentos que se presentan en las cuentas, permitiéndole devolverlos antes del pago final.*

Controles Operacionales

Autoevaluación
Realice revisiones mensuales, trimestrales, semestrales y anuales sobre los usuarios internos y la actividad de sus cuentas. Eduque a los empleados sobre las mejores prácticas para la prevención de fraude.

Controles Internos
Cree procesos para asegurar que todos los pedidos sean válidos y estén verificados. Si necesita ayuda para crear soluciones personalizadas sobre el Manejo de Efectivo por Internet, nuestros Especialistas en Administración de Tesorería están disponibles para asistirlo.

Seguridad de Dispositivos
Preste atención y compruebe siempre que los dispositivos que utiliza para el banco son seguros y se actualizan con regularidad.

*Tenga en cuenta que Positive Pay solo está disponible para los clientes que utilizan la gestión de Internet Cash Management.

Recursos de FirstBank

¡Estamos para ayudarlo! A continuación se presentan algunas de nuestras soluciones para ayudar a su empresa prevenir el fraude.

Departamento de Administración de Tesorería

Disponible de lunes a viernes, de 7:30am a 5:30pm. Se puede comunicar con el Departamento de Administración de Tesorería al 303.235.1378 o al 855.426.1500, opción 5.

Departmento de 24 Horas

Fuera del horario comercial regular, se puede comunicar con nuestro Departamento de 24 Horas al 303.237.5000 o 1.866.239.6000.

Foro de Seguridad Anual

FirstBank realiza un foro de seguridad cada año para hablar de las tendencias y prevención del fraude. Comuníquese con nosotros al 855.426.1500, opción 5 para aprender más.

Contacto en la Sucursal

Si tiene preguntas adicionales, visite cualquiera de nuestras sucursales. Para encontrar la sucursal más cercana, visítenos en efirstbank.com/locations.

Gracias

business banking for good

Miembro FDIC