Las Estafas y Su Pequeño Negocio

Una Guía Para los Negocios

La Comisión Federal de Comercio | business.ftc.gov

Las estafas y su pequeño negocio

Si es dueño de un pequeño negocio o forma parte de una organización sin fines de lucro, usted invierte mucho tiempo y esfuerzo para asegurarse de que la organización funcione bien. Pero cuando los estafadores atacan su organización, eso puede perjudicar su reputación y resultar en pérdida de dinero. ¿Cuál es su mejor protección? Entérese de cuáles son los indicios de las estafas dirigidas contra los negocios. Y luego dígales a sus empleados y colegas a qué cosas le deben prestar atención para evitar las estafas.

Las tácticas de los estafadores

- **Los estafadores se hacen pasar por alguien en quien usted confía.** Adoptan un aspecto de credibilidad fingiendo estar conectados con una compañía que usted conoce o con una agencia del gobierno.
- **Los estafadores crean una sensación de urgencia.** Lo apuran para que tome una decisión rápida antes de que usted analice la situación.
- **Los estafadores usan tácticas de intimidación y miedo.** Le dicen que está por ocurrir algo terrible para que usted les envíe un pago antes de tener la oportunidad de verificarlo.
- **Los estafadores usan métodos de pago que no dejan rastros.** Con frecuencia quieren que se les pague por medio de transferencias de dinero, tarjetas recargables o tarjetas de regalo, lo cual implica transacciones casi imposibles de revertir o rastrear.

¿Cómo puedo proteger a mi negocio?

Capacite a sus empleados

- Su mejor defensa es contar con un personal bien informado. Explíqueles cómo ocurren las estafas y comparta este folleto con ellos. Encargue copias gratuitas en FTC.gov/Ordenar.
- Aliente a sus empleados a hablar con sus colegas de trabajo si detectan una estafa. Los estafadores a menudo tratan de engañar a varias personas en una misma organización. Un empleado que da la voz de alerta sobre una estafa puede ayudar a prevenir que engañen a otros empleados.
- Entrene a sus empleados a no enviar contraseñas ni información sensible por email, aunque el email parezca provenir de un jefe, y nunca le pida información sensitiva a sus empleados por email.

Verifique las facturas y los pagos

- Verifique todas las facturas. No pague a menos que sepa que la factura corresponde a artículos efectivamente pedidos y recibidos. Dígale a su personal que haga lo mismo.
- Asegúrese de que los procedimientos para aprobar facturas o gastos sean claros. Para reducir el riesgo de un error costoso, limite la cantidad de personas autorizadas a hacer órdenes de pedido y pagar facturas. Revise sus procedimientos para asegurarse de que los gastos importantes no se originen a partir de una llamada, factura o email inesperados.
- Preste atención a cómo le piden que pague. Dígale a su personal que haga lo mismo. Si le piden un

pago a través de una transferencia de dinero, tarjeta recargable o tarjeta de regalo, puede estar seguro que se trata de una estafa.

Domine la tecnología

- No crea en lo que indica el aparato de identificación de llamadas. Impostores falsean la información que aparece en el aparato de identificación de llamadas con la intención de que usted les crea cuando dicen que llaman de parte de una agencia del gobierno o de un proveedor en el que usted confía.

- A los estafadores les resulta fácil falsear domicilios de email y sitios web para que parezcan legítimos. Antes de hacer clic, pare y piense si podría ser una estafa. Los estafadores incluso pueden piratear las cuentas de redes sociales de la gente en la que usted confía y enviarle mensajes que parecen provenir de esas cuentas. No abra ningún archivo adjunto ni descargue archivos de emails inesperados; pueden tener virus que pueden dañar su computadora.

- Proteja los archivos, contraseñas e información financiera de su organización. Para más información sobre cómo proteger el sistema informático de su pequeño negocio u organización sin fines de lucro, consulte el artículo de la FTC Conceptos básicos sobre seguridad informática para pequeños negocios en FTC.gov/PequenosNegocios.

Sepa con quién está tratando

- Antes de hacer negocio con una nueva compañía, busque en internet el nombre de la compañía junto con términos como “scam” o “complaint”, si hace la búsqueda en español, use palabras como “estafa” o “queja”. Lea la opinión de los demás sobre esa compañía.

- Y con respecto a los productos y servicios para su negocio, pida recomendaciones a otros propietarios de negocios de su comunidad. La opinión positiva de gente que le merece confianza es más fiable que cualquier argumento de ventas.
- No pague por información “gratis”. Es posible que pueda conseguir asesoramiento y consejos sobre desarrollo de negocios realmente gratis a través de programas como **SCORE.org**.

Estafas comunes dirigidas contra pequeños negocios

Facturas falsas

Los estafadores crean facturas falsas que parecen ser por productos o servicios que usa su negocio – tal vez artículos de oficina o productos de limpieza, o registros de nombres de dominios. Los estafadores esperan que la persona que se ocupa de pagar sus facturas asuma que son para cosas que su compañía realmente encargó. Los estafadores saben que cuando la factura es por algo que es crucial para su negocio u organización, como mantener su sitio web en funcionamiento, es posible que usted pague primero y pregunte después. Excepto que es todo falso, y si usted paga, es posible que su dinero desaparezca.

Artículos de oficina y otros productos no pedidos

Alguien llama para confirmar una orden de pedido de artículos de oficina u otra mercadería, verificar un domicilio o para ofrecer un catálogo o muestra gratis. Si usted dice sí, entonces aparece la sorpresa – mercadería que nadie

encargó llega a su puerta seguida de exigencias de pago de alta presión. Si usted no paga, el estafador incluso podría llegar a reproducir una grabación de la llamada previa como una “prueba” de que se hizo el pedido. Tenga presente que si recibe mercadería que no pidió, usted tiene el derecho legal de quedársela sin pagar nada.

Estafas de anuncios y publicaciones en guías comerciales

Los estafadores oportunistas tratan de engañarlo para que pague por anuncios inexistentes o por la publicación del nombre de su negocio u organización en una guía que no existe. A menudo se hacen pasar por representantes de las Páginas Amarillas. Puede que le pidan información de contacto para un nuevo listado “gratis” o decirle que el propósito de la llamada es simplemente confirmar su información para una orden existente. Después, usted recibe una gran factura, y para presionarlo a pagar, el estafador puede usar detalles o incluso una grabación de la llamada previa.

Estafas de impostores de compañías de servicios públicos

Los estafadores fingen llamar de parte de una compañía de servicio de gas, electricidad o agua diciendo que están por cortar el servicio a su negocio. Quieren asustarlo haciéndole creer que debe pagar de inmediato una factura atrasada, a menudo por medio de una transferencia de dinero o una tarjeta recargable o tarjeta de regalo. Llamadas a una hora clave crean una sensación de gran urgencia, por ejemplo, a la hora pico de la cena en un restaurante.

Estafas de impostores que simulan trabajar para el gobierno

Hay estafadores que se hacen pasar por agentes del gobierno y amenazan con suspender las licencias comerciales, imponer multas o incluso tomar acciones legales si usted no paga los impuestos, renueva las licencias o registros expedidos por el gobierno o si no paga otros cargos. A algunos negocios los han presionado para que compren afiches de cumplimiento de normas del personal que se pueden obtener gratis en el Departamento de Trabajo de Estados Unidos. A otros negocios los han engañado para que paguen a cambio de subsidios para negocios que no existen de programas gubernamentales que tampoco existen. Hay negocios que han recibido cartas, que a menudo dicen ser de parte de la Oficina de Marcas y Patentes de EE. UU., advirtiéndoles que perderán sus marcas si no pagan un cargo inmediatamente o diciendo que adeudan dinero por servicios de registro adicionales.

Estafas de soporte técnico

Las estafas de soporte técnico comienzan con una llamada o mensaje pop-up alarmante de parte de una supuesta compañía reconocida que le indica que hay un problema con su seguridad informática. Su objetivo es obtener su dinero, acceder a su computadora, o ambas cosas. Podrían pedirle que les pague para reparar un problema que en realidad no existe o para inscribir a su negocio en un programa de mantenimiento de computadoras inexistente o inútil. Incluso podrían llegar a acceder a datos sensibles como contraseñas, registros de los clientes o información de tarjetas de crédito.

Ingeniería de redes sociales, phishing y programas de rescate

Los ciber-estafadores pueden engañar a los empleados para convencerlos de que suministren información confidencial o delicada, como contraseñas o datos de cuentas bancarias. Este tipo de estafas suele comenzar con un email de tipo phishing, un contacto en las redes sociales o por medio de una llamada que parece ser de una fuente confiable, como un supervisor u otro empleado, pero que crea una sensación de urgencia o temor. Los estafadores les dicen a los empleados que hagan una transferencia de dinero o que les permitan acceder a información delicada de la compañía. También se pueden recibir emails que parecen ser solicitudes de rutina para actualizar contraseñas u otros mensajes automatizados, pero en verdad esos emails tienen la intención de robarle su información. Los estafadores también pueden usar programas maliciosos para bloquear los archivos de las organizaciones y retenerlos a la espera del pago de un rescate.

Estafas de capacitación y promoción comercial

Algunos estafadores venden falsos servicios de capacitación para negocios y promoción en internet. Por medio de testimonios falsos, videos, presentaciones en seminarios y llamadas de telemercadeo, los estafadores hacen falsas promesas sobre resultados asombrosos e investigaciones de mercado exclusivas a la gente que esté dispuesta a pagar sus cargos. También es posible que lo tienten con costos bajos inicialmente, para luego pedirle miles de dólares. En realidad, estos estafadores dejan a los emprendedores sin la ayuda que estaban buscando y con miles de dólares en deudas.

Cambio de comentarios en internet

Hay algunos estafadores que dicen que pueden reemplazar comentarios negativos que hayan en internet sobre su producto o servicio, o mejorar su puntuación en los sitios web de calificación. Pero lo que usted debe saber es que publicar comentarios falsos es ilegal. Las directivas de la FTC indican que los endosos – incluidos los comentarios – deben reflejar las opiniones y experiencias honestas del endosante.

Estafas de servicios de procesamiento de tarjetas de crédito y alquiler del equipo

Los estafadores saben que los negocios están buscando maneras de reducir los costos. Algunos prometen falsamente reducir las tarifas por el procesamiento de las transacciones con tarjeta de crédito o mejores ofertas en el alquiler del equipo. Estos estafadores esconden detalles en la letra chica, carecen verdades a medias y puras mentiras para conseguir que el dueño de un negocio ponga su firma en un contrato. Algunos agentes de ventas inescrupulosos les piden a dueños de negocios que firmen documentos en blanco. No lo haga. Otros estafadores hasta han cambiado los términos después de la firma del contrato. Si un vendedor se niega a entregarle copias de todos los documentos en el momento – o trata de postergarlo con promesas de enviárselos más tarde – eso puede ser un signo de que está tratando con un estafador.

Estafas de cheques falsos

Las estafas de cheques falsos suceden cuando un estafador le paga de más con un cheque y le pide a usted que le gire el dinero extra a otra persona. Los estafadores siempre tienen una buena historia para explicar el

sobrepago – como que están fuera del país, necesitan que usted les cubra los impuestos o cargos, o le dicen que tendrá que comprar materiales o alguna otra cosa. Pero cuando el banco descubre que usted depositó un cheque falso y sin fondos, el estafador ya tiene el dinero que usted le envió y usted queda obligado a devolverle el dinero al banco. Esto incluso puede suceder después de que los fondos se acrediten a su cuenta y que el banco le haya dicho que el cheque estaba "aprobado".

Aprenda

- Para más recomendaciones sobre cómo proteger a su organización contra las estafas, visite **FTC.gov/SmallBusiness**.
- Manténgase conectado con la FTC suscribiéndose a los artículos del blog para negocios de la FTC en **FTC.gov/Subscribe** o suscríbase para recibir alertas de estafas en **FTC.gov/Estafas**.
- Encargue copias gratuitas en **FTC.gov/ordenar**.

Reporte

- Si detecta una estafa, repórtela en **FTC.gov/Queja**. Su reporte pueda ayudar a frenar la estafa.
- Alerte al Fiscal General de su estado. Puede encontrar la información de contacto en **NAAG.org**.

Comprométase

- Recuerde que su mejor defensa es contar con un personal bien informado.
- Hable con su personal sobre cómo ocurren las estafas.
- Comparta este folleto.

Acerca de la FTC

La FTC trabaja para ayudar a los dueños de pequeños negocios a evitar estafas, proteger sus computadoras y sistemas de red, y mantener la información de sus clientes segura. Para más información visite **FTC.gov/SmallBusiness**. En ese sitio web encontrará información sobre estafas que afectan a los pequeños negocios y cómo evitarlos, además de información sobre ciber-seguridad para ayudar a los dueños de pequeños negocios a mantener sus sistemas de red seguros.

This article is part of the FTC's efforts to help small business owners avoid scams. It explains common scams that target small businesses and non-profit organizations, describes scammers' tactics, and provides steps business owners can take to protect their company from scams. Order print copies for free at **FTC.gov/bulkorder**.

La Comisión Federal de Comercio
business.ftc.gov
May 2018