

Las estafas y su pequeño negocio

Una guía para los negocios



[ftc.gov/PequenosNegocios](https://www.ftc.gov/PequenosNegocios)



Las estafas y su pequeño negocio

Cuando los estafadores atacan a su negocio u 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 dígalas a sus empleados y colegas a qué cosas le deben prestar atención para evitar las estafas.

- ▶ **Las tácticas de los estafadores**
 - ▶ **Protega su negocio**
 - ▶ **Estafas comunes dirigidas contra pequeños negocios**
 - ▶ **Otras prácticas cuestionables**
-

► Las tácticas de los estafadores

- **Los estafadores se hacen pasar por alguien en quien usted confía.** Fingen estar conectados con una compañía o una agencia del gobierno que usted conoce para convencerle que les pague. Pero es una estafa.
- **Los estafadores crean una sensación de urgencia, intimidación y miedo.** Quieren que usted tome una decisión rápida antes de analizar la situación. No se deje presionar para hacer un pago o proveer información sensible acerca de su negocio.
- **Los estafadores le piden que pague usando métodos de pago específicos.** Con frecuencia, insisten que se les pague por medio de transferencias de dinero, con una criptomoneda o con tarjetas de regalo. No le pague a alguien que insista en un pago con uno de estos métodos. Es una estafa.

► Protega su negocio

Capacite a sus empleados

Su mejor defensa es contar con un personal bien informado. Entrene a sus empleados a no enviar contraseñas ni información sensible por email, aunque el email parezca provenir de un jefe. Explíqueles cómo ocurren las estafas y alíentelos a hablar con sus

colegas de trabajo si detectan una estafa. Encargue copias gratuitas de este folleto en ftc.gov/ordenar y compártalo con sus empleados.

Verifique las facturas y los pagos

Asegúrese de que los procedimientos para aprobar facturas o gastos sean claros y pídale a sus empleados que verifiquen todas las facturas. Preste atención a cómo le piden que pague y díglele a su personal que haga lo mismo. Si le piden un pago a través de una transferencia de dinero, con criptomoneda, o con una tarjeta de regalo, no pague. Es una estafa.

Reconozca las estafas relacionadas a la tecnología

Los impostores falsean sus números de teléfono, de modo que no debe creer la información que aparece en el aparato de identificación de llamadas. Si recibe un mensaje de texto o correo electrónico que no esperaba, no haga clic en un enlace, no abra ningún archivo adjunto ni descargue archivos. Es de esa manera que los estafadores instalan programas maliciosos en su red o tratan de convencerle a enviar dinero o compartir información sensible. Los estafadores incluso pueden piratear las cuentas de redes sociales de gente que usted conoce y enviarle mensajes que parecen ser reales pero que no lo son. Para más información sobre cómo proteger a su

pequeño negocio u organización sin fines de lucro contra los estafadores y los piratas informáticos, consulte **Ciberseguridad para pequeños negocios** en ftc.gov/ciberseguridad.

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. Pida recomendaciones a gente en quien confía. Es posible que pueda conseguir asesoramiento y consejos sobre desarrollo de negocios gratis a través de programas como SCORE.org.

► Estafas comunes dirigidas contra pequeños negocios

Facturas falsas y mercadería que no pidió

Los estafadores crean facturas falsas que parecen ser por productos o servicios que usted ordenó para su negocio. Los estafadores esperan que la persona que se ocupa de pagar sus facturas asuma que son reales y que las pague. Pero todo es falso. O un estafador podría llamar para confirmar una orden de pedido, verificar un domicilio o para ofrecer un catálogo o muestra gratis. Si usted dice que sí, mercadería que nadie encargó llegará a su puerta seguida de

exigencias de pago de alta presión. No pague. Y recuerde, que si recibe mercadería que no pidió, usted tiene el derecho legal de quedársela y usarla sin pagar nada.

Estafas de anuncios y listados en guías comerciales en internet

Los estafadores oportunistas tratan de engañarlo para que pague por anuncios inexistentes o por la publicación del nombre de su negocio en una guía comercial que no existe. Puede que le pidan información de contacto para un nuevo listado “gratis” o que le digan que el propósito de la llamada es simplemente confirmar su información. Después, usted recibirá una gran factura, y para presionarlo a pagar, el estafador puede usar detalles, o incluso una grabación, de la llamada previa en la cual le presionaron para que pague.

Estafas de impostores de negocios y agencias del gobierno

Los estafadores fingen ser alguien que conoce o en quien usted confía y tratan de asustarlo o apresurarlo para que les pague o les de información. Por ejemplo:

- Los estafadores dicen que están llamando de parte de una compañía de servicio de gas, electricidad o agua y que están por cortar el servicio a su negocio porque hay una factura atrasada (la cual fue inventada.)

- Los estafadores se hacen pasar por agentes del gobierno y amenazan con suspender sus licencias comerciales, imponerle multas o incluso tomar acciones legales. Puede que le digan que es porque usted debe impuestos o necesita renovar una licencia o registro expedido por el gobierno.
- Algunos estafadores le convencen a que compre afiches de cumplimiento de normas del personal que se pueden obtener gratis en el Departamento de Trabajo de Estados Unidos.
- Algunos estafadores lo engañan para que pague a cambio de subsidios para negocios que no existen de programas gubernamentales que tampoco existen.
- Los estafadores se hacen pasar por un representante de la Oficina de Marcas y Patentes de EE. UU., y le amenazan que perderá sus marcas si no paga un cargo inmediatamente. A veces, le mienten y le dicen que adeuda dinero por servicios de registro adicionales.
- Algunos estafadores dicen que están llamando de una compañía de tecnología y que su negocio perderá su domicilio web si no les paga inmediatamente.

Estafas de soporte técnico

Las estafas de soporte técnico comienzan con una llamada o mensaje pop-up alarmante en su pantalla.

Los estafadores fingen ser representantes de una compañía reconocida y le dicen que hay un problema con la seguridad de su computadora. 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, para inscribir a su negocio en un programa de mantenimiento de computadoras inexistente o inútil, o llegar a acceder a datos sensibles que pueden usar para cometer robo de identidad.

Ingeniería de redes sociales, phishing y programas de rescate

Los ciber-estafadores pueden engañar a los empleados para convencerlos de que envíen dinero o suministren información confidencial o delicada, como contraseñas o datos de cuentas bancarias. Este tipo de estafa 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, que crea una sensación de urgencia o temor. También se pueden recibir emails que parecen ser solicitudes de rutina para actualizar contraseñas u otros mensajes automatizados, pero en verdad 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 asesoría comercial

Algunos estafadores venden falsos servicios de asesoría para negocios y frecuentemente usan testimonios falsos, videos, presentaciones en seminarios y llamadas de telemarketing. Los estafadores hacen falsas promesas sobre resultados asombrosos a la gente que esté dispuesta a pagar por su sistema que supuestamente está probado que le dará éxito en el negocio. También es posible que lo tiente 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, agregar comentarios positivos, 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

Algunos estafadores 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. Pídale al vendedor que le entregue copias de todos los documentos en el momento – si se niega a hacerlo o lo posterga con promesas de enviárselos más tarde – eso puede ser un signo de que está tratando con un estafador.

Estafas de cheques falsos

Algunos estafadores le dan una razón creíble por la cual le quieren pagar con un cheque por un monto más grande de lo debido. Luego, le piden a usted que les gire el dinero extra a ellos u a otra persona. Aunque el banco le diga que el cheque estaba “aprobado”, resulta ser un cheque falso. 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.

► Otras prácticas cuestionables

A veces, los estafadores se esconden detrás de otras prácticas cuestionables, como afirmar que ofrecen trabajos independientes que pagan bien, pero luego no cumplen con sus promesas de grandes ganancias. O pueden tratar de venderle servicios innecesarios con la afirmación falsa de que debe pagar para mejorar el informe crediticio de su negocio. Y después de que ocurren los desastres naturales, los contratistas sin licencia y los estafadores pueden aparecer con falsas promesas de que le ayudaran a poner su negocio en marcha con reparaciones rápidas, limpieza o remoción de escombros que nunca ocurren.

▶ Aprenda más

- Para más recomendaciones sobre cómo proteger a su organización contra las estafas, visite ftc.gov/PequenosNegocios.
- Manténgase conectado con la FTC suscribiéndose al blog para negocios de la FTC en ftc.gov/subscribe.

▶ Reporte

- Si detecta una estafa, repórtela en ReporteFraude.ftc.gov. Su reporte pueda ayudar a frenar la estafa.
- Alerta 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.
- Ordene copias gratuitas de este folleto en ftc.gov/ordenar.

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/PequeñosNegocios. 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.

Para obtener la información más reciente para pequeños negocios suscríbase para recibir el Blog de la FTC para Negocios en ftc.gov/subscribe.

This brochure 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](https://www.ftc.gov/bulkorder).



**COMISIÓN FEDERAL
DE COMERCIO**

[ftc.gov/empresarios](https://www.ftc.gov/empresarios)

Julio 2023