CIBERSEGURIDAD PARA
PEQUEÑOS NEGOCIOS

CONCEPTOS BÁSICOS DE CIBERSEGURIDAD

Los delincuentes cibernéticos atacan a compañías de todo tamaño.

El hecho de conocer algunos conceptos básicos de ciberseguridad lo ayudará a proteger su negocio y reducir los riesgos de sufrir un ataque cibernético.

PROTEJA
SUS ARCHIVOS Y SUS DESPOTIVOS

Actualice sus programas

Esto incluye aplicaciones, navegadores web y sistemas operativos. Configure las actualizaciones para que se activen automáticamente.

Proteja sus archivos

Haga copias de seguridad fuera de internet de todos los archivos importantes en un dispositivo externo o en la nube. Asegúrese de almacenar sus archivos impresos de manera segura.

Exija usar contraseñas

Todas las computadoras portátiles, tablets y teléfonos inteligentes deben usar contraseñas. No deje estos dispositivos sin vigilancia en lugares públicos.

Codifique los dispositivos

y otros soportes de datos que contengan información personal delicada. Esto incluye computadoras portátiles, tablets, teléfonos inteligentes, discos extraíbles, cintas de copias de seguridad y soluciones de almacenamiento en la nube.

Use un sistema de autenticación de múltiples factores

Exija una autenticación de múltiples factores para acceder a las áreas de su red que contengan información delicada. Esto requiere seguir algunos pasos adicionales además de iniciar la sesión con una contraseña – por ejemplo, una contraseña temporaria en un teléfono inteligente o una llave que se inserta en una computadora.

APRENDA MÁS EN
FTC.gov/PequeñosNegocios

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology
U.S. Department of Commerce

SBA U.S. Small Business Administration

CIBERSEGURIDAD PARA PEQUEÑOS NEGOCIOS

PROTEJA SU RED INALÁMBRICA

Resguarde su enrutador

Cambie el nombre y contraseña predeterminados, desactive la administración remota del aparato y desconéctese como administrador del enrutador cuando ya esté configurado.

Para codificarlo, use como mínimo el acceso protegido WPA2

Asegúrese de que su enrutador le ofrezca una codificación tipo WPA2 o WPA3, y verifique que esté activada. La codificación protege la información que se envía a través de su red para que las personas ajenas a su negocio no puedan leerla.

USE HABITUALMENTE UNA SEGURIDAD INTELIGENTE EN SU NEGOCIO

Exija contraseñas sólidas

Una contraseña sólida tiene por lo menos 12 caracteres con una combinación de números, símbolos y letras mayúsculas y minúsculas.

Nunca reutilice las contraseñas y no las comparta por teléfono, mensajes de texto ni por email.

Limite el número de atentos de acceso para así limitar los ataques que tratan de averiguar la contraseña.

Capacite a todo el personal

Cree una cultura de seguridad implementando un programa regular de capacitación para sus empleados. Actualice la capacitación de sus empleados a medida de que se entere de nuevos riesgos y vulnerabilidades. Si hay empleados que no participan en la capacitación, considere bloquearles el acceso a la red.

Tenga un plan

para guardar los datos, seguir adelante con su negocio y notificar a los clientes en caso que sufra un incidente de seguridad de datos. La guía para negocios de la FTC *Data Breach Response: A Guide for Business* (disponible en inglés) le brinda los pasos que puede seguir.

APRENDA MÁS EN FTC.gov/PequeñosNegocios

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

CIBERSEGURIDAD PARA
PEQUEÑOS NEGOCIOS

RANSOMWARE

Una persona de su compañía recibe un email.

Parece legítimo – pero con sólo hacer clic en un enlace o descargar un archivo adjunto, todo queda bloqueado fuera de su red. Desde ese enlace se descargó un programa que le secuestra sus datos como rehén. Eso es un ataque de un programa de rescate o ransomware.

Los atacantes le piden dinero o una cripto-moneda, pero aunque les pague, usted no sabe si los ciber-delincuentes se quedarán con sus datos o destruirán sus archivos. Mientras tanto, la información que necesita para operar su negocio y los datos delicados de sus clientes, sus empleados y su compañía están ahora en las manos de delincuentes. El ataque de ransomware puede tener un costo muy alto para su negocio.

CÓMO OCURRE

Los delincuentes pueden iniciar un ataque de ransomware de varias maneras.

Mensajes electrónicos fraudulentos
con enlaces y archivos adjuntos que ponen en riesgo sus datos y su red. Estos emails phishing son el origen de la mayoría de los ataque de programas de rescate o ransomware.

Sitios web infectados
que descargan automáticamente programas maliciosos en su computadora.

Vulnerabilidades del servidor
que pueden ser explotadas por los piratas informáticos.

Anuncios en línea
que contienen un código malicioso – incluso en sitios web conocidos y en los que confía.

APRENDA MÁS EN
FTC.gov/PequeñosNegocios

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology
U.S. Department of Commerce

SBA
U.S. Small Business Administration

CIBERSEGURIDAD PARA PEQUEÑOS NEGOCIOS

CÓMO PROTEGER SU NEGOCIO

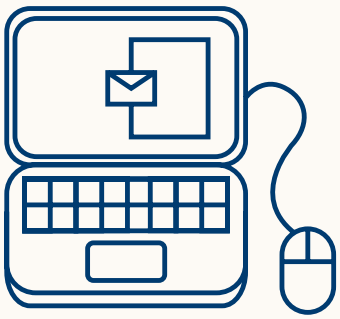
Implemente un plan
¿Cómo hará su negocio para mantenerse en pie y seguir operando después de un ataque de ransomware? Ponga el plan por escrito y compártalo con todo aquel que necesite conocerlo.

Haga copias de seguridad de sus datos
Guarde lo archivos importantes con regularidad en un disco externo o servidor que no esté conectado a su red. Haga copias de seguridad de datos como parte de sus operaciones comerciales de rutina.

Mantenga actualizada su seguridad
Instale siempre los parches de seguridad y actualizaciones más recientes. Busque otros medios de protección, como la autenticación de email y programas de prevención de intrusión, y configúrelos para que se actualicen automáticamente en su computadora. Es posible que tenga que hacerlo manualmente en los dispositivos móviles.

Alerte a su personal
Enséñeles cómo evitar las estafas de phishing y muéstreles algunas de las maneras más comunes en que se infectan los dispositivos y las computadoras. Incluya consejos para detectar los ataques de programas de rescate y protegerse contra ellos en sus sesiones regulares de capacitación y en sus comunicaciones.

QUÉ HACER SI LO ATACAN



Limite los daños
Desconecte inmediatamente de su red todas las computadoras o dispositivos infectados. Si le robaron sus datos, tome medidas para proteger a su compañía y notifique a aquellos que podrían estar afectados.

Mantenga su negocio en funcionamiento
Ahora es el momento de implementar ese plan. Tener copias de seguridad de sus datos lo ayudará.

Establezca contacto con las autoridades
Reporte el ataque de inmediato a su departamento de policía local. Si no están familiarizados con las investigaciones de compromisos de información, establezca contacto con su oficina local del FBI.

¿Debería pagar el rescate?
Las autoridades no lo recomiendan, pero es usted quien debe determinar si los riesgos y costos de pagar justifican la posibilidad de recuperar sus archivos. Sin embargo, es posible que el pago del rescate no le garantice la recuperación de sus datos.

Notifique a los clientes
Si sus datos o la información personal quedó comprometida, asegúrese de notificar a las partes afectadas ya que podrían estar en riesgo de un robo de identidad. Busque información sobre cómo hacerlo en *Data Breach Response: A Guide for Business* (disponible en inglés).

APRENDA MÁS EN FTC.gov/PequeñosNegocios

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

CIBERSEGURIDAD PARA
PEQUEÑOS NEGOCIOS

PHISHING

Recibe un email que parece enviado por alguien que usted conoce.

Pareciera que el email se lo envió uno de sus proveedores y le piden que haga clic en un enlace para actualizar la cuenta de su negocio. ¿Debería hacer clic? Quizás el email podría parecer ser de su jefe y le pide la contraseña de su red. ¿Debería responder? En cualquiera de los casos, la respuesta es probablemente no. Estos pueden ser intentos de phishing o pesca de información.

CÓMO FUNCIONA

EL PHISHING

Usted recibe un email o mensaje de texto

Parece que se lo envió alguien que usted conoce, y le pide que haga clic en un enlace, o que le dé su contraseña, número de cuenta bancaria de su negocio u otra información delicada.

Es urgente

En el mensaje lo presionan para que actúe de inmediato—o de lo contrario sucederá algo malo.

Pero, ¿será verdad?

Es fácil falsificar logotipos y establecer domicilios de email falsos. Los estafadores usan nombres de compañías que suenan familiares o se hacen pasar por alguien que usted conoce.

Lo que pasa después

Si hace clic en un enlace, los estafadores pueden instalar un programa de rescate (ransomware, en inglés) u otros programas que pueden bloquear acceso a sus datos y diseminar ese bloqueo a la toda la red de la compañía. Si usted comparte información, a los estafadores tendrán acceso a todas esas cuentas.

LO QUE PUEDE HACER

Antes de hacer clic en un enlace o compartir cualquiera de los datos delicados de su negocio, haga lo siguiente:

Verifíquelo

Busque el sitio web o número de teléfono de la compañía o persona que está detrás del mensaje de texto o email. Asegúrese de contactar a la verdadera compañía o sitio para evitar descargar un programa malicioso o hablar con un estafador.

Hable con alguien

El hecho de hablar con un colega lo podría ayudar a sacar en claro si ese es un pedido auténtico o un intento de phishing.

Si tiene dudas, haga una llamada

Llame a ese proveedor, colega o cliente que le envió el email. Confirme que realmente necesitan que usted les dé esa información. Use un número que le conste que es el correcto, no llame al número de teléfono que aparezca en el email o mensaje de texto.

APRENDA MÁS EN
FTC.gov/PequeñosNegocios

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology
U.S. Department of Commerce

SBA U.S. Small Business Administration

CIBERSEGURIDAD PARA PEQUEÑOS NEGOCIOS

CÓMO PROTEGER SU NEGOCIO

Haga copias de seguridad de sus datos

Haga copias de seguridad de sus datos con regularidad y asegúrese que esas copias de seguridad no estén conectadas a la red. Así podrá restaurar sus datos si sufre un ataque de phishing y los piratas informáticos logran acceder a su red. Adopte la tarea de hacer copias de seguridad de datos como parte de sus operaciones comerciales de rutina.

Mantenga actualizada su seguridad

Instale siempre los parches de seguridad y actualizaciones más recientes. Busque otros medios de protección, como la autenticación de email, programas de prevención de intrusión, y configúrelos para que se actualicen automáticamente en su computadora. Es posible que tenga que hacerlo manualmente en los dispositivos móviles.

Alerte a su personal

Comparta esta información con ellos. Incluya consejos para detectar los ataques de programas de rescate y protegerse contra ellos en sus sesiones regulares de orientación y capacitación.

Despliegue una red de seguridad

En primer lugar, use tecnología de autenticación de emails para ayudar a prevenir que los emails tipo phishing lleguen a los buzones de entrada de emails de la compañía.

¿QUÉ HACER SI CAE EN LAS REDES DE UN ESQUEMA DE PHISHING?

Alerte a los demás

Hable con sus colegas y comparta su experiencia. Los ataques de phishing suelen afectar a más de una persona dentro de una compañía.

Limite los daños

Cambie inmediatamente cualquier contraseña comprometida y desconecte de la red toda computadora o dispositivo que esté infectado con un programa malicioso.

Siga los procedimientos de su compañía

Esto puede incluir la notificación de personas específicas de su organización o contratistas que lo ayudan con las tareas de tecnología de la información.

Notifique a los clientes

Si sus datos o la información personal quedó comprometida, asegúrese de notificar a las partes afectadas ya que podrían estar en riesgo de un robo de identidad. Busque información sobre cómo hacerlo en *Data Breach Response: A Guide for Business* (disponible en inglés).

Repórtelo

Reenvíe los emails phishing a spam@uce.gov (un domicilio electrónico utilizado por la FTC) y a reportphishing@apwg.org (un domicilio electrónico utilizado por el Grupo de Trabajo Anti-Phishing, que incluye proveedores de servicio de internet, proveedores de productos y servicios de seguridad, instituciones financieras y agencias a cargo del cumplimiento de la ley). Infórmele lo sucedido a la compañía o a la persona cuyo nombre fue usado para perpetrar el esquema de phishing. Y repórtelo a la FTC en ftc.gov/queja.

APRENDA MÁS EN FTC.gov/PequeñosNegocios

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

CIBERSEGURIDAD PARA
PEQUEÑOS NEGOCIOS

IMPOSTOR DE EMAILS DE NEGOCIOS

Un estafador establece un domicilio de email que parece ser de su compañía.

Entonces, el estafador envía mensajes usando ese domicilio de email. Esta práctica se llama ataque de suplantación, "spoofing" en inglés, y el estafador es lo que llamamos un impostor de emails de negocios.

Los estafadores hacen esto para conseguir contraseñas y números de cuentas o para logar que alguien les envíe dinero. Si sucede, su compañía tiene mucho que perder. Clientes y asociados podrían perder la confianza e irse a otro negocio – y su compañía podría perder dinero.

CÓMO PROTEGER SU NEGOCIO

Use un sistema de autenticación de email

Cuando establezca el sistema de correo electrónico de su negocio, asegúrese de que el proveedor de alojamiento web le ofrezca tecnología de autenticación de correo electrónico. De esa manera, cuando envíe un email desde el servidor de su compañía, los servidores receptores pueden confirmar que el email fue realmente enviado desde su negocio. Si no lo pueden confirmar, los servidores pueden bloquear ese email e impedir un incidente de impostor de emails de negocios.

Mantenga actualizada su seguridad

Instale los parches de seguridad y las actualizaciones más recientes. Configúrelos para que se actualicen automáticamente. Busque otros medios de protección, como un software de protección contra intrusiones, que vigila la actividad sospechosa en su red y le envía alertas si encuentra alguna actividad sospechosa.

Capacite a su personal

Enséñeles cómo evitar las estafas de phishing y las maneras más comunes en que los atacantes pueden infectar las computadoras y los dispositivos con un programa malicioso. Incluya consejos para detectar las amenazas cibernéticas y protegerse contra ellas en sus sesiones de capacitación y comunicaciones regulares.

APRENDA MÁS EN
FTC.gov/PequeñosNegocios

FEDERAL TRADE COMMISSION

Homeland Security

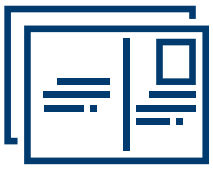
NIST National Institute of Standards and Technology
U.S. Department of Commerce

SBA U.S. Small Business Administration

CIBERSEGURIDAD PARA
PEQUEÑOS NEGOCIOS

QUÉ HACER
SI ALGUIEN MANIPULA LA CUENTA DE EMAIL DE SU COMPAÑÍA

Repórtelo
Reporte la estafa a las autoridades de seguridad locales, al Centro de Quejas de Delitos en Internet del FBI en ic3.gov, y a la FTC en ftc.gov/queja. También puede reenviar los emails phishing a spam@uce.gov (un domicilio electrónico utilizado por la FTC) y a reportphishing@apwg.org (un domicilio electrónico utilizado por el Grupo de Trabajo Anti-Phishing, que incluye proveedores de servicios de internet, proveedores de productos y servicios de seguridad, instituciones financieras y agencias a cargo del cumplimiento de la ley).



Notifique a sus clientes
Si descubre que hay estafadores que se hacen pasar por su negocio, infórmeselo a sus clientes a la brevedad posible – por correo, email o a través de los medios sociales. Si envía un email a sus clientes, no incluya hipervínculos para que su notificación no parezca una estafa de phishing. Recuérdeles a sus clientes que no compartan ninguna información personal a través del correo electrónico o mensajes de texto. Si le roban los datos de sus clientes, dígales que visiten Robodeldentidad.gov para conseguir un plan de acción para recuperarse.

Alerte a su personal
Use esta experiencia para actualizar las prácticas de seguridad de su negocio y capacitar a su personal acerca de las amenazas cibernéticas.

CIBERSEGURIDAD PARA
PEQUEÑOS NEGOCIOS

SEGURIDAD FÍSICA

La ciberseguridad comienza con una sólida seguridad física.

Los fallos de la seguridad física pueden poner en riesgo datos delicados de su compañía que podrían usarse para el robo de identidad. Por ejemplo:

Un empleado deja accidentalmente un dispositivo de almacenamiento de datos en la mesa de una cafetería. El dispositivo – que contiene cientos de números de tarjetas de crédito de los clientes – desapareció.

Otro empleado tira viejos registros bancarios de la compañía al cesto de la basura, y un delincuente los encuentra.

Un ladrón entra a su oficina por una ventana abierta y roba archivos y computadoras.

CÓMO PROTEGER LOS EQUIPOS Y LOS ARCHIVOS DE PAPEL

Estas son algunas recomendaciones para proteger la información contenida en archivos de papel y en los discos duros, dispositivos de almacenamiento de datos, computadoras portátiles, dispositivos utilizados en puntos de venta y demás equipos.

Guarde todo de manera segura

Cuando los archivos de papel o los dispositivos electrónicos contengan información delicada, guárdelos en un gabinete o en un lugar cerrado con llave.

Limite el acceso físico

Cuando los registros o dispositivos contengan información delicada, permita el acceso únicamente a aquellos que lo necesiten.

Envíe recordatorios

Recuérdeles a los empleados que deben guardar los archivos de papel en gabinetes con llave y desconectarse de su red y aplicaciones. Recuérdeles que nunca deben dejar al descuido un archivo ni un dispositivo que contenga datos delicados.

Controle su inventario

Lleve un control y proteja todos los aparatos que recolecten información delicada de los clientes.

APRENDA MÁS EN
FTC.gov/PequeñosNegocios

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology
U.S. Department of Commerce

SBA U.S. Small Business Administration

CIBERSEGURIDAD PARA PEQUEÑOS NEGOCIOS

CÓMO PROTEGER LOS DATOS DE SUS DISPOSITIVOS

Cualquier cosa puede suceder. Pero hay menos probabilidades que se produzca un incidente de seguridad de datos en aquellos dispositivos que están protegidos. Estas son algunas maneras de hacerlo:

Exija contraseñas complejas

Exija que se establezcan contraseñas extensas, complejas y únicas. Y asegúrese de que esas contraseñas se guarden de manera segura. Considere usar un programa de administración de contraseñas.

Use un sistema de autenticación de múltiples factores

Exija autenticación de múltiples factores para acceder áreas de su red que contengan información delicada. Esto requiere pasos adicionales además de iniciar la sesión con una contraseña – como un código temporario en un teléfono inteligente o una llave que se inserta en una computadora.

Limite la cantidad de intentos de inicio de sesión

Limite la cantidad de intentos incorrectos de inicio de sesión para desbloquear los dispositivos. Esto lo ayudará a protegerse de los intrusos.

Codificación

Codifique los dispositivos portátiles, incluyendo las computadoras portátiles y pequeños dispositivos de almacenamiento de datos que contengan información delicada. Codifique todos los datos delicados que envíe fuera de la compañía, por ejemplo, a un contador o a un servicio de despacho y entrega.

CAPACITE A SUS EMPLEADOS

Incluya el tema de la seguridad física en sus sesiones de capacitación y comunicaciones regulares. Recuérdeles a los empleados que:

Trituren los documentos

Siempre deben triturar documentos que con datos delicados antes de tirarlos a la basura.

Borren correctamente los datos

Deben usar un programa para borrar los datos antes de donar o descartar computadoras, dispositivos móviles, fotocopiadoras digitales y dispositivos de almacenamiento de datos en desuso. No deben confiar únicamente en la función “eliminar”.

Promuevan prácticas de seguridad en todos los lugares

Se deben mantener prácticas de seguridad incluso cuando se trabaja remotamente desde sus casas o durante un viaje de negocios.

Estén al tanto del plan de respuesta

Todo el personal debe saber qué hacer en caso de una pérdida o robo de los equipos o archivos de papel, incluidos el nombre de las personas a las que deben notificar y los pasos a tomar. Busque información sobre cómo crear un plan de respuesta en *Data Breach Response: A Guide for Business* (disponible en inglés). Puede consultar esta guía en ftc.gov/databreach.

APRENDA MÁS EN FTC.gov/PequeñosNegocios

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

CIBERSEGURIDAD PARA
PEQUEÑOS NEGOCIOS

ACCESO REMOTO SEGURO

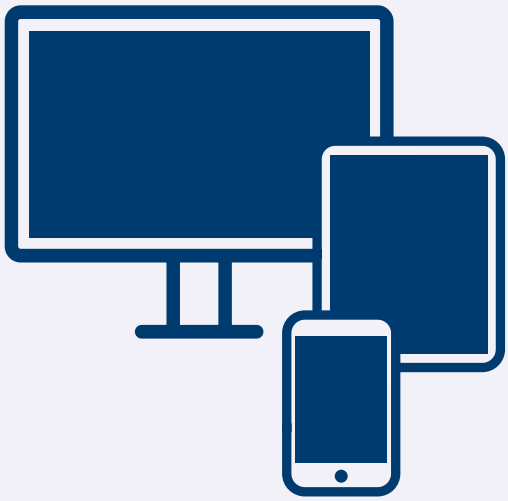
Es posible que los empleados y proveedores necesiten conectarse a su red de manera remota.

Ponga la seguridad de su red en primer lugar. Exíjales a todos que sigan sólidos estándares de seguridad antes de conectarse a su red. Ofrézcales las herramientas para que incorporen la seguridad a su rutina de trabajo.

CÓMO PROTEGER LOS DISPOSITIVOS

Cuando los empleados o proveedores se conectan de manera remota a su red, ya sea a través de los dispositivos de propiedad de su compañía o de sus propios dispositivos, esos dispositivos deben estar protegidos. Siga estas recomendaciones — y asegúrese de que sus empleados y proveedores también lo hagan:

- Cambie la contraseña preestablecida y el nombre predeterminado de su enrutador. Y mantenga actualizado el programa del enrutador; es posible que para hacerlo tenga que visitar a menudo el sitio web del enrutador.
- Considere activar la codificación completa de los discos de las computadoras portátiles y otros dispositivos móviles que se conectan a su red de manera remota. Busque esta opción en su sistema operativo que protegerá todos los datos almacenados en el dispositivo en caso de robo o pérdida. Esto es especialmente importante si en el dispositivo se almacena información personal delicada.
- Cambie la configuración de los teléfonos inteligentes para impedir las conexiones automáticas a las redes Wi-Fi de uso público.
- Mantenga actualizado el programa antivirus en los dispositivos que se conectan a su red, incluidos los dispositivos móviles.



APRENDA MÁS EN
FTC.gov/PequeñosNegocios

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology
U.S. Department of Commerce

SBA U.S. Small Business Administration

CIBERSEGURIDAD PARA PEQUEÑOS NEGOCIOS

CÓMO CONECTARSE REMOTAMENTE A LA RED

Exíjales a los empleados y proveedores que usen conexiones seguras cuando se conecten a su red de manera remota. Ellos deberían:

Usar un enrutador con una codificación de tipo WPA2 o WPA3 cuando se conecten desde sus casas. La codificación protege la información que se envía a través de una red para que las personas ajenas a su negocio no puedan leerla. Los sistemas de codificación WPA2 y WPA3 son los únicos estándares de codificación que protegerán la información enviada a través de una red.

Usar únicamente una red Wi-Fi pública cuando también estén usando una red virtual privada (VPN, por sus siglas en inglés) para codificar el tráfico entre sus computadoras e internet. Las redes Wi-Fi de uso público no ofrecen una conexión segura a internet por sí solas. Sus empleados pueden obtener un VPN, o tal vez le convenga crear una red virtual privada empresarial para que la usen todos sus empleados.

QUÉ TIENE QUE HACER PARA MANTANER LA SEGURIDAD

Capacite a su personal:

Incluya información sobre acceso remoto seguro en las sesiones regulares de capacitación y en las reuniones de orientación para el personal nuevo.

Establezca políticas que cubran los conceptos básicos de ciberseguridad, entrégueles copias a sus empleados y explique la importancia de cumplir dichas políticas.

Antes de permitir la conexión de cualquier dispositivo a su red — ya sea desde la casa de un empleado o desde la red de un proveedor — asegúrese de que el usuario cumpla con los requisitos de seguridad de su red.

Informe a su personal acerca del riesgo que presentan las redes Wi-Fi de uso público.

Ofrézcales a los miembros de su personal las herramientas que los ayudarán a mantener la seguridad:

- Exíjales a los empleados que usen contraseñas únicas y complejas para la red y que eviten que los puestos de trabajo abiertos queden al descuido.
- Considere crear una red VPN para los empleados conectarse a la red del negocio de manera remota.
- Exija una autenticación de múltiples factores para acceder a las áreas de su red que contengan información delicada. Esto requiere algunos pasos adicionales además de iniciar la sesión con una contraseña — como un código temporario enviado a un teléfono inteligente o una llave que se inserta en una computadora y genera un código.
- Si en su negocio ofrece una red Wi-Fi para visitantes y clientes, asegúrese de que esté separada y no conectada a la red de su negocio.
- Incluya disposiciones de seguridad en sus contratos con los proveedores, especialmente si el proveedor se conectará a su red de manera remota.

APRENDA MÁS EN FTC.gov/PequeñosNegocios

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

CIBERSEGURIDAD PARA
PEQUEÑOS NEGOCIOS

SEGURIDAD DE LOS PROVEEDORES

Puede que su negocio tenga proveedores con acceso a su información delicada.

Asegúrese de que esos proveedores estén tomando las medidas necesarias para proteger sus propias computadoras y redes. Por ejemplo, ¿qué sucedería si su contable pierde su computadora portátil con toda su información financiera? ¿O si la red de un proveedor que está conectada con su red sufre un ataque? El resultado: los datos de su negocio y la información personal de sus clientes puede terminar en las manos equivocadas — lo cual pone en riesgo a su negocio y a sus clientes.

CÓMO MONITOREAR A SUS PROVEEDORES

Póngalo por escrito

Incluya disposiciones de seguridad en los contratos con sus proveedores, como por ejemplo, un plan para Wevaluar y actualizar los controles de seguridad debido a que en las amenazas cambian. No negocie las disposiciones de seguridad que son cruciales para su compañía.

Verifique el cumplimiento

Establezca procesos que le permitan confirmar que los proveedores cumplen sus reglas. No crea sólo en las palabras.

Haga cambios según sean necesarios

Las amenazas de seguridad cibernética cambian rápidamente. Asegúrese de que sus proveedores mantengan su seguridad actualizada.

APRENDA MÁS EN
FTC.gov/PequeñosNegocios

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology
U.S. Department of Commerce

SBA U.S. Small Business Administration

CIBERSEGURIDAD PARA PEQUEÑOS NEGOCIOS

CÓMO PROTEGER SU NEGOCIO

Controle el acceso

Establezca controles en las bases de datos que contengan información delicada. Limite el acceso según lo que sea necesario que sepa cada proveedor, y sólo por la cantidad de tiempo que el proveedor lo necesite para hacer un trabajo.

Use un sistema de autenticación de múltiples factores

Exija una autenticación de múltiples factores para acceder a las áreas de su red que contengan información delicada. Esto requiere algunos pasos adicionales además de iniciar la sesión con una contraseña – como un código temporario en un teléfono inteligente o una llave que se inserta en una computadora.

Proteja su red

Exija contraseñas sólidas: por lo menos 12 caracteres con una combinación de números, símbolos y letras mayúsculas y minúsculas. Nunca reutilice las contraseñas, no las comparta y limite la cantidad de intentos incorrectos de inicio de sesión para restringir los ataques de predicción de contraseñas.

Salvaguarde sus datos

Use un sistema de codificación potente y correctamente configurado. Esto protege la información delicada en el proceso de transferencia y almacenamiento.

QUÉ HACER SI UN PROVEEDOR SUFRE UN INCIDENTE DE SEGURIDAD DE DATOS

Establezca contacto con las autoridades

Reporte el ataque de inmediato a su departamento de policía local. Si no están familiarizados con las investigaciones de compromisos de información, establezca contacto con su oficina local del FBI.

Confirme que el proveedor haga las reparaciones

Si su negocio decide seguir trabajando con ese proveedor, asegúrese de que repare las vulnerabilidades y le garantice que su información estará protegida en el futuro.

Notifique a los clientes

Si sus datos o la información personal quedó comprometida, asegúrese de notificar a las partes afectadas ya que podrían estar en riesgo de un robo de identidad. Busque información sobre cómo hacerlo en *Data Breach Response: A Guide for Business* (disponible en inglés).

APRENDA MÁS EN FTC.gov/PequeñosNegocios

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology U.S. Department of Commerce

SBA U.S. Small Business Administration

CIBERSEGURIDAD PARA
PEQUEÑOS NEGOCIOS

Qué es y cómo funciona

EL MARCO DE CIBERSEGURIDAD DEL NIST

Es posible que haya escuchado hablar del Marco de Ciberseguridad del NIST, ¿pero qué es exactamente?

¿Y es aplicable para usted?

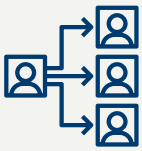
NIST es el acrónimo de Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, en inglés) dependiente del Departamento de Comercio de EE. UU. El Marco de Ciberseguridad del NIST ayuda a los negocios de todo tamaño a comprender mejor sus riesgos de ciberseguridad, administrar y reducir sus riesgos, y proteger sus redes y datos. Este Marco es voluntario. Le brinda a su negocio una reseña de las mejores prácticas para ayudarlo a decidir dónde tiene que concentrar su tiempo y su dinero en cuestiones de protección de ciberseguridad.

Usted puede implementar el Marco de Ciberseguridad del NIST en su negocio en estas cinco áreas: identificación protección, detección, respuesta y recuperación.

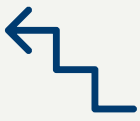
1. IDENTIFICACIÓN

Haga una lista de todos los equipos, programas software y datos que use, incluyendo computadoras portátiles, teléfonos inteligentes, tablets y dispositivos utilizados en puntos de venta.

Elabore y comparta una política de ciberseguridad de la compañía que cubra los siguientes puntos:



Funciones y responsabilidades de los empleados, proveedores y todo aquel que tenga acceso a datos delicados.



Pasos a seguir para protegerse contra un ataque y limitar el daño si se produce un ataque.

2. PROTECCIÓN

- Controle quiénes acceden a su red y usan sus computadoras y otros dispositivos.
- Use programas de seguridad para proteger los datos.
- Codifique los datos delicados, tanto cuando estén almacenados o en tránsito.
- Haga copias de seguridad de los datos con regularidad.
- Actualice los programas de seguridad con regularidad, en lo posible, automatice estas actualizaciones.
- Implemente políticas formales para la eliminación segura de archivos electrónicos y dispositivos en desuso.
- Capacite sobre ciberseguridad a todas las personas que usen sus computadoras, dispositivos y redes. Usted puede ayudar a los empleados a comprender su riesgo personal además de la función crucial que cumplen en el lugar de trabajo.

APRENDA MÁS EN
FTC.gov/PequeñosNegocios

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology
U.S. Department of Commerce

SBA U.S. Small Business Administration

CIBERSEGURIDAD PARA

PEQUEÑOS NEGOCIOS

3. DETECCIÓN

Monitoree sus computadoras para controlar si detecta acceso de personal no autorizado a sus computadoras, dispositivos (soportes de almacenamiento de datos de tipo USB) y software.

Revise su red para controlar si detecta usuarios o conexiones no autorizados.

Investigue cualquier actividad inusual en su red o por parte de su personal.

4. RESPUESTA

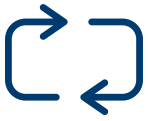
Implemente un plan para:

- Notificar a los clientes, empleados y otros cuyos datos pudieran estar en riesgo.
- Mantener en funcionamiento las operaciones del negocio.
- Reportar el ataque a los encargados del cumplimiento de la ley y otras autoridades.
- Investigar y contener un ataque.
- Actualizar su política y plan de ciberseguridad con las lecciones aprendidas.
- Prepararse para eventos inadvertidos (como emergencias climáticas) que puedan poner en riesgo los datos.

Ponga a prueba su plan con regularidad.

5. RECUPERACIÓN

Después de un ataque:



Repare y restaure los equipos y las partes de su red que resultaron afectados.

Mantenga informados a sus empleados y clientes de sus actividades de respuesta y recuperación.

Para más información sobre el Marco de Ciberseguridad del NIST y los recursos para los pequeños negocios, visite nist.gov/CyberFramework y nist.gov/programs-projects/small-business-corner-sbc.

APRENDA MÁS EN
FTC.gov/PequeñosNegocios

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology
U.S. Department of Commerce

SBA U.S. Small Business Administration