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

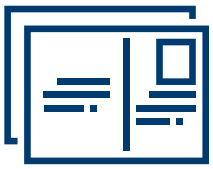
NIST National Institute of Standards and Technology
U.S. Department of Commerce

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.