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