Agosto 2023

# BOLETÍN INFORMATIVO

## Acerca de Chubb

Con operaciones en 54 países y territorios, Chubb ofrece seguros comerciales y personales de propiedad y accidentes, accidentes personales y seguro médico complementario, reaseguro y seguro de vida a un grupo diverso de clientes. Como empresa de suscripción, evaluamos, asumimos y gestionamos el riesgo con conocimiento y disciplina. Atendemos y pagamos nuestros reclamos de manera justa. La compañía también se define por su amplia oferta de productos y servicios, amplias capacidades de distribución, solidez financiera excepcional y operaciones locales a nivel mundial. La empresa matriz Chubb Limited cotiza en la Bolsa de Valores de Nueva York (NYSE: CB) y es un componente del índice S&P 500. Chubb mantiene oficinas ejecutivas en Zurich , Nueva York , Londres , París y otras ubicaciones, y emplea aproximadamente a 33.000 personas en todo el mundo.

## “Cómo mejorar la seguridad cibernética para su pequeña empresa “

**El hecho de que tenga una pequeña empresa no significa que esté fuera del alcance de un hacker. Las pequeñas empresas suelen tener los mismos tipos de información confidencial de los clientes que las empresas más grandes. Eso, combinado con su falta percibida de conocimiento y recursos de seguridad cibernética, los convierte en un objetivo atractivo para los piratas informáticos.**

**Según una encuesta reciente de la SBA, el 88 % de los propietarios de pequeñas empresas consideraron que su negocio era vulnerable a un ataque cibernético. Sin embargo, muchas empresas no pueden permitirse soluciones de TI profesionales, tienen un tiempo limitado para dedicarse a la seguridad cibernética o no saben por dónde empezar.**

**La mejor manera para que los propietarios de pequeñas empresas estén adecuadamente preparados es informarse sobre las amenazas comunes y las mejores estrategias para defenderse de un ataque cibernético.**

# Amenazas cibernéticas comunes para las pequeñas empresas

## Fraude de ingeniería social

El fraude de ingeniería social consiste en manipular a las personas para que divulguen información confidencial, como contraseñas, números de seguridad social o información de tarjetas de crédito. La forma más común de fraude de ingeniería social son los correos electrónicos de phishing, que están diseñados para parecer enviados por una organización legítima o un individuo conocido y engañar a las víctimas para que paguen dinero o revelen datos confidenciales. Una pequeña empresa que busca nuevos productos y proveedores, por ejemplo, para ayudar a sistematizar sus operaciones diarias, puede ser susceptible al fraude de ingeniería social. Asegúrese de verificar la credibilidad de la organización antes de responder correos electrónicos o hacer clic en cualquier enlace de correo electrónico.

## Opciones de trabajo remoto

Muchas pequeñas empresas ofrecen opciones de trabajo desde casa y, si bien el trabajo remoto puede tener algunas ventajas, también puede exponer a las empresas a una variedad de riesgos de seguridad cibernética. Con una fuerza laboral distribuida, es importante que el personal sea aún más cuidadoso con el mantenimiento de la higiene cibernética .

## Malware

Malware es cualquier software diseñado intencionalmente para causar interrupciones y daños a una computadora, red u obtener acceso no autorizado a información privada, como virus y ransomware. Si bien los ataques de ransomware generalmente se asocian con empresas más grandes, de hecho, entre el 50 y el 70 por ciento de los ataques de ransomware están dirigidos a pequeñas y medianas empresas, y la mayoría de las pequeñas empresas fracasan dentro de los seis meses posteriores al ataque.

# Las mejores prácticas para mejorar la seguridad cibernética de las pequeñas empresas

1. **Educa a tus empleados**

A medida que los ciberdelincuentes evolucionan y se vuelven más inteligentes, es esencial actualizar periódicamente a sus empleados sobre los nuevos protocolos. Cuanto más sepan sus empleados sobre los ataques cibernéticos y cómo proteger sus datos, más segura será su empresa. Envíe recordatorios regulares para no abrir archivos adjuntos o hacer clic en enlaces en correos electrónicos de personas que no conocen o esperan; delinear procedimientos para cifrar información personal o confidencial; y capacite a los empleados para verificar si reciben solicitudes urgentes para emitir pagos inesperados, una estafa común.

**2 . Implementar prácticas de contraseñas seguras**

Muchas violaciones de datos ocurren debido a contraseñas débiles, robadas o perdidas. En el mundo actual de trabajar desde sus propios dispositivos, es fundamental que todos los dispositivos de los empleados que acceden a la red de la empresa estén protegidos con contraseña. Haga que los empleados

cambien sus contraseñas con regularidad al pedirles automáticamente que cambien sus contraseñas cada 60 a 90 días.

### 3. Asegúrese de tener los socios y las plataformas adecuados

Su seguridad cibernética es tan buena como la seguridad de las plataformas y los socios de los que depende su negocio. Compruebe lo siguiente:

¿Tiene un WAF (cortafuegos de aplicaciones web) para proteger su sitio?
¿Su plataforma de comercio electrónico cumple con el nivel 1 de PCI-DSS (estándares de seguridad de datos de la industria de tarjetas de pago)? Eso lo protegerá contra violaciones de seguridad de datos digitales en toda su red de pago, no solo en una sola tarjeta.
¿La empresa de alojamiento de su sitio web tiene personal que corrige periódicamente las vulnerabilidades de seguridad para reducir la probabilidad de ataques?
Verifique que cada computadora de la empresa tenga instalado un software antivirus. Incluso después de capacitar a los empleados sobre cómo identificar un correo electrónico de phishing, pueden ser susceptibles.

### 4. Asegure su hardware

Las violaciones de datos también pueden ser causadas por el robo de propiedad física. Si sus servidores, computadoras portátiles, teléfonos celulares u otros dispositivos electrónicos no están protegidos y son fáciles de robar, está corriendo un gran riesgo. Las cámaras de seguridad y las alarmas ayudarán, pero bloquear físicamente las computadoras y los servidores ayudará aún más. Ya sea que sus empleados trabajen desde casa, en un espacio de coworking o en una oficina tradicional, asegúrese de que entiendan cómo mantener protegidos los equipos de su empresa.

### 5. Realice copias de seguridad periódicas de todos los datos

No importa qué tan atento esté con sus estrategias de seguridad cibernética, aún pueden ocurrir violaciones de datos. La información más importante para respaldar es:

bases de datos
Archivos financieros
archivos de recursos humanos
Archivos de cuentas por cobrar/pagar

Asegúrese también de hacer una copia de seguridad de todos los datos almacenados en una unidad en línea y verifique su copia de seguridad regularmente para asegurarse de que funcione correctamente.

Su compañía de seguros también puede proporcionar servicios de gestión de riesgos y consultoría cibernética, así que consulte con su agente o corredor al elegir su cobertura de seguro cibernético. ¡También puede contratar a un experto externo para evaluar los riesgos!