CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
CENTER FOR CONSUMER INFORMATION & INSURANCE OVERSIGHT

Mejores prácticas para seguridad cibernética

Según una encuesta de la Agencia Federal para el Desarrollo de la Pequeña Empresa (SBA, en inglés), el 88% de los dueños de pequeñas empresas creía que su empresa estaba vulnerable a ataques cibernéticos. No obstante, muchas empresas no saben por dónde empezar cuando se trata de la seguridad cibernética. Esta hoja de consejos provee las mejores prácticas de seguridad cibernética para agentes e intermediarios para evitar ataques cibernéticos.

Cómo crear una contraseña fuerte

Agentes e intermediarios deben usar los siguientes consejos para crear contraseñas que harán que sea más difícil para los hackers obtener acceso no autorizado a sus cuentas. Para mantener una buena higiene de contraseñas, los agentes e intermediarios deben:

- Hacer contraseñas únicas y utilizar una contraseña distinta por cada una de sus cuentas.
- Usar contraseñas que son de 8 a 12 caracteres.
  - Evitar contraseñas que podrían ser adivinadas fácilmente por conocidos o basado en información fácilmente accesible (por ejemplo, información de cuentas de redes sociales).
  - Un ejemplo de una contraseña fuerte sería "Y&%145zL".
  - Un ejemplo de una contraseña débil sería "ACAagent91".
- Evite contraseñas que contienen información personal o palabras o frases comunes. Información personal podría incluir apodos, cumpleaños, el nombre de su calle o los nombres de los miembros de su familia.
- Revisar frecuentemente y cambar su contraseña con frecuencia para que sea más difícil que los hackers la rastreen.
- Utilice Autenticación por Múltiples Factores (MFA, en inglés) siempre que sea posible para que sea más difícil para los hackers obtener acceso no autorizado a las cuentas.

Cómo usar Wi-Fi seguramente

Los agentes e intermediarios no deben usar redes gratuitas de Wi-Fi cuando acceden a cuentas con información personalmente identificable (PII, en inglés) de los consumidores.

- Los hackers podrían estar al acecho en las redes gratuitas de Wi-Fi, tales como las redes de cafeterías, aeropuertos y hoteles. Agentes e intermediarios deben tener cuidado cuando usan Wi-Fi durante viajes o cuando trabajan a distancia. Se recomienda el uso de redes de Wi-Fi protegidas con contraseñas solamente.

Escenario: Taylor está viajando y el hotel donde se aloja ofrece Wi-Fi gratis. ¿Está bien que ella utilice esta red de Wi-Fi para acceder a su correo electrónico de la empresa y archivos protegidos de la empresa?

Respuesta: No. Al conectarse a redes de Wi-Fi gratuitas y no seguras, podría exponer su computadora a riesgos de seguridad innecesarios. Si ella necesita acceder o enviar información confidencial mientras usa redes de Wi-Fi públicas, debe usar un servicio de Red Privada Virtual (VPN, en inglés). También podría usar su dispositivo móvil para crear un punto de acceso de Wi-Fi que solamente ella y personas a quienes ella les autoriza acceso pueden usar.

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
CENTER FOR CONSUMER INFORMATION & INSURANCE OVERSIGHT

Cómo usar una Red Privada Virtual (VPN, en inglés)

Agentes e intermediarios que necesitan acceder a redes de Wi-Fi públicas frecuentemente deben considerar el uso de un servicio de VPN.

- Un servicio de VPN le permite conectarse a distancia a una red corporativa a través de un túnel seguro. Los usuarios pueden aprovechar de los servicios y protecciones internas que se ofrecen normalmente a los usuarios en el sitio, tales como el correo electrónico, depósitos de documentos confidenciales y cortafuegos de perímetro.
- Agentes e intermediarios deben fortalecer la VPN contra riesgos al reducir la superficie de ataque del servidor de VPN de las siguientes maneras:
  - Configurar criptografía y autenticación fuertes
  - Ejecutar solamente las funciones estrictamente necesarias
  - Proteger y monitorear el acceso de entrada y salida de la VPN

Para aprender más sobre las redes de VPN, consulte la hoja informativa sobre Cómo seleccionar y fortalecer las soluciones de VPN para acceso a distancia de la Administración de Seguridad Nacional (NSA, en inglés) y la Agencia de Seguridad Cibernética y Seguridad de Infraestructura (CISA, en inglés).

Cómo utilizar el cifrado

El cifrado es la mejor herramienta disponible para asegurar que la PII no pueda ser interceptada. El cifrado utiliza un código clave, que parece ser una serie aleatoria de letras, números y caracteres, para enviar información confidencial. Agentes e intermediarios deben usar el cifrado cuando envían documentos o correos electrónicos con la PII de consumidores u otra información confidencial. Para una guía detallada sobre cómo implementar el Cifrado, consulte los consejos de CISA sobre Cómo entender el cifrado.

> **Escenario:** Michael necesita enviar un archivo con PII del consumidor a su colega. ¿Cómo debe Michael enviar esta información a su colega?
>
> **Respuesta:** Primero, debe cifrar el archivo y enviar a su colega el código clave. Después, puede enviar el archivo cifrado a su colega por correo electrónico y su colega puede usar el código clave para acceder seguramente al archivo.

Para aprender otras mejores prácticas de seguridad cibernética, consulte esta Capacitación Basada en Computadora (CBT, en inglés) sobre el Mercado y la Seguridad Cibernética.