Trabajar desde casa:

Siete maneras fáciles de mantener su seguridad y la de su lugar de trabajo en línea

Agosto de 2022

No importa en qué parte del mundo se encuentre, es probable que el COVID-19 lo haya afectado de alguna manera. La pandemia ha enviado a los trabajadores y estudiantes a sus hogares, canceló eventos sociales como graduaciones y bodas, y puso en riesgo a las poblaciones masivas, especialmente a los ancianos e inmunocomprometidos.

A la luz de las restricciones en torno al COVID-19, muchos empleadores están pidiendo a sus empleados que trabajen desde casa. Si tiene la suerte de tener esta opción, es importante asegurarse de no ponerlo a usted ni a su lugar de trabajo en mayor riesgo de daño digital. Los ataques de suplantación de identidad (phishing) y ransomware están aumentando a medida que el COVID-19 se propaga; Cloudflare informó que los ataques cibernéticos crecieron un 37 por ciento en el Reino Unido en marzo de 2020.

> No le pediría a un médico o enfermera que trabaje sin equipo de protección personal. Usted tampoco debería hacerlo.

Prepárese: siga estos sencillos consejos para asegurar el trabajo que realiza en su hogar y en su red doméstica.

1. Mantenga a sus asistentes inteligentes fuera de la habitación mientras trabaja.

Los asistentes inteligentes siempre escuchan una palabra que los "despierte", como cuando su Amazon Echo comienza a prestar atención al audio cuando escucha "Alexa". Esto hace que los asistentes inteligentes sean un posible espía involuntario en conversaciones de trabajo confidenciales durante llamadas de video y telefónicas.

Una solución fácil es apagar o mover su asistente inteligente a otra habitación mientras mantiene sus conversaciones de trabajo. No lo necesitará para reproducir música, actualizar su lista de compras o hacerle una pregunta rápida durante sus llamadas. Si aún lo quiere cerca, asegúrese de desactivar el modo de audición o simplemente desenchúfelo durante las conversaciones. Si accidentalmente mantiene una conversación de trabajo dentro del alcance de un asistente inteligente, es posible que pueda eliminar la grabación de manera manual. Por ejemplo, puede

eliminar archivos de audio guardados de Siri en la "Configuración" de un dispositivo Apple y eliminar grabaciones de dispositivos Google Home. Tenga en cuenta que el proveedor de servicios aún puede mantener una copia de las grabaciones aunque el usuario las haya eliminado de su cuenta, y esto puede o no ser evidente para el usuario. Por lo tanto, es mejor errar por el lado de la precaución y desactivar los dispositivos durante las llamadas de trabajo como se describió anteriormente.

2. Use contraseñas únicas y un administrador de contraseñas.

Puede ser conveniente usar la misma contraseña para todo lo relacionado con el trabajo, pero esto pone a su lugar de trabajo en mayor riesgo de infracción de datos o pirateo de una cuenta. Una vez que alguien descubre su contraseña, puede acceder fácilmente a todos sus sistemas de trabajo y comprometer tanto sus datos como los de su empleador.

Dado que es difícil recordar contraseñas únicas para cada sistema de trabajo, considere usar un administrador de contraseñas. Esto le permite guardar todas sus contraseñas únicas en un solo lugar y, a menudo, incluye una función que ingresa automáticamente sus contraseñas al iniciar sesión en diferentes cuentas. El beneficio de esta solución es que solo debe recordar una contraseña maestra para acceder a todas sus cuentas. Muchos sitios y plataformas diferentes ofrecen pautas sobre cómo elegir el administrador de contraseñas adecuado para usted; eche un vistazo a algunos recursos aquí, aquí y aquí.

Cifrado de extremo a extremo (E2E) Este tipo de cifrado es altamente seguro y garantiza que solo el remitente y el destinatario puedan leer mensajes e información. Con el cifrado E2E, ni el servicio de comunicación puede acceder a la información.

3. Implemente la autenticación de dos factores siempre que sea posible.

Las contraseñas únicas y los administradores de contraseñas son útiles e importantes, pero puede y debe ir aún más lejos para proteger sus sistemas de trabajo. Si desea llevar la seguridad de la contraseña al siguiente nivel, averigüe cuáles de sus sistemas de trabajo ofrecen autenticación de dos factores.

Existen diferentes tipos de autenticación de dos factores. Una forma es que le envíen un código por SMS o correo electrónico cuando inicie sesión en un sistema de trabajo. Tenga en cuenta que este método no es seguro porque los SMS y el correo electrónico a menudo no están cifrados. Cuando su única opción es SMS, es importante que proteja su número de teléfono móvil de un ataque de intercambio de SIM. Algunos operadores móviles permiten a los usuarios habilitar un PIN o una contraseña secreta para evitar tales ataques.

Una mejor opción sería usar una aplicación de autenticación, que puede permitirle abrir la aplicación para demostrar que realmente está iniciando sesión, o puede generar diferentes códigos para que ingrese cada vez que inicie sesión en un sistema de trabajo. Los códigos a menudo tienen un límite de tiempo, por lo que incluso si un atacante tiene acceso a ellos a través de sus correos electrónicos o mensajes SMS, no podrán volver a usarlos más tarde.

Una opción aún mejor sería usar un token de autenticación física (por ejemplo, Yubikey). Esta es una pequeña memoria USB que puede colocar en su llavero y usar siempre que inicie sesión en un servicio que lo admita.

4. Opte por servicios en línea con cifrado fuerte.

El cifrado es la mejor manera de mantener sus datos seguros mientras trabaja desde su casa. Es una de las herramientas más sólidas que los sistemas en línea pueden usar para proteger la información del usuario, los datos y los sistemas de información central. Si no está utilizando sistemas protegidos por un cifrado seguro, sus propios datos y la información de su empleador corren un mayor riesgo de infracción de la seguridad.

> Los sistemas con cifrado seguro dificultan el acceso de otras personas a sus comunicaciones, aseguran que su contenido no sea legible incluso si alguien tiene acceso y ayudan a evitar que un atacante cambie la información.

Para los sistemas de trabajo nuevos y existentes, averigüe si un sistema en línea cifra automáticamente las comunicaciones y los datos al revisar sus declaraciones de privacidad y seguridad (también conocidas como "políticas"). También puede hacer una búsqueda simple en línea para ver si los servicios específicos usan el cifrado y lo que cifran, pero al igual que con todo lo que busca, asegúrese de que los recursos en los que confía sean creíbles y estén actualizados. El cifrado de extremo a extremo ofrece el mayor nivel de seguridad de las comunicaciones, así que asegúrese de que esté implementado antes de usar un nuevo software. A veces, las aplicaciones no activan el cifrado automáticamente, así que asegúrese de verificar que puede activarlo usted mismo. Asegúrese de que su teléfono inteligente, tableta, computadora portátil o cualquier otro dispositivo conectado que use esté cifrado y protegido con una contraseña segura y única siempre que sea posible.

5. Utilice una VPN, incluso en la red de su hogar.

Cuando inicia sesión en la red de su empleador mientras está en la oficina, es posible que no siempre piense en asegurarse de que tu conexión sea segura. Su empresa puede hacer parte de ese trabajo por usted a través de una intranet a la que se accede a través de un portal seguro. Pero cuando trabaja de forma remota, asegúrese de proteger todo su tráfico. Una red privada virtual (VPN) puede ser una herramienta adecuada.

Algunos empleadores pueden incluir VPN automáticamente en las computadoras portátiles de trabajo que los empleados se llevan a casa. Si está trabajando en una computadora personal o su computadora de trabajo aún no tiene una VPN, lea sobre cómo elegir y descargar una que asegure

su actividad en línea en los sistemas de su lugar de trabajo. Pero tenga cuidado con las VPN "gratuitas": si no cobran a sus usuarios, es posible que estén ganando dinero vendiendo sus datos personales, que pueden incluir su historial de navegación.

6. Actualice su software.

Es fácil hacer clic en "recordarme mañana" cuando su software le notifique las actualizaciones, pero las actualizaciones a menudo vienen con algo más que nuevas características. También incluyen correcciones a errores o vulnerabilidades de seguridad. Puede mejorar significativamente la seguridad de su computadora y de los datos al estar al tanto de las actualizaciones de software. Esto también mantendrá la red de su empleador más segura en el proceso.

Actualizar su software es aún más fácil cuando trabaja desde casa. Intente actualizar su software mientras se prepara en la mañana, en un descanso para almorzar o después de haber terminado su trabajo del día.

7. Haga una copia de seguridad de sus archivos.

Cualquiera puede ser víctima de un ataque ransomware. En este tipo de ataques, los delincuentes bloquearán el acceso a los datos, sistemas e información guardada, y mantendrán a la información como rehén hasta que la víctima pague un rescate. Si bien su lugar de trabajo siempre debe hacer una copia de seguridad de los archivos, debe ser muy diligente para proteger sus archivos mientras trabaja desde su casa.

Comience pidiéndole orientación a su empleador sobre cómo hacer una copia de seguridad de sus archivos cuando trabaje de forma remota. Esto se puede hacer usando un proveedor en la nube o un dispositivo de almacenamiento externo. Asegúrese de desconectar el dispositivo que contiene sus archivos con respaldo cuando no esté en uso para que pueda acceder a ellos si sus archivos originales están en peligro. La copia de seguridad debe estar cifrada y protegida con contraseña.

Para obtener más información sobre cómo puede mantenerse seguro en su lugar de trabajo, consulte nuestra hoja informativa de Next Century Cities.

Para obtener más información sobre de qué forma el cifrado cumple un papel crucial en la seguridad de nuestras actividades cotidianas, visite https://www.internetsociety.org/es/action-plan/2022/encryption/