

CYBER READINESS INSTITUTE

Las tres principales acciones que deben hacer y evitar los trabajadores remotos

Los ciberdelincuentes están utilizando la pandemia de la COVID-19 para aprovecharse de los trabajadores remotos, robando sus datos personales y profesionales. Para protegerse en este entorno de amenazas cada vez mayor y en la nueva realidad de la seguridad, a continuación se describe qué hacer y qué evitar para estar más preparados en el ciberespacio.

Desde el comienzo de la pandemia, todo el mundo ha aprendido a realizar tres acciones sencillas para mantenerse saludable. Lavarse las manos durante 20 segundos. No tocarse la cara. Mantenerse a dos metros de distancia. Está claro que supuso un cambio de comportamiento pero, probablemente, después de unas semanas ya se acostumbró. Ahora debe adoptar la misma actitud positiva y cambiar unos sencillos comportamientos con respecto a cómo usa su ordenador, tablet o smartphone.

La ciberseguridad requiere un esfuerzo comunitario de colaboración, similar a lo que se necesita para combatir el coronavirus. Así pues, comparta esta guía con sus compañeros de trabajo, familiares y amigos.

Qué hacer

- ☒ Utilizar contraseñas/frases de contraseña independientes para el trabajo y el uso personal; lo ideal sería que tuvieran 16 caracteres como mínimo
- ☒ Actualizar todo el software en todos los dispositivos periódicamente, lo ideal sería una vez por semana
- ☒ Usar la autenticación multifactor (siempre que sea posible)

Qué evitar

- ☒ Hacer clic en enlaces o archivos adjuntos de correos electrónicos de remitentes que no puede verificar
- ☒ Enviar información financiera o personal por correo electrónico hasta que haya llamado para verificar la transacción
- ☒ Utilizar dispositivos USB, ordenadores o Wi-Fi públicos (en la medida de lo posible)



Busque más consejos y herramientas del Cyber Readiness Institute (CRI) en las próximas semanas. Nos comprometemos a ser un recurso fundamental para ayudar a las pequeñas y medianas empresas (pymes) a compaginar el trabajo remoto y la ciberseguridad. Para acceder a guías adicionales sobre preparación cibernética para trabajadores remotos, visite <https://www.cyberreadinessinstitute.org/remote-work-resources>

Para obtener más información sobre nuestro Programa de preparación cibernética gratuito y cómo convertirse en un responsable cibernético, visite www.cyberreadinessinstitute.org.

Acerca del Cyber Readiness Institute

El Cyber Readiness Institute es una iniciativa sin fines de lucro que reúne a líderes empresariales de todos los sectores y zonas geográficas para compartir recursos y conocimientos que impulsan el desarrollo de herramientas de seguridad cibernética gratuitas para las pequeñas y medianas empresas (pymes). El Programa de preparación cibernética autodirigido y en línea se encuentra disponible en chino, inglés, francés, español, portugués, árabe y japonés. Póngase en contacto con nosotros si tiene preguntas, comentarios o casos de éxito (guides@cyberreadinessinstitute.org).