RECURSOS DE TRABAJO REMOTO DEL CRI

CYBER READINESS
INSTITUTE

Proteger a una plantilla remota

Los próximos meses supondrán un reto para casi toda la población mundial, ya que el coronavirus altera las rutinas cotidianas. Los niños y profesores colaborarán de forma remota, los trabajadores harán su trabajo desde casa y los propietarios de las empresas manejarán sus negocios desde su sala de estar, en lugar de la sala de juntas.

Por suerte, las tecnologías avanzadas de hoy en día nos permiten a muchos de nosotros continuar nuestro trabajo con mínimas interrupciones. La disponibilidad de potencia informática barata, el acceso a servicios en la nube y las conexiones a Internet de alta velocidad hacen que el trabajo remoto sea una alternativa viable que podría ayudar a frenar esta crisis sanitaria mundial.

Pero a medida que más personas se unen a la plantilla cibernética, debemos ser conscientes de que estamos expuestos a otros riesgos. A medida que todos los lugares de trabajo, grandes y pequeños, se vuelven remotos, todos debemos estar muy atentos a las buenas prácticas de higiene cibernética.

A continuación, presentamos algunos pasos fundamentales que todos podemos seguir para proteger nuestra seguridad en línea.

A medida que todos los lugares de trabajo, grandes y pequeños, se vuelven remotos, **todos debemos estar muy atentos a las buenas prácticas de higiene cibernética.**

guide@cyberreadinessinstitute.org

Aspectos básicos

Contraseñas

Las contraseñas siguen siendo la defensa de primera línea para acceder a datos y aplicaciones esenciales. El trabajo remoto aumenta la complejidad de confiar en la seguridad de la red doméstica de cada empleado.

- Asegúrese de que la contraseña del router doméstico no sea fácil de adivinar y no incluya su dirección o nombres personales.
- Active la autenticación de múltiples factores (contraseña + otro requisito, como un mensaje de texto) siempre que sea posible, además de incluir el acceso a los datos esenciales en las aplicaciones de la nube que se utilizan para compartir datos y documentos.

Parches

Los parches de seguridad del sistema operativo se deben aceptar y mantener actualizados.

- Exija a los empleados que tengan sus sistemas operativos configurados para que se actualicen automáticamente.
- Recuerde cada semana a los empleados que acepten todos los parches de seguridad relevantes.

Phishing

Cuantos más de nosotros estemos en línea durante las próximas semanas, más estafas en línea, ingeniería social y ataques de phishing podremos esperar. Seguramente los piratas informáticos y los ciberdelincuentes se aprovecharán de la preocupación por la propagación del virus y el deseo insaciable de noticias para engañar a las personas.

- "Coloque siempre el ratón" sobre el nombre del remitente del correo electrónico para determinar el verdadero origen del remitente y asegurarnos de que el nombre del remitente no sea fraudulento.
- La mayoría de los correos electrónicos de ransomware individuales son falsos. Si es posible, asegúrese de que un profesional de seguridad verifique los correos electrónicos antes de responderlos.
- Todas las empresas deben identificar un punto de contacto dentro de la empresa al que todos los empleados deben dirigirse cuando reciban un correo electrónico de phishing o un ransomware individual. Esta concienciación y comunicación informará a los empleados de las tácticas actuales de los actores maliciosos.

Distanciamiento social

El distanciamiento social también funciona en línea.

- Limite la cantidad de datos personales que comparte en las redes sociales para reducir su panorama de amenazas.
- Comparta todos los datos en línea a través de aplicaciones seguras en la nube. Las memorias USB no se deben utilizar para compartir datos, ya que pueden propagar malware.