Coronavirus y trabajo remoto: lo que necesita saber

1. Facilite a los usuarios comenzar.

Los usuarios remotos pueden necesitar configurar dispositivos y conectarse a servicios importantes (correo, servicios internos, fuerza de ventas, etc.) sin entregarlos físicamente al departamento de TI. Busque productos (de seguridad y de otro tipo) que ofrezcan un Portal de autoservicio (SSP) que permita a los usuarios hacer cosas por sí mismos.

2. Asegúrese de que los dispositivos y sistemas estén completamente protegidos

Vuelva a lo básico: asegúrese de que todos los dispositivos, sistemas operativos y aplicaciones de software estén actualizados con los últimos parches y versiones. Con demasiada frecuencia, el malware infringe las defensas de una organización a través de un dispositivo no protegido o sin protección

3. Cifrar dispositivos siempre que sea posible

Cuando las personas están fuera de la oficina, a menudo existe un mayor riesgo de pérdida o robo de dispositivos; por ejemplo, teléfonos que quedan en cafés, computadoras portátiles robadas de automóviles. La mayoría de los dispositivos incluyen herramientas de cifrado nativas como BitLocker; asegúrese de usarlas.

4. Cree una conexión segura de regreso a la oficina

El uso de una red privada virtual (VPN) garantiza que todos los datos transferidos entre el usuario doméstico y la red de la oficina estén encriptados y protegidos en tránsito. Además, facilita a los empleados hacer su trabajo.

5. Escanee y proteja el correo electrónico y establezca prácticas saludables

El trabajo a domicilio probablemente conducirá a un gran aumento en el correo electrónico, ya que las personas ya no pueden hablar con sus colegas en persona. Los delincuentes son

conscientes de esto y ya utilizan el coronavirus en correos electrónicos de phishing como una forma de atraer a los usuarios a hacer clic en enlaces maliciosos. Asegúrese de que su protección de correo electrónico esté actualizada y concientice sobre el phishing

6. Habilite el filtrado web

La aplicación de reglas de filtrado web en los dispositivos garantizará que los usuarios solo puedan acceder al contenido apropiado para el "trabajo" mientras los protegen de sitios web maliciosos.

7. Habilite el uso del almacenamiento en la nube para archivos y datos

El almacenamiento en la nube permite que las personas aún tengan acceso a sus datos si su dispositivo falla mientras trabajan de forma remota. No deje archivos y datos en la nube desprotegidos y accesibles para nadie. Como mínimo, los empleados deben autenticarse con éxito. La autenticación de múltiples factores lleva eso un paso más allá.

8. Administre el uso de almacenamiento extraíble y otros periféricos

Trabajar desde casa puede aumentar las posibilidades de que las personas conecten dispositivos inseguros a la computadora de su trabajo: para copiar datos de una memoria USB o para cargar otro dispositivo. Teniendo en cuenta que el 14% de las amenazas cibernéticas ingresan a través de dispositivos USB / externos *, es una buena idea habilitar el control del dispositivo dentro de su protección de punto final para gestionar este riesgo.

9. Controlar dispositivos móviles

Los dispositivos móviles son susceptibles de pérdida y robo. Debe poder bloquearlos o borrarlos si esto sucede. Implemente restricciones de instalación de aplicaciones y una solución Unified Endpoint Management para administrar y proteger dispositivos móviles.

10. Asegúrese de que las personas tengan una manera de informar problemas de seguridad

Con el trabajo a domicilio, las personas no pueden dirigirse al equipo de TI si tienen un problema. Brinde a las personas una forma rápida y fácil de informar problemas de seguridad, como una dirección de correo electrónico fácil de recordar.