IJALTI CLUSTER MANAGER

CSW Guadalajara

MEDIDAS DE SEGURIDAD PARA TELETRABAJO

1. **AVERIGÜE SI SU ORGANIZACIÓN** tiene reglas o políticas para el teletrabajo y, de ser así, asegúrese de leerlas y cumplirlas. Por ejemplo, puede estar bien que use su propia computadora para leer el correo electrónico de la empresa, pero no para acceder a datos confidenciales del cliente.

2. **PROTEJA LAS COMUNICACIONES** de su computadora contra escuchas. Si utiliza Wi-Fi (redes inalámbricas) en casa, asegúrese de que su red esté configurada de forma segura. Específicamente, observe si está utilizando la seguridad "WPA2" o "WPA3", y asegúrese de que su contraseña sea difícil de adivinar. Si no está seguro de cómo hacer esto, puede encontrar un video o lista de verificación en línea haciendo una búsqueda de su marca y modelo de enrutador Wi-Fi.

3. **SI SU ORGANIZACIÓN** tiene una VPN (red privada virtual), úsela en su dispositivo de teletrabajo para una mayor protección (las reglas o políticas de teletrabajo de su organización probablemente le dirán si la tiene). Si no es así, considere usar su propia VPN, para lo cual puede encontrar numerosos proveedores en línea.

4. **SI ESTÁ UTILIZANDO** su propia computadora o dispositivo móvil (algo no proporcionado por su organización) para el teletrabajo, asegúrese de haber habilitado las funciones básicas de seguridad. Simplemente habilitar la función de PIN, huella dactilar o identificación facial evitará que las personas entren en su dispositivo si se aleja de éste. Cualquier PIN o contraseña que use debe ser difícil de adivinar.

5. **MANTENGA SUS COMPUTADORAS** y dispositivos móviles parcheados y actualizados. La mayoría ofrece una opción para verificar e instalar actualizaciones automáticamente. Habilitar esa opción puede ser una buena idea si no desea buscar actualizaciones periódicamente.

6. **SI OBSERVA ACTIVIDAD** inusual o sospechosa en cualquier dispositivo que esté utilizando para teletrabajar (computadora, dispositivo móvil o red doméstica), solicite ayuda, más vale prevenir que curar. Póngase en contacto con la mesa de ayuda o el centro de operaciones de seguridad de su organización para informar la actividad.

ESTÉ ATENTO a los intentos de ingeniería social, como correos electrónicos de phishing o estafas telefónicas relacionadas con el teletrabajo. La ingeniería social es cuando alguien intenta engañarte para que hagas algo o regale información personal. Los estafadores y los delincuentes utilizan todos los eventos importantes para idear nuevos esquemas, y con usted y otros teletrabajando de repente, los atacantes intentarán aprovechar este entorno cambiante. Si recibe correos electrónicos de cuentas desconocidas con archivos adjuntos extraños, si las personas llaman para reclamar ser personal técnico y le solicitan sus contraseñas o le dicen que vaya a un sitio web para “escanear” su computadora, si recibe solicitudes de reuniones web inusuales, no lo haga. Dude en hacer preguntas y verificar las cosas por teléfono u otros medios antes de continuar.

Fuente: NIST (www.nist.gob)