CEO Confederación empresarial de Ourense
Praza das Damas 1
32005 Ourense
Tel.: 988 391 110
Fax: 988 391 957
ceo@ceo.es
www.ceo.es

Consejos de ciberseguridad para el teletrabajo

a) No te conectes a redes públicas.

Este consejo es el top number one en lo relativo a ciberseguridad. Conectarse a redes públicas implica ceder datos de tu empresa; además son fácilmente hackeables por usuarios mal intencionados. Si no tienes una VPN (red privada virtual) segura en tu casa, conéctate desde el teléfono móvil. Eso sí, evita redes wifi públicas.

b) Asegúrate de que tu equipo está protegido.

Al igual que harías con el ordenador de tu empresa, debes asegurar que el ordenador desde el que te conectas también está protegido. Utiliza antivirus actualizados, y si puedes, ahórrate problemas trayéndote el ordenador de tu puesto de trabajo a casa.

c) Ojo con el phising.

Aunque parezca mentira muchos hackers ven esta situación desesperada como oportunidades para encriptar todos tus datos. **Así que mucho cuidado de no abrir o interactuar con contenido multimedia recibido de remitentes sospechosos.** Ten muy claro a quién (qué dirección email) solicitas contenido y qué tipo de contenido.

d) Accede a páginas con conexión https..//

Esa "s" final nos indica que el lugar o página web es segura.

e) Actualiza contraseñas.

Haz que sean robustas (mayúsculas, minúsculas, números y signos) y que solo las conozcas tú. ¿A qué no dejarías la puerta de tu casa abierta o sin cerrar con llave? Pues lo mismo sucede con tu equipo de trabajo.

f) Prevención.

Y por último, como es mejor prevenir que lamentar, realiza copias de seguridad de la información para, en caso de que la pierdas, sea sencillo recuperarla. Y así, te ahorrarás algún que otro susto.

g) Período de implantación y pruebas.

Implantar el teletrabajo en la empresa no es una cuestión que se realice rápidamente porque se deben valorar diferentes escenarios y configuraciones. Una implementación demasiado rápida del teletrabajo, sin respetar las recomendaciones de seguridad, puede suponer la apertura de la puerta de la empresa a los ciberdelincuentes o el vernos envueltos en una brecha de información accidental. Un incidente de seguridad ocasionado por habilitar el teletrabajo de una manera insegura puede provocar unas pérdidas económicas y reputacionales mucho peores que no permitirlo y dejar de trabajar unos días.

h) Carga de trabajo.

Otro aspecto a tener en cuenta, que afecta sobre todo a grandes organizaciones, es la carga de trabajo que ocasione en los sistemas internos de la empresa el teletrabajo. Cuando una cantidad más o menos grande de empleados realiza teletrabajo se pueden producir comportamientos inestables del sistema. Una buena práctica, siempre que sea posible, es realizar pruebas de carga en escenarios simulados antes de permitir teletrabajar a un gran volumen de empleados.

i) Actualiza los sitemas.

Mantén todos los sistemas y aplicaciones actualizados", tanto las puramente profesionales como las de nivel usuario, ya que pueden convertirse en puerta de entrada para los ciberdelincuentes.