arsys

Principales medidas de seguridad para los teletrabajadores

Conceptos de seguridad y consejos para teletrabajar con total seguridad. Desafíos de seguridad durante la cuarentena por COVID-19

A raíz de la actual **crisis sanitaria** causada a lo largo y ancho de todo el mundo por el **COVID-19**, miles de empresas han tenido que desplegar en tiempo récord puestos de trabajo remotos para sus trabajadores. El **teletrabajo** está a la orden del día y, si todo va bien, una vez que termine la pandemia y salgamos de nuestro confinamiento podemos asistir a la implantación de este tipo de trabajo como herramienta habitual en las empresas.

Durante las últimas semanas hemos estado repasando muchos conceptos relacionados con el teletrabajo, desde cómo planteárselo desde un punto de vista empresarial hasta una serie de webinars para desarrollar cualquier solución que nos interese durante este confinamiento; pasando por las herramientas que nos facilitan la "vida en remoto", como los escritorios virtuales o con Office 365.

Hoy hablaremos de los **riesgos de seguridad a los que se enfrenta el teletrabajador** y cómo podemos hacerles frente para evitar males mayores.

Riesgos de ciberseguridad para los teletrabajadores

Muchos trabajadores se enfrentarán al trabajo en remoto por primera vez. Es más, muchas empresas se habrán planteado esta medida en serio por primera vez, y eso significa que puede que no estén del todo preparadas para «blindar» los puestos remotos, y que los trabajadores no conozcan las principales precauciones de seguridad en esta modalidad de trabajo.

Algunas de las actividades maliciosas a las que se enfrentan los teletrabajadores son tan conocidas como los ataques de phishing o la violación y robo de datos confidenciales, entre otras.

Evitar WiFi público

Es crítico **evitar el uso de redes WiFi públicas** cuando se trabaja de forma remota. Estas WiFi públicas constituyen una invitación a los ciberdelincuentes porque son redes inseguras donde se hace muy difícil detectar su presencia. El ataque más típico en estas redes WiFi son los conocidos como *'Man-in-the-Middle'*. Por otro lado, lo lógico es utilizar una red de Internet doméstica (la propia, y no cualquiera de las otras que detectan nuestros equipos), aislada y convenientemente protegida, para trabajar. De esta manera se mantendrán más seguros los dispositivos personales.

Establecer contraseñas seguras

Esta es una medida básica de seguridad, teletrabajemos o no. Casi todo está asegurado mediante el uso de **contraseñas** (aunque empiezan a ser más habituales los sistemas de autenticación basados en parámetros biométricos, y la **autenticación en dos pasos**, que veremos más abajo). **Las contraseñas seguras, únicas y complejas** son muy importantes si queremos evitar la violación de datos y otras actividades maliciosas.

Utilizar VPN corporativa

Las **VPN** o redes privadas virtuales constituyen una forma rápida, segura y fiable de compartir información a través de redes informáticas abiertas o no seguras, como Internet. Las VPN usan tráfico encriptado a través de la línea de comunicaciones, lo que hace que sea imposible que los ciberdelincuentes lo descifren y, por lo tanto, se protege la información en tránsito.

Sistema Operativo y antivirus, siempre actualizados

Todos los programas instalados en los dispositivos de los empleados deben estar correctamente actualizados, pero muy especialmente sistema operativo y software antimalware. Este último es muy importante para mantenerse alejado del cualquier tipo de software malicioso como virus, gusanos, troyanos, spam...

Habilitar la autenticación de dos factores

La **autenticación de dos factores** o 2FA añade una capa de seguridad adicional a la red. Normalmente, se requiere al usuario que tenga dos de tres tipos de credenciales: algo que conozca (por ejemplo, una contraseña); algo que tenga físicamente (por ejemplo, una tarjeta de coordenadas); y algo que sea «biométrico», como una huella digital registrada, reconocimiento facial… De esta manera, para acceder a las cuentas o servicios hay que introducir correctamente dos de estos parámetros, lo que hará mucho más difícil que un ataque surta efecto.

Configuración del firewall

Los **firewalls** son, básicamente, aplicaciones software que ayudan a proteger los dispositivos contra amenazas. Habitualmente, lo que hacen es filtrar las comunicaciones y mantener a los extraños fuera de la red que protegen. Existen dos tipos principales de firewalls: los de red y los basados en host.

Establecer el bloqueo de pantalla en los dispositivos

Aunque si trabajamos desde casa puede ser menos relevante, es conveniente acostumbrarse a ocultar el trabajo de la vista de otras personas que estén a nuestro alrededor cuando estamos fuera de la oficina. E incluso en nuestro lugar de trabajo habitual también puede ser conveniente. Configurar el sistema para que la pantalla se bloquee automáticamente tan pronto como estemos inactivos unos segundos (los suficientes como para que no se nos apague mientras leemos un documento) es un plus de seguridad.

Cifrado de correos electrónicos

Es una gran barrera de seguridad para evitar que alguien intercepte nuestros emails de trabajo que, posiblemente, contienen información sensible.

Estos consejos sirven hoy, en pleno confinamiento, y siempre. Lo más importante a la hora de teletrabajar es disponer de unas directrices sólidas por parte de la empresa; disponer de las mejores herramientas y soporte posible; y ser conscientes de las amenazas a la seguridad que podemos sufrir. No estamos protegidos por la gran red interna de la empresa, sino que estamos en nuestras casas, y por eso es importante aprender cómo protegernos.

arsys

www.arsys.es

www.facebook.com/arsys.es

twitter.com/arsys

www.linkedin.com/company/arsys-internet/