Publicado en Madrid el 18/06/2020

Las cuatro claves para teletrabajar en casa de forma cibersegura

La compañía de ciberseguridad S2 Grupo destaca que, tras la actual crisis sanitaria, el teletrabajo continuará creciendo en España y es fundamental que tanto empresas como empleados refuercen sus medidas de seguridad para evitar ser víctimas de ciberdelincuentes. Los expertos de la empresa recomiendan cambiar las contraseñas del router, aprender a distinguir ataques de ingeniería social o configurar los equipos informáticos con una sesión destinada exclusivamente al ámbito laboral

Desde que se decretó el estado de alarma, España ha vivido un crecimiento vertiginoso del teletrabajo. En este contexto, desde un comunicado S2 Grupo destaca que es fundamental que tanto empresas como empleados se conciencien de que deben implementar medidas que les ciberprotejan en esta modalidad del desarrollo de su negocio.

“Todo lo que se ha vivido en este tiempo, ha puesto de manifiesto cómo los ciberdelincuentes están al acecho para aprovechar cualquier situación que les permita ganar dinero que, al final, es su objetivo. Más gente teletrabajando supone más gente y empresas con información jugosa en la red y, por tanto, mayor número de posibles candidatos a víctimas de estas redes de delincuencia”, ha explicado José Rosell, socio-director de S2 Grupo.

“No obstante, hay que tener en cuenta que el teletrabajo puede tener muchísimas ventajas y que es una tendencia que cada vez se va a quedar más instalada en el sistema laboral español. Por tanto, es necesario que las empresas implanten medidas que ciberprotejan la continuidad de su negocio teniendo en cuenta todos los puntos por donde podrían entrar un ciberdelincuente y, por supuesto, que los empleados se conciencien y conozcan cómo blindarse frente a la acción de éstos”, ha enfatizado Miguel A. Juan, socio-director de S2 Grupo

Si bien la implantación de sistemas VPN u otro tipo de software similar es una de las medidas más importantes que deben implantar el equipo de informática de las empresas, también hay algunas medidas muy importantes que pueden poner en marcha los empleados para convertir su hogar en un lugar de trabajo ciberseguro.

En primer lugar, hay que proteger la conexión a Internet. Desde S2 Grupo insisten en que aunque la contraseña que aparece en el router es larga y parece compleja, es muy insegura, porque puede ser averiguada fácilmente. "Por tanto, es esencial cambiar la clave que aparece por defecto para acceder a Internet", enfatiza el comunicado.

Por otro lado, hay que preparar los equipos informáticos para el teletrabajo. Si el ordenador personal es utilizado por toda la familia, es aconsejable crear un usuario exclusivamente para el trabajo. Esto permite protegerse con una clave y que la información que contiene no se vea afectada por la acción de otro miembro de la familia, ya que por error puede verse manipulada, borrada, consultada, etc.

Además, S2 Grupo aconseja que este nuevo usuario no tenga permisos de administrador. De esta forma, tendrá una funcionalidad limitada y esto protegerá de instalaciones no deseadas, lo que sirve para frenar la acción de un malware, por ejemplo, porque cuando se intente instalar el software no lo podrá hacer sin la contraseña de un usuario con permiso de administrador.

En tercer lugar, es fundamental instalar un antivirus y mantenerlo actualizado. A la vez, hay que mantener actualizados el sistema operativo y los programas instalados para protegernos de posibles fallos de seguridad.

Como cuarta medida, hay que aprender a reconocer ataques de ingeniería social. Hay que tener en cuenta que los ciberdelincuentes se aprovechan de situaciones puntuales para engañar a sus víctimas y que realicen alguna acción. Los ejemplos más comunes son confirmar datos bancarios, meter la contraseña para certificar un servicio, rellenar un formulario, etc. Éstos hacen que al clicar en un enlace, se descargue malware. Esto es un ataque de ingeniería social y durante esta crisis sanitaria S2 Grupo ha detectado muchos ejemplos de este tipo de ataques como mensaje de correos que alertan de un próximo envío; de Netflix; sobre la declaración de la Renta; descuentos en supermercados; o devolución de facturas, entre otros.

"Es muy importante para no caer en estas trampas reconocer una web falsa. Esto suele quedar evidenciado en que la URL no comienza por https o porque no se puede ver un candado cerrado al lado. La mejor forma de ser precavidos es escribir la dirección que se quiere visitar en el navegador en lugar de clicar en enlace", finaliza el comunicado de la empresa española especializada en ciberseguridad S2 Grupo.

Datos de contacto:
lununcan
667574131

Nota de prensa publicada en: Madrid

Categorías: Nacional Emprendedores E-Commerce Ciberseguridad Recursos humanos Otros Servicios