Evita hackeos: consejos de ciberseguridad para minimizar los riesgos al hacer home office

18/07/2020

Tras el **brote de COVID-19 en México**, muchas empresas decidieron que sus empleados debían **trabajar desde casa** como una medida sanitaria para mitigar los contagios de la enfermedad. Si bien en la actualidad se están reabriendo las actividades y una parte de los empleados **han vuelto a sus oficinas**, los que se mantienen en casa deben estar alerta de los **posibles riesgos en cuanto a su ciberseguridad**.

Y es que el hecho de **modificar el espacio de trabajo** también conlleva una **serie de cambios** en cuanto a las **medidas de seguridad** que se deben establecer con el fin de **minimizar los riesgos tanto para la compañía como para las personas**.

Kaspersky Lab, una de las empresas más importantes de ciberseguridad a nivel mundial, señala que el **riesgo de robo o filtración de datos** durante el trabajo remoto es algo factible, pues los empleados **trabajan con un proveedor de servicio de** internet, del cual no se sabe mucho acerca de sus **filtros de seguridad**.

Además, según un análisis desarrollado por esta empresa y la consultora de estudios de mercado CORPA, señala que el **25% de los latinoamericanos no cuenta con un computador portátil destinada sólo para trabajar** y, si lo tiene, el 30% de ellos se conecta a una **red pública** cuando está **fuera de la oficina**. De éstos, únicamente el 8% asegura que se conecta a una **red virtual privada (VPN)**.

La seguridad en las redes puede ser uno de los temas más complejos para los empleados que trabajan desde casa. (Foto: Steve Marcus/Reuters)

Ante ello es importante siempre **conectarse a una VPN de confianza** y así establecer un **canal de comunicación seguro para los datos entre la estación de trabajo y al infraestructura de la corporación**. Aunado a ello, también **recomiendan prohibir conectarse a redes externas con recursos de la empresa**.

En este sentido, cambiar la contraseña del wifi es uno de los **consejos más importantes que suelen dar los expertos en el tema**, pues al realizar esta acción se establecen **medidas de seguridad más fuertes**, además de que proporcionan **mayor confianza** a los usuarios.

Asimismo, si se va a utilizar la **PC familiar**, será necesarios crear un nuevo usuario para uso laboral, y **evitar que tenga privilegios de administrador.** No es conveniente **compartir el usuario común** de la computadora para **realizar tareas del trabajo**.

Otro de los **posibles ataques** que se podrían dar durante esta dinámica es la de los **correos electrónicos que buscan estafar**, también conocidos como **phishing**. El hecho de que **no haya contacto físico** con las personas puede provocar que sea **complicado detectar estos mensajes** que buscan sacar **datos personales** o de la propia **empresa**.

(Foto: Shutterstock)

Ante esto, los especialistas recomiendan usar exclusivamente el **correo corporativo**, lo cual haría más sencillo **detectar los intentos de los cibercriminales de hacerse pasar por otro empleado**. Asimismo, contar con servidores de correo electrónico capaces de detectar **manipulaciones** en los mensajes también es una buena inversión de cara a este entorno.

Respecto a las **herramientas de colaboración**, como **documentos compartidos**, es importante que se **configuren correctamente**, pues en caso de hacerlo de manera inapropiada, podrían ser fáciles de encontrar a partir de **búsquedas sencillas y convertirse en una fuente de filtración**. Este punto también aplica con los datos almacenados en la nube.

Otros elementos fundamentales son tener tanto los **equipos** como las **aplicaciones actualizadas** y **realizar copias de seguridad de la información crítica** en discos externos, los cuales no deben estar conectados a los aparatos las **24 horas**, sino exclusivamente en el momento en que se usan para **transferir la información**.

Por último, una de las recomendaciones más relevantes es que los empleados tengan instalado un **software antivirus doméstico**, sin importar que se trata de una solución **gratuita**. "Lo idóneo es que permitas que estos dispositivos se conecten a tus redes cooperativas **una vez que se haya garantizado la instalación de una solución de seguridad**", concluye Kaspersky.