COVID-19: Con defensas bajas en ciberseguridad ante home office

El teletrabajo, también conocido como **home office,** se ha vuelto una alternativa para que colaboradores y empresas mantengan sus **actividades habituales** ante la pandemia.

Esto, se ha implementado como una medida de precaución, para cumplir a tiempo con las medidas preventivas de distanciamiento social frente al **COVID-19.**

Sin embargo, con esto, llegan **nuevos virus** que afectan a los usuarios de internet: **los ciberataques.** Los cuales han ido en aumento aprovechándose de la existencia de la nueva cepa, afirman especialistas en seguridad informática.

Félix Barrio, director del **Hub de Ciberseguridad del Tec de Monterrey,** comparte las consideraciones básicas que deben tomar en cuenta empresas y empleados en este aislamiento.

“El mayor reto que tienen en general todas las empresas, es el teletrabajo, esto está suponiendo un escenario nuevo en el que hay que hacer una labor de preparación,

***“Por desgracia, 46% de los ataques cibernéticos se están dirigiendo a pequeñas y medianas empresas** que son las más vulnerables”, compartió.*

width="1920" loading="lazy">

Estas son algunas prácticas muy básicas pero que desgraciadamente, las seguimos sin llevar a cabo en nuestra vida cotidiana:

1. Cambiar las contraseñas

“Se ha dicho mil veces, pero hay que cambiar las contraseñas de manera periódica, hacer contraseñas muy robustas que combinen un número suficiente de letras, números, símbolos especiales, mayúsculas y minúsculas para dificultar que un ciberatacante pueda romper la contraseña”.

2. Cuidar el almacenamiento de los datos

“Como cada vez hay más tipos de virus que van destinados a hacer ***ransomware****, es decir a secuestrar tu equipo encriptando todos los datos que hay en él,* ***tenemos que tener la precaución de tener una copia de seguridad de nuestros equipos en algún dispositivo diferente al que pueda estar en peligro,***

“Eso nos permitirá que ***en caso de que perdamos el control de nuestro dispositivo, o se vea infectado, podamos para recuperar nuestro trabajo e información*** *que muchas veces puede ser vital para una empresa”, destacó.*

3. Como organización, hacer un análisis de riesgos

“Para las empresas, bancos, o cualquier tipo de organización, hacer un análisis de riesgos, con ayuda de un profesional de ***ciberseguridad*** *para conocer a que se enfrentan, qué necesidades van a tener* ***para estar protegidos para articular un sistema de teletrabajo lo menos vulnerable posible***.

“Eso es algo fundamental que por desgracia las pequeñas y medianas empresas tienen más dificultades y les supone un mayor reto que a las grandes”, comentó.

4. Dotar el teletrabajo de un canal cifrado mediante una red VPN

*“Mediante una red virtual que esté securizada, eso implica que t****anto trabajador desde su hogar como la empresa, tienen que tener un sistema doble de conexión cifrada,*** *mediante esa VPN que impida que un tercero pueda acceder y robar los datos que se están transfiriendo entre uno y otros.*

“Eso evidentemente, es una de las necesidades que se va a tener primero para que realmente tú puedas hacer el teletrabajo de una manera securizada con tu empresa”, enfatizó.

Un ejemplo de esto, podría ser que cuando los empleados se conecten a su centro de trabajo, lo hagan mediante una autenticación reforzada, a la vez que meten su contraseña de usuario reciben un mensaje por ejemplo, en su celular, que se asegura que son ellos.

5. Concientización

“Debemos tener claro a qué tipo de riesgos nos estamos enfrentando no solo nosotros, sino para nuestra empresa si descargamos archivos adjuntos que vengan en correos electrónicos que no nos den confianza,

“Evitemos hacer algún tipo de práctica no aconsejable, *por ejemplo, conectarnos desde equipos que no tengan antivirus, el software no esté actualizado, todo eso son elementos que son posibles si los teletrabajadores reciben una suficiente guía de buenas prácticas para que nuestra labor dentro de la empresa en remoto sea segura”.*

“Es importante tomar en cuenta estas recomendaciones básicas en materia de ciberseguridad de manera urgente”, concluyó.

SEGURO QUERRÁS LEER: