Publicado en Madrid el 02/04/2020

Aumentan los intentos de ciberataques durante el confinamiento: ¿cómo teletrabajar con seguridad?

Ante el incremento que las compañías de ciberseguridad han detectado estas semanas de ciberataques contra empresas públicas y privadas, la división IT de Spring Professional ha diseñado un decálogo con consejos útiles para los teletrabajadores

En estas semanas en los que miles de trabajadores en España se ven abocados a teletrabajar desde el confinamiento, muchos de ellos por primera vez (hasta hace unos meses solo el 7,9% de los españoles había trabajado en remoto de manera habitual[1]), es un momento delicado para ser víctimas de posibles ciberataques si las empresas y los trabajadores no han seguido un mínimo de instrucciones básicas pero importantes para garantizar esa seguridad.

Es por eso que la división IT de Spring Professional, la firma del grupo Adecco especializada en consultoría de selección para mandos intermedios y directivos, ha elaborado un sencillo decálogo con consejos y pautas para poder teletrabajar de manera segura.

Tal y como explica Sara Álvarez, IT manager de Spring Professional: “es momento de no bajar la guardia en lo que a ciberseguridad se refiere. Si esta es un área cada vez más importante en el día a día de las empresas, ahora lo es más, con muchas compañías viéndose en la necesidad de instalar una política de teletrabajo masivo que, en muchos casos, no estaba en funcionamiento para el 100% de los empleados de la plantilla. Aunque las compañías están trabajando al 200% para asegurar que ese teletrabajo es efectivo y no supone una brecha en la seguridad de la empresa, conviene que los trabajadores que están operativos en sus hogares adopten algunas medidas sencillas que contribuirán a garantizar esa ciberseguridad”.

Como han recogido diversas fuentes de la Policía Nacional y del Instituto Nacional de Ciberseguridad en España, estas semanas se han detectado intentos de ciberataques en los que el señuelo era el Covid - 19, aprovechando el auge informativo que la pandemia está teniendo en la sociedad.

Pero evitar esos ataques puede ser sencillo con algunas pequeñas instrucciones y consejos de seguridad.

Hacia un teletrabajo seguro

Spring Professional ha ideado un sencillo decálogo con consejos para teletrabajar de manera segura:

Primero que todo, y aunque parezca obvio, es bueno utilizar siempre los equipos que la propia empresa ha facilitado para realizar ese trabajo en remoto (si han dotado de un portátil, teléfono de empresa, etc.).

Además, asegurar de que dichos equipos tengan antivirus y las aplicaciones actualizadas, de manera

que todos los equipos y aplicativos cuenten con los parches de seguridad correspondientes.

A la hora de navegar por Internet, es recomendable acceder solamente a sitios web que utilizan el protocolo HTTPS, pues la 's' final indica que es un sitio seguro ya que ofrece tres capas de seguridad: cifrado en las comunicaciones, integridad de los datos y autenticación.

Hay que evitar utilizar redes Wi-Fi de terceros o públicas que pueden ser más vulnerables a la hora de no cumplir los protocolos y convertirse en una posible brecha para la seguridad.

Siempre que sea posible, es mejor utilizar la conexión VPN para acceder a los servidores de la empresa. Esta conexión es privada, con acceso protegido y la información que se envía y a la que se accede suele estar cifrada, por lo que la seguridad es mayor.

Se recomienda cambiar cada poco tiempo la contraseña de conexión Wi-Fi y del router para asegurar que la conexión con la que se trabaja sea lo más segura posible.

También se aconseja realizar copias de seguridad de manera periódica para evitar que la información se pierda, ya sea por accidente o por infecciones de ransomware (es decir, malwares que bloquean el equipo informático o el acceso a datos del sistema y que para poder recuperar exigen un pago económico por parte de los hackers, es una técnica que también se conoce como el secuestro de datos).

Activar el bloqueo automático de los dispositivos y no compartir la contraseña con los demás miembros de la familia es otra práctica recomendable cuando se trabaja desde casa.

Además, es muy importante extremar el cuidado con el phishing, y no acceder a enlaces provenientes de correos sospechosos. Si se recibe un archivo adjunto, se recomienda verificar la extensión del archivo (.docx, .pdf, .xlsx) y comprobar que no presente ningún patrón inusual (.exe, .vbs, .ps1, .jar, etc.). El phishing es un tipo de ataque en el que el hacker, valiéndose habitualmente del envío de correos electrónicos o SMS provenientes de "fuentes fiables" (se pueden hacer pasar por bancos, empresas energéticas, servicios públicos…) solicitan datos personales o credenciales de carácter confidencial.

Por último, es muy útil utilizar la nube corporativa para guardar información y documentos y así evitar almacenar información sensible en dispositivos USB o personales.

[1] Según se recoge en el Monitor Adecco de Oportunidades y Satisfacción en el Empleo: https://www.adeccogroup.es/wp-content/uploads/2020/03/NdP-La-cifra-de-espan%CC%83oles-que-teletrabajan-crece-y-alcanza-el-79-de-ocupados-ma%CC%81s-de-15-millones-de-personas-01.pdf

Datos de contacto:
Adecco
914325630

Nota de prensa publicada en: Madrid

Categorías: Nacional Emprendedores E-Commerce Ciberseguridad Recursos humanos

NotasdePrensa
https://www.notasdeprensa.es