Cómo gestionar la ciberseguridad en pleno auge del teletrabajo

PA DIGITAL ofrece unos sencillos consejos para reforzar la ciberseguridad desde casa

En la Unión Europea, según un informe de Eurostat apenas **el 5,2 % de las personas de entre 15 y 64 años teletrabajaba desde casa en 2018.** Sin embargo, la crisis del coronavirus ha disparado forzosamente el número de compañías que han recurrido al teletrabajo. Los ciudadanos deben quedarse en casa, por lo que trabajar desde el hogar se ha convertido en la única opción para mantener la actividad empresarial.

El confinamiento ha hecho que tener presencia digital sea más importante que nunca: **el entorno online es el canal principal para comunicarse con los consumidores**. Los clientes no pueden acudir a los establecimientos físicos, pero **siguen informándose, haciendo búsquedas y consultando las redes sociales**.

No obstante, el teletrabajo también obliga a vigilar más de cerca la seguridad, ya que **los empleados tienen que trabajar sin los recursos de la compañía**. Por eso, muchos pequeños negocios han tenido que **plantearse si su política de ciberseguridad es adecuada** para afrontar una situación como la actual.

Según datos que maneja www.padigital.es, la empresa líder en soluciones de marketing digital para pymes y autónomos, las ciberamenazas que más están proliferando en las últimas semanas debido a la situación de teletrabajo de muchos trabajadores son:

Phishing. Se trata del ataque más utilizado actualmente, este método consiste en el envío de emails a nuestro correo electrónico, mensajes de Whatsapp o SMS haciéndose pasar por una persona o empresa de confianza suplantando su identidad para pedirle, normalmente, hacer click en un enlace o en un archivo y de esta manera obtener información sensible como pueden ser nuestras credenciales, datos de las tarjetas de crédito o números de cuentas bancarias.

Ataques a la Nube. Mediante estos ataques a la nube, lo que los ciberdelincuentes buscan es el robo de nuestras credenciales y de esta forma poder acceder a información sensible de la empresa.

Criptojacking. En este caso el ataque no trata de hacerse con nuestros datos, si no utilizar los recursos de nuestros ordenadores. Cuando alguien hace una operación con criptomonedas esta conlleva una serie de problemas matemáticos muy complejos que verifican que la transacción es segura. Hay personas que cobran por realizar estas operaciones, que se conocen como "minado de criptomonedas" que consumen muchos recursos tanto informáticos como eléctricos. Al igual que con el phishing, cuando hacemos click en un enlace malintencionado o instalamos una aplicación no oficial que contiene malware, el ciberdelincuente puede tomar el control de nuestro ordenador para realizar estas operaciones de minado, consumiendo nuestros recursos, que más tarde cobrará.

Ransomware o "secuestro de datos". Es cuando un ciberdelincuente se hace con el control de un dispositivo y "secuestra" la información cifrándola, esta información no se puede leer sin una contraseña que la descifre, contraseña que nos proporcionará a cambio de un rescate económico.

Por estos motivos, PA DIGITAL da algunos consejos para reforzar la ciberseguridad desde casa y reducir al mínimo los riesgos por el teletrabajo:

1. Proporcionar dispositivos a los empleados

Utilizar un ordenador o móvil personal implica ciertos riesgos que, trabajando en la oficina, se podrían evitar. Por ejemplo, un empleado puede infectar un documento de la empresa con un virus de su equipo personal. Si ese archivo se sube al servidor corporativo, todo el contenido quedaría contaminado.

Si es imprescindible que los empleados usen sus equipos particulares, esto es lo que deberían de hacer: **mantener actualizado el sistema (**Windows, Linux, Mac OSX, iOS o Android) **y disponer de un antivirus,** tanto en el ordenador como en los dispositivos móviles**, activar el cortafuegos**, **crear dos sesiones separadas** (una personal y otra profesional) y **evitar conectar memorias USB desconocidas** que puedan contener virus.

La empresa evitará estos riesgos si facilita dispositivos a los empleados donde ya estén contempladas estas y otras medidas de seguridad, incluyendo además medidas de cifrado para evitar fugas de información. En caso de utilizar los ordenadores personales es recomendable el "uso de escritorio remoto" que permite a los trabajadores hacer uso de un ordenador virtual y que lleva instaladas las aplicaciones necesarias para trabajar como si estuvieran en la oficina.

2. Crear contraseñas fuertes en los servicios de la empresa Tener una buena gestión de contraseñas es uno de los pilares de la ciberseguridad. Usar una contraseña corta y previsible hará que los equipos y servicios corporativos sean más vulnerables. Una contraseña robusta debe ser larga, de **al menos ocho caracteres, y tener mayúsculas y minúsculas**. Añadirle también **números y caracteres especiales** hará que aún sea más difícil de descifrar para los ciberdelincuentes. Para reforzarlas más, lo ideal es **cambiar las contraseñas regularmente**.

3. Uso del doble factor de autentificación

Algunos programas y servicios en la nube permiten el uso del doble factor de autentificación. Es una forma más sólida de proteger el acceso a los servicios. En primer lugar, hay que insertar una contraseña; después, se pide otra información más para confirmar la identidad del usuario (por ejemplo, introducir un código numérico que se recibe por SMS, la huella dactilar o el reconocimiento facial).

4. Utilizar VPN (Virtual Private Network)

Se trata de una tecnología de red que se utiliza para conectar uno o más ordenadores a una red privada de la empresa. De esta manera los empleados, desde sus casas, puedan acceder a recursos corporativos, de forma totalmente segura, que, de otro modo, no podrían.

5. Realizar copias de seguridad

Perder datos relevantes durante el teletrabajo es uno de los posibles riesgos que corren las pymes. Para evitarlo, es importante **realizar copias periódicamente**. Para asegurar la información lo máximo posible, es recomendable **tener tres copias**: una en la que trabajar y dos más. Además, es mejor si se guardan en sitios distintos (por ejemplo, el ordenador, la nube y un USB). Si el teletrabajo se alarga más allá de la cuarentena y se convierte en rutina, también es recomendable que una de las copias se guarde fuera del hogar. Si la información que se trata es sensible, siempre las copias deberán ir cifradas.

6. Cifrar la información

Proteger los archivos que se tienen almacenados es indispensable para evitar que terceros puedan leerlos. Para ello, es recomendable **tener los archivos relevantes cifrados.** En caso de que la nube sufra un incidente de seguridad también conocido como "hackeo", la información cifrada estará a salvo. Tanto los dispositivos Apple como aquellos con Windows disponen de **herramientas de cifrado ya preinstaladas** (FireVault para Apple y BitLocker para Windows). En el caso de los móviles Android, se puede cifrar información desde la ventana de «Ajustes» y «Cifrado y credenciales». En los dispositivos iOS, los datos se cifran automáticamente cuando se elige una contraseña para desbloquearlos. Igualmente, es posible cifrar el contenido de un dispositivo USB con las herramientas de Windows y Apple.

7. Evitar el uso de redes WiFi públicas

Preferiblemente se utilizará la red doméstica. En caso de no usar la red doméstica se hará uso de la red 4G, que está considerada como un canal seguro.

8. No abrir documentos de origen desconocido ni descargar software "pirata".

Por último, si estamos utilizando un ordenador personal para trabajar es fundamental evitar abrir documentos de origen desconocido o descargar aplicaciones de sitios que no sean seguros**,** los conocidos como "sitios piratas".

Este software descargado no sabemos si puede contener malware. Además, es muy importante no facilitar la contraseña si nos llaman de un servicio técnico haciéndose pasar por el de nuestra empresa.

Francisco Javier de la Fuente Cagigós, responsable de Ciberseguridad de PA DIGITAL, ha declarado: *"La crisis del coronavirus ha obligado a muchas empresas a adaptarse al teletrabajo rápidamente, casi sin tiempo para reaccionar y, en algunos casos, sin respetar las recomendaciones de seguridad. Las empresas más que nunca deben ser conscientes de la importancia de sus datos y los riesgos a los que están expuestos en situaciones como la actual. No pueden permitirse brechas que hagan caer su página web, sus redes sociales o poner en peligro su información. Por eso, hemos querido dar unos consejos sencillos, pero eficaces, para ayudar a que las pequeñas empresas puedan continuar su labor con cierta seguridad".*