

Cómo mantener protegidas las redes sociales este verano, según Súmate

Los riesgos por hackeo de las redes sociales pueden incluir tanto daños morales, hacia la persona, como económicos y materiales. Evitar dar detalles personales y cambiar periódicamente las contraseñas son dos de las precauciones más importantes que se deben tomar

En estos últimos años, cada vez son más comunes los casos de hacking a los que todos los ciudadanos están expuestos. Es más, cualquiera con conocimientos y medios tecnológicos puede introducirse en el perfil de un usuario, lo que conlleva un gran peligro. Súmate Marketing Online, agencia internacional de marketing online, ofrece las claves para mantener protegidas las redes sociales (y a uno mismo) este verano y evitar riesgos que pueden dañar a una persona tanto moralmente como económica y materialmente.

Sin ninguna duda, el mayor error que se comete en el uso de las redes sociales radica en la cantidad de datos que se comparten en ellas, sin tener en cuenta los peligros que esto puede suponer. Esta información puede ser utilizada por terceros de diferentes maneras, algunas de ellas, llegando a ser hasta peligrosas: robos en viviendas, imágenes que deberían mantenerse en privado y se hacen públicas, phishing, malware, entre otros.

Tener descargado un Antivirus actualizado es algo imprescindible

Un antivirus protegerá los archivos en los dispositivos de los virus que hayan podido verse dañados; además de prevenir posibles futuros ataques. El único problema es que cada vez nacen nuevos virus, y por lo tanto hay que tener el antivirus actualizado en todo momento.

La contraseña es fundamental ante el hacking de redes sociales

El peligro en el caso de que alguien entre en el perfil de un usuario en una red social es proporcional a la información que se haya incluido en la página, tanto visible para otros usuarios como no visible, ya que, el hacker puede acceder a todo. Incluso puede secuestrar la cuenta del usuario cambiando la contraseña. Súmate Marketing Online señala que es importante: cambiar periódicamente la contraseña, utilizar contraseñas de acceso diferentes para cada red social, establecer contraseñas que no sean correlativas o con variantes obvias unas de otras y emplear siempre la página oficial de cada red social para entrar en ella, ya que circulan accesos que simulan serlo pero en realidad están pensados para hacerse con la contraseña.

Estas vacaciones, se debe cuidar la seguridad del hogar en las redes sociales

La época vacacional entraña mayores riesgos, por ello, hay que tener en cuenta lo arriesgado que es anunciar la ausencia del domicilio habitual y los peligros que esto puede conllevar, como robos e incluso ocupaciones.

Hacer copias de seguridad cada poco tiempo

Cuando hackean cualquier red social, todos los documentos, fotos o información que estén guardados se pueden ver afectados. Es recomendable realizar una copia de seguridad en una memoria externa ya sea en un usb o en un disco duro, de esa manera todos los archivos quedarán a salvo en caso de hacking.

Configurar apropiadamente la privacidad del perfil

Todas las redes sociales incluyen la posibilidad de configurar la privacidad del perfil, tanto en lo referente a los datos personales como del contenido que se publica. Es importante dedicar tiempo a configurar estos detalles para tener control sobre quién puede ver qué.

Evitar subir fotografías demasiado comprometidas o de menores

Solo en Facebook se suben más de 300 millones de imágenes al día. Es importante controlar el tipo de imágenes que se suben para evitar posibles situaciones incómodas.

Cerrar sesión en todas las aplicaciones

Esto debería hacerse durante todo el año pero especialmente ahora que se está más relajado. Si se accede a las redes sociales desde espacios públicos esta medida es imprescindible para que terceros no tengan acceso a los perfiles.

Datos de contacto:

Actitud de Comunicación
913022860

Nota de prensa publicada en: [Madrid](#)

Categorías: [Nacional](#) [Comunicación](#) [Marketing](#) [Sociedad](#) [Castilla y León](#) [E-Commerce](#) [Ciberseguridad](#)

NotasdePrensa

<https://www.notasdeprensa.es>