Consejos de seguridad en redes sociales tras los ataques a Tumblr y Myspace

La empresa de seguridad Symantec, creadora del programa Norton ha publicado que los ataques a **Tumblr y Myspace** "demuestran la importancia de una buena encriptación de los datos sensibles de usuarios", puesto que los informes acerca de la brecha de **Tumblr** indican que las contraseñas estaban encriptadas correctamente", lo que significa que es poco probable que las cuentas sean crackeadas, por lo que la información personal a la que tendrían acceso los cibercriminales se vería limitada a las cuentas de email, lo que ha sido positivo.

Recuerdan los expertos de seguridad que "**cuanto más tiempo invertimos en actualizar nuestras redes sociales, más atractivas son para los hackers"**. En 2015 las principales estafas en redes sociales fueron las ofertas falsas, llegando a sumar un 40% del total de estafas registradas, según los datos recopilados por Symantec. La empresa quiere dar unos consejos de seguridad para que el usuario de redes sociales pueda así proteger mejor su información online. Destacan los expertos que **"es bueno evitar usar información personal, repeticiones o secuencias, ya que son más fáciles de hackear"**. Aquí los consejos:

– **Utiliza contraseñas segura**s que usen al menos ocho caracteres y combinen caracteres alfanuméricos y especiales. Es recomendable u**tilizar autentificaciones en dos pasos**, que requieren que el usuario proporciona su nombre de usuario, contraseña y también un código de seguridad único de seis dígitos de un uso.

– D**uda de los nuevos seguidores. Si una persona aleatoria comienza a seguirte, no le sigas automáticamente. Comprueba sus tuits**. Puede ser un bot.

– No bases la decisión de seguir a alguien en función del número de personas que le siguen, porque pueden ser perfiles falsos o bots.

– **Evita divulgar información personal**. No compartas información personal como tu fecha de nacimiento, tu número de teléfono o la dirección en páginas web públicas.