CÓMO UTILIZAR CON MAYOR SEGURIDAD LAS REDES SOCIALES

Artículo publicado por Oscar García en Internet.

El éxito de las redes sociales no sólo está cambiando la forma de comunicarse de sus usuarios, sino también la forma de atacar de los cibercriminales, que están empezando a utilizar estas plataformas para intentar hacerse con datos de los usuarios o lanzar ataques para infectar sus ordenadores.

Según la empresa de seguridad G Data, durante los dos últimos meses se está registrando un importante incremento de la actividad delictiva en redes sociales, que ya afecta a la práctica totalidad de las plataformas.

La agrupación de un gran número de usuarios en las diferentes redes sociales (millones en cada una de ellas: Fotolog, Metroflog, My Space, Facebook, Twitter…) y su segmentación en grupos de interés, hace que sea mucho más fácil y rentable diseñar ataques dirigidos a un grupo concreto de personas, ya sea para infectar sus ordenadores, para enviar spam, para incitar a hacer compras fraudulentas, o incluso para robar sus datos personales.

Para protegerse de estos ataques, G Data recomienda tomar las siguientes precauciones:

- Un ordenador se puede ver infectado con malware con tan sólo visitar un sitio web. Los antivirus tradicionales, que solo monitorizan los archivos del sistema, resultan por tanto ineficaces. La protección adicional necesaria se ofrece mediante un escaneo http, que comprueba el contenido de la web antes de que llegue al navegador web y cause daño alguno.
- Los perfiles de la red social deben estar configurados de forma que tus datos personales sólo estén a disposición de las personas que tú decidas directamente. De otra forma, los motores de búsqueda de personas registrarán, almacenarán y pondrán a disposición de cualquiera estos datos.
- La protección antivirus, el sistema operativo y el navegador deben estar siempre actualizados a la última versión disponible. Esto elimina los agujeros de seguridad conocidos y asegura que las defensas antivirus estén siempre en vigor.

- Mantén cierto escepticismo sobre las peticiones de amistad de personas desconocidas, ya que podrían ser traficantes de datos en búsqueda de información personal que recopilar para su posterior venta.
- No respondas a aquellas notificaciones en las que se te pida que desveles contraseñas, números de cuenta, códigos PIN o cualquier otro dato personal, especialmente si se te amenaza con cerrar tu cuenta o perfil.
- Utiliza contraseñas complejas. Evita términos de fácil lectura, como nombres o fechas. De otra forma, corres el riesgo de que te roben la contraseña. Por ello, conviene escoger una contraseña que combine letras, números y caracteres especiales, algo que en definitiva no se encuentre habitualmente en un diccionario o calendario.
- Usa una contraseña distinta para cada comunidad en la que participes.