Claves para estar seguro en las redes sociales

Desde el despliegue de las redes sociales la seguridad de los usuarios siempre ha sido el principal problemas de las compañías debido a la cantidad de hackers que vulneran los sistemas para estafar.

ESET, compañía especializada en detección proactiva de amenazas, asegura que para mantener protegida toda la información personal que circula y lejos del alcance del cibercrimen, es necesario aplicar buenas prácticas que aseguren su integridad y privacidad.

Publicar solo lo necesario

Cualquier información que se publique en las redes sociales es una puerta que se abre de la vida privada. Y solo alcanza con que esa información caiga en las manos erróneas para vivir una situación indeseada, ya sea de suplantación de identidad, estafa o engaño.

Un párrafo aparte merece la publicación de fotografías de niños y niñas. Sobre todo, porque las leyes de protección del menor son cada vez más fuertes respecto del cuidado de la privacidad infantil, contemplando que todo lo que se publica en internet queda fuera del control de quién lo publicó.

Configurar la privacidad de cada cuenta

El cibercrimen ha evolucionado a tal punto que cualquier dato puede servir para suplantar la identidad o para llevar adelante algún tipo de estafa.

Es por eso que información tan sensible como la fecha de nacimiento, lugar de residencia, trabajo o estudio puede ser utilizado en contra del titular de la cuenta. Gestionar la privacidad de la información de manera correcta y consciente en cada cuenta donde se tenga un perfil, es la mejor manera de proteger esta información.

Los datos son considerados el nuevo petróleo y son tan atractivos tanto para las empresas como para los cibercriminales. ESET recomienda que antes de publicar algo se analice brevemente si es información que pueden ver todos, y en caso de que no lo sea quizás lo mejor sea no publicarla.

Esto refuerza la importancia de prestar atención a los permisos que damos a las aplicaciones que instalamos o a los servicios en los que creamos una cuenta.

Desconfiar de las personas que no se conocen

Más allá de todos los beneficios que tiene Internet, también existe un Lado B que es necesario tener en cuenta para no llevarse un gran disgusto. Los casos de fraude o acoso lamentablemente son muy comunes en el mundo digital y las redes sociales se han convertido en un nicho cada vez más explotado por los cibercriminales para realizar este tipo de prácticas.

La cautela y la desconfianza son dos grandes aliados a la hora de entablar algún tipo de contacto o relación con alguna persona desconocida. Por eso nunca es recomendable aceptar solicitudes de amistad de desconocidos, como tampoco proporcionarles información personal.

Verificar antes de hacer clic

Las redes sociales se reciben mensajes de contactos desconocidos, con promesas de algún beneficio o premio y un link que parecería ser la llave que abre el cofre del tesoro.

Pero no: un clic puede derivar a un sitio comprometido que solicita nuestros datos personales o bien la descarga de software malicioso. Desde ESET sugieren seguir una regla de oro que en estos casos aplica de manera efectiva: cuando algo es demasiado bueno para ser verdad, probablemente no lo sea.

Elegir contraseñas largas y complejas

Optar por una contraseña robusta y extensa es otro gran paso para proteger las cuentas de las diferentes redes sociales. Idealmente, deben ser frases que incluyan alrededor de 20 caracteres, letras, números, mayúsculas y caracteres especiales.

Un último tip es no reutilizar la misma contraseña en diferentes cuentas, ya que, si una se ve vulnerada, le dará al ciberatacante acceso al resto de las redes sociales. Un gran aliado para crear contraseñas fuertes y no tener que recordarlas es la implementación de un administrador de contraseñas.

Con información de Banca y Negocios