ESET preocupado por la exposición de usuarios en redes sociales

Los **delincuentes informáticos** continúan demostrando que la ingeniería social es una de las armas que más efectividad les ofrece al momento de conseguir más víctimas por medio de las redes sociales, donde muchos estudios al respecto señalan que con **falsos videos, perfiles fraudulentos y fotos comprometedoras,** entre otras técnicas siguen propagando **malware**.

Durante 12 años, Facebook se ha convertido en una de las redes sociales más populares del mundo y forma parte de los hábitos cotidianos de navegación de millones de personas expuestas a un conjunto de amenazas informáticas que pueden atentar contra su información, su dinero o incluso su propia integridad.

Como parte de una campaña de concienciación, el laboratorio de Investigación de **ESET** Latinoamérica proporciona **cinco pasos rápidos para proteger la cuenta de Facebook.**

1. **Construir una contraseña impenetrable.** Con una contraseña débil los cibercriminales podrán acceder a la cuenta sin esfuerzo. La contraseña de Facebook debe ser original y diferente al resto de las otras cuentas. Además, es recomendable el uso de mayúsculas, números, símbolos y hasta utilizar soluciones criptográficas.
2. **Controlar el inicio de sesión.** La evolución de la tecnología ha permitido que un usuario pueda estar conectado a la cuenta de Facebook en todo momento y en múltiples dispositivos al mismo tiempo. Sin embargo, puede resultar difícil no perder de vista en qué computadora, Tablet o Smartphone se ha iniciado sesión. Para ello, Facebook archiva cada inicio de la cuenta como una sesión activa, lo cual se puede administrar desde la configuración de seguridad.
3. **Detectar accesos no autorizados.** Facebook permite configurar las alertas de inicio de sesión, es decir que cada vez que un usuario inicie sesión en su cuenta desde una computadora o desde un Smartphone diferente, será notificado. Esto significa que si otro usuario ha accedido a la cuenta, se puede accionar rápidamente. Luego, Facebook realizará un proceso de autenticación en el cual el usuario deberá establecer si efectivamente estableció o no cambios.
4. **Evitar ser víctima de una campaña de phishing.** Las estafas de este tipo siempre están presentes en las redes sociales y se han vuelto cada vez más sofisticadas. Uno de las estafas más comunes utilizadas en Facebook es el enlace a noticias con videos impactantes o videos para adultos. Al hacer clic, el ciberdelincuente puede acceder a los datos del usuario y así robar sus credenciales. Por ello, es importante que el usuario no ingrese a sitios dudosos.
5. **Tener cuidado con el spam.** El spam puede aparecer de varias formas en Facebook, como oculto a través de la solicitud de un amigo, un posteo o incluso por un mensaje privado. Si se observa que la cuenta de un amigo o familiar está compartiendo reiteradas veces un mismo mensaje, el usuario deberá ser cauteloso antes de hacer clic o de compartir la información.