Cómo hacer para que los hackers no accedan a tu cuenta de Instagram: cuatro consejos útiles

28/07/2024

Instagram es una de las redes sociales con más uso en el mundo, pero como todo lo que puede ser masivo, también tiene sus riesgos si no se toman los recaudos necesarios. Es por eso que resulta **primordial contar con una contraseña segura**, pero al mismo tiempo, también una serie de opciones que podrán ser muy útiles para **no caer en manos de hackers** ni nada por el estilo.

Lo cierto es que más allá del mal trago que genera que alguien se meta en la cuenta de otra persona y pueda manipularla a su antojo, lo más riesgoso pasa por el tema del robo de datos e información personal. Esto conlleva, en la mayoría de los casos, a caer en posibles estafas virtuales.

La pérdida de la información o la divulgación de contenido

multimedia privado son algunas de las peores consecuencias que la presencia de un hacker puede generar. Incluso también enviar mensajes maliciosos a los contactos o las ya mencionadas potenciales estafas monetarias.

Lo cierto es que intentar recuperar una cuenta hackeada también suele ser un incordio notable. Por lo que extremar las medidas de seguridad para evitar todo esto sigue siendo la mejor opción.

Consejos para evitar que alguien robe una cuenta de Instagram

Uno de los primeros consejos es **activar la autenticación de dos pasos.** Esto suma una instancia adicional de seguridad, aunque sigue siendo algo permeable, por lo que no es definitiva su seguridad. Los pasos que hay que seguir para activar esto son los siguientes:

about:blank

- Abrir la aplicación y entrar al perfil.
- El siguiente paso es ir al menú de opciones y seleccionar «configuración».
- Elegir «seguridad» y luego «autenticación en dos pasos». Allí, la app ofrecerá dos opciones: una de ellas será mediante mensaje de texto y la otra mediante aplicaciones de autenticación.

Con estos pasos se logra tener una contraseña más segura, por lo que no podrá nadie acceder a la red social propia sin primero tener que tener acceso al segundo factor de autenticación.

Extremar los cuidados con nuestras redes: la clave para

evitar ser estafado. Foto: Unsplash.

La creación de una **contraseña segura** también es un factor importante a tener presente. Si bien es algo básico, resulta una barrera bastante útil contra los hackers. Para crear una contraseña segura, se pueden seguir los siguientes consejos:

- Utilizar combinaciones variadas entre mayúsculas y minúsculas.
- También utilizar letras combinadas con números y símbolos.
- No usar palabras comunes, nombres o fechas que fácilmente pudieran relacionarse con el usuario.
- Una clave segura tiene que tener al menos 12 caracteres.

Lo aconsejable, además, es no reutilizar contraseñas en diferentes cuentas.

Otros aspectos importantes es **mantener actualizada la información de contacto.** Esto, en caso de ser hackeada la cuenta, facilitará el recupero de la misma. Los datos actualizados deberían ser:

- Teléfono de contacto.
- Email de contacto.

Celular. Foto: Unsplash.

No acceder a enlaces sospechosos. Siempre hay que tener cuidado con esto, incluso por otras apps como WhatsApp y también el correo electrónico. Para ello, hay que estar atento a lo siguiente:

- Si se tiene acceso a un link, verificar la procedencia del mismo. Incluso también en la barra de direcciones, cuando un link no es seguro, se le advierte con una

leyenda al usuario.

- No acceder a mails que parezcan sospechosos. La utilización de estafas mediante correos electrónicos está muy difundida. Por eso, es preciso chequear el dominio del mail (la parte que sigue después del @) para constatar que efectivamente sea una dirección segura. Si levanta sospechas, es mejor no acceder a él. Por ejemplo, en Instagram, el dominio debe terminar en @instagram.com para que sea un enlace seguro.

Fuente: Canal 26