

Cómo saber si tu cuenta de Facebook fue hackeada

24/07/2022



Seas o no un usuario de Facebook frecuente, lo mejor que podés hacer es proteger tu cuenta de forma segura para evitar que todos los datos personales y privados que guardas en ella lleguen a manos indeseadas. **Hay 5 cosas concretas en las que podés fijarte para confirmar si otras personas tienen acceso a tu cuenta.**

Tu cuenta de Facebook puede albergar información tan importante como tu dirección de correo electrónico, tu número de teléfono, imágenes y también conversaciones de carácter privado que has mantenido a través de Facebook Messenger.

5 señales son claves para saber si fuiste hackeado

No puedes iniciar sesión con tu cuenta

La situación más grave que te puede pasar es que no puedas

iniciar sesión con tu cuenta. Es posible que los hackers hayan cambiado la contraseña y por ello no puedes entrar. Si la cuenta sigue asociada al mismo correo electrónico, aún podrías cambiar la contraseña.

El problema es más grave si los atacantes modifican también la dirección de correo electrónico porque no tendrías acceso al enlace de verificación que Facebook te envía para poder cambiar la contraseña.

Tus datos de contacto fueron modificados

Rápidamente podés saber si fuiste otra persona tiene acceso a tu usuario es el configuración general de la cuenta. **En esta sección se muestran datos como tu nombre, tu contacto y tu nombre de usuario.** Si entras y ves que alguno de fueron modificados sabrás que tu cuenta ha sido hackeada.

Tenés que entrar en Configuración y privacidad -Configuración- General.

Consultando el historial de inicio de sesión

Facebook cuenta con un apartado que te informa sobre los dispositivos en los que has iniciado sesión. Sin duda, este es otro de los lugares para chequear si alguien entró a tu cuenta.

Entra en Configuración y privacidad – Configuración – Seguridad e inicio de sesión. Una vez dentro, en el apartado «**Dónde has iniciado sesión**» podrás ver todos los dispositivos en los que se ha iniciado sesión con tu cuenta, la fecha concreta en la que tuvo lugar y si fue desde un navegador web o desde la aplicación.

Además, desde ahí puedes cerrar sesión en aquellos dispositivos que no sean tuyos.

Hay mensajes en tu muro y en Messenger que no publicaste

Es la principal señal que enciende todas tus alarmas. **Puede ser que diste permiso a alguna aplicación o juego para publicar en tu muro, o también que otras personas han logrado acceder a tu perfil sin que te des cuenta.**

Cualquier publicación de contenido que no hayas realizado es suficiente como para confirmar que no tienes el control total de tu cuenta.

Notificaciones de mensajes inusuales

Las notificaciones a las que accedes a través del botón de la campana también pueden revelarte que tu cuenta fue hackeada.

Lo importante es que te fijes en las notificaciones que te envía Facebook. Por ejemplo, puede avisarte de que se intentó iniciar sesión desde otro país o de que el archivo con toda tu información está listo para descargar.

¿Cómo recuperar tu cuenta de Facebook?

Una vez que confirmaste que tu cuenta de Facebook fue efectivamente hackeada, hay que intentar recuperarla para que el control vuelva a estar solo en tu manos.

En primer lugar, **comunica a tus contactos que ignoren cualquier comunicación que les llegue desde tu cuenta. Por supuesto, lo mejor es que no pinchen en los enlaces que reciban.**

Si tienes acceso a la cuenta, **debes cambiar rápidamente la contraseña por una nueva que sea totalmente segura. Además, cierra sesión en aquellos dispositivos que no son tuyos.** Después, repasa la configuración de la cuenta al completo para confirmar que todo vuelve a estar en su lugar.

Si ya no tenés acceso a la cuenta y no podés iniciar sesión, contacta a Facebook a través de la web para denunciar una cuenta comprometida.

Ahí tendrás que introducir todos los datos que la red social te solicite para confirmar que la cuenta hackeada realmente era tuya. Eso sí, este procedimiento puede llevar su tiempo, pues Facebook tiene que analizar la petición.

Una vez hayas recuperado tu cuenta, procede a habilitar la verificación en dos pasos, así el servicio pedirá un segundo código cuando intentes iniciar sesión desde un navegador o dispositivo móvil desconocido.