Qué es lo primero que hay que hacer si te hackean la cuenta de WhatsApp o Instagram

22/06/2026

Los ataques digitales a servicios como WhatsApp, Instagram o la banca online son cada vez más frecuentes y la diferencia entre un susto y un perjuicio mayor suele medirse en minutos. Ante un hackeo de cuentas la primera prioridad es cortar el acceso del intruso: desconectar el equipo y evitar más operaciones.

Actuá en los primeros minutos

En los primeros dos minutos hay que actuar sin titubear: apagá o desconectá Wi-Fi y datos, y **si seguís con acceso cerrá sesiones de la cuenta desde la configuración**. Si sufriste

un **hackeo de cuentas** y te sacaron el ingreso, iniciá de inmediato el trámite de recuperación oficial y **no hagas intentos repetidos que puedan bloquear tu acceso.**

Con el daño contenido, **priorizá recuperar el control**. Cambiá la contraseña desde otro dispositivo seguro, elegí una clave larga y única, activá el doble factor de autenticación y revocá accesos de aplicaciones conectadas. **Cerrá todas las sesiones abiertas y verificá que no se hayan agregado números o correos alternativos.** Si no podés entrar, contactá soporte.

No subestimes el efecto colateral: si repetiste la clave en otros servicios, también están en riesgo. En los minutos siguientes **cambiá contraseñas iguales en mail, redes y banca**; revisá movimientos recientes, mensajes enviados y cambios de datos. Dedicá especial atención al correo electrónico: suele ser la llave para restablecer cuentas y bloqueá accesos desconocidos.

Qué es lo primero que hay que hacer si te hackean la cuenta de WhatsApp o Instagram

Prevención y recuperación

El origen del problema puede estar en el propio equipo: **ejecutá un escaneo completo con un antivirus confiable, eliminá aplicaciones y extensiones sospechosas y actualizá el sistema operativo y todas las apps.** Si sospechás de malware persistente, considerá restaurar el dispositivo a ajustes de fábrica tras guardar respaldos seguros y verificar claves previas.

No pierdas tiempo en avisos: **advertí a familiares y contactos que podrías enviar mensajes fraudulentos pidiendo dinero o datos.** Reportá la cuenta a la plataforma y, ante movimientos bancarios o billeteras, contactá al banco para bloquear operaciones. Cuanto antes comuniques, más fácil es cortar cadenas de estafa y recuperar fondos si hubo extracciones.

Para reducir el riesgo futuro, **incorporá hábitos sencillos**: activá el **doble factor de autenticación** en todas las cuentas que lo permitan, usá contraseñas largas y únicas con un gestor, evitá clicar enlaces desconocidos y no compartas códigos de verificación. Mantener equipos actualizados y una solución de seguridad reduce muchísimo las probabilidades de una nueva intrusión.

Fuente: La 100