



PLAYBOOKS

Te robaron el WhatsApp: recuperalo y blindalo

«Hola, te mandé un código por error, ¿me lo pasás?» Esa frase es la puerta de entrada al robo de cuentas de WhatsApp más común de la Argentina. Este playbook te explica cómo recuperar la cuenta si ya entraron, qué hacer con tus contactos mientras tanto, y cómo dejarla blindada para que no vuelva a pasar.

Versión 1.1 · Agosto 2026

Atajo

Si te acaban de sacar la cuenta, andá directo a la sección 3. Si todavía la tenés, andá a la sección 5 y activá la verificación en dos pasos: son dos minutos y es lo único que corta este ataque de raíz.

1. Cómo te la roban (y por qué funciona)

Tu número de WhatsApp no se «hackea» en el sentido técnico. Lo que hacen es registrar tu número en otro teléfono. Para eso solo necesitan el código de 6 dígitos que WhatsApp manda por SMS. Y ese código te lo mandan a vos, así que tienen que convencerte de que se lo pases.

Las tres variantes que más se ven:

- El contacto conocido. Te escribe alguien de tu agenda —cuya cuenta ya robaron— diciendo que se equivocó y te mandó un código. Como conocés a esa persona, se lo pasás.
- El falso soporte. Un mensaje o una llamada de «WhatsApp», de un organismo, de «tu banco» o de un sorteo, que pide el código para «verificar tu identidad».
- El teléfono robado. Si te roban el equipo desbloqueado, la sesión ya está abierta y no necesitan ningún código.

La regla de oro

WhatsApp nunca te va a pedir tu código de verificación por chat, por SMS ni por teléfono. Nadie legítimo lo hace. Si alguien te lo pide, es un robo en curso, sin excepciones.

2. Señales de que algo pasó

- Te llegó un código de verificación que no pediste (alguien está intentando registrar tu número justo ahora).
- WhatsApp te cerró la sesión de golpe y te pide registrar el número de nuevo.
- Tus contactos te avisan que les llegaron mensajes raros tuyos, casi siempre pidiendo plata.
- Aparecen dispositivos que no reconocés en Ajustes > Dispositivos vinculados.
- Hay chats archivados, grupos nuevos o mensajes marcados como leídos que vos no abriste.

3. Ya entraron: recuperala ahora

La buena noticia: el número es tuyo y el registro es la prueba. Quien tiene la cuenta la pierde en cuanto vos volvéis a registrar tu número. Lo importante es hacerlo rápido, porque cada minuto es un mensaje más a tus contactos en tu nombre.

RECUPERACIÓN — en este orden

1. Abrió WhatsApp en tu teléfono y registrá tu número de nuevo. Te va a llegar un código de 6 dígitos por SMS. Ingresalo. Con eso, la sesión del atacante se cierra sola.
2. Si te pide un PIN de 6 dígitos que vos no configuraste, es porque el atacante activó la verificación en dos pasos para dejarte afuera. Elegí «¿Olvidaste el PIN?» y usá el correo de recuperación. Si no tenés correo cargado, hay que esperar 7 días para poder reiniciarlo: no hay atajo.
3. Revisá los dispositivos vinculados. Ajustes > Dispositivos vinculados: cerrá sesión en todo lo que no reconozcas. WhatsApp Web es la vía por la que se quedan escuchando aunque recuperes el teléfono.
4. Activá la verificación en dos pasos con un PIN nuevo y un correo de recuperación. Ver sección 5.
5. Avisá a tus contactos por otra vía que tu cuenta estuvo tomada y que no le crean a ningún pedido de plata de las últimas horas.

Cuidado con la segunda estafa

WhatsApp no puede recuperar la cuenta por vos ni «desbloquearla» a pedido: el procedimiento es siempre registrar tu número de nuevo. Cualquier persona o página que te ofrezca recuperarla a cambio de plata o de tus datos es una segunda estafa.

4. Mientras tanto: contené el daño

- ☐ Avisá primero a los grupos de familia. Ahí es donde el pedido de plata funciona mejor, porque la confianza ya está.
- ☐ Si sos administrador de grupos, pedí a otro administrador que te saque temporalmente o que avise en el grupo.
- ☐ Revisá si el mismo número está asociado a otras cuentas. Si el atacante llegó a tu SMS, puede intentar recuperarlas también.
- ☐ Si alguien ya transfirió plata por un mensaje falso tuyo, que haga la denuncia y avise al banco de inmediato: en las primeras horas a veces se puede frenar.
- ☐ Guardá capturas de pantalla de los mensajes fraudulentos y del código que no pediste. Sirven para la denuncia.

5. Blindaje: los cinco minutos que evitan todo esto

La verificación en dos pasos suma un PIN de 6 dígitos que WhatsApp pide al registrar tu número en un teléfono nuevo. Aunque el atacante consiga el código del SMS, sin ese PIN no entra. Es la única defensa que corta el ataque completo.

Qué activar	Dónde	Por qué
Verificación en dos pasos	Ajustes > Cuenta > Verificación en dos pasos	Sin el PIN no pueden registrar tu número en otro equipo. Cargá el correo de recuperación: sin él, si olvidás el PIN, son 7 días de espera.
Bloqueo de la aplicación	Ajustes > Privacidad > Bloqueo de pantalla	Huella o rostro para abrir WhatsApp. Protege si te roban el teléfono desbloqueado.
Revisión de dispositivos vinculados	Ajustes > Dispositivos vinculados	Hacelo cada tanto. Es donde queda escuchando quien entró por WhatsApp Web.
PIN en la tarjeta SIM	Ajustes del teléfono > Seguridad de la SIM	Si mueven tu chip a otro equipo, no arranca y no reciben tus SMS.
Foto de perfil solo para contactos	Ajustes > Privacidad > Foto de perfil	Reduce el material con el que arman perfiles falsos a tu nombre.

6. Si tenés un negocio

Para un comercio o una empresa chica, perder el WhatsApp es perder el canal de ventas y la confianza de los clientes al mismo tiempo. Tres cosas que conviene dejar resueltas antes:

- Que la cuenta no dependa de un solo teléfono personal. Usá WhatsApp Business y tené claro quién tiene acceso.
- Definí quién avisa y por dónde si la cuenta cae: redes sociales, mail, cartel en el local. Un cliente que recibe un pedido de transferencia falso desde tu número te reclama a vos.
- Nunca confirmes pagos ni cambios de CBU solo por WhatsApp. Que la regla sea verificar por llamada, siempre. Es la misma lógica del fraude del CEO.

7. Tu nido, con doble puerta

Casi todos los robos de WhatsApp se apoyan en lo mismo: un código que compartiste con alguien que parecía de confianza. Si activás la verificación en dos pasos y cargás el correo de recuperación, el ataque más común de la Argentina deja de funcionar en tu cuenta. Dos minutos, hoy.



Esto no termina acá

Si querés enterarte de las estafas que están circulando de verdad, qué revisar y los documentos nuevos, sumate al correo de CiberConscientes. Sin vueltas y con baja en un clic. www.ciberconscientes.io

Material orientativo elaborado por CiberConscientes con fines educativos. No reemplaza el asesoramiento legal ni profesional para tu caso particular. Los nombres de los menús y los procedimientos de la aplicación cambian con las actualizaciones: verificá la ayuda oficial de WhatsApp si algo no coincide con lo que ves en pantalla.

Versión 1.1 · Agosto 2026 · Próxima revisión: Febrero 2027 · www.ciberconscientes.io