

Se filtró mi contraseña: qué hacer en las primeras horas

Te avisaron de que tu correo y tu contraseña salieron en una fuga. Qué hacer primero, en qué orden y qué trampas evitar, explicado en palabras sencillas.



Te llega un correo de una tienda donde compraste hace años: «sufrimos un incidente y tu correo y tu contraseña pueden estar expuestos». O lo ves en las noticias. Es normal asustarse. Lo bueno es que lo que hay que hacer cabe en una tarde y tiene un orden. Esta guía te lo da, paso a paso.

Antes de nada: comprueba que el aviso es real

Detrás de una fuga conocida siempre llegan mensajes falsos que se aprovechan del susto. Antes de pulsar nada:

- **No entres por el enlace del mensaje.** Abre la app de la empresa o escribe tú su dirección en el navegador. Si de verdad hay algo que hacer, lo verás ahí.
- **Para saber si tu correo salió en una fuga basta con la dirección.** Hay buscadores públicos de fugas que solo piden tu correo. Si una página te pide además la contraseña «para revisar», no está revisando nada: la está recogiendo.

Paso 1: protege primero tu correo principal

Parece raro empezar por el correo y no por el banco, pero tiene lógica. Casi todas tus cuentas se recuperan con un enlace que llega a tu correo: quien lo controla puede pulsar «olvidé mi contraseña» en cualquier otra cuenta y recibir él ese enlace. El correo es la llave que abre las demás.

- Cambia la contraseña del correo desde un aparato tuyo y de confianza.
- Usa una contraseña nueva y larga, que no hayas usado en ningún otro sitio.
- Activa la **verificación en dos pasos**: un código extra que se pide además de la contraseña. Con ella, quien solo tenga tu contraseña se queda fuera.

Paso 2: cierra las sesiones que quedaron abiertas

Esto casi nadie lo sabe: cambiar la contraseña impide que alguien **entre de nuevo**, pero en muchos servicios no saca a quien **ya estaba dentro**. Una sesión abierta en otro navegador o en otro aparato puede seguir funcionando días con la contraseña vieja.

Algunos servicios cierran las demás sesiones solos al cambiar la contraseña, y otros no. Para no depender de eso, entra en el apartado de seguridad de tu correo, busca **dispositivos** o **sesiones** y cierra las demás. Tus propios aparatos vuelven a entrar con la contraseña nueva sin perder nada.

Paso 3: revisa por dónde se recupera tu cuenta

En el mismo panel mira el **correo y el teléfono de recuperación**: es a donde llega el enlace cuando alguien pulsa «olvidé mi contraseña». Si es un correo viejo que ya no abres o un número que ya no es tuyo, cámbialo. Un dato de recuperación olvidado es una puerta trasera.

Paso 4: cambia esa contraseña donde la hayas repetido

Quien tiene la lista filtrada no se queda en la tienda. Prueba la misma combinación de correo y contraseña en muchos otros servicios, de forma automática y aunque sean de otras empresas. Si repetías esa contraseña, piensa dónde.

Si no te da tiempo de hacerlo todo hoy, sigue este orden:

1. Lo que mueve dinero: banco, billeteras digitales y tiendas con tu tarjeta guardada.
2. Lo que guarda tu vida: la nube de fotos, las redes sociales y la mensajería.
3. Lo demás: foros, suscripciones y cuentas que casi no usas.

Pon una contraseña distinta en cada una. Un gestor de contraseñas te ahorra tener que recordarlas todas.

Paso 5: desconfía de la segunda oleada

En los días siguientes llegan mensajes que se hacen pasar por el soporte de la empresa afectada: «detectamos un acceso, valida tu identidad aquí». Llegan justo cuando estás preocupado, y por eso funcionan.

Una empresa seria no te pide la contraseña por mensaje ni te manda un enlace urgente para «desbloquear» tu cuenta. Si dudas, entra tú por la app o por la dirección de siempre.

Lo que no hace falta hacer

- **Borrar todas tus cuentas o cambiar de correo.** Con los pasos de arriba, tu correo vuelve a ser tuyo.
- **Pagar a alguien para «borrar» tus datos de la fuga.** Una vez filtrados circulan copias que nadie puede recoger. Lo que sí está en tu mano es que esos datos ya no abran nada.
- **Hacerlo todo en una noche.** El correo y sus sesiones, hoy; lo demás puede esperar a mañana.

Tu lista para hoy

1. Comprobé el aviso entrando yo, no desde el enlace del mensaje.
2. Cambié la contraseña de mi correo principal.
3. Activé la verificación en dos pasos en mi correo.
4. Cerré las demás sesiones.
5. Revisé el correo y el teléfono de recuperación.
6. Cambié la contraseña repetida en lo que mueve dinero.

Práctico · Módulo 1 de Tu primer escudo: Tu identidad digital

Leerlo es el primer paso; decidir con un caso delante es lo que se queda. En el módulo resuelves dos casos: el de alguien que recibe tres avisos de cambio de contraseña en un minuto y el de alguien en las horas después de una fuga. Las preguntas de esas dos salas se responden sin crear cuenta.

Empieza aquí: pro.whoami-labs.com/rutas/tu-primer-escudo/tu-identidad-digital

Esta guía en la web: pro.whoami-labs.com/guias/se-filtro-mi-contrasena