

The first-hour checklist

Do these in order, in the first hour after X tells you your email has changed.

1. Open your profile logged out. Screenshot it and several scam posts, with dates.
2. Keep X's "email changed" notice. Start a log, times in UTC.
3. Tap "Secure your account" in that notice and file the compromised-account form. Once.
4. Try the password reset once; screenshot what it offers.
5. Reply to X's automatic questions within minutes: username, every email, last access, phone.
6. Search every mailbox for x.com and twitter.com. Save it all.
7. Change your email password; switch on two-step verification there.
8. Warn people where the attacker cannot reach: LinkedIn, groups, email.
9. Ignore anyone who offers to help in DMs or replies.
10. Do not create a new account. Do not delete anything yet.

Then expect a no. Here's what comes next.

X rejected my proof of ownership twice. I still got my 2007 account back in ten days. The full guide covers everything I did, in order:

- Which X teams actually act, and which only send canned replies
- 12 copy-and-paste templates, including the GDPR and copyright letters
- The Persona ID check, and the four statements X asks you to make
- Clearing 2,746 scam posts once I was back in

Get the full guide: Getting a Hijacked X Account Back

neiljstanley.gumroad.com/l/hacked-x-account