Hijacked account checklist

What to do when a social media or email account is hijacked. Work down the list in order and tick each step as you finish it. The full guide, with the reasons behind every step, is at confirmedstolen.com/hacked-accounts/.

In the first hour

- [ ] **Secure your email account first, from a device you trust**
  Change the password on the email account linked to the hijacked profile. Email is the master key: every "forgot password" link for your other accounts lands there.
- [ ] **Remove recovery details and forwarding rules you did not add**
  Attackers often add their own recovery phone number, backup address or a filter that forwards or deletes security alerts. Delete anything you do not recognize.
- [ ] **Start the platform's official account-recovery flow**
  Use only the recovery pages inside the app or on the platform's own help center. For Facebook and Instagram, Meta's hacked-account flow starts at facebook.com/hacked (www.facebook.com/hacked).
- [ ] **Ignore anyone who messages you offering to recover the account**
  People who reach out by direct message, comment or email promising to restore access for a fee are running a recovery scam. Platforms do not charge to restore accounts.
- [ ] **Save evidence before the attacker deletes it**
  Screenshot security alert emails, changed profile details, suspicious posts and messages sent from the account, and note the dates and times.

Within 24 hours

- [ ] **Sign out of every active session once you regain access**
  Open the platform's security settings, find the list of logged-in devices, and end every session you do not recognize, or all of them.
- [ ] **Set a new, unique password with a password manager**
  Generate a long password that you have never used anywhere else. Reused passwords are how many takeovers begin.
- [ ] **Revoke third-party app and connected-service access**
  Remove apps, browser extensions and "log in with" connections you do not recognize. A malicious app can keep posting even after a password change.
- [ ] **Turn on MFA with an authenticator app or passkey, not SMS**
  Text-message codes can be intercepted through a SIM swap (confirmedstolen.com/sim-swap/). An authenticator app, hardware security key or passkey is much harder to steal.

- [ ] **Warn your contacts through another channel**
  Tell friends, followers and customers that messages sent during the takeover were not from you, especially requests for money, gift cards, cryptocurrency or login codes.

- [ ] **Remove content and settings the attacker changed**
  Delete posts, messages, ads and listings the attacker created, and restore your name, profile photo, email address and phone number.

This week

- [ ] **Report impersonation or copycat profiles**
  Use the report option on the fake profile's menu, or the impersonation form in the platform's official help center, and ask friends to report it as well.

- [ ] **Audit admins and ad accounts on every business page**
  Check each admin, editor and advertiser role, remove anyone unfamiliar, and confirm which payment methods are attached to linked ad accounts.

- [ ] **Check linked payment methods for unauthorized charges**
  Review card statements, PayPal, app-store purchases and ad spend, and dispute any charge you did not authorize with the provider.

- [ ] **Report any financial loss to the FBI IC3**
  If you lost money, file a complaint with the FBI Internet Crime Complaint Center (www.ic3.gov/) and keep the confirmation for your bank and insurer.

- [ ] **Submit the hijacked account to Confirmed Stolen for verification**
  We accept reports of hijacked social media accounts through our report page (confirmedstolen.com/report/). We verify and document cases; we do not recover accounts.

Prevent it happening again

- [ ] **Add a second trusted admin to every business page**
  A colleague with full admin rights, also protected by MFA, can restore access if one person's login is lost or taken.

- [ ] **Store backup codes somewhere offline**
  Save recovery codes in a password manager or print them, so a lost phone does not lock you out.

- [ ] **Run each platform's security checkup every few months**
  Google, Meta and most major platforms offer a built-in review of devices, connected apps and recovery options.

- [ ] **Treat any request for a login code as an attack**
  No legitimate contact needs your verification code. Anyone who asks for it, including a "friend," is trying to take an account.

Your case record

Platform and account handle

Platform support case number

Date access recovered

IC3 complaint number

Contacts warned (date)

Notes

Version November 6, 2026. General information, not legal advice. Agencies change their procedures, so confirm each step with the organization named. Confirmed Stolen is an independent reference; it is not law enforcement and does not recover property. Free to print and share with attribution.