



INCIDENT RESPONSE

If You've Been Hacked Checklist

What to do in the next 24 hours

Six steps to take right now. Work through these in order — each one matters.

- 1 Change the password — from a different device**
Use a phone or computer you know wasn't compromised. Change only the hacked account's password first. Make it unique and store it in your password manager.
- 2 Revoke all active sessions**
In the account's security settings, look for 'Active sessions', 'Logged-in devices', or 'Where you're signed in'. Sign out everywhere. This kicks out the attacker even if they still have your old password.
- 3 Remove unknown connected apps**
Go to the account's connected apps or third-party access settings. Remove anything you don't recognize. Attackers often install persistent access this way.
- 4 Enable MFA if it wasn't on**
Turn on two-factor now using Authy (authy.com). If the attacker already added their own MFA device, contact the platform's support to recover the account.
- 5 Alert your contacts**
Send a message to your close contacts: 'My [account] was compromised. Ignore any recent messages from me asking for money, gift cards, or personal info.' Attackers impersonate victims to scam their contacts.
- 6 Check other accounts with the same password**
Visit haveibeenpwned.com with your email. Change the password on every account that used the same one. Each account needs a unique password going forward.