



If You Think an Account Was Hacked

Calm first steps for protecting an online account.

Before You Start

Keep your device charged · Use your usual Wi-Fi · Stay signed in to your own account

- 1 Use a device you trust and open the provider's official app or type its known website address yourself. Do not use a link from the warning message.
- 2 Change the password to a new, unique one. Sign out other sessions if the provider offers that option, then turn on two-step verification (an extra sign-in check after your password).
- 3 Check the recovery phone number, recovery email, forwarding rules, and recent activity. Remove changes or devices you do not recognize.
- 4 If money or payment details may be involved, contact the bank or card issuer using the number on the card or statement. Tell contacts if the account sent messages without you.
- 5 Keep copies of relevant alerts and report the incident through the provider's official support channel. Do not pay someone who promises guaranteed account recovery.

Official Resources: CISA — Secure Our World

When to Ask for Help: If you see activity you do not recognize, money may be involved, or you cannot sign in.

Questions You Can Ask: What should I change first? · How do I remove an unfamiliar device? · Which official support route should I use?

NOTES TO KEEP NEARBY
