

CyberGuardLab

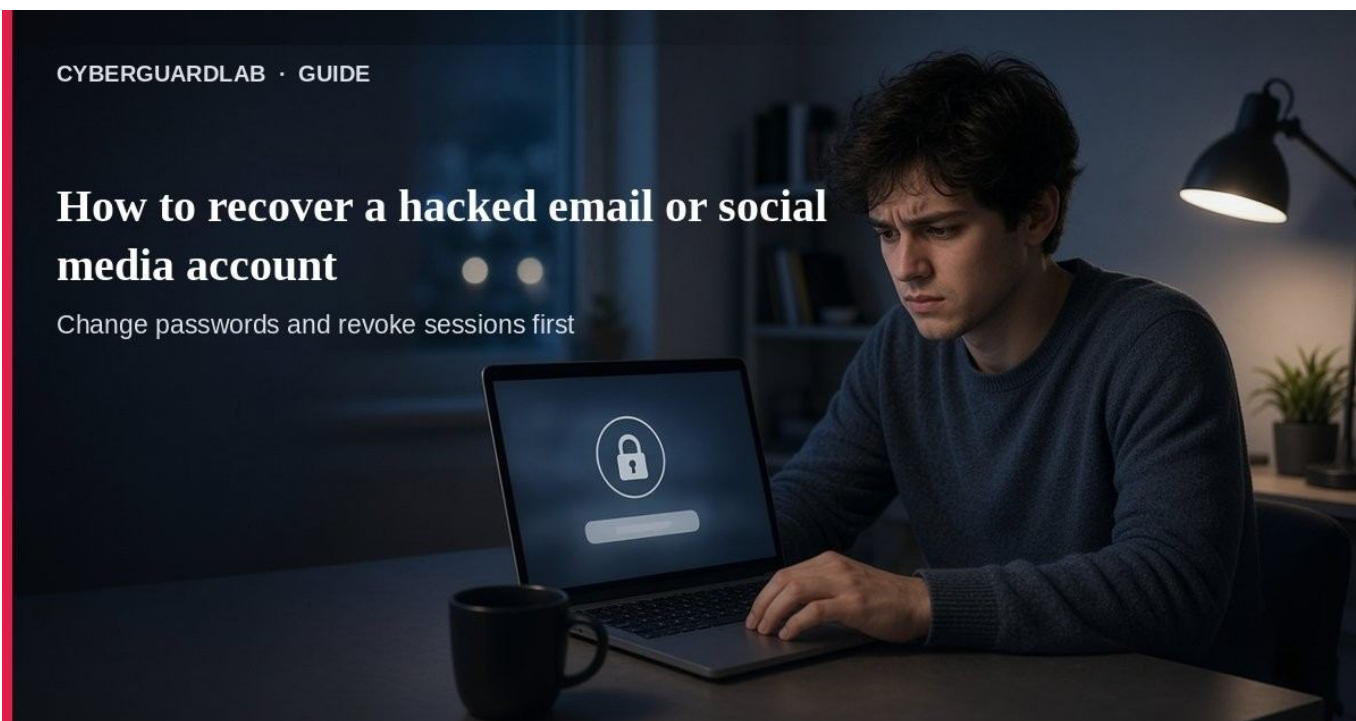
Household antivirus, explained

cyberguardlab.com

How to recover a hacked email or social media account

<https://cyberguardlab.com/blog/hacked-email-social-account>

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.



CYBERGUARDLAB · GUIDE

How to recover a hacked email or social media account

Change passwords and revoke sessions first

If your email or social media account is hacked, someone else can read private messages, reset other accounts through your inbox, or scam your friends. Per the FTC, signs include lockouts, password/email/phone changes you did not make, login alerts from unknown places, and friends getting messages you never sent. This guide covers email and social takeover recovery for a US household - not Amazon shopping accounts or kids' game accounts. You can start with free Defender / provider recovery pages; buying a suite is optional.

1. Signs your account was taken over

From FTC recovery guidance and the Oct 2024 consumer alert:

Paid link

Norton 360 | See the Norton first-year offer



[See the Norton first-year offer](https://cyberguardlab.com/norton)

Offer page: <https://cyberguardlab.com/norton> Hop: <https://trysecurities.com/offer/norton?dtm=gg&cid=>

- * You cannot log in.
- * You get a notice that your password, email, or phone number changed - and you did not change it.
- * A login or attempted login from a device or location you do not recognize.
- * Friends or family get emails/DMs you did not send (links, fake help/money asks).

2. Get back in (first hour)

- * Update security software and scan the PC - FTC: run a scan, remove anything suspicious, restart, then recover the account (so malware does not steal the new password). Microsoft Defender / Windows Security is enough for many homes; see Is Microsoft Defender enough?.
- * Use the provider's official recovery page - FTC links recovery for Facebook, Google, Instagram, Microsoft, X, Yahoo, and others. Type the help URL yourself; do not trust a "support" stranger in chat.
- * If you can still log in - Change to a strong unique password (FTC suggests aiming for 12-15 characters or a passphrase), then sign out of all devices.
- * Turn on 2FA / MFA - Password plus a second factor (app, SMS, or hardware). See FTC two-factor guidance and turn on 2FA.
- * Fix recovery email and phone - Confirm only numbers/addresses you control are listed.

3. After you regain control

- * Email forwarding rules - Delete auto-forward rules you did not create.
- * Sent / trash folders - Look for mail the attacker sent or deleted.
- * Social cleanup - Remove strange posts, DMs, and new "friends" you do not recognize.
- * Warn contacts - Tell friends not to click links "from you" and to ignore money/help pleas.
- * Protect email first going forward - FTC: a hacked inbox can reset your other accounts. Unique password + 2FA on email is priority.
- * If personal data was stolen - Use IdentityTheft.gov for a recovery plan (also covered in report identity theft).

4. Reduce the chance it happens again

- * Unique passwords (or a manager) - see password manager vs browser passwords.
- * 2FA on email, bank, and social first.
- * Check breach exposure on high-value emails - check email data breach.
- * Ignore unexpected password-reset links; start resets only from the real site/app.
- * Keep Windows and browsers updated (CISA: update software).

FAQ

What should I do first if my Gmail or Facebook is hacked?

Scan the PC, use the official recovery flow, change the password, sign out everywhere, enable 2FA, and check recovery contacts - per FTC steps.

Do I need to buy antivirus to recover an account?

No. A current Windows Security / Defender scan is a valid first step. Suites are optional later for multi-device households.

Why is email more important than social?

FTC: password-reset links for other services land in email. If email is owned by an attacker, they can take over banks, shopping, and social next.

What if friends already got scam messages from me?

Warn them quickly not to click or send money, and clean sent/DM history after you regain access.

Where do I report stolen personal information?

IdentityTheft.gov and ReportFraud.ftc.gov.

If you still want a paid suite

Recovering a hacked inbox is mostly account hygiene + official recovery. Microsoft Defender is a valid buy-nothing scan choice. If the household later wants multi-device paid protection, use only these on-site paid links: TotalAV (paid link), Norton (paid link), Bitdefender (paid link), McAfee (paid link), Avast (paid link).

Sources

- * How To Recover Your Hacked Email or Social Media Account (FTC)
- * Email or social media hacked? Here's what to do (FTC)
- * Use Two-Factor Authentication To Protect Your Accounts (FTC)
- * What To Do if You Were Scammed (FTC)
- * IdentityTheft.gov
- * ReportFraud.ftc.gov (FTC)
- * Turn On MFA (CISA)
- * Use Strong Passwords (CISA)
- * Update Software (CISA)
- * Windows Security overview (Microsoft)

Also read

- * Amazon account hacked: first hour
- * Kids' game account hacked
- * Turn on 2FA for Gmail, Apple, and bank
- * Check if your email was in a data breach
- * Password manager vs browser passwords