CyberGuardLab

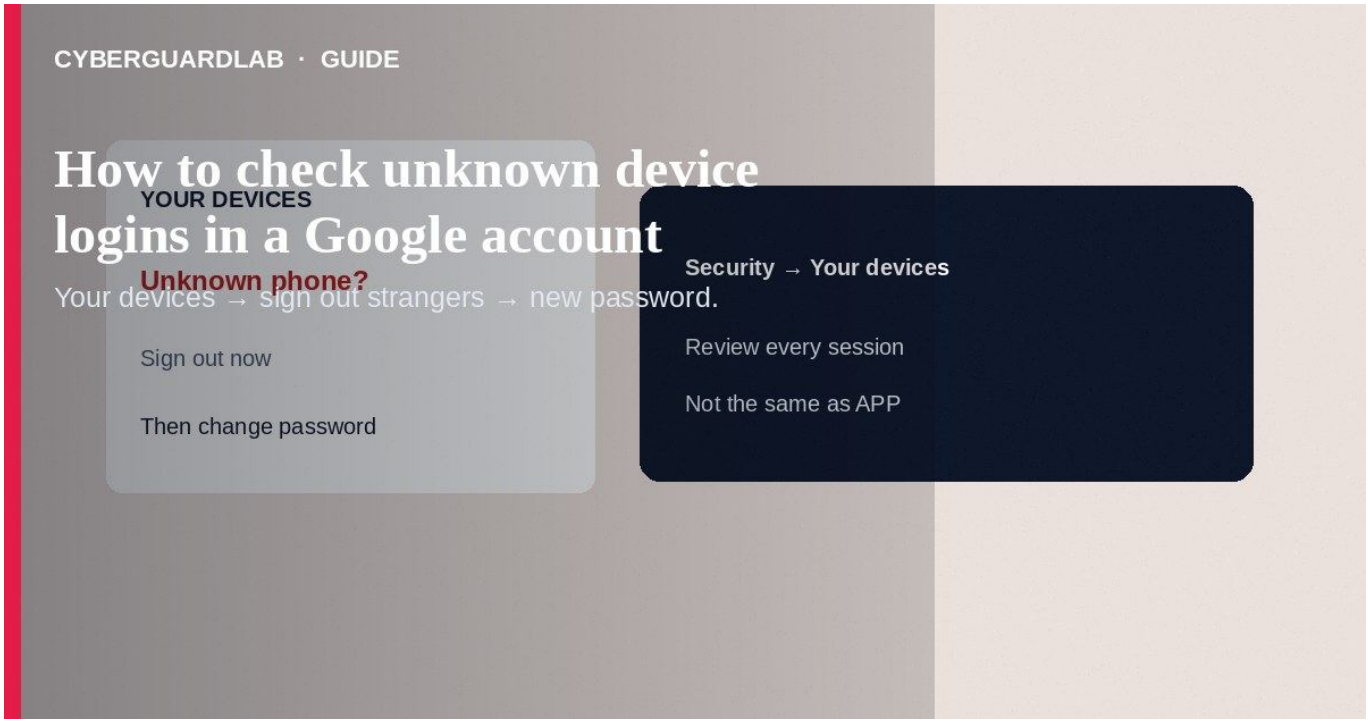
Household antivirus, explained

cyberguardlab.com

# How to check unknown device logins in a Google account

https://cyberguardlab.com/blog/google-unknown-device-logins

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.




To check unknown device logins on a Google account, open myaccount.google.com -> Security -> Your devices (wording may say "devices" or "manage all devices"), review each phone, tablet, and computer, and sign out anything you do not recognize. Then change the password from a device you trust and review recent security activity. This how-to is session hygiene-not enrolling in Advanced Protection, not third-party app OAuth review alone, and not Find My Device setup.

## 1. Why this matters

A password leak or reused credential can leave an attacker signed in on a spare browser profile. APP raises future sign-in difficulty; device review removes sessions that are already there.

**Paid link**

**Norton 360 | See the Norton first-year offer**

Shared Android tablets often stay signed into a parent Google account for years. After any password scare, remove old tablets from the device list even if "nobody hacks"-stale sessions are still sessions.

## 2. Legitimate vs suspicious cues

Cue | Likely fine | Investigate

Device name | Your current phone model / home PC | City or model you never owned

Timing | Matches when you traveled or used a hotel PC briefly | Sign-in while you slept, no travel

Duplicate browsers | Chrome on laptop + phone you use daily | Many "Windows" or "Linux" entries you never set up

Recovery changes | None, or ones you remember | New recovery email/phone you did not add

## 3. Steps: review devices and activity

* On a computer or phone you control, go to https://myaccount.google.com (type it; do not use an email link).
* Open Security.
* Under Your devices / Devices, select Manage all devices (labels vary).
* For each entry, check device name, location approximate, and last activity. Sign out / remove anything unknown.
* Open Recent security activity (or similar) and expand unfamiliar events-new sign-ins, password changes, recovery edits.
* If anything looks wrong: change password, turn on or strengthen 2-Step Verification, and review recovery phone/email.
* Review third-party apps with account access and revoke strangers.
* On Android, also check Settings -> Google -> Manage your Google Account -> Security for the same device list when convenient.

## 4. If you find an unknown device

* Sign it out immediately from the devices page.
* Change the Google password on a clean device.
* Check Gmail filters, forwarding, and "less secure" leftovers if any remain.

* Alert banks if you reuse that password elsewhere (you should not).
* Scan personal PCs with Norton or Bitdefender; one primary product is enough (TotalAV, McAfee, Avast on-site).
* Consider Advanced Protection if you are a high-risk target and can manage keys.

## FAQ

### Google shows a city I visited last month-is that a hack?

Often it is your own session with coarse geolocation. Still sign out old hotel or library machines you forgot.

### Is this the same as Advanced Protection?

No. Device review removes current sessions. APP changes how future sign-ins work.

### Should I use an email "security alert" button?

Open myaccount.google.com yourself. Phishing emails fake those alerts.

### Do I need to wipe my phone?

Not for a remote browser session alone. Wipe only if the phone itself is compromised or stolen-after backing up if you still control it.

## If you still want a paid suite

Avoiding how to check unknown device logins in a Google account does not require paid antivirus. Careful habits and official support paths are a valid buy-nothing stack. If you want multi-device paid protection later, use only these on-site paid links: TotalAV (paid link), Norton (paid link), Bitdefender (paid link), McAfee (paid link), Avast (paid link).

## Sources

* Google Account Help: Manage devices
* Google Account Help: Security checkup
* CISA: Compromised accounts guidance (general)
* FTC: IdentityTheft.gov

## Also read

* How to turn on Google Advanced Protection Program
* How to review Google account third-party app access
* How to spot a fake Google Play billing phishing email
* How to turn on enhanced Safe Browsing in Chrome
* How to check if your email was in a data breach