

CyberGuardLab

Household antivirus, explained

cyberguardlab.com

How to turn on Google Advanced Protection Program

<https://cyberguardlab.com/blog/google-advanced-protection-program>

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 turn on Google Advanced Protection Program

ADVANCED PROTECTION

Security keys required
Security keys / passkeys — Google's strictest tier.

- Tighter recovery rules
- Blocks risky OAuth apps

myaccount.google.com

- Register TWO keys first
- Test before you travel

Google Advanced Protection Program (APP) is Google's highest personal account security tier: it requires stronger sign-in (typically security keys or passkeys), tightens recovery, and blocks many risky apps. Enroll at myaccount.google.com under Advanced Protection *after* you have working security keys or passkeys and a recovery plan. This how-to is APP enrollment-not day-to-day unknown device login review, not Chrome Enhanced Safe Browsing, and not Play billing phishing.

1. Who should turn this on

Who should turn this on

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>

Journalists, activists, executives, high-value targets, and anyone who already uses hardware keys or passkeys and can accept stricter recovery. Casual accounts may find APP too restrictive (some apps and recovery options are limited). If you only need to kick off a strange phone, use the devices list first-APP is a different control plane.

Before you enroll

- * Buy or register at least two compatible security keys (or set up passkeys on trusted devices per Google's current APP requirements).
- * Update phones and browsers you use daily.
- * Save backup codes offline if Google still offers them for your setup; store a second key away from the first.
- * List apps that must keep Google access-APP can block less-secure or unverified OAuth clients.
- * Confirm you can open myaccount.google.com from a trusted device today.

Never enroll with only one key left in a travel bag. Register two keys, test both, and store one separately before you rely on APP for a high-risk trip.

2. Advanced Protection vs unknown device checks

Topic | Advanced Protection | Unknown device logins

Goal | Raise the bar for every future sign-in and app grant | Find and remove sessions that already look wrong

When | Proactive enrollment | Ongoing hygiene or after a scare

Hardware keys | Usually required or strongly preferred | Optional; password + 2SV may still apply

This guide | Yes | See unknown-device guide

3. Steps: turn on Advanced Protection

- * On a trusted computer or phone, open <https://myaccount.google.com> and sign in.
- * Go to Security (or search "Advanced Protection").
- * Open Advanced Protection Program / Get started.
- * Follow Google's enrollment wizard: register security keys or passkeys as required, confirm recovery contacts/options

Google still allows under APP, and acknowledge app restrictions.

- * Complete enrollment. Sign out other sessions if prompted.
- * Test sign-in on your phone and laptop with the new factors before you travel.
- * Review third-party app access and revoke anything you do not need.

4. After enrollment

- * Keep a spare key offline. Losing your only key without recovery is painful.
- * Prefer passkeys/security keys over SMS codes wherever Google allows.
- * If a PC feels compromised after phishing, change the password from a clean device, review devices, and scan with Norton or Bitdefender. Keep one primary suite-TotalAV, McAfee, and Avast are other on-site options.

FAQ

Is Advanced Protection the same as 2-Step Verification?

No. 2SV is the baseline. APP is a stricter program on top with tighter keys, recovery, and app rules.

Will APP stop every phishing page?

No. It makes stolen passwords far less useful and blocks many risky apps, but you must still refuse fake Google login pages.

Can I turn APP off later?

Google documents an exit path; expect delays and re-verification. Plan before you enroll if you share the account for work tools that may break.

Do I still need to check unknown devices?

Yes. APP reduces risk; device and session review remains healthy hygiene.

If you still want a paid suite

Avoiding how to turn on Google Advanced Protection Program 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: Advanced Protection Program
- * Google Safety Center: Advanced Protection
- * CISA: Multifactor authentication
- * FTC: Protect your personal information

Also read

- * How to check unknown device logins in a Google account
- * How to review Google account third-party app access
- * How to turn on enhanced Safe Browsing in Chrome
- * How to use Safari passkeys instead of passwords on iPhone
- * How to turn on 2FA for Gmail, Apple, and bank