CyberGuardLab

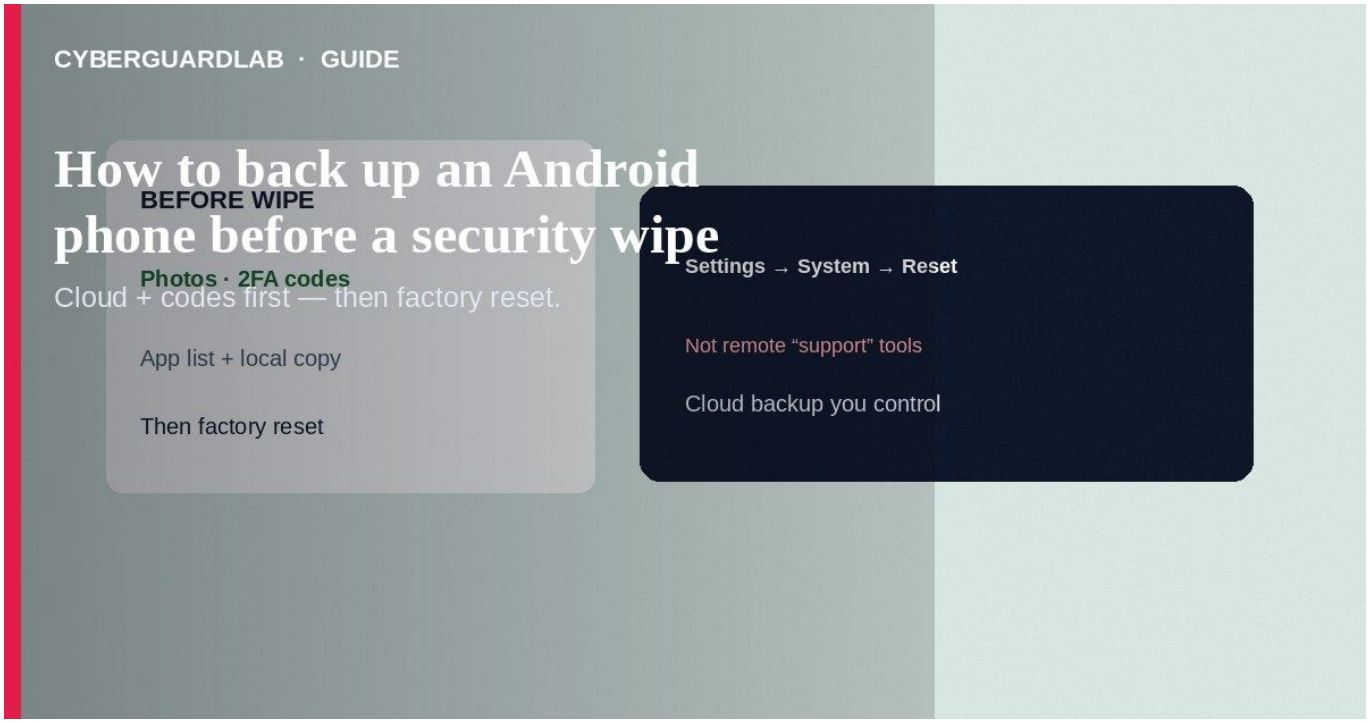
Household antivirus, explained

cyberguardlab.com

How to back up an Android phone before a security wipe

https://cyberguardlab.com/blog/android-backup-before-security-wipe

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.



Before a security wipe (factory reset after malware or account takeover), back up photos, messages you still need, 2FA backup codes, and app lists-then reset from Settings -> System -> Reset, not from a stranger's remote-support tool. Prefer cloud backups you control plus a quick local copy of irreplaceable files. This how-to is pre-wipe backup-not Private DNS, not Find My Device setup alone, and not the wipe steps for a phone you no longer hold.

1. What to capture before erase

* Photos/videos: Google Photos backup completed, or copy to a computer/SD card.
* 2FA: Export or write backup codes for authenticator apps; note hardware-key serials.
* SMS/call logs if your OEM or a trusted app still supports export (many do not-screenshot critical OTPs threads only if needed for fraud reports).
* WhatsApp/Signal: Use each app's official chat backup flow before reset.

* Offline files: Downloads, documents, VPN profiles you still trust.
* App list: Screenshot Play Store library or note paid apps.
* SIM / eSIM: Know how to re-download eSIM from the carrier after wipe.
* Work profile: Ask IT before wiping a managed device.

Remote helpers who ask you to install AnyDesk before a "free malware cleanup" often steal banking sessions. Backup yourself, wipe yourself, then restore-no gift-card "verification."

2. Backup vs wipe goals

Goal | Do this | Avoid

Keep memories | Photos + documents off-device | Skipping backup "to save time"

Remove malware | Factory reset after backup | Restoring a full rogue APK backup image from unknown USB

Account safety | New passwords + device review post-wipe | Reusing the same password the stealer already has

3. Steps: backup then security wipe

* Charge the phone above 50%. Connect to trusted Wi-Fi.
* Open Settings -> Google -> Backup (or System -> Backup) and run backup; wait until it shows success.
* Confirm Google Photos and any OEM cloud backup finished.
* Copy irreplaceable folders to a PC or encrypted drive.
* Sign out of banking apps after you no longer need in-app access for dispute screenshots.
* Uninstall malware first if Android still allows-then proceed to wipe if infection persists.
* Settings -> System -> Reset options -> Erase all data (factory reset). Confirm.
* After setup wizard, restore from the Google backup you created; reinstall apps from Play only.
* Change Google and important passwords from a clean browser if the wipe followed compromise.

* Re-enable Play Protect, screen lock, and Find My Device.

4. If malware blocked Settings

* Try Safe Mode (OEM power-menu variants differ) and uninstall the bad app, then backup and wipe.
* If the UI is locked, use android.com/find erase from another device when Find My Device was already on-accept that local-only files may be gone.
* Scan PCs that exchanged files with Norton or Bitdefender (TotalAV, McAfee, Avast on-site).

FAQ

Will Google Backup restore SMS?

Depends on Android version and OEM. Do not assume texts return-save fraud evidence first.

Is a full Titanium-style root backup safe after malware?

Risky. Prefer cloud app data + media, then clean Play reinstalls.

Should I wipe before or after changing the Google password?

If you still control a clean device, change the password first, then wipe the infected phone. If the phone is your only factor, use backup codes carefully.

Does this replace Advanced Protection?

No. Backup/wipe is incident response; APP is long-term hardening.

If you still want a paid suite

Avoiding how to back up an Android phone before a security wipe 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

* Android Help: Back up or restore
* Android Help: Factory reset
* CISA: Malware basics
* FTC: Malware

Also read

* How to spot a fake carrier 5G upgrade malware APK
* How to wipe a device before selling
* How to turn on Google Find My Device before you lose a phone
* How to turn on Private DNS on Android
* How to use a work profile to isolate risky Android apps