

CyberGuardLab

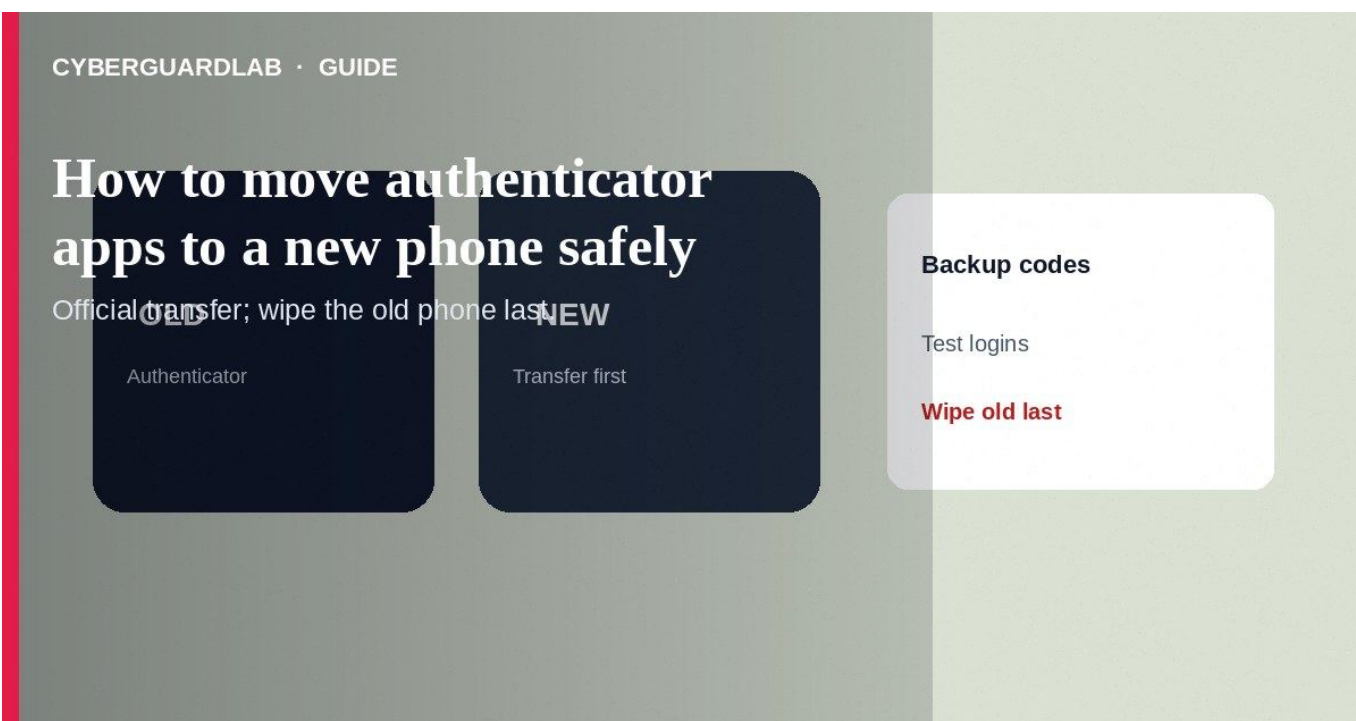
Household antivirus, explained

cyberguardlab.com

How to move authenticator apps to a new phone safely

<https://cyberguardlab.com/blog/move-authenticator-apps-new-phone>

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.



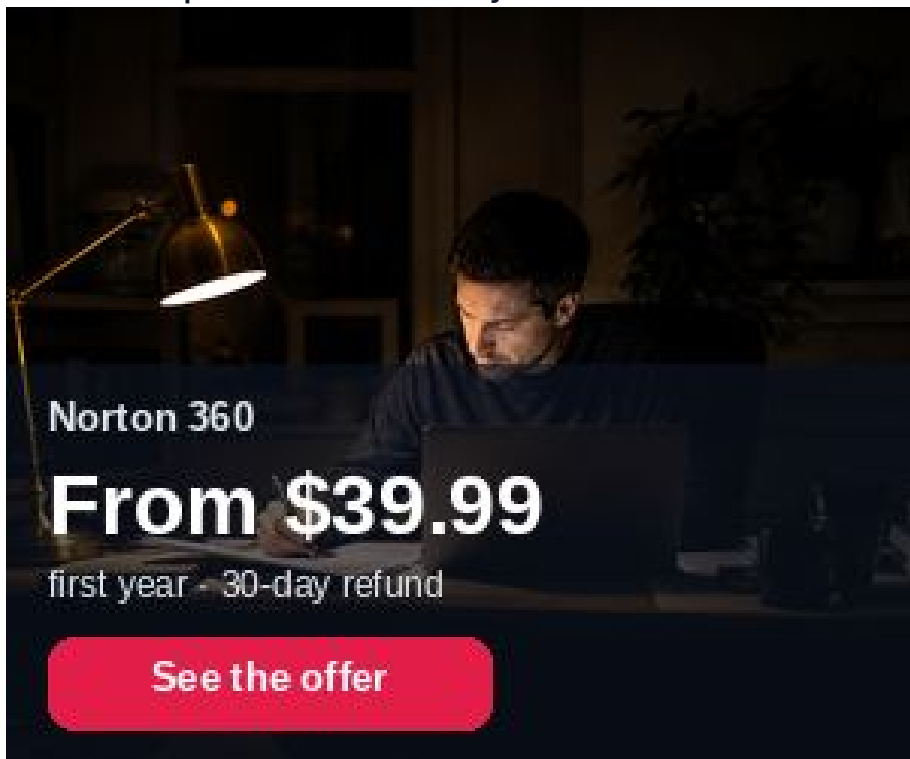
Moving authenticator apps to a new phone means transferring time-based one-time password (TOTP) accounts-or re-enrolling each service-without locking yourself out or exposing backup codes to phishing. Use each authenticator's official transfer/export feature while both phones are in your hands, keep printed backup codes offline, and remove the old device only after test logins succeed. This how-to is about safe authenticator migration-not fake 2FA SMS, not carrier SIM locks, and not switching Google specifically to Prompt (though you may do that in parallel).

1. Plan before you wipe the old phone

Inventory accounts that use authenticator apps (email, banking, password manager, work VPN, social). Locate backup/recovery codes for each critical service. Charge both phones. Do not factory-reset the old phone until every high-value account produces a working code on the new phone.

Paid link

Norton 360 | See the Norton first-year offer



Norton 360

From \$39.99

first year - 30-day refund

See the offer

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

Offer page: <https://cyberguardlab.com/norton>

Chat ads offering to "move your Google Authenticator for a fee" are high-risk. Keep both phones physically present, use official export QR flows, and never send backup codes to a stranger.

2. Transfer checklist

Item | Before wipe | After wipe

Email 2FA | Codes work on new phone | Old phone removed from trusted devices

Banking | Re-enrolled or transferred | Test one login

Backup codes | Printed / stored offline | Still reachable without the old phone

Carrier locks | Number lock on; PIN set | Still on after eSIM move

3. Steps: migrate safely

- * Install the same authenticator app from the official app store on the new phone (Google Authenticator, Microsoft Authenticator, Authy, or your password manager's TOTP-follow that product's docs).
- * Prefer built-in transfer: many apps show a QR export on the old phone and a scan-to-import on the new phone. Complete transfer over your local screens-not by emailing screenshots to "support."
- * If an app lacks transfer, open each important website/app -> Security -> 2FA -> change authenticator device, scan the new QR, confirm a code, and save fresh backup codes.
- * For Google accounts, you may add Google Prompt on the new phone and keep backup codes-see Google Prompt instead of SMS.
- * Test sign-in on email and banking with the new phone's codes while the old phone still works.
- * Only then remove 2FA from the old authenticator or wipe the old phone per the manufacturer's steps.
- * Store backup codes in a sealed offline place or a locked password manager-never in SMS or an unmarked cloud note titled "codes."

* If anything looks like malware during installs, pause and scan with a trusted tool such as Norton or Bitdefender. Keep one primary real-time antivirus-avoid stacking full suites. TotalAV, McAfee, and Avast are other on-site comparison options.

4. If something goes wrong

- * Locked out: use each service's official account-recovery and backup codes-not a freelancer who asks for remote access.
- * QR export photographed by others: treat secrets as exposed; rotate 2FA on those accounts.
- * Cloud sync authenticator you did not intend: review that vendor's security docs; add app locks and device encryption.
- * Old phone lost before transfer: use backup codes immediately; freeze risky financial accounts if needed.

FAQ

Can I just screenshot all QR codes?

Screenshots in cloud camera rolls are easy to steal. Prefer in-app transfer and offline backup codes.

Is this the same as turning on Google Prompt?

No. Prompt is a Google sign-in approval method. Authenticator migration moves TOTP secrets (or re-binds them) across phones.

Do I need to disable carrier number lock to migrate authenticators?

Usually no. Number lock affects SIM/porting, not app installs. Only adjust locks if you are also changing SIM/eSIM.

What if my authenticator used SMS as backup?

Replace SMS backups with codes or security keys when the service allows-SMS remains phishable.

If you still want a paid suite

Avoiding how to move authenticator apps to a new phone safely 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 Authenticator Help: transfer to a new phone
- * Google Account Help: 2-Step Verification
- * FTC: Protect your personal information
- * IdentityTheft.gov
- * FTC ReportFraud

Also read

- * How to spot a fake two-factor authentication text
- * How to turn on Google Prompt instead of SMS codes
- * How to turn on number lock at T-Mobile, Verizon, or AT&T
- * How to set a carrier account PIN to stop SIM swap
- * How to run a Google Account Security Checkup