How to back up your 2FA codes

You're juggling more passwords than a Vegas magician, and suddenly it hits you – what if your fancy smartphone takes a swan dive off your yacht?

(Or, let's be real, into your toilet bowl during a late-night scroll session.)

That WOULD be an issue, especially if you're using a 2FA app like Authy or Google Authenticator.

2FA, or 2 Factor Authentication, is a method of securing your account by entering a code given to you on a different device.

It's no Yubikey, but it's a pretty good method. (Except text-based 2FA, where they send you a code through text. That's the least secure.)

Since your codes are secured in an app, the best way to keep them safe is to back them up somewhere. If you lose your phone… you're kind of screwed.

Google Authenticator codes are based on a mathematical equation, not stored by Google. There's no "forgot password" option.

But, fear not.

I'm about to show you how to turn that old brick of a phone gathering dust in your junk drawer into a Fort Knox for your digital keys. And then an extra “paper” method to stay super safe.

There are two main migration methods.

Export/Import (Easiest Method):

- Open Google Authenticator and tap the three dots in the upper right.
- Select "Export accounts."
- Choose which codes to export (up to 10 at a time).
- A large QR code will be generated.
- On your backup phone, open Google Authenticator and select "Scan QR code."
- Scan the generated QR code to import all selected accounts.

Note: This exported QR code only works with Google Authenticator, not other authenticator apps.

Manual Migration (Time-consuming):

- Log into each account individually.
- Navigate to the security or 2FA settings.

- Either turn off 2FA and set it up again, or add a new authenticator device.
- Scan the new QR code with both your current phone and backup phone.

This method is more time-consuming but allows you to switch to a different authenticator app or reset potentially compromised codes.

Here’s the super-secure way to export/import your codes onto that old phone:

Step 1: Dig out that old phone. You know the one – it's probably nestled between your collection of embarrassing campaign buttons and that survival seed vault you bought during your prepper phase.

Step 2: Fire that bad boy up.

Step 3: Delete every app you don't need. And I mean EVERY app. If it's not essential for running authenticators, it's gotta go. Think of it as a digital Marie Kondo session – if it doesn't spark joy (or security), out it goes.

Step 4: Update that sucker. I know, I know – waiting for a phone from the Obama era to update is about as exciting as watching paint dry in a Venezuelan inflation crisis. But trust me, it's worth it. You want this thing locked down tighter than Fort Knox during a gold rush.

Step 5: Time to connect to the WiFi and download your authenticator apps. Google Authenticator, Authy – pick your poison. Just make sure it's from the official app store.

Step 6: Now for the fun part – transferring your existing authenticators. Use the export feature on your current phone, or if you're feeling particularly masochistic, enter those secret keys manually. It's a great way to test your patience and your eyesight simultaneously.

You'll usually find this feature hiding in the settings, probably under some innocuous name like "Transfer accounts" or "Move to another device." Once you've found it, the app will likely generate a QR code.

Step 7: Scan the code.

You'll need to scan this QR code with your old phone's authenticator app.

Step 8: Lock this thing down. Once you've got everything set up, treat this phone like it's carrying state secrets.

Keep it offline when you're not using it. Store it somewhere safe – and no, the bowl of loose change on your nightstand doesn't count.

PRO-TIP: For added security, you can take a picture of the export QR code, print it out, and keep it in your safe. If you ever need it, simply scan the QR code from the paper and voila, you're back in the game.