Google Authenticator finally, mercifully adds account syncing for two-factor codes

Google Authenticator is adding a long-standing customer request: you can now sync your two-factor authentication codes to your Google account. So when you set up a new phone and log in to your account, Authenticator will be ready to go without requiring its own setup process. This also means that if you lose your phone or it's stolen, getting back into your accounts from another device will be less of a nerve-racking ordeal.

Cloud syncing has become relatively common across other two-factor tools like Authy, but Google really dragged its feet bringing it to Authenticator, which launched all the way back in 2010.

"One major piece of feedback we've heard from users over the years was the complexity in dealing with lost or stolen devices that had Google Authenticator installed," Google's Christiaan Brand wrote in a blog post. "Since one time codes in Authenticator were only stored on a single device, a loss of that device meant that users lost their ability to sign in to any service on which they'd set up 2FA using Authenticator."

"With this update we're rolling out a solution to this problem, making one time codes more durable by storing them safely in users' Google account," Brand wrote. "This change means users are better protected from lockout and that services can rely on users retaining access, increasing both convenience and security."

To enable cloud syncing for two-factor codes, you'll need to update to the latest version of the Authenticator app for Android and iOS. Google has a support page that goes into more detail on the feature, confirming that "if you're signed into your Google Account within Google Authenticator, your codes will automatically be backed up and restored on any new device you use."

That sound you hear is IT support staffers everywhere breathing an enormous sigh of relief. This was a much-needed step to make one-time codes easier to use. Authenticator and other apps like it are a much safer option than relying on SMS codes. Did you know that iOS can now do this natively? Not everyone is aware. The more friction you can eliminate, the more adoption there will be.

The convenience of cloud syncing potentially comes with added risk

But cloud syncing of one-time passcodes could potentially make targeting Google accounts even more tempting for malicious actors. If you can break into an account, you could gain access to a bevy of sensitive accounts. Google spokesperson Kimberly Samra confirmed that account syncing is totally optional. But if you enable it, don't expect any extra security precautions beyond Google's standard measures. To keep out uninvited guests, Authy has both a unique password for restoring two-factor backups *and* a toggle to allow (or prevent) multiple devices from being used with an account.

With this update, the Authenticator app is also switching to a new logo, ditching the drab vault look for an asterisk in Google's colors. "While we're pushing towards a passwordless future, authentication codes remain an important part of internet security today, so we've continued to make optimizations to the Google Authenticator app," Brand wrote.

Update April 24th, 4:00PM ET: *The article has been updated*

with confirmation from a Google spokesperson that account syncing is optional.

https://www.theverge.com/2023/4/24/23696058/google-authenticator-app-account-syncing-multiple-devices