

How to set up two-factor authentication on your online accounts

An extra step of security never hurt anybody

By **Natt Garun** and **Barbara Krasnoff** | Updated Jun 10, 2021, 8:10am EDT

If you buy something from a Verge link, Vox Media may earn a commission. See our [ethics statement](#).

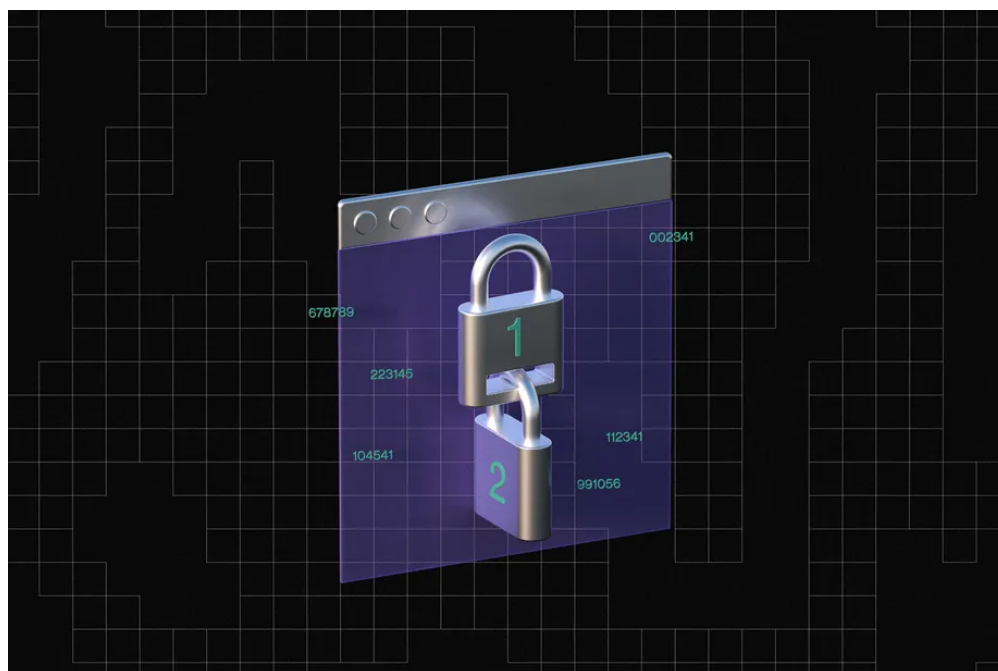


Illustration by Maria Chimishkyan

Part of
Lock it down

Just about any account you own on the internet is prone to being hacked. After numerous widespread breaches through the past few years, tech companies have been working together to [develop a standard](#) that would make passwords a thing of the past, replacing them with more secure methods like biometric or PIN-based logins that do not require transferring data over the internet.

But while those standards are still being adopted, the next best way to secure your accounts is two-factor authentication, or 2FA. This is a process that gives web services secondary access to the account owner (you) in order to verify a login attempt. Typically, this involves a phone number and / or email address. This is how it works: when you log in to a service, you use your mobile phone to verify your identity by either clicking on a texted / emailed link or typing in a number sent by an authenticator app.

If you want something that doesn't depend on software to keep your device safe, you can also opt for a security key. The USB- or NFC-based hardware plugs into your computer or mobile device to authenticate, making it harder for hackers to intercept since security keys can't be duplicated. For more information on how security keys work, [check out our security key guide](#).

WHAT ARE AUTHENTICATOR APPS?

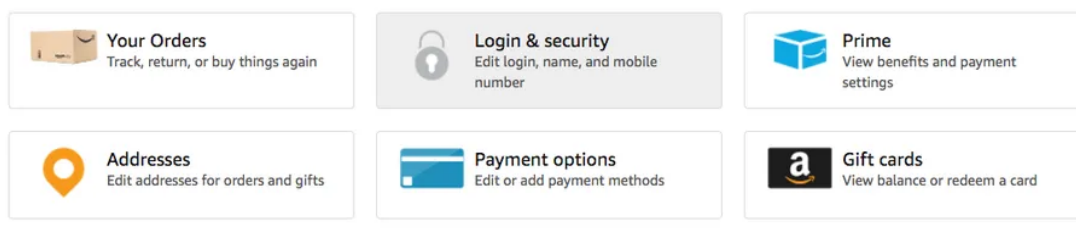
Authenticator apps are [considered more secure than texting](#). They also offer flexibility when you're traveling to a place without cellular service. Popular options include [Authy](#), [Google Authenticator](#), [Microsoft Authenticator](#), and [Hemng OTP](#) (iOS only). These apps mostly follow the same procedure when you're adding a new account: you scan a QR code associated with your account, and it is saved in the app. The next time you log in to your service or app, it will ask for a numerical code; just open up the authenticator app to find the randomly generated code required to get past security.

While 2FA — via text, email, or an authenticator app — does not completely cloak you from potential hackers, it is an important step in preventing your account from being accessed by unauthorized users. Here's how to enable 2FA on your accounts across the web. (We've listed the services in alphabetical order.)

AMAZON

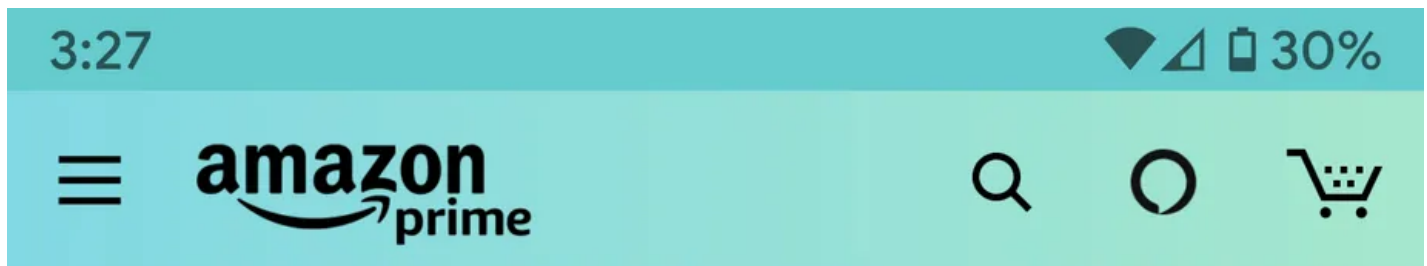
Go to the Amazon homepage and log in. Hover over “Accounts & Lists” and click on “Account.” A box labeled “Login & security” will be at the top of the page, so click on that and then click the “Edit” button on “Two-Step Verification (2SV) Settings.” (You may be asked to reenter your password first.) You can also navigate directly to that page by [following this link](#).

Click “Get Started” and Amazon will walk you through the process of registering your phone number, or you can opt to use your preferred authenticator app by syncing it through a QR code.



Start with Amazon’s “Login & security” section.

You can activate 2FA on both the Android and iOS Amazon app by tapping the three-line “hamburger” menu on the left side and finding “Your Account” > “Login & security.” The same “Two-Step Verification (2SV) Settings” selection should be available for you to edit and toggle on 2FA.

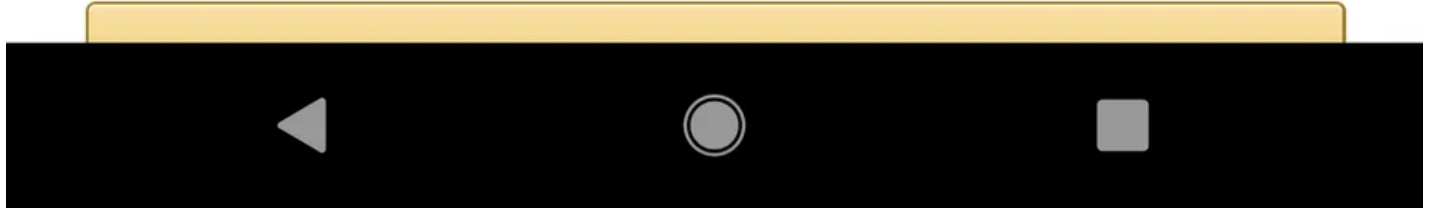


Login & security

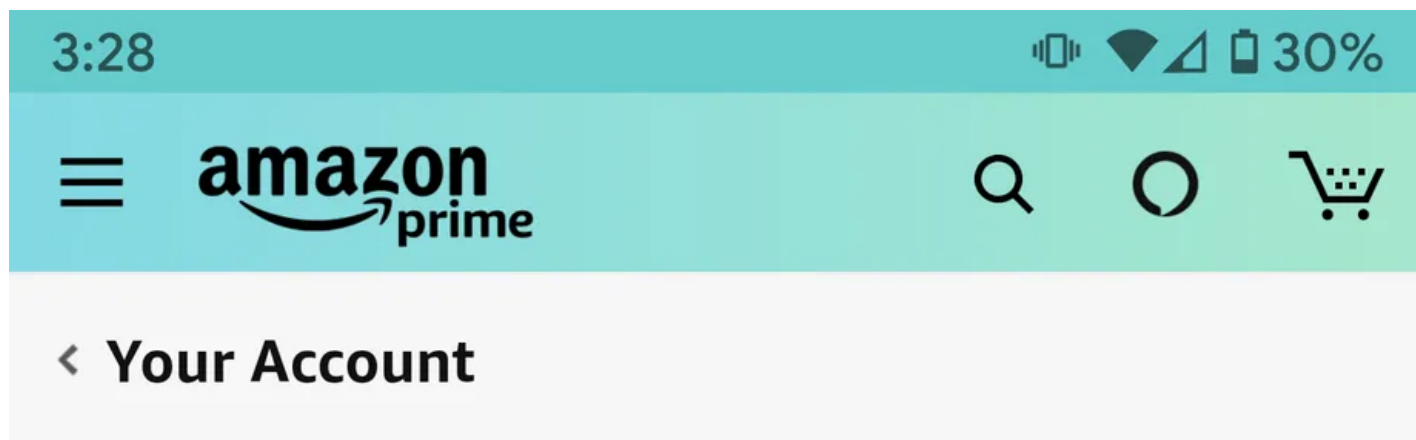
Name: B	Edit
Email: @	Edit
Mobile Phone Number: Why add a mobile number?	Add
Password: *****	Edit
Two-Step Verification (2SV) Settings:	Edit

Settings.

Manage your Two Step Verification (2SV) Authenticators



The Amazon app also lets you set up two-step verification.



Two-Step Verification (2SV) Settings

Two-Step Verification

Disable

Enabled

Preferred method

Authenticator App

[Change](#)

1 app enrolled

[Add new app](#)

Backup methods

No methods specified

Add new phone

Devices that suppress OTP

You may suppress future OTP challenges by



You can use a third-party authenticator app.

Once your phone number or authenticator app has been verified, you can select trusted devices to bypass 2FA or generate a code to log in via a mobile app.

APPLE

Two-factor authentication is currently offered to Apple users on iOS 9 and later, and on macOS X El Capitan and later.

IOS

The steps are slightly different depending on how updated your iOS software is. For those using iOS 10.3 or later, you can enable 2FA on your Apple ID by going to “Settings” > [Your Name] > “Password & Security” > “Two-Factor Authentication.” Turn on 2FA to receive a text message with a code each time you log in.

For those using iOS 10.2 or earlier, the settings are under “iCloud” > “Apple ID” > “Password & Security.”

MACOS

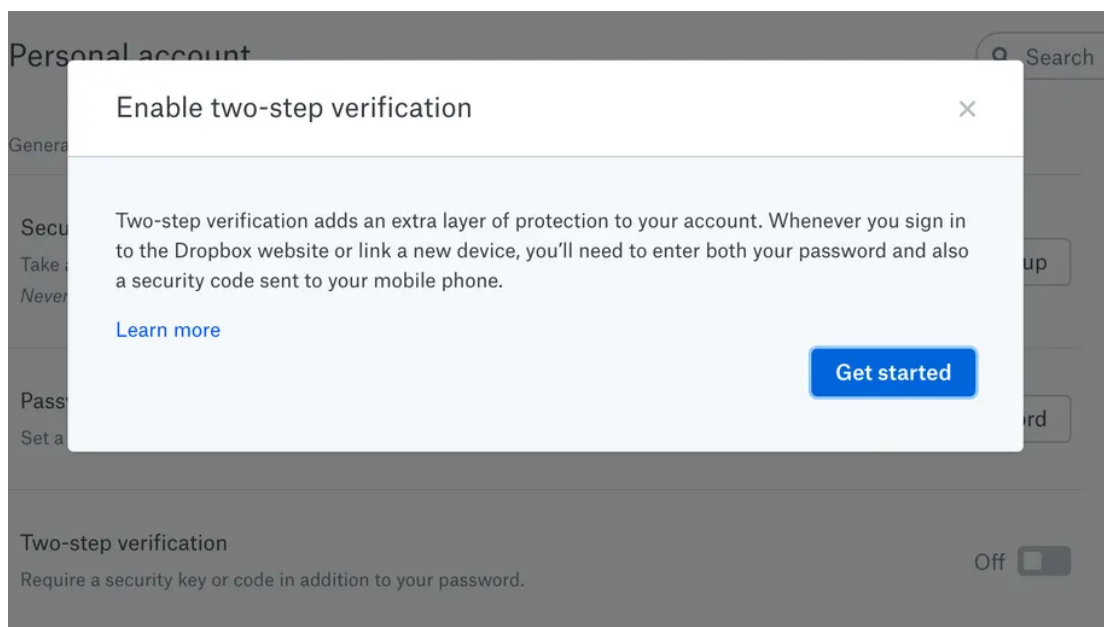
Again, steps are slightly different depending on your version of macOS. If you’re using Catalina or later, click the Apple icon on the upper-left corner of your screen, then click “System Preferences” > “Apple ID.” Click on “Password & Security” under your name, and then select “Turn On Two-Factor Authentication.”

For Mojave and earlier, after you click the Apple icon, click “System Preferences” > “iCloud” > “Account Details.” (You can shorten this step a bit by typing in “iCloud” using Spotlight.) Click on “Security” and you’ll see the option to turn on 2FA.

The remainder of the steps, for iOS or Mac, are the same. You can opt for Apple to send you a six-digit verification code by text message or phone call. macOS system preferences don’t support physical security keys, but you may be able to set one up through the security key’s software if you want to use one.

DROPBOX

From your Dropbox homepage on the web, click your profile avatar and select “Settings,” then go to the “Security” tab. Find “Two-Step Verification,” which will tell you the status of your 2FA. Toggle to turn the feature on and choose to receive 2FA through a text or your authenticator app.



Dropbox also lets you use a text or authenticator app.

FACEBOOK

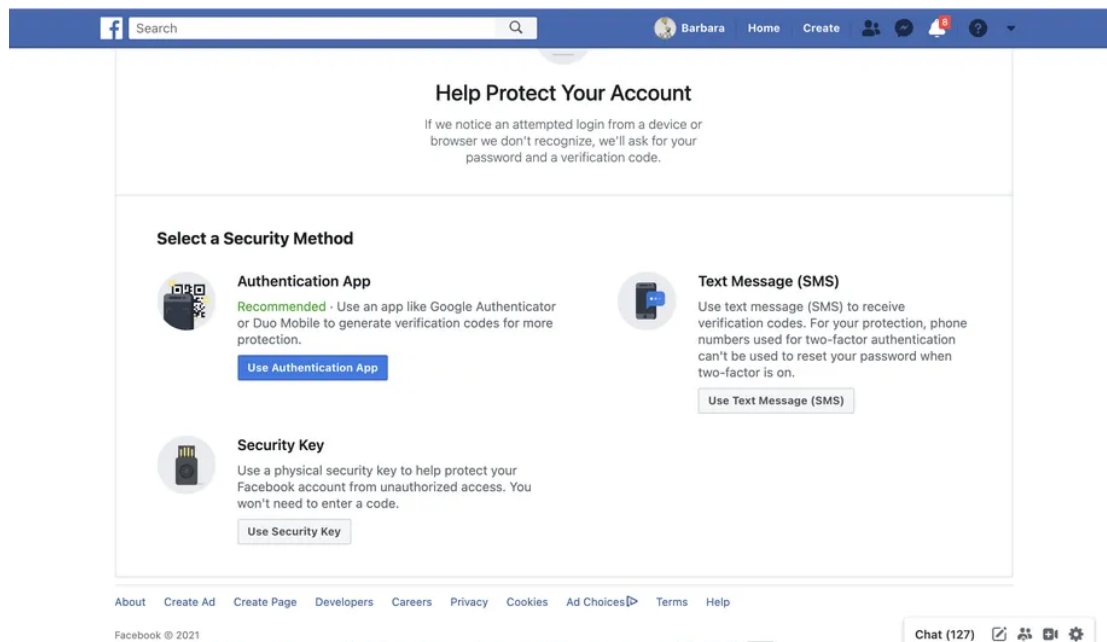
The way to access Facebook’s 2FA settings is a bit different between the app and the web (and Facebook tends to update both layouts often).

On the mobile app, you can access your privacy settings by tapping the hamburger icon on the upper-right corner (Android) or the lower-right corner (iOS) and scrolling down to

the bottom to find the “Settings & Privacy” menu. Tap “Settings” > “Security and Login” and select “Use two-factor authentication.”

You can opt for a text message, an authenticator app, or a security key.

On the web, click the down arrow in the upper-right corner, and select “Settings & Privacy” > “Privacy Shortcuts.” Look for the “Account Security” heading and click on “Use two-factor authentication.”



Facebook lets you authenticate via text message, an authenticator app, or a security key.

Additionally, for apps that don't support 2FA when logging in with a Facebook account (such as Xbox and Spotify), you can generate a unique password specifically associated with that account. From the original down arrow, select “Settings & Privacy” > “Settings,” and then, from the menu on the left, “Security and Login” > “App passwords” (under the “Two-Factor Authentication” subhead). After resubmitting your Facebook password, you'll be able to name the app, click generate, and save that password for the next time you have to log in. Under the same “Two-Factor Authorization” subhead, you can choose specific iterations of the app (say, on your laptop) where you can forgo the login code.

FITBIT

Fitbit has only recently added 2FA — in fact, as this was written, the feature was rolling out, but we haven't seen it yet, so we haven't been able to verify these steps. But

assuming you've got access to the new feature, here's what you do:

To turn 2FA for your Fitbit, tap on the "Today" tab in your app and then on your profile image. Select "Account Settings" > "Two Factor Authorization" and turn 2FA on. Fitbit will send you a text message with a verification code; once you enter that, along with your password, you're in. (Unfortunately, Fitbit only uses text messages for verification, rather than giving you an option for an authenticator app.)

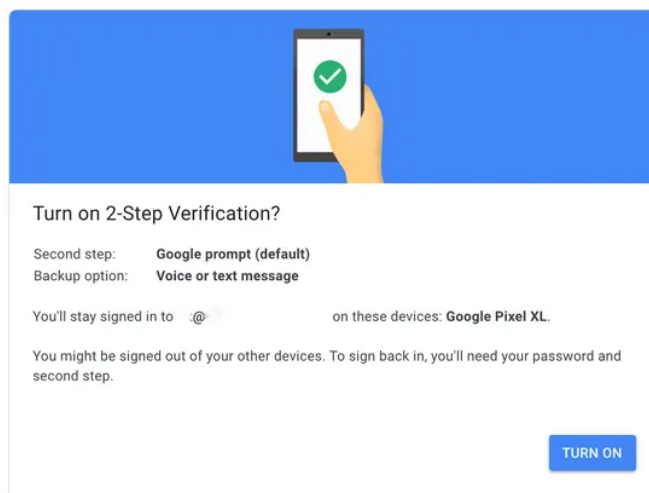
Fitbit gives you a recovery code to use in case you lose or change your phone. The company recommends that you put that code somewhere safe; if you lose the code, you can get another one by using the app to turn off 2FA and then turn it on again.

GOOGLE

The easiest way to turn on 2FA across your Google accounts (e.g., Gmail, YouTube, or Google Maps) is by heading over to the main [2FA landing page](#) and clicking "Get Started." You'll be asked to log in and then select your mobile device from a list. (If you have an iPhone, you may have to download a separate app.) If Google succeeds in sending a message to that phone, you will be asked to enter a phone number, and then you can choose whether you want to receive verification codes by text message or phone call. Again, Google will try out your chosen method.

After that, Google will first send prompts to your phone that allow you to simply select "Yes" or "No" when a login attempt occurs. If that doesn't work, it will send the text message or phone call.

← 2-Step Verification



Once 2FA is enabled, Google will send a notification asking you to authenticate.

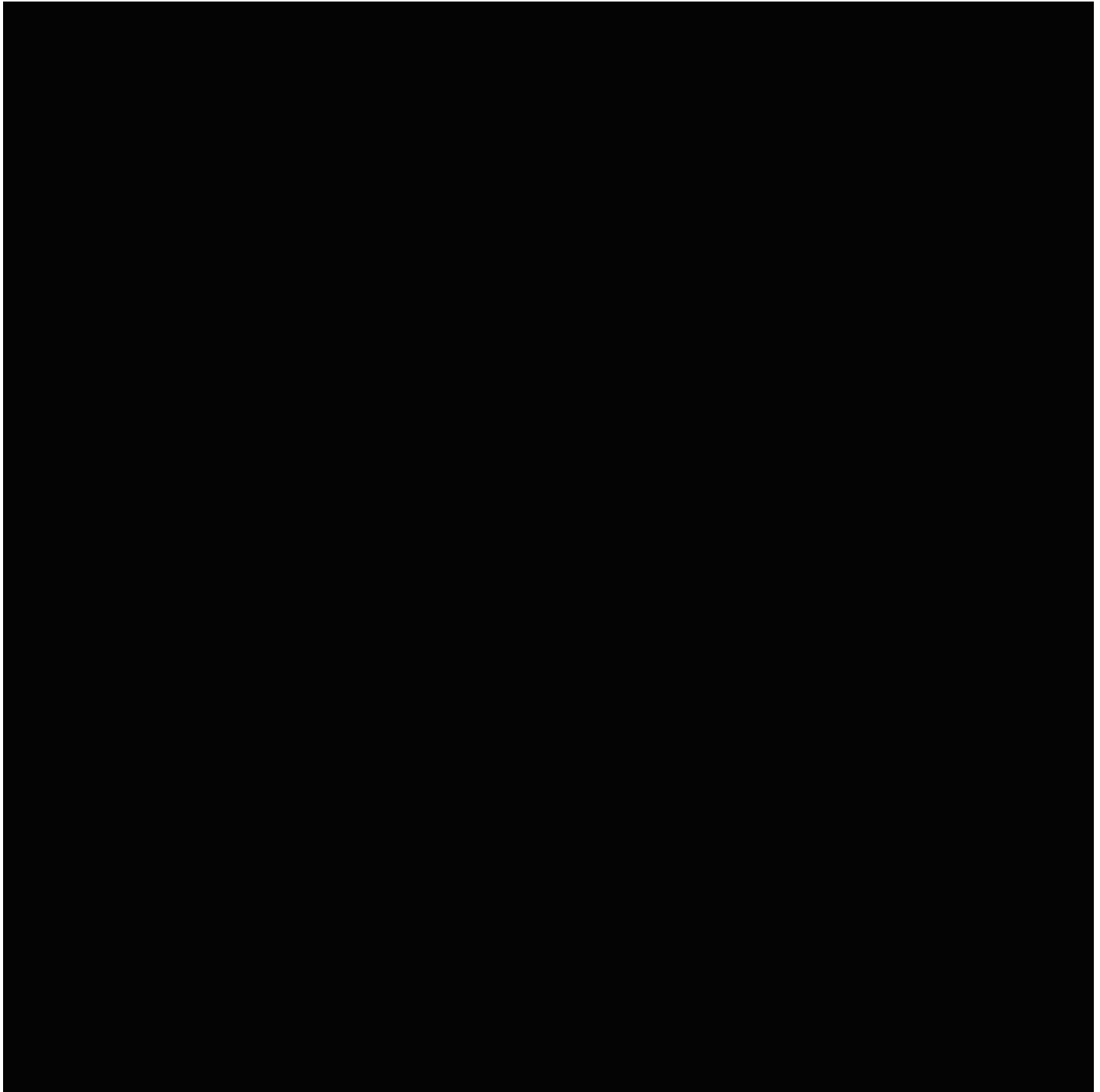
You can also generate backup codes for offline access. Google generates 10 codes at a time and they're designed to be single-use, so once you've successfully used one, cross it out (assuming you've printed them), as it will no longer work.

INSTAGRAM

Instagram added 2FA to its mobile app in 2017, but now you can also activate it through the web.

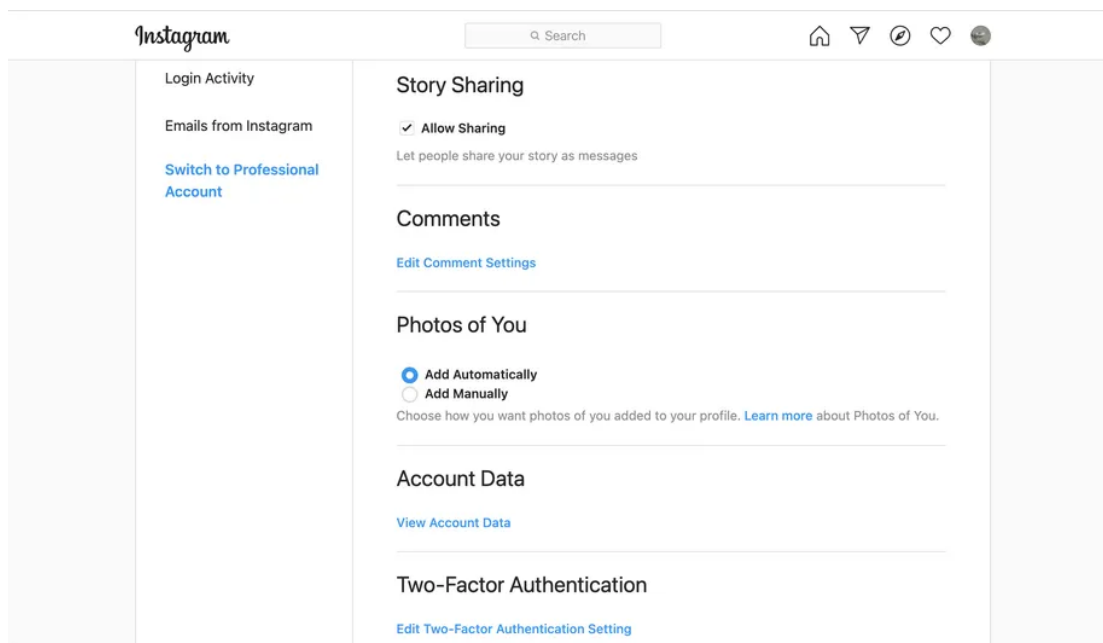
To activate 2FA on your mobile app, tap on your profile and select the hamburger menu on the upper-right corner. Look for "Settings" > "Security," where you'll find a menu item for "Two-Factor Authentication."

Here, you can choose between text message-based verification or a code sent to your authenticator app.



GIF by Amelia Krales / The Verge

To turn on 2FA using the web, log in to Instagram, click on your profile icon in the upper-right corner, and select “Settings” from the drop-down menu. Clicking this will pop open a settings menu, where you can find the same “Privacy and Security” section as on the app. From here, you can turn on 2FA and, just as in the app, choose your method for verification.



Go to the Instagram settings page, then “Privacy and Security.”

MICROSOFT

Log in to your Microsoft account and find the “[Security settings](#)” menu (there are several ways to get there; click on the link for the easiest). Look for the “Two-step verification” section and click on the setup link. You’ll be walked through the steps needed to use either the Microsoft Authenticator app or a different authentication app. You’ll also be able to create passwords for apps that don’t accept 2FA.

NEST

Smart home products like Nest are not exempt from getting hacked. Current Nest users will have signed in to the app via their Google accounts, and so will be using Google’s 2FA feature (see above).

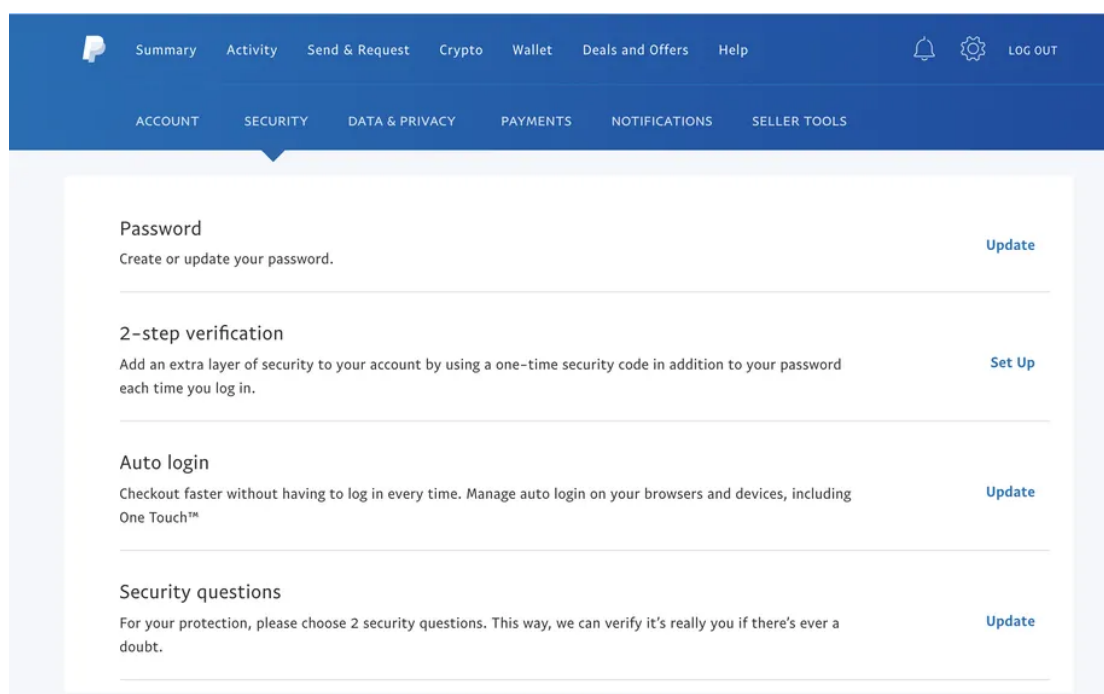
If you’ve resisted migrating your existing Nest account to your Google account, you may still be able to use 2FA. On the home screen, go to “Settings” > “Account” > “Manage account” > “Account security,” and select two-step verification. Toggle the switch to on. A series of prompts will ask for your password, phone number, and the verification code that will be sent to your phone.

Keep in mind that all of your devices will be automatically signed out, so you’ll have to sign in again using two-step verification.

If all your family members don't have their own logins and have been using yours, it's a good idea to set them up with separate logins using Family Accounts. Otherwise, when they try to log on using two-step verification, the necessary code will be sent to your phone, not theirs.

PAYPAL

On the main Summary page, click the gear icon and select the "Security" tab. Look for the section called "2-step verification" and click on the "Set Up" link. You'll be able to choose whether to have a code texted to you or to use an authenticator app. (PayPal also offers to find an authenticator app if you want one.)



PayPal will offer to find an authenticator app if you don't have one.

If you lose your phone, change numbers, or decide to revoke authorization rights, come back to this menu to make adjustments.

Note that the interface is different if you use PayPal as a business account. From the main "Summary" page, click the gear icon to be taken to the "Settings" page. Under "Login and Security," look for the "Security Key" option to add your phone number or a security key as your 2FA method.

RING

Like with Nest, make sure your Ring app is up to date. Swipe over from the left, then go to “Account” > “Two-Step Verification” (you’ll find it under “Account Security”). Tap the big “Turn on two-factor” button. A series of prompts will ask for your password, phone number, and the verification code that will be sent to your phone.

From then on, you’ll need both your password and an SMS verification code whenever you want to log in to Ring from a new device. You can also opt to have the codes sent to an email address instead of over SMS.

SIGNAL

Rather than traditional 2FA, Signal uses a PIN. Select your profile icon on the upper-left side to reach the “Settings” menu, and then select “Account.” If you toggle on “Registration Lock,” each time you re-register your phone number, you’ll need to enter your PIN (which you were asked for when you originally registered). Signal requires your PIN to be at least four digits long, up to a maximum of 20 digits.

When you first enable Registration Lock, Signal will ask you to type in your PIN for the first six and 12 hours after being enabled. The company says this is designed to help you to remember it through random repetition. So after the first day, it will ask you to enter it in the next day, then in three days, after a full week, and finally one last time after 14 days.

If you happen to forget your PIN and can’t log in to Signal, you will have to wait for seven days of inactivity for your registration lock to expire, after which you can log in to your app again to set up a new PIN. Those already actively using Signal won’t have to worry about the Registration Lock resetting, as that clock starts only when the app isn’t open.

SLACK

To enable 2FA, you’ll first need to find the “Account Settings” page. There are two ways to access this:


- Click on your username or profile picture in the Slack app to open a drop-down menu, and then select “View profile.” Your account information will now display on the right side of the chat window. Under your avatar, next to the “Edit Profile” button, click the three-dot icon for additional actions, and select “Account settings.” You can also head straight to my.slack.com/account/settings.

- You should immediately see the selection for “Two-Factor Authentication.”

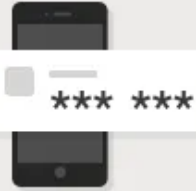
If you do not see the option for 2FA, check whether your Slack account is for work. Some employers may use single sign-on services that bypass the need for 2FA, which would remove this option from Slack’s Account Settings page.

How would you like to receive your authentication codes?

You will be asked for an authentication code when you sign in to your account.

*** **

SMS Text Message →
Receive a text message to your mobile device when signing in.

*** **

Use an app →
Retrieve codes from an authentication app on your device, like Google Authenticator, Duo Mobile, Authy, or Windows Phone Authenticator.

Like most other apps, Slack lets you use either SMS or an authentication app.

If this is a personal Slack, however, then select “Expand” on “Two-Factor Authentication” and hit the “Set Up Two-Factor Authentication” button to verify your information via an SMS or authenticator app. If you have multiple email addresses, you may need to select a default one before you can decide on your preferred 2FA method.

SNAPCHAT

From the app’s main camera screen, tap your profile icon and find the gear icon to access your settings. Select “Two-Factor Authentication” and choose whether to receive a text message verification or hook it up to your authenticator app.

Once 2FA has been enabled on your Snapchat account, you can add trusted devices, plus request a recovery code for when you’re planning to be somewhere without cellular service. Snapchat does not seem to currently support security-key logins.

TIKTOK

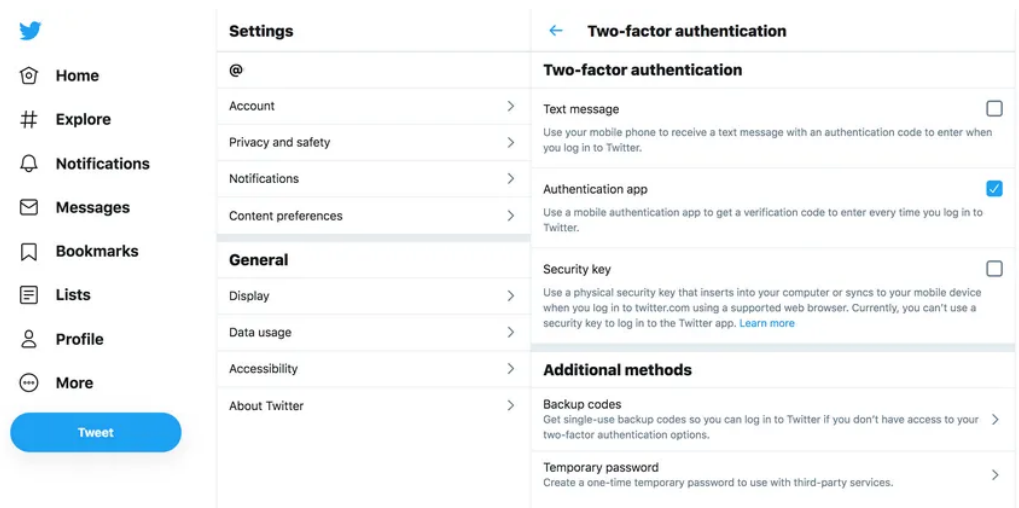
To set up 2FA on TikTok (in this case, we’re assuming a mobile device), tap your profile icon on the lower right, then the three dots in the upper right of the screen. Go to “Security and login” and you’ll see “2-step verification.” TikTok offers to send a verification code via a text message or email.

TWITTER

On the Twitter mobile app, tap the three-line “hamburger” icon at the top left of the screen and select “Settings and privacy.” Go to “Account” > “Security.” Tap “Two-factor authentication” and follow the directions.

On the web, click on “More” in the left-hand menu and find “Settings and privacy.” Click on “Security and account access” (or you can just follow [this link](#)). Select “Security” > “Two-factor authentication.”

Once you’re all set up, Twitter will give you the option to verify through an authenticator app or via a text message with a code sent to your phone. Twitter has also added security-key support.



Twitter lets you use a text message, an app, or a security key for authentication.

As with other services mentioned above, you can generate a backup code to use when you're traveling and will be without internet or cell service. You may also see an option to create a temporary app password that you can use to log in from other devices. This can be used to log in to third-party apps if you have them linked to your Twitter account. Note that the temporary password expires one hour after being generated.

WHATSAPP

Open WhatsApp and find the "Settings" menu under the upper-right dots icon. Look under "Account" > "Two-step verification" > "Enable." The app will ask you to enter a six-digit PIN to use as verification. You can optionally add an email address in case you forget your PIN.

Having an email associated with your WhatsApp account is important since the service won't let you reverify yourself if you've used WhatsApp within the last seven days and have forgotten your PIN. So if you can't wait a week to reverify, it's helpful to have entered an email address so you can log yourself in or disable 2FA. In the same vein: be cautious of emails encouraging you to turn off 2FA if you didn't request it yourself.

DID WE MISS YOUR FAVORITE APPS?

For more information, check out the [2FA Directory](#), which categorizes and lists companies that support 2FA, and gives you the option to message a company on Twitter, Facebook, or email to request that 2FA be added.

A final note: while adding 2FA is great for an extra layer of security on all your accounts, remember that you should be changing and updating your passwords regularly even with 2FA enabled, just to stay in tip-top shape. If that's not your style, you can also use a password manager to automatically take care of it for you.

Update June 10th, 2021, 8:00AM ET: This article was originally published on June 19th, 2017, and has been checked and updated several times so that the instructions for adding 2FA to these apps remain current. This is the latest update. Instructions for Fitbit and TikTok have also been added.

Correction June 16th, 2021, 9:15AM ET: An earlier version of this story said that macOS lets you set up a physical security key under System Preferences. It does not, and we regret the error.

LOCK IT DOWN

Ten years of breaches in one image

How to make your offline self harder to find online

How to use a two-factor security key

Is there any way out of Clearview's facial recognition database?

How to set up a VPN

Inside the cryptocurrency scam vortex

How to stop your emails from being tracked

When does sharing become oversharing?

The race is on for quantum-safe cryptography
