Contributor, PCWorld | OCT 11, 2017 3:00 AM PT | **Ian Paul**

What is two-factor authentication?

The age of widespread fingerprint and face-scanning authentication is almost here. Yet even in the age of Apple's Face ID and Windows 10's Hello, passwords are still the main way we log in to our various accounts. That's why two-factor authentication (2FA) is still important.

Table of Contents

Show More

Two-factor, or multi-factor, authentication is an additional login code for an account—a second line of defense to your sensitive info. There are a number of ways you can get these short, secondary login codes. In a moment, we'll take a look at some of the most popular methods for using two-factor authentication. Before we do that, however, here's a quick review of what two-factor authentication is.

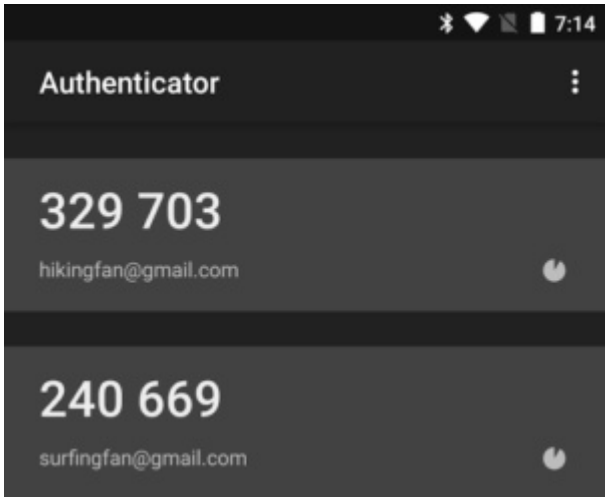
The basic idea is that a single password for your important accounts simply isn't enough. If your password is guessed, or hackers steal a database with your login information in plain text, your account is a sitting duck. Two-factor authentication tries to solve that flaw by requiring a secondary code—usually six characters in length and generated by a smartphone app—before you can gain access to your account. That way even if a hacker has your password they'll still need to crack a secondary code, which makes getting in that much harder.

[Further reading: How to remove malware from your Windows PC]

2FA isn't foolproof, however. If you decide to get your 2FA codes via SMS, for example, the code could potentially be intercepted by hackers, as researchers for Positive Technologies recently demonstrated. That's why using a software- or hardware-based solution on a device you own is preferable.

Any service that supports the standard 2FA approach will work with all of the apps below, and that includes most mainstream websites and services. One notable exception is Steam, which provides a homegrown 2FA option in its mobile app.

Google Authenticator: Easiest to use



Google

One of the more common ways of doing two-factor authentication is Google Authenticator. This is a free smartphone app from Google available for both Android and iOS.

Using it is very simple and can introduce beginners to the basic premise of most 2FA apps. What you do is enable two-factor authentication on your services such as Facebook, Gmail, Dropbox. etc. Once it's enabled, the service will ask you to take a snapshot of a QR code using the app—Android users need to download a QR code reading app to work with Google Authenticator.

Note: In some cases, 2FA is also called two-step verification, which is a distinction we won't get into here.

Once the QR code's been read, Authenticator will start generating codes and the service will typically ask you to input the current one to verify 2FA is working. You can add as many accounts as you like to Google Authenticator as long as they support 2FA.

LastPass Authenticator: Runner up

LastPass

LastPass's free authentication app uses a feature called one-tap push notifications that lets you log in to select sites on PCs with a click instead of entering codes. LastPass has a video on YouTube demonstrating the feature.

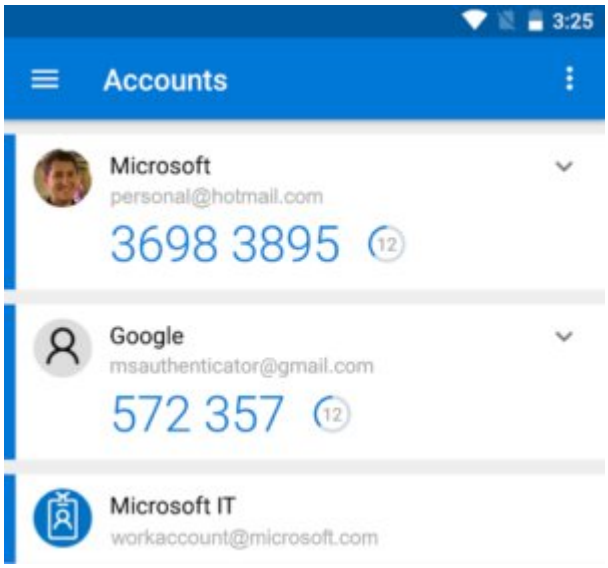
One-tap logins work with LastPass itself, and also with five third-party sites including Amazon (not including AWS), Google, Dropbox, Facebook, and Evernote. To use one-tap notifications you must have the LastPass extension installed in your browser and enabled. That means you must have a LastPass account, but a free one will do. These one-tap logins are browser specific so if you one-tap log in on Chrome you will have to log in again if you use Microsoft Edge, for example.

It may all seem rather mysterious, but here's what's going on behind the scenes with one-tap logins on third-party sites. When a user logs in to a compatible site, the LastPass browser extension sends a push notification

to the user's phone, which alerts the user that a login is being requested. The user taps *Allow* on the phone, and a confirmation message is returned to the extension that includes the required 2FA code. The extension receives this information, provides it to the website, and the user is logged in.

LastPass Authenticator also integrates with several sites owned by the password manager's parent company, LogMeIn, to offer a similar type of one-tap login. These sites include LastPass, LogMeIn Pro/Central, GotoAssist, LogMeIn Rescue, Xively.

Microsoft Authenticator



Microsoft

Microsoft also has a free authenticator app for Android, iOS, and Windows 10 Mobile. It grabs codes for sites like Facebook and Dropbox by snapping a QR code just like the others. For personal Microsoft Accounts, however, it supports one-tap notifications similar to LastPass.

Microsoft's feature can log you in to your account on any device. All you have to do is approve the login and it's as good as entering the short code. It's not a huge time saver, but it is slightly more convenient.

Authy: Best multi-device solution

Twilio

If you've used 2FA for any length of time then you know that one of the downsides is you have to go through the hassle of re-enabling your authentication codes every time you switch to a new smartphone.

If you have 10 accounts with 2FA that means snapping 10 QR codes all over again. If you're a smartphone addict who likes to switch devices every one or two years that process can be a hassle.

Authy's free service aims to solve that problem by storing all your 2FA tokens—the behind the scenes data that makes your 2FA codes work—in the cloud on its servers. To use this feature you have to enable encrypted backups first, and then your tokens are stored on Authy's servers.

That way when you log in to any Authy app, be it on your smartphone, tablet, or Windows or Mac laptop, you've got access to your codes. There's even a Chrome app for Chrome OS users.

Multi-device access to your 2FA codes is great, but it does come with a drawback. Authy says your backups are encrypted based on a password entered on your smartphone before hitting the cloud. That means your passcode is the only way to decrypt them, and Authy doesn't have it on file. If you forget your passcode you can get locked out of your accounts since you won't have the 2FA codes. How you regain access to each account depends on that service's account recovery policies.

If you are new to 2FA this might not be the app for you unless you're prepared to take proper steps to ensure you never lose access to Authy—like writing down your passcode and storing it somewhere safe.

Yubico Authenticator

Image: FIDO Alliance

This last one is my personal favorite. Yubico's YubiKey is a hardware-based 2FA solution. It's a small card-like device with one end that slots into a USB port. It usually verifies authentication with a button press instead of entering a short code.

That one-tap approach only works for accounts that support the FIDO U2F standard such as Google and GitHub. For those that don't, a YubiKey can also store 2FA tokens and display codes on the Yubico Authenticator app.

How you use Yubico Authenticator to get a 2FA code depends on whether you're using the authenticator app on a PC or an Android smartphone. On the desktop, you just insert the key into a USB port, and the authenticator immediately displays your short codes and lets you add new ones. Remove your YubiKey, and the app stops showing codes immediately. Yubico Authenticator on the desktop works with most YubiKey models except the basic FIDO U2F key.

On Android you can only use the YubiKey Neo since that is the only key that currently supports NFC. With Neo all you do is open Authenticator on your phone, tap the key

YubiKey NEO

$50.00MSRP $50.00
View
on Amazon

near your NFC chip, and your codes will display.

Similar to Authy, the beauty of YubiKey is that it allows you to easily transfer your authenticator codes from one device to the next. The downside is that if you ever lose or break your YubiKey (they are quite durable and waterproof) you have to switch your second-factor authentication method.

Two-factor authentication is an important step to take to protect your important accounts whenever possible. It may seem like a pain at times to enter that extra code—which you may only have to do once per device or once every 30 days—but it's a price worth paying to make your online accounts more secure.

To comment on this article and other PCWorld content, visit our Facebook page or our Twitter feed.
