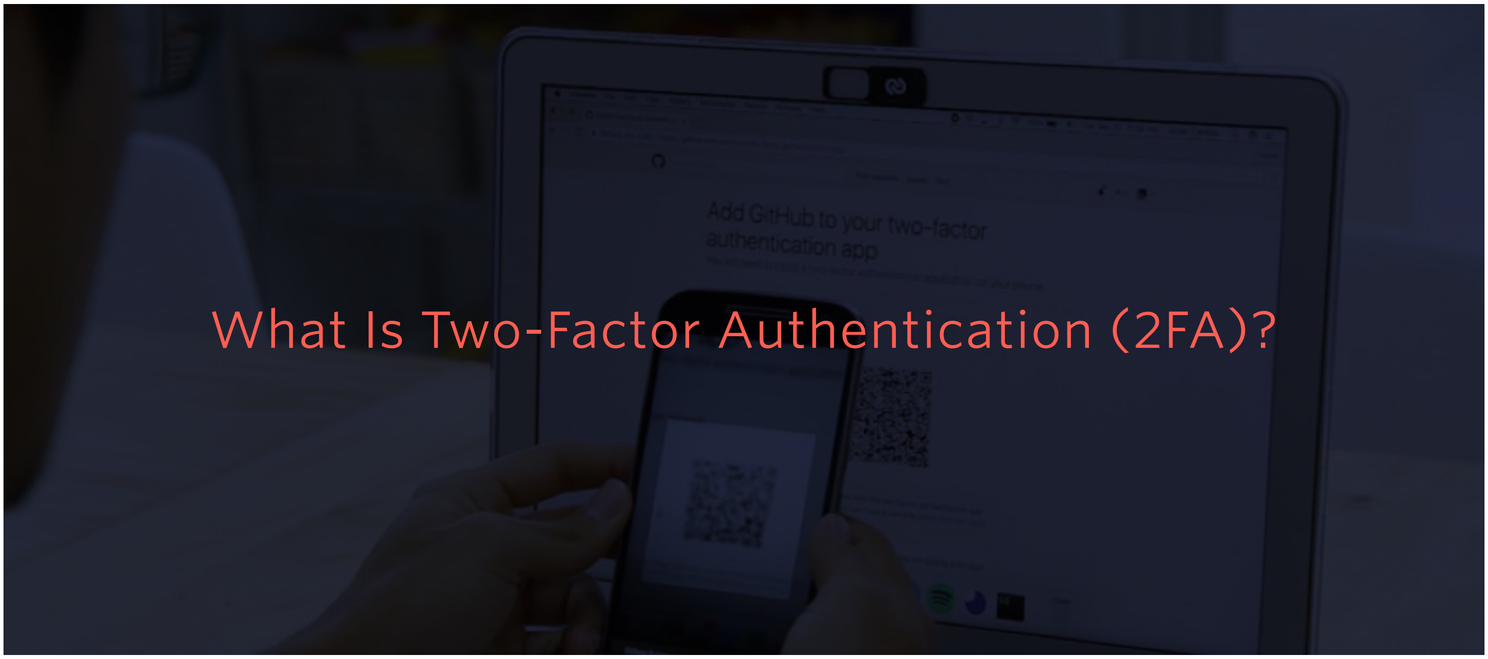


What Is Two-Factor Authentication (2FA)?

And why aren't passwords good enough?

Before addressing the question 'what is two-factor authentication' or 'what is 2FA,' let's consider why it's important to do everything you can to improve your online account security. With so much of our lives happening on mobile devices and laptops, it's no wonder our digital accounts have become a magnet for criminals. Malicious attacks against governments, companies, and individuals are more and more common. And there are no signs that the hacks, data breaches, and other forms of cybercrime are slowing down!

Luckily, it's easy for businesses to add an extra level of protection to user accounts in the form of two-factor authentication, also commonly referred to as 2FA.

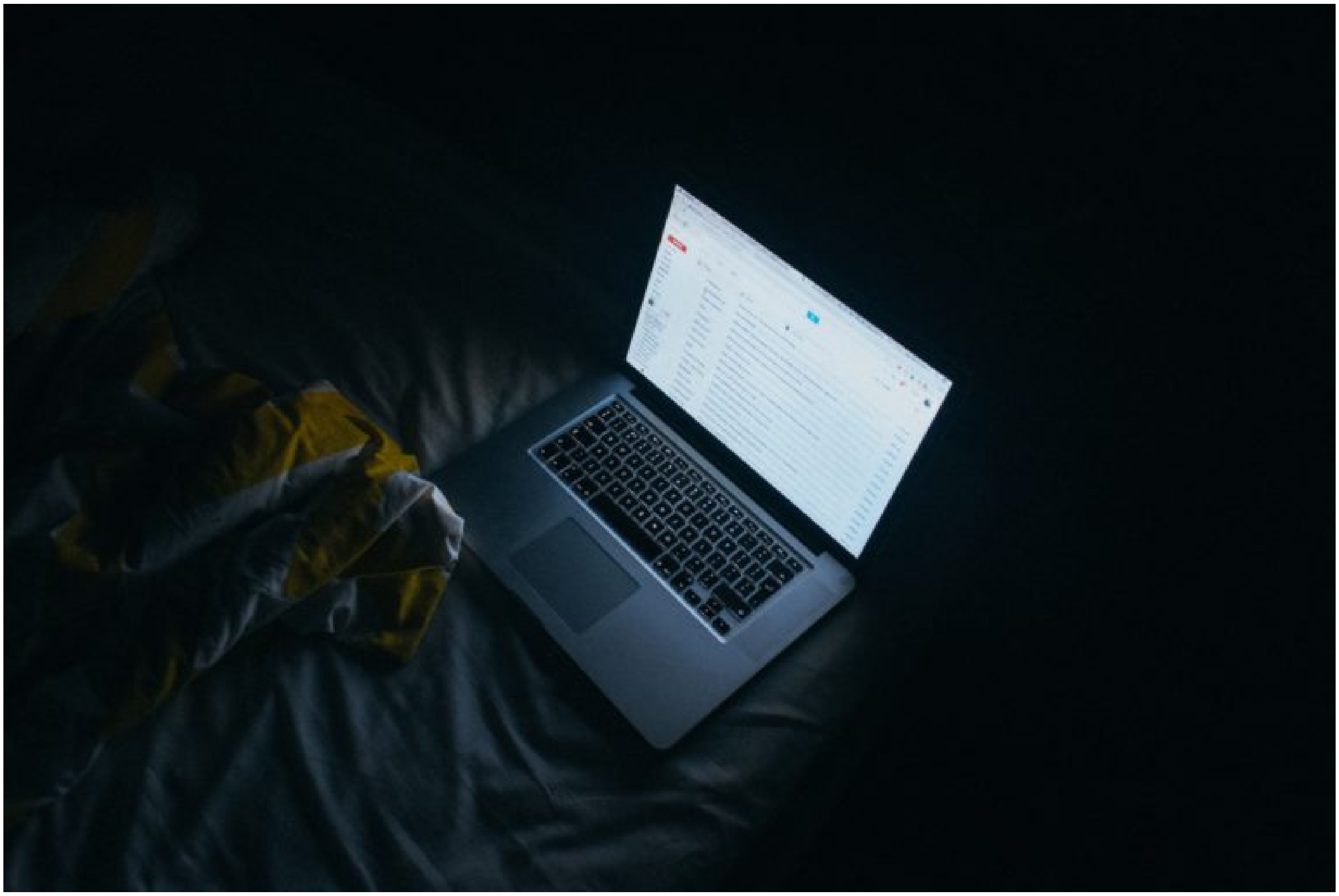
ARE YOU A DEVELOPER INTERESTED IN ADDING 2FA TO YOUR APPLICATION? SEE TWILIO APIs & TUTORIALS

Rise in Cybercrime Requires Stronger Security With 2FA

In recent years, we've witnessed a massive increase in the number of websites losing personal data of their users. And as cybercrime gets more sophisticated, companies find their old security systems are no match for modern threats and attacks. Sometimes it's simple human error that has left them exposed. And it's not just user trust that can be damaged. All types of organizations—global companies, small businesses, start-ups, and even non-profits—can suffer severe financial and reputational loss.

For consumers, the after-effects of targeted hack or identity theft can be devastating. Stolen credentials are used to secure fake credit cards and fund shopping sprees, which can damage a victim's credit rating. And entire bank and cryptocurrency accounts can be drained overnight. A recent study revealed that in 2016 over $16 billion was taken from 15.4 million U.S. consumers. Even more incredible, identify thieves stole over $107 billion in the past six years alone.

Clearly, online sites and apps must offer tighter security. And, whenever possible, consumers should get in the habit of protecting themselves with something that's stronger than just a password. For many, that extra level of security is two-factor authentication.



Passwords: Historically Bad But Still In Use

How and when did passwords get so vulnerable? Back in 1961, the Massachusetts Institute of Technology developed the Compatible Time-Sharing System (CTSS). To make sure everyone had an equal chance to use the computer, MIT required all students to log in with a secure password. Soon enough, students figured out that they could hack the system, print out the passwords, and hog more computer time.

Despite this, and the fact that there are much more secure alternatives, usernames and passwords remain the most common form of user authentication. The general rule of thumb is that a password should be something only you know while being difficult for anyone else to guess. And while using passwords is better than having no protection at all, they're not foolproof. Here's why:

- **Humans have lousy memories.** A recent report looked at over 1.4 billion stolen passwords and found that most were embarrassingly simple. Among the worst are "111111," "123456," "123456789," "qwerty," and "password." While these are easy to remember, any decent hacker could crack these simple passwords in no time.
- **Too many accounts:** As users get more comfortable with doing everything online, they open more and more accounts. This eventually creates too many passwords to remember and paves the way for a dangerous habit: password recycling. Here's why hackers love this trend: it takes just seconds for hacking software to test thousands of stolen sign-in credentials against popular online banks and shopping sites. If a username and password pair is recycled, it's extremely likely it'll unlock plenty of other lucrative accounts.
- **Security fatigue sets in:** To protect themselves, some consumers try to make it harder for attackers by creating more complex passwords and passphrases. But with so many data breaches flooding the dark web with user information, many just give up and fall back to using weak passwords across multiple accounts.

2FA To The Rescue

2FA is an extra layer of security used to make sure that people trying to gain access to an online account are who they say they are. First, a user will enter their username and a password. Then, instead of immediately gaining access, they will be required to provide another piece of information. This second factor could come from one of the following categories:

- **Something you know:** This could be a personal identification number (PIN), a password, answers to "secret questions" or a specific keystroke pattern
- **Something you have:** Typically, a user would have something in their possession, like a credit card, a smartphone, or a small hardware token
- **Something you are:** This category is a little more advanced, and might include biometric pattern of a fingerprint, an iris scan, or a voice print

With 2FA, a potential compromise of just one of these factors won't unlock the account. So, even if your password is stolen or your phone is lost, the chances of a someone else having your second-factor information is highly unlikely. Looking at it from another angle, if a consumer uses 2FA correctly, websites and apps can be more confident of the user's identity, and unlock the account.

Common Types of 2FA

If a site you use only requires a password to get in and doesn't offer 2FA, there's a good chance that it will be eventually be hacked. That doesn't mean that all 2FA is the same. Several types of two-factor authentication are in use today; some may be stronger or more complex than others, but all offer better protection than passwords alone. Let's look at the most common forms of 2FA.

Hardware Tokens for 2FA

Probably the oldest form of 2FA, hardware tokens are small, like a key fob, and produce a new numeric code every 30-seconds. When a user tries to access an account, they glance at the device and enter the displayed 2FA code back into the site or app. Other versions of hardware tokens automatically transfer the 2FA code when plugged into a computer's USB port.

They've got several downsides, however. For businesses, distributing these units is costly. And users find their size makes them easy to lose or misplace. Most importantly, they are not entirely safe from being hacked.

SMS Text-Message and Voice-based 2FA

SMS-based 2FA interacts directly with a user's phone. After receiving a username and password, the site sends the user a unique one-time passcode (OTP) via text message. Like the hardware token process, a user must then enter the OTP back into the application before getting access. Similarly, voice-based 2FA automatically dials a user and verbally delivers the 2FA code. While not common, it's still used in countries where smartphones are expensive, or where cell service is poor.

For a low-risk online activity, authentication by text or voice may be all you need. But for websites that store your personal information — like utility companies, banks, or email accounts — this level of 2FA may not be secure enough. In fact, SMS is considered to be the least secure way to authenticate users. Because of this, many companies are upgrading their security by moving beyond SMS-based 2FA.

Software Tokens for 2FA

The most popular form of two-factor authentication (and a preferred alternative to SMS and voice) uses a software-generated time-based, one-time passcode (also called TOTP, or "soft-token").

First, a user must download and install a free 2FA app on their smartphone or desktop. They can then use the app with any site that supports this type of authentication. At sign-in, the user first enters a username and password, and then, when prompted, they enter the code shown on the app. Like hardware tokens, the soft-token is typically valid for less than a minute. And because the code is generated and displayed on the same device, soft-tokens remove the chance of hacker interception. That's a big concern with SMS or voice delivery methods.

Best of all, since app-based 2FA solutions are available for mobile, wearables, or desktop platforms — and even work offline — user authentication is possible just about everywhere.

Push Notification for 2FA

Rather than relying on the receipt and entry of a 2FA token, websites and apps can now send the user a push notification that an authentication attempt is taking place. The device owner simply views the details and can approve or deny access with a single touch. It's passwordless authentication with no codes to enter, and no additional interaction required.

By having a direct and secure connection between the retailer, the 2FA service, and the device, push notification eliminates any opportunity for phishing, man-in-the-middle attacks, or unauthorized access. But it only works with an internet-connected device, one that's able to install apps to. Also, in areas where smartphone penetration is low, or where the internet is unreliable, SMS-based 2FA may be a preferred fall-back. But where it is an option, push notifications provide a more user-friendly, more secure form of security.

Other Forms of Two-Factor Authentication

Biometric 2FA, authentication that treats the user as the token, is just around the corner. Recent innovations include verifying a person's identity via fingerprints, retina patterns, and facial recognition. Ambient noise, pulse, typing patterns, and vocal prints are also being explored. It's only a matter of time before one of these 2FA methods takes off…and for biometric hackers to figure out how to exploit them.

Everybody Should 2FA

According to a recent report, stolen, reused, and weak passwords remain a leading cause of security breaches. Unfortunately, passwords are still the main (or only) way many companies protect their users. The good news is that cybercrime is in the news so much that 2FA awareness is quickly growing and usres are demanding that the companies they do business with have improved security. We agree: “Everybody Should 2FA”

Want To Learn More About 2FA?

Consumers: Don’t know if your favorite sites or apps have 2FA? Visit TwoFactorAuth.org to find out. Or visit the following links to learn more:

- Download Authy 2FA app for iOS, Android, or Desktop
- Get Better Security on Your Twitter Account
- See How To Enable 2FA For Your Favorite Sites
- Understanding 2FA, the Authy App, and SMS

- Understanding Authy 2FA’s Multi-Device Feature
- How Authy 2FA Backups Work

Businesses: Rather than building 2FA themselves, many businesses find that it’s smarter and more cost-effective to partner with an expert. Twilio offers a comprehensive suite of developer-friendly authentication APIs and an SDK that can turn any app into a self-branded authenticator. Check out these useful links for businesses and developers:

- Cross-Industry Security: 4 Brands Getting 2FA Right
- Whitepaper: Account Security Best Practices Guide
- EBook: Upgrade 2FA By Downgrading SMS
- Step-by-Step 2FA Tutorials
- Sign Up To Try Twilio’s 2FA APIs for Free