# Two Step Authentication


- What is Two-Step Authentication
  - Three Possible Factors
  - Benefits
  - Drawbacks
  - Plugins for Two-Step Authentication
- Related


Also known as Two-Factor Authentication.

Two-step authentication is showing up all over the Internet as more sites look for better ways to secure logins, which are the weakest part of anything a user does online.

# What is Two-Step Authentication

Passwords are the de-facto standard for logging in on the web, but they're relatively easy to break. Even if you make good passwords and change them regularly, they need to be stored wherever you're logging in, and a server breach can leak them. There are three ways to identify a person, things they are, things they have, and things they know.

Logging in with a password is single-step authentication. It relies only on something you know. Two-step authentication, by definition, is a system where you use two of the three possible factors to prove your identity, instead of just one. In practice, however, current two-step implementations still rely on a password you know, but use your Phone or another device to authenticate with something you have.

## Three Possible Factors

There are three possible ways to identify users.

**Something You Are**

There are a lot of properties that are unique to each user and can be used to identify them. The most popular is fingerprints, but retinas, voice, DNA, or anything else specific to an individual will work. This is called biometric information because these pieces of information all belong to a

person’s biology.

Biometric factors are interesting because they are not easily forged and the user can never lose or forget them. However, biometric authentication is tricky because a lost fingerprint can never be replaced. If hackers were to gain access to a database of fingerprints, there is no way that users could reset them or get a new set.

In 2013, Apple released TouchID which lets users unlock their iPhones using their fingerprints. This technology is interesting because the fingerprints are stored locally on the phone, not in the cloud where they would be easier for hackers to steal. There are still trade-offs with this kind of approach, but it is the most widespread consumer use of biometric authentication to date.

**Something You Have**

Also known as the possession factor, users can be identified by the devices which they carry. Traditionally, a company that wanted to enable two-step authentication would distribute secure keychain fobs to users. The keychain fobs would display a new number every 30 seconds, and that number would need to be typed along with the password every time a user logged in.

Modern two-step authentication more frequently relies on a user’s smartphone than on a new piece of hardware. One common model of this uses SMS in order to provide an easy second factor. When the user enters their password, they are sent a text message with a unique code. By entering that code, after the password, they supposedly prove that they also have their phone. Unfortunately, SMS is not a secure communication channel, so smartphone apps and plugins have been developed to create that secure channel.

**Something You Know**

The most familiar form of authentication is the knowledge factor, or password. As old as Open Sesame, passwords have long been a standard for anonymous authentication. In order for a knowledge factor to work, both parties need to know the password, but other parties must not be able to find or guess it.

The first challenge is in exchanging the password with the trusted party safely. On the web, when you register for a new site, your password needs to be sent to that site’s servers and might be intercepted in the process (which is why you should always check for SSL when registering or logging in — HTTPS).

Once the password has been received, it must be kept secret. The user shouldn’t write it down or use it anywhere else, and the site needs to carefully guard its database to ensure that hackers can’t access the passwords.

Finally, the password needs to be verified. When a user visits the site, they need to be able to provide the password and have it verified against the stored copy. This exchange can also be intercepted (and so should always be done over SSL — HTTPS) and exposes the user to another

risk.

## Benefits

There are a lot of different places to increase the security of a site, but the WordPress Security Team has said that “The weakest link in the security of anything you do online is your password,” so it makes sense to put energy into strengthening that aspect of your site.

## Drawbacks

As the name implies, two-step authentication is adding a step to a process that can already be long and painful. While most very high-security logins are protected by two-step authentication today, most consumer applications barely offer it as an option if they offer it at all. This is because users are less likely to sign up for and log in to a service if it is more difficult.

Two-step authentication can also prevent legitimate logins. If a user forgets their phone at home and has two-step authentication enabled, then they won’t be able to access their account. This is one of the main reasons why smartphones have been useful for two-step authentication — users are more likely to be carrying their phones than almost anything else.

## Plugins for Two-Step Authentication

You can search for two-step authentication plugins available in the WordPress.org plugin repository. Here are some of the most popular ones to get you started (in alphabetical order):

- Duo
- Google Authenticator
- Rublon
- Two-Factor
- WordFence

# Related

- Brute Force Attacks

---

□□□ #2
□ □□□ □□□ 2026-10-31 18:05:25 UTC
□ □□□ □□□ 2026-10-31 18:05:27 UTC