

Password Managers and Two-Factor Authentication (2FA)

A simple guide to making your online accounts safer and easier to use

For some time, I have been meaning to write this up about the password manager and two-factor authentication (2FA) apps that I use so I could share them with others.

I know that setting up something new on your computer or phone can sometimes seem intimidating, especially when there are quite a few steps involved. The good news is that it really isn't that difficult once you get started.

Having these apps by themselves makes managing passwords and 2FA easier, but integrating them with your phone and web browser really takes it to the next level. Once everything is set up, something that initially seems complicated becomes surprisingly easy to use.

This guide explains what password managers and 2FA are, why I use them, and how I set them up.

What Is a Password Manager?

Essentially, a password manager is a secure digital vault where you can keep and manage your login information.

The biggest advantage is that you no longer have to remember dozens of different passwords. Instead, you only need to remember **one master password** that unlocks your password manager.

A good password manager can:

- Store your usernames and passwords securely.
- Generate long, random passwords when you create new accounts.
- Help you avoid using the same password on multiple websites.
- Automatically fill in usernames and passwords on websites and apps.
- Synchronize your information between your phone and computer.
- Allow you to use your fingerprint or face to unlock it on supported devices.

Password managers use encryption to protect the information they store. In other words, your stored information is scrambled so that it cannot simply be read by someone who doesn't have the proper access.

One of my favorite features is the ability to generate a completely random password when creating a new account. You don't have to come up with something yourself, and you don't have to remember it. The password manager does that part for you.

Once everything is integrated with your phone and browser, you generally don't even need to think about your passwords anymore. You visit a website, the password manager recognizes the website, and it can fill in your login information for you.

One Very Important Password

There is one password you **do** need to remember: your password manager's **master password**.

This is the password that protects the rest of your passwords, so choose it carefully. Don't use a password that you already use somewhere else.

If you forget your master password, you may not be able to get back into your password manager, so make sure you have a way to remember it.

What Is 2FA?

Two-factor authentication, usually called **2FA**, is an additional security step that helps protect your online accounts.

Normally, logging into an account requires something you know — your password. With 2FA enabled, you are required to provide a second piece of information as well.

Two-factor authentication uses two different types of information from these categories:

- **Something you know:** A password, PIN, or passphrase.
- **Something you have:** A phone, hardware token, or security key.
- **Something you are:** A fingerprint or facial scan.

For example, you might enter your username and password and then be asked for a six-digit code generated by an authenticator app on your phone.

Some websites require 2FA every time you log in. Others may only ask for it when you are logging in from a new or unfamiliar device.

Common 2FA Methods

There are several ways a website can provide two-factor authentication.

Text Message (SMS)

A temporary code is sent to your phone by text message.

This is better than having no second factor at all, but it is generally not considered as strong as some of the other options.

Authenticator Apps

Apps such as Microsoft Authenticator, Google Authenticator, and 2FAS can generate short-lived codes that change regularly.

Push Notifications

A notification appears on your phone asking you to approve or deny a login attempt.

Important: Never approve a login request that you did not initiate yourself.

Physical Security Keys

These are small physical devices that you plug into a computer or tap against a compatible device.

Why Does 2FA Matter?

Passwords can be guessed, stolen through phishing scams, or exposed when a company experiences a data breach.

If someone obtains your password, having 2FA enabled gives them another obstacle to overcome before they can access your account.

It doesn't make an account completely impossible to break into, but it can make unauthorized access considerably more difficult.

One particularly important rule is: **NEVER give your 2FA code to another person.**

Your bank, Microsoft, Google, Apple, Amazon, or any other legitimate company should never need you to tell them the authentication code you just received.

Scammers sometimes try to convince people that they need the code to "verify" their identity or fix an account. If you receive a 2FA request or code that you did not initiate, don't approve it and don't give the code to anyone.

The Password Manager I Use: Bitwarden

There are quite a few password managers available, and some of them are free.

If you use an Android phone and have signed into a Google account, you may already have Google Password Manager available. I used it for years without any problems.

I eventually decided to switch to a password manager that was separate from my Google account. The password manager I have been using for the past year is **Bitwarden** (<https://bitwarden.com/>).

Bitwarden stores my passwords and some personal information and works seamlessly between my phone and computer. It also has a free version that is more than adequate for many individual users.

Here is how I set it up.

Setting Up Bitwarden

On Your Computer

1. Go to Bitwarden (<https://bitwarden.com/>).
2. Click **Get Started Free**.
3. Make sure you are looking at the **Personal** option rather than the Business option.
4. Scroll down to the free option and choose **Create Free Account**.
Bitwarden offers paid plans as well, so the free option isn't necessarily the first thing you will see. For basic personal password management, the free plan may be all you need.
5. Enter your email address and create your account.
6. Create your **Master Password**.

Take Your Master Password Seriously

Your master password is extremely important because it protects everything stored in Bitwarden.

Make it something you can remember, but don't use a password that you already use for another website.

I also recommend taking a little time to think about how you will remember this password. If you forget it, recovering access to your password vault can be difficult or, depending on the circumstances, impossible.

Setting Up Bitwarden on Your Phone

Now install Bitwarden on your phone.

1. Open the **Apple App Store** or **Google Play Store**.
2. Search for **Bitwarden Password Manager**.
3. Download and install the app.
4. Open Bitwarden and sign in using the email address and master password you created earlier.

Once you have signed in, your passwords should be available on your phone.

Android Phones

On newer Android phones, you may need to tell Android which password manager you want to use.

The exact location of this setting can vary depending on the phone manufacturer and Android version.

On my phone, it is located under:

Settings → Passwords, passkeys and accounts

Look for the setting that allows you to choose your preferred password service and select **Bitwarden**.

Once this is set up, your phone should be able to offer Bitwarden when an app or website asks you to enter a username or password.

If Bitwarden doesn't automatically offer to fill in the information, you can always open the Bitwarden app, find the account you need, and copy the username or password.

When you select a saved login in Bitwarden, you can copy the username or password to your clipboard and then paste it into the website or app.

Setting Up Two-Factor Authentication

There are also quite a few authenticator apps available.

The one I use is **2FAS** (<https://2fas.com/>), which is a free, open-source authenticator app.

I chose 2FAS because I like its simplicity and its backup options. Having a backup is especially important for an authenticator app because your phone can be lost, damaged, or simply stop working.

In fact, my phone recently died, and having my 2FA information backed up was a lifesaver.

Some websites can be extremely difficult to recover if you lose access to your 2FA method, so I strongly recommend paying attention to the backup or recovery options when setting up your authenticator.

Installing 2FAS on Your Phone

1. Open the **Apple App Store** or **Google Play Store**.
2. Search for **2FAS Authenticator**.
3. Download and install the app.
4. Open the app and follow the setup instructions.
5. If you are offered a backup option, I recommend setting it up.

The exact screens and backup options may change as the app is updated, so follow the current instructions shown by 2FAS.

Adding an Account to 2FAS

When a website gives you the option to enable 2FA, it will usually display a QR code as part of the setup process.

This is how you connect that website to your authenticator app.

In 2FAS:

1. Open the app.
2. Tap the + button.
3. Choose the option to scan a QR code.
4. Point your phone's camera at the QR code displayed by the website.

2FAS will then add the account to your list.

From that point forward, when the website asks for a 2FA code, you can open 2FAS, find that account, and enter the current code.

The codes change regularly, so don't be concerned when you see the number counting down or changing. That's how it is supposed to work.

Remember: **Never give an authentication code to another person.**

The code is for **you** to use when you are logging into the account.

Setting Up Bitwarden and 2FAS in Chrome

The final step is integrating everything into your web browser.

I use Google Chrome, so these instructions are written for Chrome. Other browsers have similar extensions and settings, although the exact steps may be different.

The browser integration is what really makes these tools convenient.

Installing the Bitwarden Extension

In Chrome:

1. Open the Chrome Web Store.
2. Search for **Bitwarden Password Manager**.
3. Install the Bitwarden extension.
4. Sign in to Bitwarden using your account information.

The Bitwarden icon should now be available in Chrome.

This allows Bitwarden to recognize websites where you have saved login information and makes it much easier to fill in your username and password.

Installing the 2FAS Extension

Next, search the Chrome Web Store for:

2FAS Auth - Two Factor Authentication

Install the extension.

Once it is installed, you need to connect the Chrome extension to the 2FAS app on your phone.

1. Open the 2FAS extension options.
2. Choose **ADD ANOTHER DEVICE**.
3. Follow the instructions to pair the extension with the 2FAS app on your phone.

The exact wording or appearance may change as the extension is updated, so follow the instructions shown on your screen.

If you don't immediately see the 2FAS extension next to the address bar, click the **puzzle-piece Extensions icon** in Chrome and look for it there.

What This Looks Like in Everyday Use

Once everything is set up, this is where the whole process becomes worthwhile.

Let's say you want to log into a website where you have an account.

Instead of trying to remember your username and password:

1. Open the website.
2. Bitwarden recognizes the website.
3. Use Bitwarden to fill in your username and password.
4. The website asks for your 2FA verification.
5. 2FAS can provide the verification code or, when supported, send a request to your phone.
6. Approve the request on your phone or enter the code.
7. You're logged in.

You don't have to remember a complicated password, and you don't have to type a six-digit code while watching the timer count down.

Once you get used to it, it becomes almost second nature.

A Few Important Rules

There are a few things I strongly recommend remembering after everything is set up.

1. Don't reuse passwords.

If one website is hacked and your password is exposed, you don't want that same password to give someone access to your email, bank account, or other websites.

Let Bitwarden generate unique passwords for you instead.

2. Never give someone your 2FA code.

Even if someone says they are from your bank, Microsoft, Google, Amazon, or another company, don't give them the code.

3. Don't approve an unexpected 2FA request.

If your phone suddenly asks you to approve a login and you aren't trying to log in, deny it. Someone may be trying to log into your account using your password.

4. Keep your recovery information safe.

Make sure you understand how to recover your Bitwarden and 2FAS accounts if you lose your phone or forget a password.

Don't wait until your phone is broken to discover that you don't know how to recover your accounts.

5. Keep your phone and computer updated.

Security updates aren't just about adding new features. They often fix security problems as well.

When your phone or computer tells you that an important update is available, I recommend installing it.

Final Thoughts

I realize that this looks like a lot of steps when it is all written down.

The good news is that you only have to do most of this once.

After everything is installed and connected, the day-to-day process becomes much easier. Instead of remembering dozens of passwords, you have one password manager handling them for you. Instead of worrying about whether you remembered the right password, Bitwarden can generate and remember it. And instead of relying solely on a password to protect your accounts, 2FA provides an additional layer of protection.

I have been using this setup myself and have found it to be both more secure and more convenient than trying to keep track of passwords on my own.

The hardest part is getting everything set up.

Once you do that, **the security actually becomes easier to use, rather than harder.**

I hope you find this helpful. If you have questions, run across something in these instructions that doesn't look right, or find a part of the process that could be explained better, please let me know. I'd be happy to improve this guide as things change.