

# TWO-FACTOR AUTHENTICATION

**TWO-FACTOR AUTHENTICATION** is known by many names, such as 2FA, Two-Factor Auth, Two-Step Verification, Multifactor Authentication (MFA) and so on. You can learn more at <https://eff.org/common2FA>. It's generally defined as:

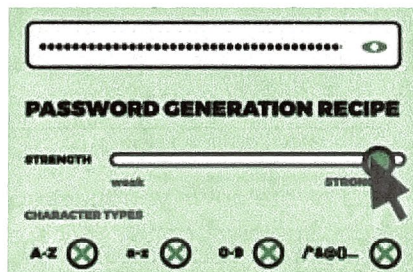
- 1) Something you know**  
This is the first factor: your username and password.
- 2) Something you have**  
This is the second factor: your device that you carry with you.

Follow the suggested guidelines to bump up your account security!

## 1 SOMETHING YOU KNOW: USE STRONG PASSWORDS

**EACH PASSWORD FOR EACH ACCOUNT SHOULD BE:**

- Random
- Long
- Unique



Check out EFF's guide on generating strong passwords:

<https://ssd.eff.org/en/module/creating-strong-passwords>

**BUT HOW CAN I POSSIBLY REMEMBER ALL THESE RANDOM, LONG, UNIQUE PASSWORDS?**

Depending on your security plan, you may want to use a password manager!

Watch EFF's video on using a password manager here:

<https://ssd.eff.org/en/module/animated-overview-using-password-managers-stay-safe-online>

**LOOKING FOR A PASSWORD MANAGER?**

Check out one option for a password manager here:

<https://ssd.eff.org/en/module/how-use-keepassxc>

2

## SOMETHING YOU HAVE: CHOOSE YOUR METHOD



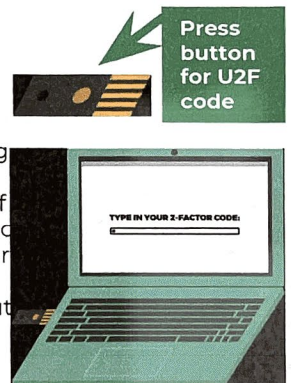
**Hardware token**



You plug in the hardware token in the USB port, and press the button when a service prompts you for 2FA.

**The good:** Codes are stored on your hardware token. It is the most recommended option for those concerned about account security. Since it's not on your phone, it's not susceptible to phone malware getting the codes.

**The bad:** You have to purchase one of these (Yubikey is a popular option) and carry it with you. Keeping track of your token can be a hassle. If you lose your hardware token, you will be locked out of your accounts (unless you wrote down backup codes).



Press button for U2F code

## Authentication apps



You type in the six-digit code when your service prompts you for 2FA. For the time-based authentication apps, you need to type in the code before it refreshes.

**The good:** Codes are stored on your smartphone or tablet. They are not visible to any service provider. App information is protected by encryption.

**The bad:** If your phone has malware, then an attacker can read off the codes. If you lose your phone, you will be locked out of your accounts (unless you wrote down backup codes).

Your authentication code is: 140471

**SMS-based 2FA**

Services send you a six-digit text message to your phone. You type this code when prompted for login. Some services only offer this form of 2FA.

**The good:** It's convenient. If you change phones and don't change phone numbers, you will get your codes.

**The bad:** SMS is not secure. If you go to another country and don't have service, you won't get a code. If you change phone numbers, you won't have your codes. If your phone has malware, then an attacker can read off the codes.