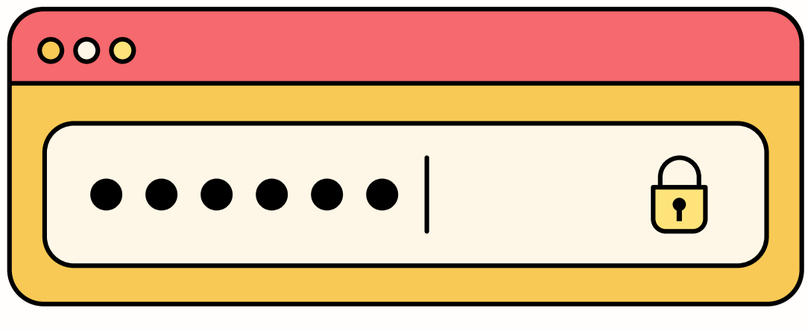
THE MOST SECURE GENERATION

With threats like identity theft and social engineering on the rise, it's more important than ever to secure your online accounts.

CREATE A SECURE PASSWORD/PASSPHRASE



Lots of password managers come with a password generator, or you can use a free online passphrase generator.

Even better than a password is a **passphrase**:

- Like a sentence, made up of 4 or more words
- The best combination of memorability and security
- e.g.: AtomicSailBoatFever, icecreamandapplepie

USE A PASSWORD MANAGER

- **It's convenient**: you won't need to remember a unique password for every one of your online accounts. You only need a master password for the password manager itself
- **It's secure**: now that you don't need to remember all those passwords, it's easy to have a unique password for every account

Click here for our password manager recommendations

USE MULTI-FACTOR AUTHENTICATION (MFA)

It's unsafe to rely on passwords alone; password theft occurs often!

Over 1 billion people were victims of a data breach in 2024 [1]

... and 9.9+ billion passwords were leaked online! [2]

With MFA, your account is protected by two things:

- something you ***know***: your password
- something you ***have or are:*** a code from your phone, your fingerprint, faceID, or other physical token (security key)

It's a good idea to add MFA on all your accounts; it helps defend against ***credential stuffing*** attacks!

What is "credential stuffing?"

Credential stuffing is a funny name for an easy attack;
first the attacker gains access to one of your passwords,
often through a data breach. Then, they "stuff" that password
into as many other sites as they can, hoping you've reused it.

Do you use the same password on more than one account?

Uh-oh! Attackers can easily break into anywhere that uses that same password.

Use a unique password for each account instead.

[1] Identity Theft Research Center

[2] Forbes