



How to Build and Remember a Strong Password

Because long and memorable beats short and complicated

1 Think Long, Not Complex



Short passwords can be more easily cracked, even with symbols



Long passwords are much **stronger** and **easier to remember**.



Think in **phrases**, not single words.

How Long Should it Be?

(Longer is better)

13 Under 14 = **Weak Security**

14-19 14 - 19 = **Strong Security**

20+ 20+ = **Ideal Security**

2 The Strong Password Recipe



Word

+



Word

+



Word

+



Symbol

+



Number

Word + Word + Word + Symbol + Number

3 Examples



Strong Example

SunnyForestTrail#47

Long, unique, and easy to remember.



Weak Example

~~P@ssw0rd123~~

Too short and easy to guess or crack.

4 Make It Stick



Create a short story or image for your password.

Example:

SunnyForestTrail#47 = a sunny trail you walk in 47 steps

Use a Password Manager

- Creates and stores strong, unique passwords
- Fills them in when you log in
- Remember one strong master password

Examples: Bitwarden, 1Password, KeePass



Extra Protection: Turn on MFA



Multi-factor authentication adds an additional layer of security even if someone obtains your password.



CRITICAL: Never reuse your work password on any other account. Reusing passwords is the number #1 reason accounts get compromised.

