Password Safety

Why Passwords Matter

Your passwords are often the only thing protecting your identity online. A weak or reused password can:

- Expose your personal data in a breach
- Allow attackers to hijack your accounts
- Create ripple effects across platforms (banking, email, socials)

Strong passwords = stronger digital privacy.

What Makes a Password Strong?

A strong password should be:

- Long (at least 12 characters)
- Unpredictable (not a word or phrase)
- Complex (uses a mix of letters, numbers, symbols)

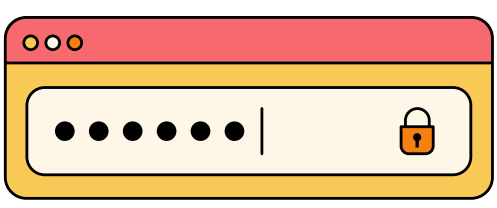
Understanding Password Entropy

Entropy = randomness and unpredictability.

Password	Entropy Score	Security
dog123	Low (~18 bits)	Easy to guess
Mypassword1!	Medium (~34 bits)	Better, but still guessable
gT!92@qz$VuL	High (>70 bits)	Strong

More entropy = exponentially harder to brute force.

How Password Strength is Really Measured



Use our tool to check your password strength. it's powered by zxcvbn, an open-source library by Dropbox that goes way beyond just checking length.

It uses real-world breach data, pattern recognition, and entropy models to estimate how easily a hacker could guess your password.

What Happens Behind the Scenes

When you test a password, zxcvbn analyses:

- **Length & Variety** – Are there symbols, digits, uppercase letters?
- **Dictionary Words** – Common terms like "password" or "summer"
- **Repetition & Sequences** – Examples: aaaa1111, abcd1234
- **Keyboard Patterns** – Like qwerty, asdfgh
- **Leaked Passwords** – Cross-checked with real-world breach data

How "Crack Time" is Calculated

Estimates are based on different types of attacks:

Attack Type	Example Speed
Slow offline attacks	e.g., bcrypt @ 10K/sec
Fast online attacks	Up to billions/sec

Weak Password Examples

Weak Pattern	Why It's Weak
password123	Found in **dictionary lists** - common and
qwertyuiop	A simple **keyboard pattern** - fast for
Emma1995!	Includes **personal info** (name + year)
LetMeIn!!!	Found in **breached password**
aaaaaaa111	**Repeating characters** = low

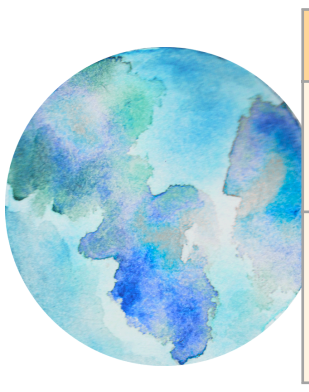
Smart Tips Based on zxcvbn Logic

Tip	Why It Helps
Use uncommon word combos	Harder to match with **dictionary attacks**
Don't rely on !@# substitutions	**Password crackers** try common symbol swaps too
Mix upper/lowercase & symbols	Increases **entropy** (more possible combinations)
Avoid personal info	Can be guessed using **social media or public data**
Break up patterns	Unpredictable combos like Rain!Planet7Jazz resist automated guesses better

Check if a Password Was Leaked

Use our tool to check if your password has been exposed! it's powered by **Have I Been Pwned**, a trusted breach database. Even strong passwords are unsafe if they've appeared in real-world data leaks. It:

- Checks billions of real leaked passwords
- Uses K-anonymity: your full password is never sent
- Helps avoid already-compromised credentials



Risk Level	What It Means	Action
Not found	Password not in breaches	Use a password manager anyway
Found in breaches	Password is public	Change immediately & don't reuse

Smart Habits & Tips for Stronger Passwords

- **Use a password manager:** Stores strong, unique passwords securely
- **Don't reuse passwords:** One breach can compromise all accounts
- **Avoid personal info**: Names and birthdays are easy to guess
- **Enable 2FA**: Adds a second layer of security
- **Use 14+ characters**: Longer = harder to crack
- **Use passphrases:** e.g. Mango!Guitar$Sunset@6pm
- **Don't rely on tricks**: P@sswOrd! is still guessable
- **Choose smart security answers:** Avoid anything obvious
- **Use a generator:** Random passwords beat human ones

Try our password generator!