RESOURCE CENTER

# How to create strong password ideas for better security

Get the full interactive view at https://bitwarden.com/resources/how-to-create-strong-password-ideas-for-better-security/

bitwarden

Strong password ideas are essential for protecting your accounts and personal data. This guide covers practical and effective strategies for online account security to help you create strong password ideas and enhance your overall digital security.

## Why strong password ideas matter

With the average user managing hundreds of accounts, using a unique, strong password for each one is crucial. A weak or reused password can compromise multiple accounts if one is breached, so it's essential to use strong passwords to keep your accounts safe from brute force attacks.

A brute force attack is a method used by malicious actors who deploy software to systematically try every possible password combination until the correct one is found. These attacks can crack simple passwords in minutes, highlighting the importance of creating strong and unique passwords to enhance security.

Using secure passwords helps protect sensitive logins and the data they secure, like bank accounts, email, and social security numbers.

Weak credentials account for 46% of unauthorized access to cloud environments.

## What makes a password strong?

A strong password idea should be:

- **Long** – At least 14 characters.
- **Varied** – Uses a combination of letters, numbers, and symbols.
- **Random** – Doesn't include dictionary words, patterns, or personal information.
- **Unique** – Not reused across other accounts.

## Key components of a strong password idea

### 1. Length

Longer passwords are more secure. An 8-character password can be cracked in minutes. A 16-character password could take billions of years.

### 2. Character variety

Use a combination of:

- Uppercase and lowercase letters
- Numbers
- Symbols

This variety makes passwords more complex and harder to guess.

"Password length is a primary factor in characterizing password strength."

**National Institute of Standards and Technology (NIST)**

### 3. Randomness

Avoid predictable patterns, common passwords, or personal details, like names or birthdates. Random, machine-generated passwords are significantly more secure.

### 4. Unique

Each password should be unique, meaning it is not used for any other account. It should also not have any personal information, like dates, names, or the user's favorite car. A unique password should not be linked to the user.

**Try it:** Use the Bitwarden Password Strength Checker to assess your current passwords.

## How to generate strong passwords

Memorizing secure passwords can be challenging. According to a global survey:

- 25% of people reuse passwords across 11–20+ accounts.
- 36% use personal information in their passwords that can be found on social media or public forums.

Regularly updating created passwords is essential to enhance security against evolving cyber threats. Here are two easy methods for generating strong password ideas.

**Try it:** Use the Bitwarden Password Generator for strong, secure suggestions.

### Option 1: Use a passphrase

A passphrase combines unrelated words into a single, memorable string.

- **Example**: Anew-Slather-Unseated-Uncle-Sandy
- Add character transformations for extra strength: ShyL!0nS33S@w-p00l

You can also adapt phrases you'll remember:

- "I love eating pizza on Fridays!" → ILoEaPiOnFr!

### Option 2: Use a password generator

Password managers often include built-in password or passphrase generators. These tools create secure, random credentials instantly.

## Common password mistakes to avoid

There are several common mistakes to avoid when creating strong password ideas.

| Mistake | Why it's risky | What to do instead |
| --- | --- | --- |
| Reusing passwords | A breach in one account puts all reused accounts at risk. | Use unique passwords for each account. |
| Using personal info | Names, birthdays, and addresses are easy for hackers to find and guess. | Keep passwords random and unrelated to your life. |
| Using common words or patterns | Passwords like 123456 or qwerty are among the first that hackers try. | Use password generators and avoid predictable patterns. |

**Tip:** Regularly review and update weak or reused passwords.

Identifying a weak password is crucial. They are often short, predictable, or based on personal information, all of which makes them easy targets for bad actors.

## Use a password manager for better security

A password manager makes it easy to generate, store, and manage all your passwords securely, ensuring they are strong and unique for every account.

**Key benefits**

- **Autofill login info**: Save time and reduce errors.
- **Phishing protection**: Won't autofill credentials on suspicious or fake websites.
- **Built-in password generator**: Instantly create secure passwords or passphrases.
- **Customizable options**: Adjust length and character types to meet account requirements.
- **End-to-end encryption**: Data is encrypted before leaving the device.
- **Password audits**: Identify weak, reused, or breached passwords.
- **Secure sharing**: Safely share credentials with family or coworkers.
- **Two-factor authentication (2FA) support**: Adds an extra layer of security.

Learn more about how Bitwarden keeps your data secure.

## Enable two-factor authentication (2FA)

Adding 2FA to your accounts is a simple way to significantly boost security once a strong password is in place. Many online accounts, including those with sensitive information like online banking, typically offer this additional layer of security to protect users from unauthorized access. It requires a second form of verification, such as a code from an app, in addition to the password.

Many password managers support 2FA directly or integrate with authentication apps for convenience.

## Make security easier

Strong password ideas don’t need to be difficult. A trusted password manager can reduce mental load, simplify your workflow, and improve your overall digital hygiene.

- Store everything securely in one encrypted vault.
- Create strong passwords with one click.
- Get notified about weak or compromised credentials.
- Sync your data across devices.

Get started today! Easily keep track of passwords with Bitwarden.