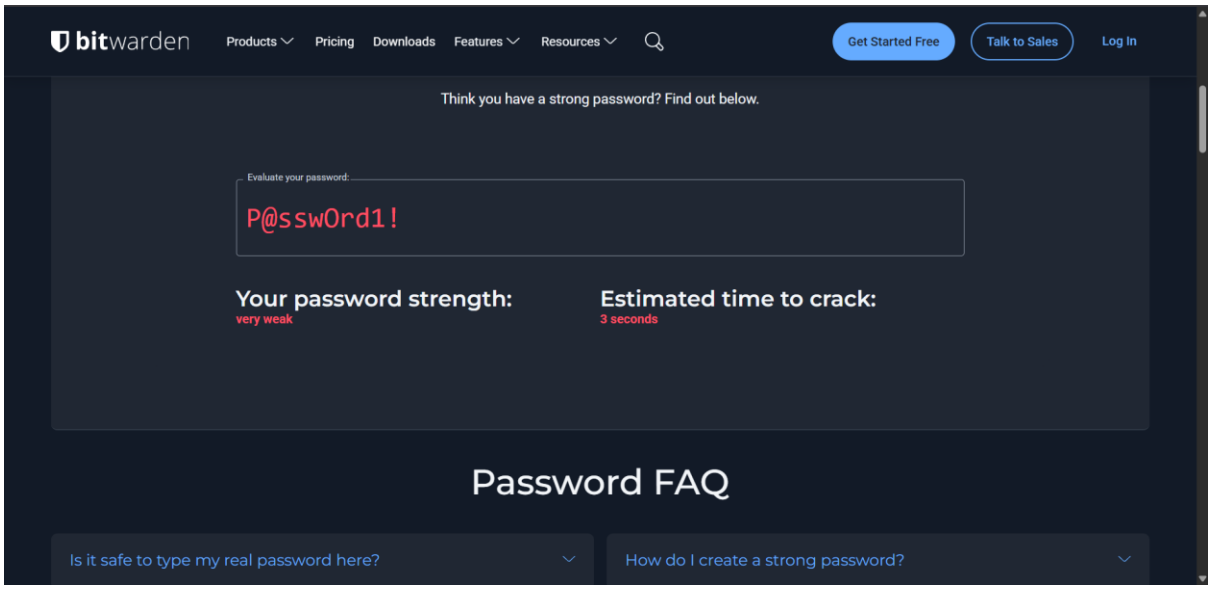
1.Create multiple passwords with varying complexity.

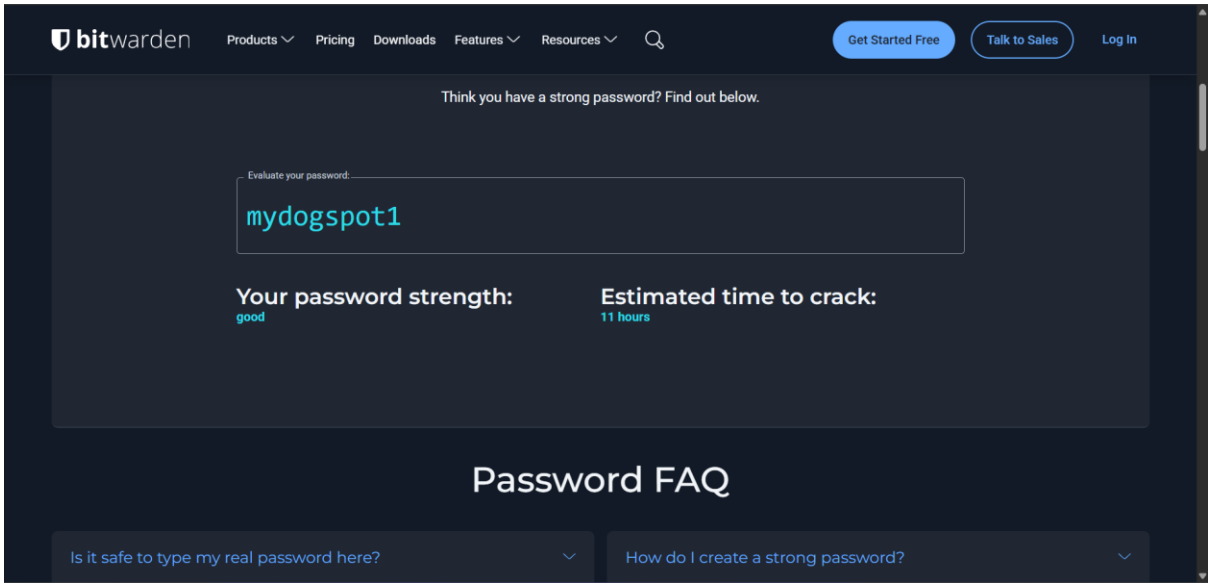
Password
P@sswOrd1!
mydogspot1
Secure_Pwd_2025
A1b2C3d4
L0ng&C0mpl3xK3y

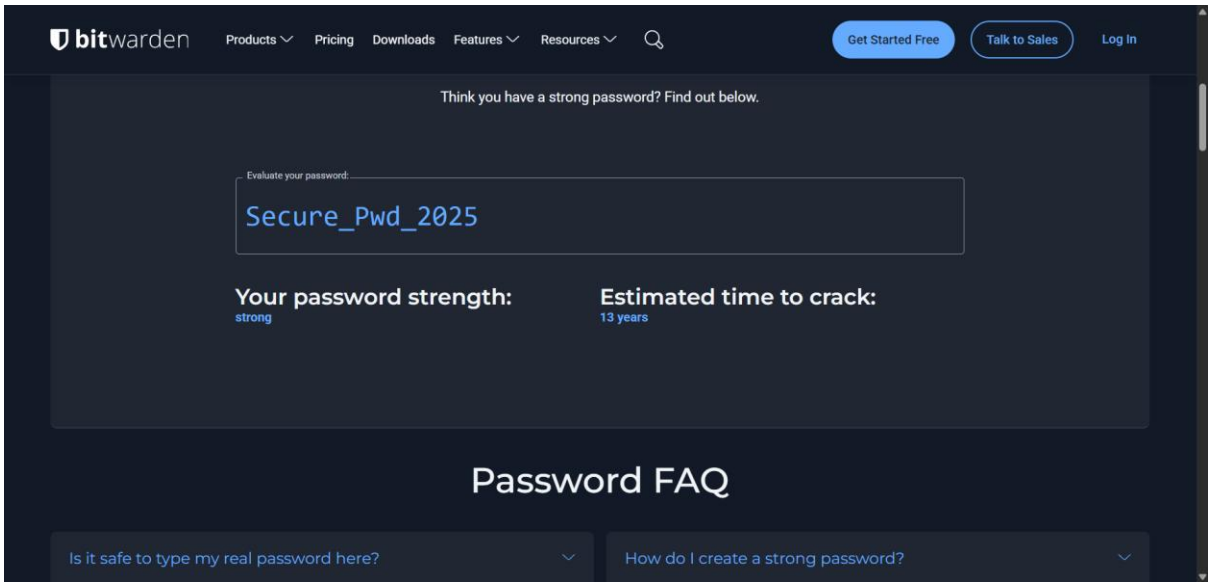
2.Use uppercase, lowercase, numbers, symbols, and length variations.

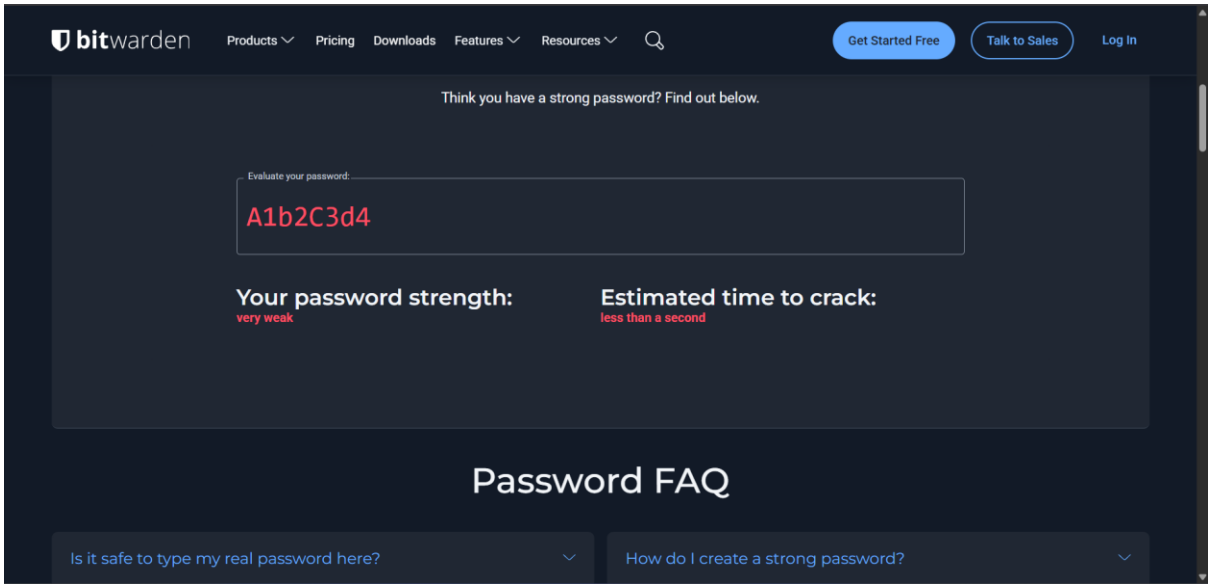
Password	Length	Components	Hypothetical Score (Out of 100)	Hypothetical Feedback
P@sswOrd1!	12	Uppercase, lowercase, numbers, symbols	85	Excellent. Good mix of characters and length. Contains common word fragments.
mydogspot1	10	Lowercase, numbers	25	Very Weak. Too short, lacks variety, and uses dictionary words.
Secure_Pwd_2025	16	Uppercase, lowercase, numbers, symbols	95	Excellent. Long, varied, and uses uncommon phrase components.
A1b2C3d4	8	Uppercase, lowercase, numbers	40	Weak. Too short, pattern is predictable (simple alternation).
L0ng&C0mpl3xK3y	17	Uppercase, lowercase, numbers, symbols	100	Excellent/Max Score. Very long, uses a mix of all character types, and avoids common patterns.

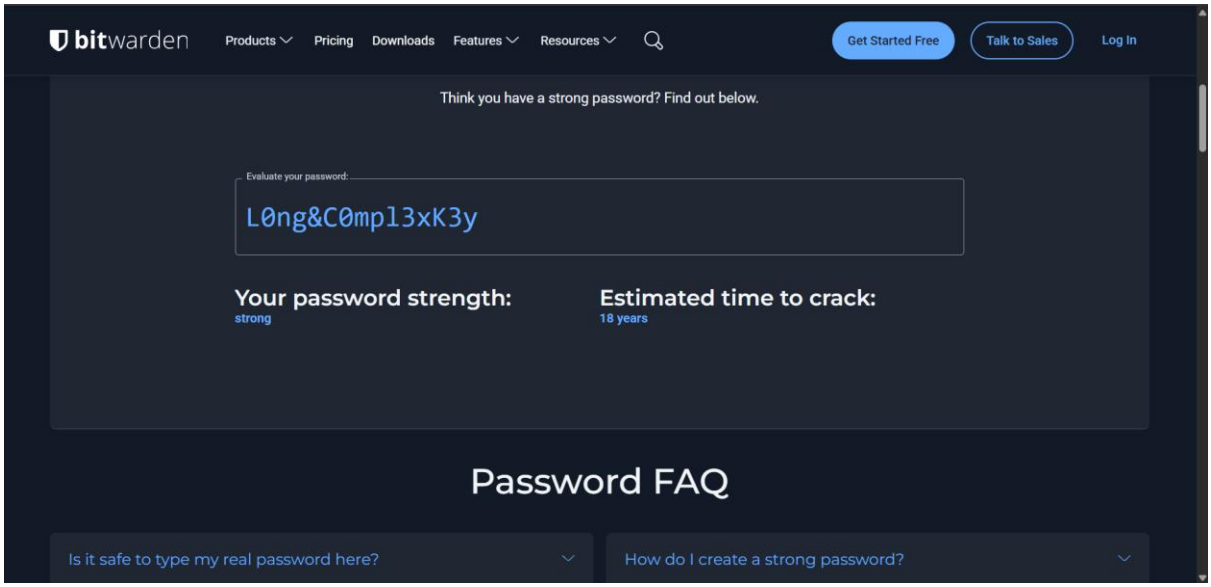
3.Test each password on password strength checker and Note scores and feedback from the tool.




bitwarden
Products
Pricing
Downloads
Features
Resources
Get Started Free
Talk to Sales
Log In
Think you have a strong password? Find out below.
Evaluate your password:
mydogspot1
Your password strength:
good
Estimated time to crack:
11 hours
Password FAQ
Is it safe to type my real password here?
How do I create a strong password?


bitwarden
Products
Pricing
Downloads
Features
Resources
Get Started Free
Talk to Sales
Log In
Think you have a strong password? Find out below.
Evaluate your password:
Secure_Pwd_2025
Your password strength:
strong
Estimated time to crack:
13 years
Password FAQ
Is it safe to type my real password here?
How do I create a strong password?


bitwarden
Products
Pricing
Downloads
Features
Resources
Get Started Free
Talk to Sales
Log In
Think you have a strong password? Find out below.
Evaluate your password:
A1b2C3d4
Your password strength:
very weak
Estimated time to crack:
less than a second
Password FAQ
Is it safe to type my real password here?
How do I create a strong password?



4.Identify best practices for creating strong passwords.

- **Maximum Length:** Aim for a minimum of 12 characters, and ideally **15 characters or more**. Longer passwords are exponentially harder to crack.
- **Character Diversity:** Include a mix of **uppercase letters**, **lowercase letters**, **numbers**, and **symbols** (e.g., `!@#$%^&*`).
- **Avoid Predictable Patterns:** Don't use simple sequences (`123456`), keyboard patterns (`qwerty`), or easily guessable alterations (`A1b2C3d4`).
- **Steer Clear of Dictionary Words and Personal Info:** Never use common words, names, birthdays, pet names, or any information easily linked to you.
- **Use Passphrases:** Create a long, memorable phrase that is broken up and includes substitutions. For example, turn a sentence like "I love coffee in the morning of 2025" into **!L0v3C0fF33iNth3M0rNiNg*25** (a strong, complex passphrase).

5.Write down tips learned from the evaluation.

- **Length Trumps Complexity:** While complexity matters, **length is the single most important factor** in password strength. A very long, slightly less complex password can be stronger than a very short, highly complex one.
- **Substitution is Key:** Replace letters with symbols or numbers (e.g., 'o' → '0', 's' → '$', 'a' → '@') to defeat dictionary and common substitution attacks.
- **Use a Password Manager:** A good password manager can generate and store unique, highly complex passwords for every single account, eliminating the need to memorize them.

6.Research common password attacks (brute force, dictionary).

✓ Brute-Force Attack 🔨

- **Mechanism:** This is a relentless, automated process where an attacker's software tries **every single possible combination** of letters, numbers, and symbols until the correct password is found.
- **Target:** It targets the entire "keyspace" of possible characters.
- **Defense:** The primary defense is **Length**. Every additional character added to the password exponentially increases the time required for a brute-force attack to succeed, quickly making it infeasible.

✓ Dictionary Attack 📚

- **Mechanism:** A more intelligent attack where the software tests passwords against a pre-compiled list (a "dictionary") of the **most commonly used passwords**, actual words, common names, dates, and passwords previously exposed in data breaches.
- **Efficiency:** This is much faster than brute-force because it ignores most random combinations and focuses only on likely words and phrases.
- **Defence:** The defence is **Uniqueness and Randomness**. Avoid using dictionary words, personal information, or common substitution patterns (like replacing 'S' with '$' or 'A' with '@'), as cracking tools automatically check for these simple variations.

7.Summarize how password complexity affects security.

Factor	Mechanism	Security Impact
Key space	Total possible combinations: K=CL	Goal is to maximize this number.
Length (L)	It is the exponent in the formula.	Most critical factor. Exponentially increases cracking time from hours (8 chars) to millions of years (14+ chars).
Diversity (C)	Increases the character set size (e.g., C=26 vs. C=94).	Dramatically expands the search space, defending against simple and dictionary attacks.
Conclusion	Long, diverse passwords.	They force attackers to use slow, impractical Brute-Force Attacks, making the cost and time to crack prohibitive.