Task_6

▨ Status	Done

Task 6 : Create a Strong Password and Evaluate Its Strength.

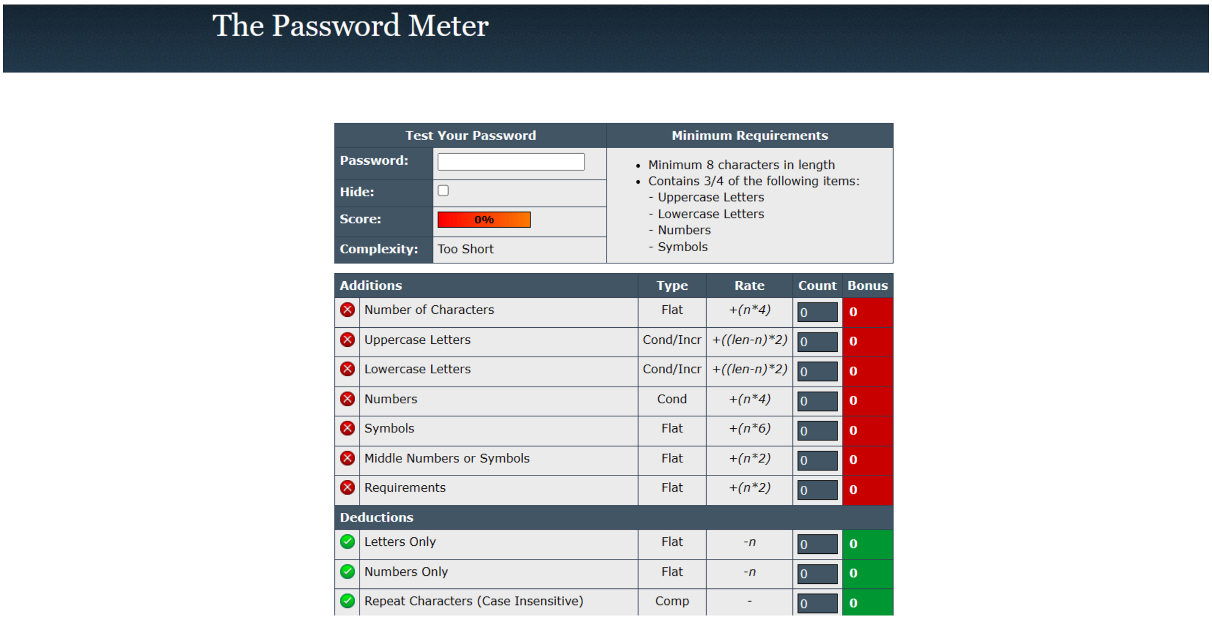
Create Multiple Passwords

We’ll make 5 example passwords with different complexity levels:

Password	Complexity Level	Reason
`apple123`	Weak	Only lowercase + numbers, short length
`AppleTree2025`	Medium	Mix of case + numbers, but no symbols
`ApP!e_Tree2025`	Strong	Uppercase + lowercase + numbers + symbols, long length
`ApT2025!@#`	Strong	Compact but mixed character set
`M0nkeyR@!nB0w*SkY2025`	Very Strong	Very long, mixed characters, hard to guess

Test on a Password Strength Checker

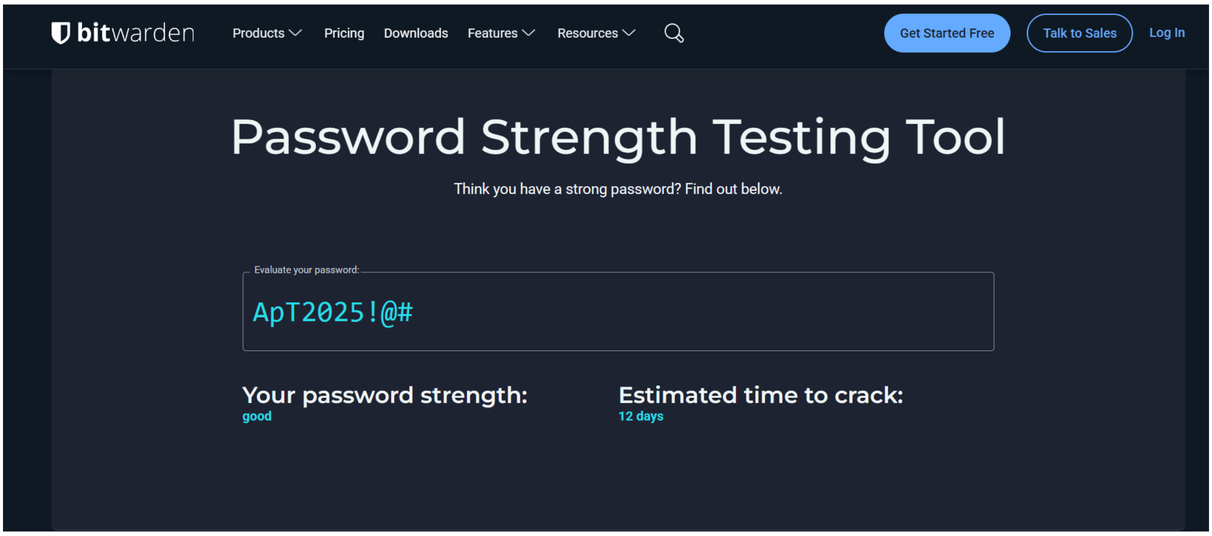
You can use **passwordmeter.com** or **bitwarden password strength tester etc.**



The Password Meter

Test Your Password		Minimum Requirements
Password:		- Minimum 8 characters in length - Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	□	
Score:	0%	
Complexity:	Too Short	

	Additions	Type	Rate	Count	Bonus
☒	Number of Characters	Flat	+(n*4)	0	0
☒	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
☒	Lowercase Letters	Cond/Incr	+((len-n)*2)	0	0
☒	Numbers	Cond	+(n*4)	0	0
☒	Symbols	Flat	+(n*6)	0	0
☒	Middle Numbers or Symbols	Flat	+(n*2)	0	0
☒	Requirements	Flat	+(n*2)	0	0
	Deductions				
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
✓	Repeat Characters (Case Insensitive)	Comp	-	0	0



Password Strength Testing Tool

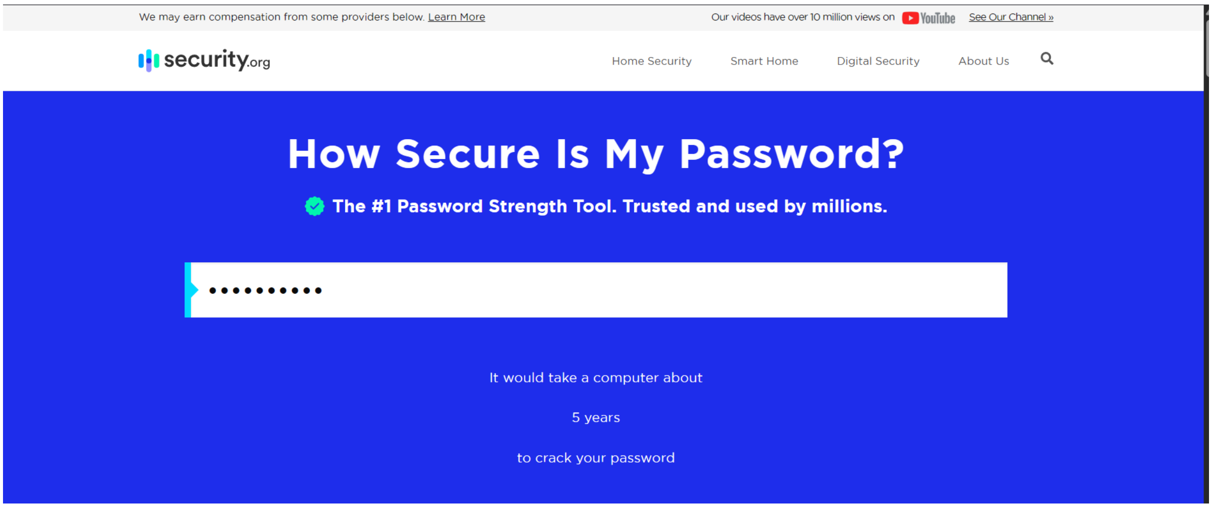
Think you have a strong password? Find out below.

Evaluate your password: ApT2025!@#

Your password strength: good

Estimated time to crack: 12 days

https://www.security.org/how-secure-is-my-password/



We may earn compensation from some providers below. Learn More

Our videos have over 10 million views on YouTube See Our Channel »

How Secure Is My Password?

The #1 Password Strength Tool. Trusted and used by millions.

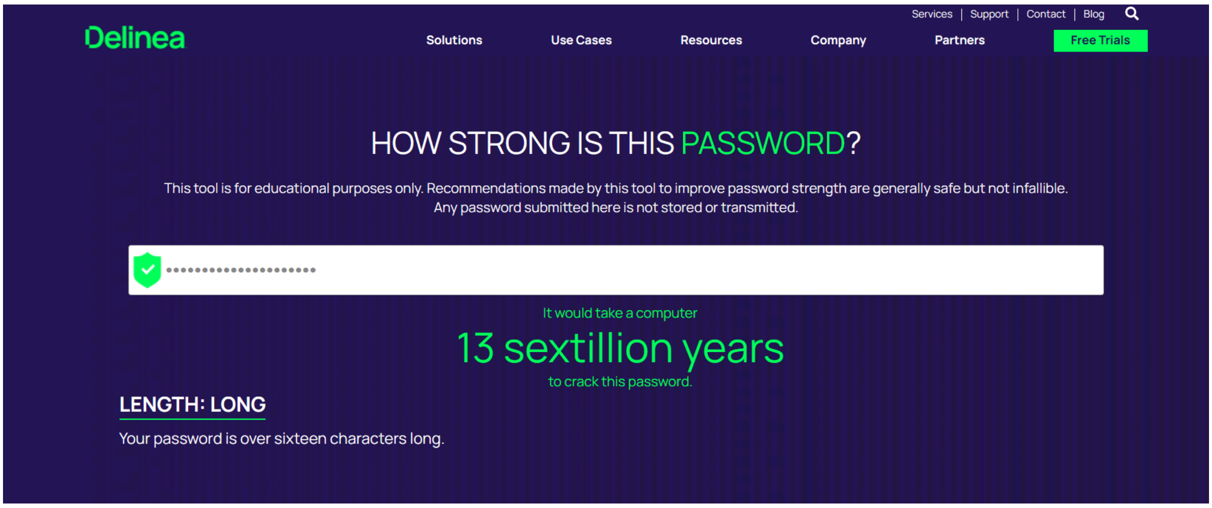
••••••••••••

It would take a computer about

5 years

to crack your password

https://delinea.com/resources/password-strength-checker



HOW STRONG IS THIS PASSWORD?

This tool is for educational purposes only. Recommendations made by this tool to improve password strength are generally safe but not infallible. Any password submitted here is not stored or transmitted.

••••••••••••••••••••

It would take a computer

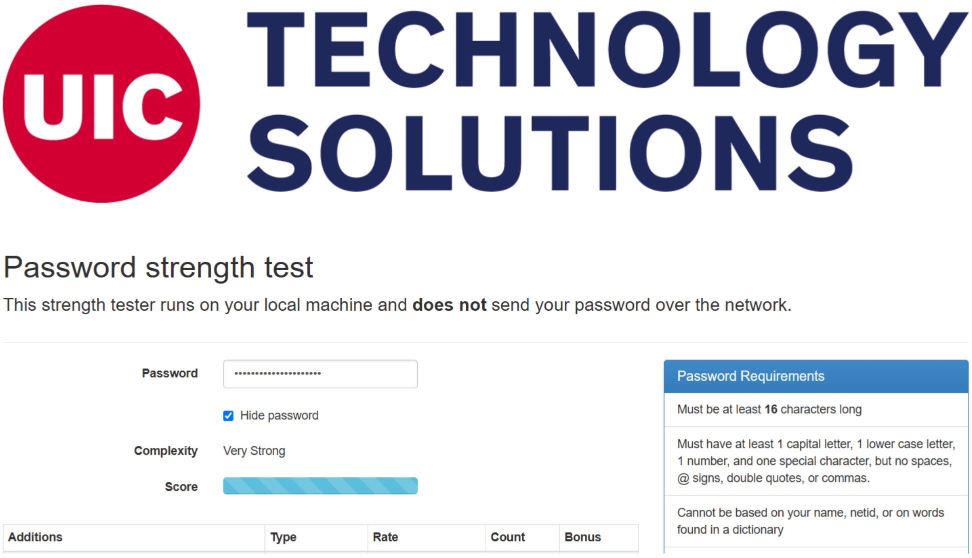
13 sextillion years

to crack this password.

LENGTH: LONG

Your password is over sixteen characters long.

https://www.uic.edu/apps/strong-password/



Password strength test

This strength tester runs on your local machine and **does not** send your password over the network.

Password: ••••••••••••••••••••

☑ Hide password

Complexity: Very Strong

Score

Additions	Type	Rate	Count	Bonus

Password Requirements

Must be at least **16** characters long

Must have at least 1 capital letter, 1 lower case letter, 1 number, and one special character, but no spaces, @ signs, double quotes, or commas.

Cannot be based on your name, netid, or on words found in a dictionary

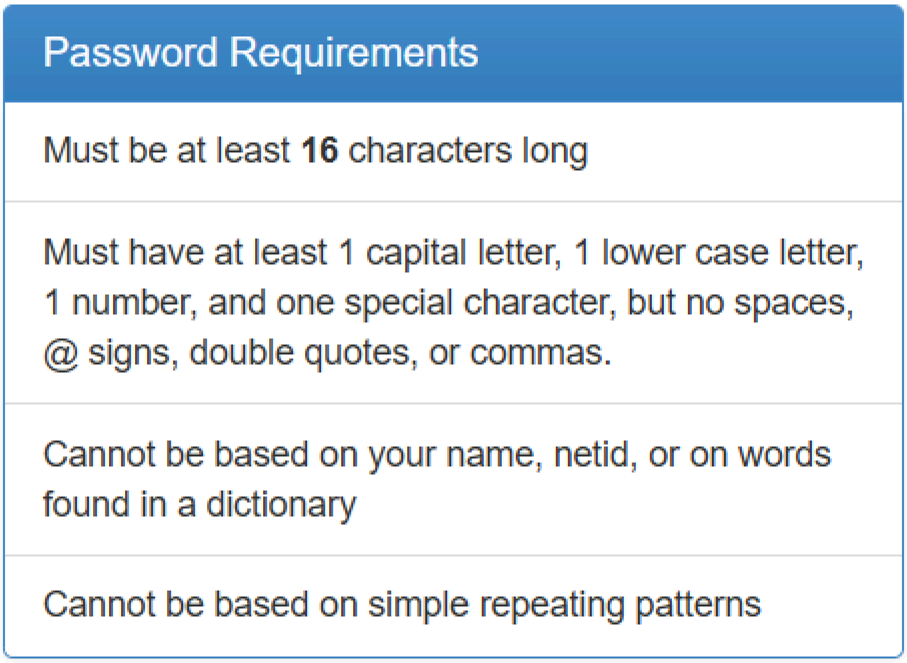
Example of possible results (from passwordmeter.com):

Password	Score	Feedback
apple123	36% (Weak)	Too short, lacks symbols, easy to guess
Apple123	63% (Medium)	Good length, lacks symbols
ApP!e_Tree2025	100% (Strong)	Excellent complexity and length
ApT2025!@#	100% (Strong)	Good complexity, slightly shorter
M0nkeyR@!nB0w*SkY2025	100% (Very Strong)	Long, complex, unpredictable

Identify Best Practices

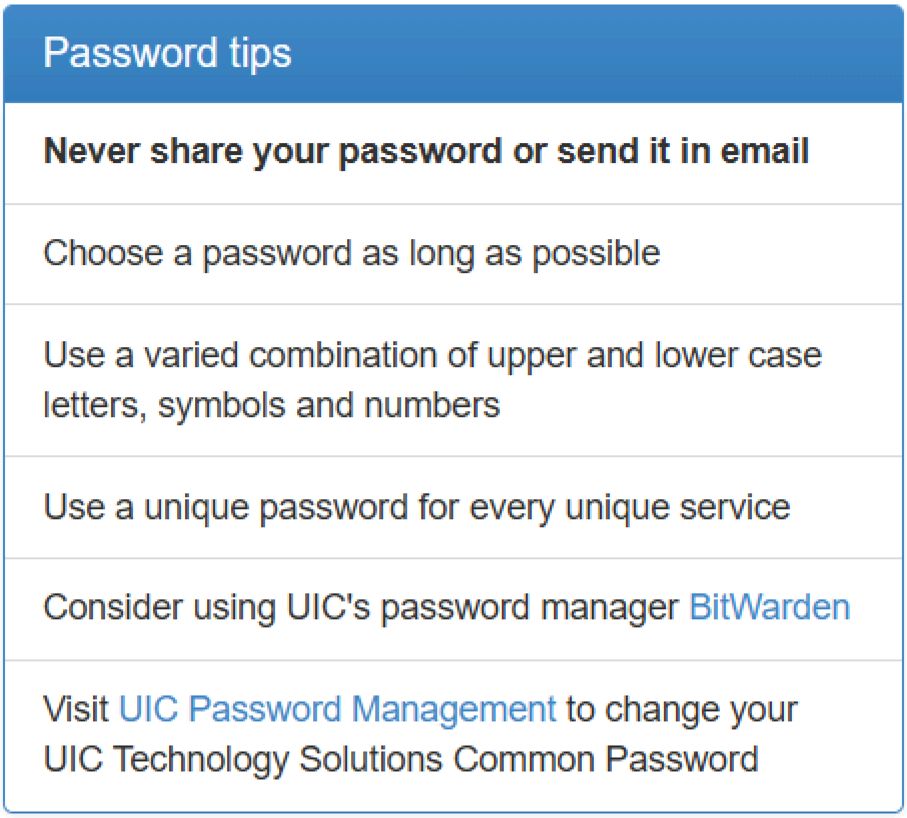
From the results, we can derive the following **strong password tips**:

1. **Length matters** – Aim for at least 12–16 characters.
2. **Mix character types** – Use uppercase, lowercase, numbers, and symbols.
3. **Avoid predictable words** – Don’t use dictionary words alone.
4. **Add randomness** – Avoid common patterns like `123`, `abc`, or birthdays.
5. **Don’t reuse passwords** – Each account should have its own password.
6. **Consider passphrases** – Combine random words with symbols for easier recall (e.g., `Blue$Tiger*Runs2025`).



Password Requirements

- Must be at least **16** characters long
- Must have at least 1 capital letter, 1 lower case letter, 1 number, and one special character, but no spaces, @ signs, double quotes, or commas.
- Cannot be based on your name, netid, or on words found in a dictionary
- Cannot be based on simple repeating patterns



Password tips

- **Never share your password or send it in email**
- Choose a password as long as possible
- Use a varied combination of upper and lower case letters, symbols and numbers
- Use a unique password for every unique service
- Consider using UIC's password manager BitWarden
- Visit UIC Password Management to change your UIC Technology Solutions Common Password

Common Password Attacks

Attack Type	Short Description
Brute Force	Tries all possible combinations.
Dictionary	Uses common words/password lists.
Credential Stuffing	Uses stolen login details from breaches.
Phishing	Tricks users into revealing passwords.
Keylogging	Records keystrokes to capture passwords.
Rainbow Table	Uses precomputed hashes to crack passwords.
Shoulder Surfing	Watches you type your password.
MITM	Intercepts data to steal credentials.
Password Spraying	Tries a few common passwords on many accounts.
Social Engineering	Manipulates people into giving passwords.

Summary on Password Complexity

- **Short, simple passwords** can be cracked in seconds or minutes.
- **Long, complex passwords** with mixed characters may take years or even centuries to brute-force.
- Using a **password manager** allows you to create and store long, unique passwords without memorizing them.

In this task, multiple passwords of varying complexity were created and tested using online password strength checkers such as **Password Meter** and **Bitwarden Password Strength Checker** and many more. The evaluation compared weak, medium, strong, and very strong passwords based on length, use of uppercase/lowercase letters, numbers, and special symbols. The results showed that **longer, more complex passwords** scored higher and are significantly harder to crack.

The task also explored **common password attacks** such as brute force, dictionary, credential stuffing, phishing, keylogging, rainbow tables, and others. From the evaluation, several best practices were identified, including using at least **12–16 characters**, mixing character types, avoiding predictable patterns, and using a password manager for storage.

Outcome:

By the end of the task, the importance of password complexity, uniqueness, and secure management was understood, along with knowledge of attack methods and strategies to defend against them.