



8/12/2025

Evaluate Password Strength



@SRCybersecurity

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

Objective: Understand what makes a password strong and test it against password strength tools.

Tools: Online free password strength checkers (e.g., passwordmeter.com).

Deliverables: Report showing password strength results and explanation. Following step by step task with examples where needed.

1. Create Multiple Passwords with Varying Complexity

- Let's generate passwords with different levels of complexity:

Password	Description
apple123	Simple: lowercase + numbers
Apple123	Adds uppercase
Apple@123	Adds a symbol
Appl3@2025!	More complex, slight substitution
Ap1le@234S5&#	High complexity, mix of everything
xY9@jF!3R#u2L&wT	Random complex password

2. Passwords with Uppercase, Lowercase, Numbers, Symbols, and Length Variations

- Lowercase only: apple
- Lowercase + Numbers: apple123
- Mixed Case + Numbers: Apple123
- Mixed + Numbers + Symbols: Apple@123
- Complex Mixed + Numbers + Symbols: Appl3@2025!
- Full complexity + longer length: Ap1le@234S5&#
- Random complex password: xY9@jF!3R#u2L&wT

3. Test Each Password on a Password Strength Checker

Tool Used:

- <https://www.security.org/how-secure-is-my-password/>
- <https://passwordmeter.com/>

Run each password through the given site and noted the given password's security measures.

- Lowercase only: apple

The image shows two browser windows. The top window is from security.org, displaying the 'How Secure Is My Password?' tool. It features a red background with a white password input field containing 'apple'. Below the field, it states 'Your password would be cracked Instantly'. The bottom window is from passwordmeter.com, showing 'The Password Meter' interface. It includes a 'Test Your Password' section with a table of requirements and a 'Minimum Requirements' section with a list of criteria.

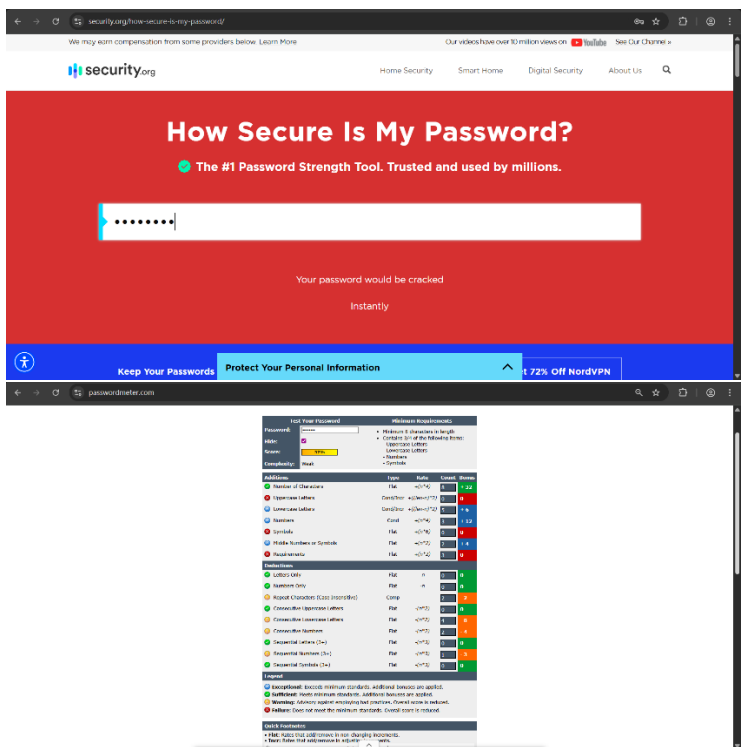
Additions	Type	Rule	Count	Points
Number of Characters	Min	>=12	1	100
Uppercase Letters	Cond/Min	>=1(12)	0	0
Lowercase Letters	Cond/Min	>=1(12)	0	0
Numbers	Cond	>=1(12)	0	0
Symbols	Min	>=1(12)	0	0
Mix of Uppercase and Lowercase	Min	>=1(12)	0	0
Requirements	Min	>=1(12)	1	0

Disincentives	Type	Rule	Count	Points
Letters Only	Min	<=1	0	0
Numbers Only	Min	<=1	0	0
Repeat Characters (Case Insensitive)	Comp	<=1	0	0
Consecutive Uppercase Letters	Min	<=1	0	0
Consecutive Lowercase Letters	Min	<=1	0	0
Consecutive Numbers	Min	<=1	0	0
Sequential Letters (3-1)	Min	<=1	0	0
Sequential Numbers (3-1)	Min	<=1	0	0
Sequential Symbols (3-1)	Min	<=1	0	0

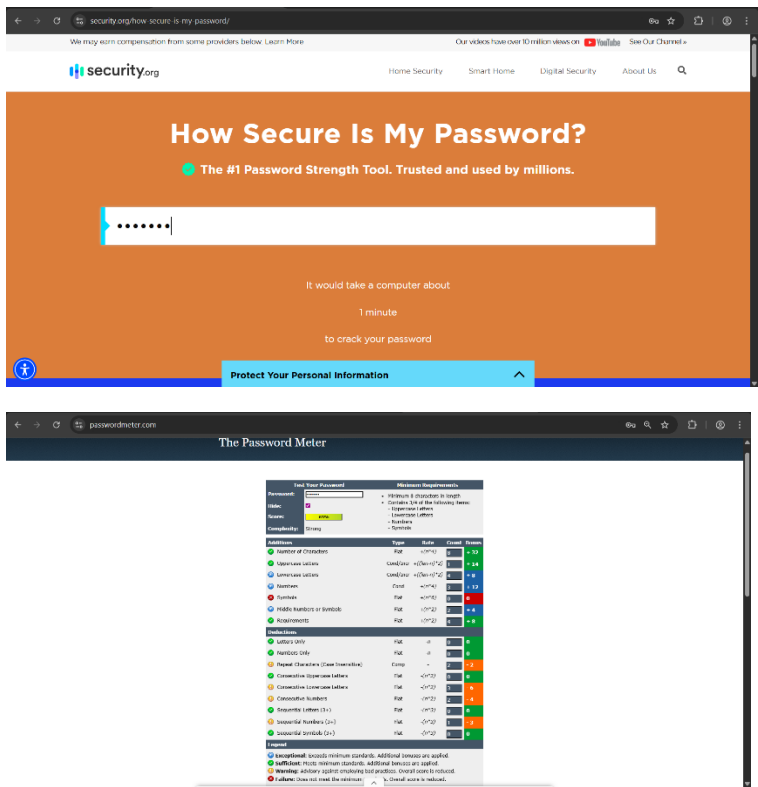
Legend

- ✔ **Excellent:** Exceeds minimum standards. Additional bonuses are applied.
- ⚠ **Sufficient:** Meets minimum standards. Additional bonuses are applied.
- ✖ **Warning:** Advisory against employing bad practices. Overall score is reduced.
- ✖ **Failure:** Does not meet the minimum. % Overall points is reduced.

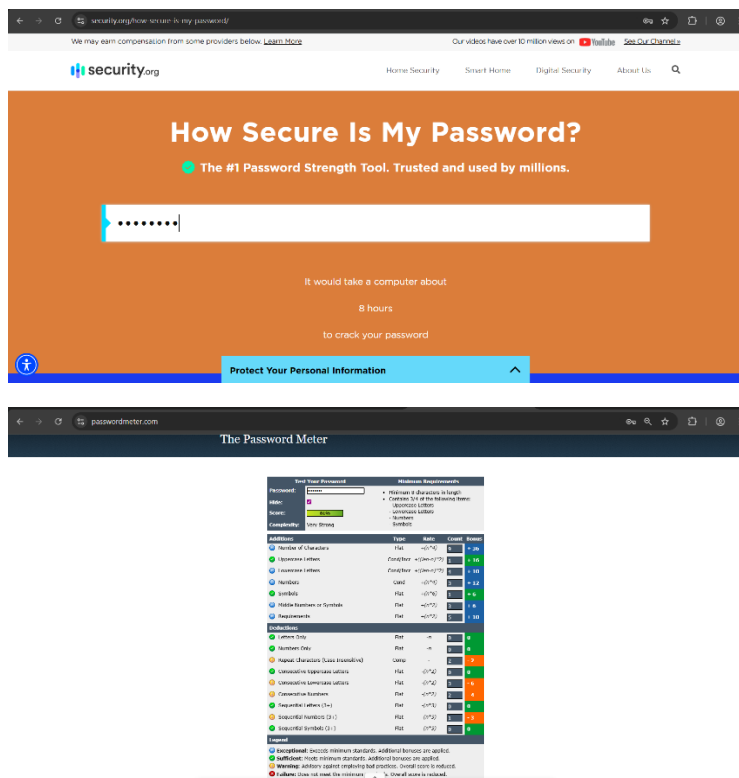
- Lowercase + Numbers: apple123



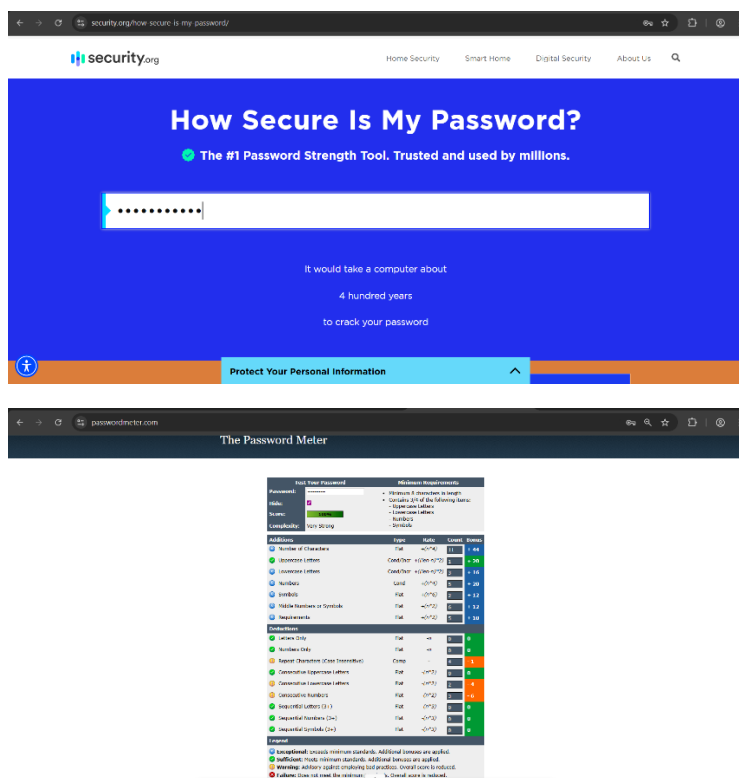
- Mixed Case + Numbers: Apple123



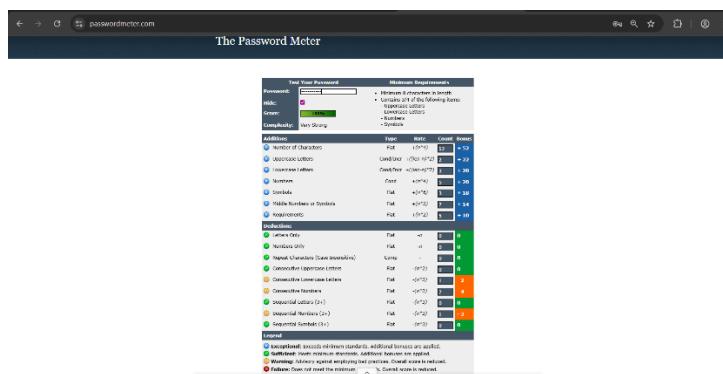
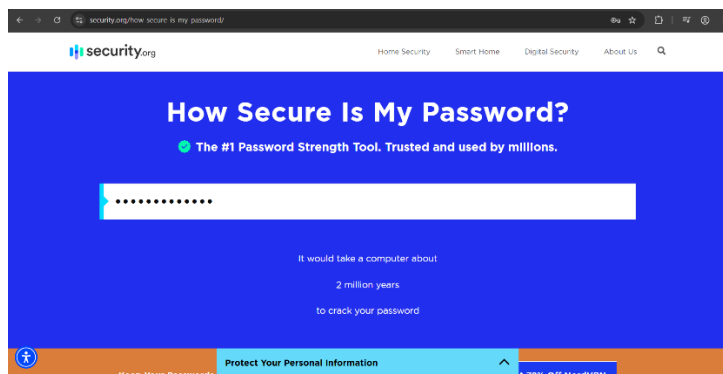
- Mixed + Numbers + Symbols: Apple@123



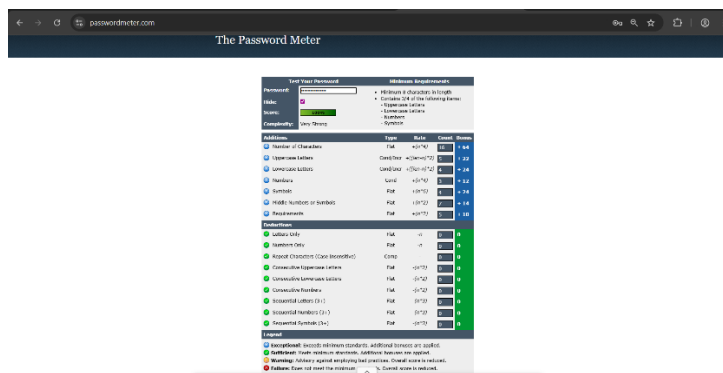
- Complex Mixed + Numbers + Symbols: Appl3@2025!



- Full complexity + longer length: Ap1le@234S5&#



- Random complex password: xY9@jF!3R#u2L&wT



4. Scores and Feedback from the Tool

Password	Estimated Crack Time	Feedback
apple	Instantly	Very Weak, lacks numbers, symbols
apple123	Few seconds	Too common, lacks symbols
Apple123	A few minutes	Add special characters
Apple@123	A few hours	Could be longer
Appl3@2025!	A few hundred years	Strong
Ap1le@234S5&#	Million years	Strong
xY9@jF!3R#u2L&wT	Trillion Years	Excellent

5. Best Practices for Creating Strong Passwords

From the testing and feedback:

- Use a mix of uppercase, lowercase, numbers, and symbols.
- Avoid dictionary words and common patterns.
- Make it at least 12–16 characters long.
- Don't reuse passwords across multiple sites.
- Use a passphrase or random words for memorability and complexity.
- Consider using a password manager to store and generate secure passwords.

6. Tips Learned from the Evaluation

Tips:

- The longer the password, the better (exponential increase in security).
- Complexity (mixed characters) drastically increases security.
- Substituting numbers for letters (e.g., 3 for e) helps a little but isn't foolproof.
- Random character placement is more effective than predictable patterns.
- Passphrases like AppleFruitIsNotForFree! are both strong and memorable.

7. Common Password Attacks

Brute Force Attack

- Tries every possible combination.
- Longer and more complex passwords take exponentially longer to crack.
- Tools: Hydra, John the Ripper, Hashcat

Dictionary Attack

- Uses a list of common passwords or words.
- Faster than brute force.
- Can be defeated with unique and non-dictionary passwords.

Credential Stuffing

- Uses stolen username/passwords from breaches.
- Emphasizes the importance of not reusing passwords.

8. Password Complexity Affects Security Summary:

- Password complexity greatly enhances security.
- Simple passwords using common words or patterns are vulnerable to dictionary and brute-force attacks.
- Complexity achieved by including uppercase and lowercase letters, numbers, symbols, and longer lengths dramatically increases the time and computing power required to crack a password.
- Unique, unpredictable passwords are best defence against modern password cracking techniques.

END