TASK 6: CREATE A STRONG PASSWORD AND EVALUATE ITS STRENGTH

Cybersecurity Lab Report

VOONNA VENKATESH
ELEVATE LABS

Task 6:

Creating a Strong Password and Evaluating its Strength

Index:

1.Create multiple passwords with varying complexity.

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

3.Test each password on password-strength checker.

4.Note scores and feedback from the tool.

5.Identify best practices for creating strong passwords.

6.Write down tips learned from the evaluation.

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

8.Summarize how password complexity affects security.

Objective

Understanding what makes a password strong and testing it with various password strength tools

Tools Used

- Passwordmeter
- Kaspersky
- Security.org

Steps Performed:

Step 1: Create Multiple Passwords with Varying Complexity

Start by creating a list of 6–8 passwords that vary by:

- Length
- Use of uppercase/lowercase letters
- Use of numbers
- Use of symbols
- Simple vs complex structures

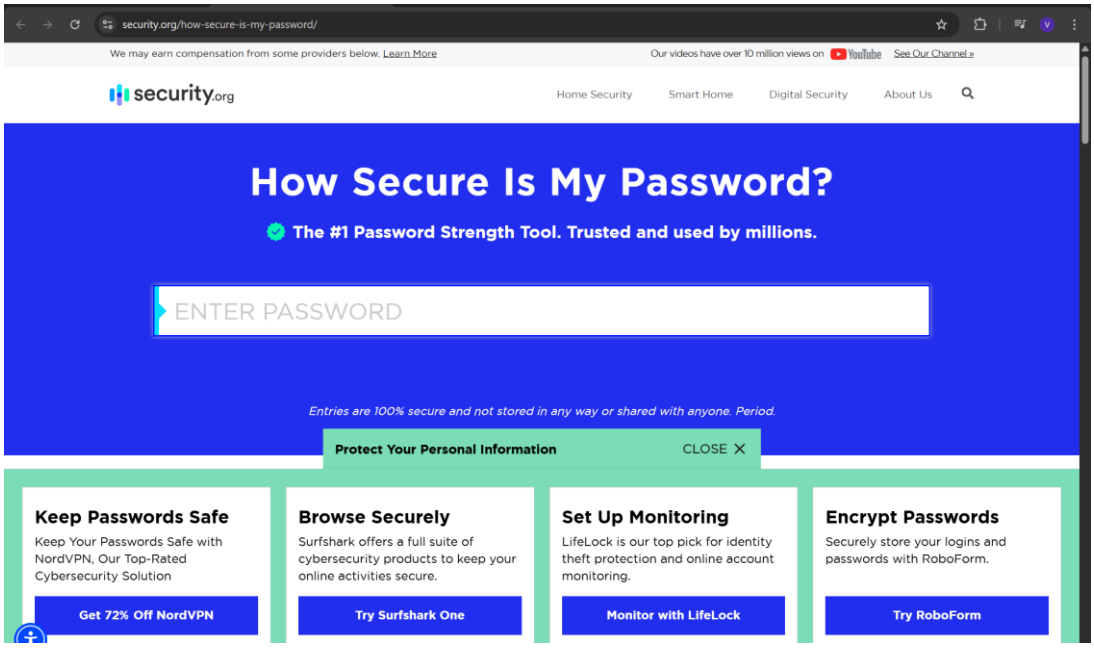
Sample Passwords:

1. password123
2. Password123
3. Pass@123
4. P@55w0rD!
5. P@$$w0rD!2025
6. xY8#qL2@!zM$1
7. vV!9tL@92#bX$hZ%W2

Step 2: Use a Password Strength Checker Tool

Go to an online tool like:

- 🔗 https://www.passwordmeter.com
- 🔗 https://www.security.org/how-secure-is-my-password/
- 🔗 https://www.kaspersky.com/password-check



Step 3: Record Scores and Feedback in a Table

Password	Score / Rating	Time to Crack	Tool Feedback
password123	Weak (20%)	Instant	Too common, no symbols or caps
Password123	Moderate (40%)	3 hours	Add symbols
Pass@123	Strong (65%)	2 days	Consider more length
P@55w0rD!	Very Strong (85%)	5 years	Good complexity
P@$$w0rD!2025	Excellent (95%)	1 Billion years	Excellent password
xY8#qL2@!zM$1	Excellent (100%)	14 Trillion years	Very high complexity
vV!9tL@92#bX$hZ%W2	Excellent (100%)	>Trillions of years	Extremely secure

Step 4: Identify Best Practices for Strong Passwords

From tool feedback and scores, extract these best practices:

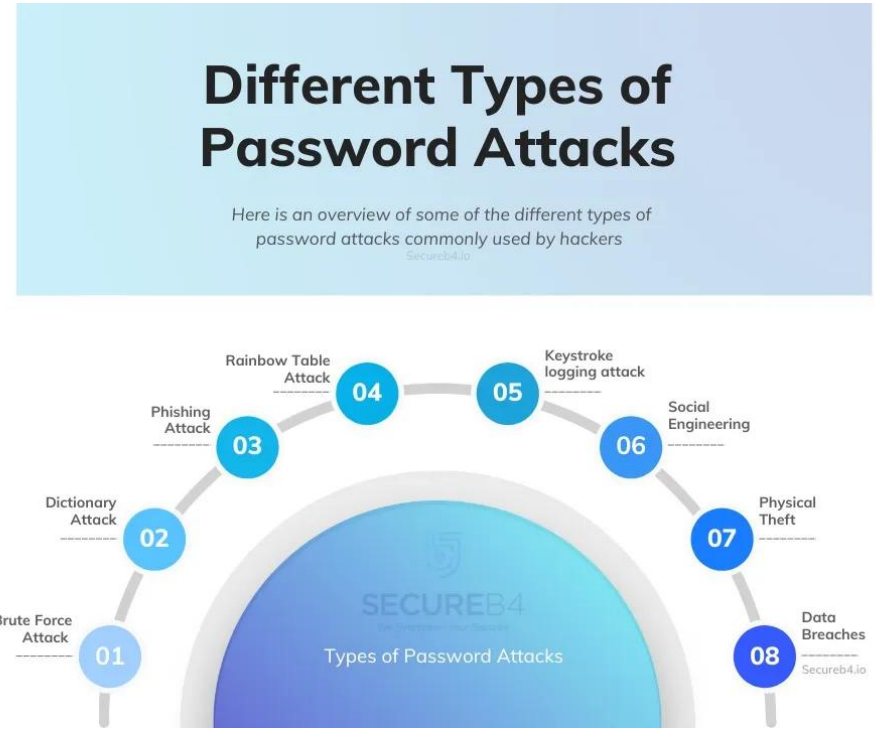
- Use 12+ characters.
  Mix uppercase, lowercase, numbers, symbols.
  Avoid dictionary words or predictable patterns.
- Do not reuse old passwords.
- Use passphrases when possible (e.g., Purple$Sky2025@).
  Randomness is key—avoid names, birthdays, common phrases.

Step 5: Research on Common Password Attacks

- **Brute Force Attack**
- Tries all combinations until it finds the correct one
- Longer, more complex passwords take much more time to crack
- **Dictionary Attack**
- Uses a list of common passwords or words
- Common passwords like password123 are cracked instantly
- **Credential Stuffing**
- Uses leaked username/passwords across different sites
- Reused passwords make this dangerous

- **Phishing**

- Tricks you into revealing your password (email, fake login pages)
- Not related to complexity but important for context



Step 6: Impact of Password Complexity on Security

Password complexity increases:

- Entropy: A measure of unpredictability
- Time to crack: More combinations = more time for brute-force
- Resistance to attacks: Complex and long passwords withstand most automated attacks

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

Conclusion:

In this task, we explored how password complexity directly impacts security. By creating and testing multiple passwords with varying lengths, character types, and structures using password strength checkers, we observed that simple and predictable passwords are easily cracked, while long, random combinations with a mix of uppercase, lowercase, numbers, and special characters are significantly more secure.

We also researched common password attacks such as brute force and dictionary attacks, which highlighted the importance of unpredictability and length in password creation. The tools used provided valuable feedback and reinforced best practices, such as avoiding reused or common passwords and using passphrases or password managers for better security.

Overall, this task demonstrated that a strong password is a critical line of defence in cybersecurity, and following password complexity guidelines greatly reduces the risk of unauthorized access.