TASK 6:

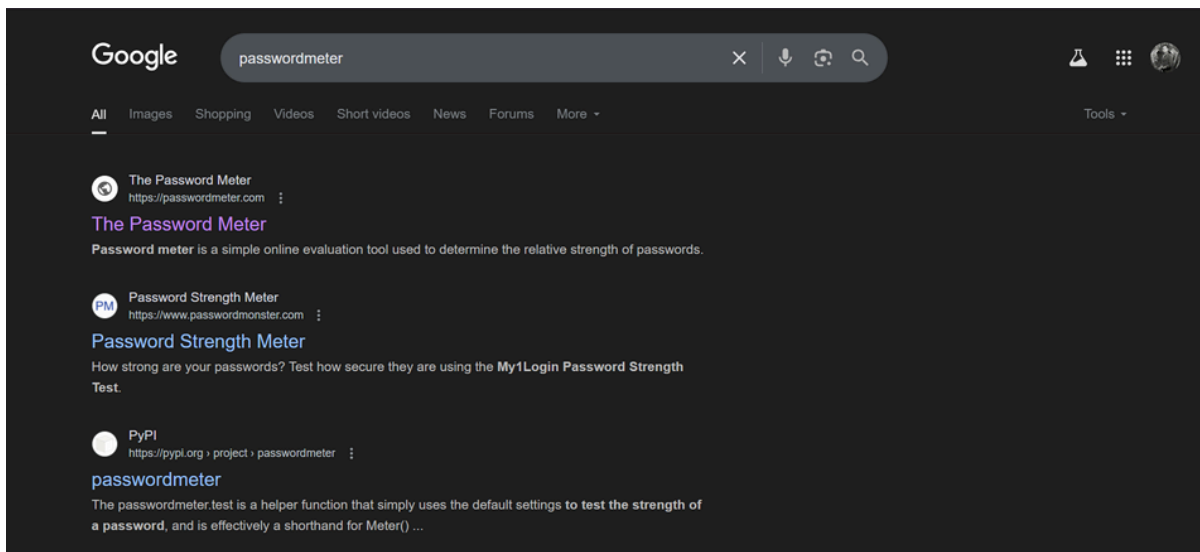## Create a Strong Password and Evaluate Its Strength..

JUN 3, 2025

ADHIKRISHNAN M

adhikrishnan9943@gmail.com

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.

Step 2:

The Password Meter

Test Your Password		Minimum Requirements
Password:	•••••••	• Minimum 8 characters in length
Hide:	☑	• Contains 3/4 of the following items:

Score:	31%	– Uppercase Letters
		   – Lowercase Letters
		   – Numbers
		   – Symbols

Complexity:	Weak	

Additions	Type	Rate	Count	Bonus
❌ Number of Characters	Flat	+(n*4)	7	+ 28
❌ Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
🔵 Lowercase Letters	Cond/Incr	+((len-n)*2)	4	+ 6
🔵 Numbers	Cond	+(n*4)	3	+ 12
❌ Symbols	Flat	+(n*6)	0	0
🔵 Middle Numbers or Symbols	Flat	+(n*2)	2	+ 4
❌ Requirements	Flat	+(n*2)	2	0

STEP 3

STEP 4

The Password Meter

Test Your Password		Minimum Requirements
Password:	●●●●●●●●●●●●	• Minimum 8 characters in length
Hide:	☑	• Contains 3/4 of the following items:
Score:	100%	- Uppercase Letters
Complexity:	Very Strong	- Lowercase Letters
		- Numbers
		- Symbols

Additions		Type	Rate	Count	Bonus
⊗	Number of Characters	Flat	+(n*4)	12	+ 48
⊗	Uppercase Letters	Cond/Incr	+((len-n)*2)	3	+ 18
⊗	Lowercase Letters	Cond/Incr	+((len-n)*2)	2	+ 20
⊗	Numbers	Cond	+(n*4)	3	+ 12
⊗	Symbols	Flat	+(n*6)	4	+ 24
⊗	Middle Numbers or Symbols	Flat	+(n*2)	5	+ 10
⊗	Requirements	Flat	+(n*2)	5	+ 10

✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
✓	Repeat Characters (Case Insensitive)	Comp	-	0	0
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
✓	Consecutive Lowercase Letters	Flat	-(n*2)	0	0
✓	Consecutive Numbers	Flat	-(n*2)	0	0
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
✓	Sequential Numbers (3+)	Flat	-(n*3)	0	0
✓	Sequential Symbols (3+)	Flat	-(n*3)	0	0

Legend

⊗ **Exceptional:** 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 standards. Overall score is reduced.

Quick Footnotes

• **Flat:** Rates that add/remove in non-changing increments.
• **Incr:** Rates that add/remove in adjusting increments.

Second Life

Password	Complexity Features Used	Strength Score (%)	Tool Feedback
abcd1234	lowercase + numbers	26%	Too short, predictable, lacks s
Abcd1234	Uppercase + lowercase + numl	46%	Moderate strength; lacks symb
Abc@1234	Uppercase + lowercase + numl	68%	Good; suggest increasing lengt
A!b2#C3@d4	Mixed case + numbers + multip	94%	Strong password
3X!r$T9&uV^0@	Upper/lower + numbers + spec	100%	Excellent; highly secure

Attack Type	Description	Defense (Password Strategy)
Brute Force	Tries all possible combinations (e.g., aaaa	Longer, complex passwords increase time
Dictionary	Uses a list of common words/passwords (	Avoid using common words or patterns.
Credential Stuffing	Tries known passwords from leaked datab	Use **unique** passwords for each site.