1. Creating multiple passwords with varying complexity using uppercase, lowercase, numerics & symbols

Here we use chatgpt in order to create multiple passwords of several complexities by providing the prompt "*Generate sample passwords for a practical evaluation, use uppercase, lowercase, numerics & symbol. Generate multiple passwords and categorize them into easy, medium, hard, extreme & unhackable"*

Which produces the output "*Here are sample passwords categorized by complexity level, using a mix of uppercase, lowercase, numbers, and symbols, ideal for a practical evaluation or cyber security training:*

1. Easy (Minimal complexity – 8 characters, simple patterns)
    - *Pass123!*
    - *Hello@21*
    - *Test#456*
    - *Moon2024!*
    - *Qwerty#7*
- Characteristics: Easy to remember, but susceptible to brute force/dictionary attacks.

2. Medium (Moderate complexity – 10–12 characters, better mix, common substitutions)
    - *Gr33n$Appl3*
    - *SunSh!ne92*
    - *C0ffee#Bean*
    - *T1ger@Cl4wz*
    - *W1nter#2025*
- Characteristics: Slight obfuscation and better entropy. Somewhat resistant to basic attacks.

3. Hard (Strong mix – 14–16 characters, non-obvious, multi-layered)
    - *D3lt@Force#92Xy*
    - *R!verFlow_2025x*
    - *M@trix_Sh1ft*33*

- *F@stTrack99_Bz*
- *N1ght$T0rm!420*

- Characteristics: Good randomness, suitable for secure systems. Harder to crack via brute force.

4. Extreme (High entropy – 18–22 characters, minimal patterns, strong randomness)

    - *kX$71pA#rT!9wZqV0uMn*
    - *Bl@ckT!gr_P8z3#xY12w*
    - *V0id@N3bul@!82XmTkqZ*
    - *S!l3nt#V0!ce_452Xmpq*
    - *Y!ggDr@5!l_R1v3rM0ss_*

- Characteristics: Designed to be very difficult to guess. Suitable for privileged accounts or vaults.

5. Unhackable (Randomly generated – 24+ characters, virtually impossible to crack)

    - *cA!9Tz@L4#vRpE3xMn$7bFzYw*
    - *X1@o$K8!9rLzp!WyR2u&VmJcTq*
    - *#Gqv7M@xZ^tF9e!B8WxRp!nY3K*
    - *pL!z9Tr#m7AqX@Y^zB5EvwQs0j*

- Characteristics: Near-perfect entropy. Meant for machine use or password managers, not memorization.

2. Testing each password on password strength checker & Noting scores & feedback for the password

1. Easy

- Pass123!

Test Your Password		Minimum Requirements
Password:	Pass123!	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:		
Score:	77%	
Complexity:	Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	8	+ 32
Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 14
Lowercase Letters	Cond/Incr	+((len-n)*2)	3	+ 10
Numbers	Cond	+(n*4)	3	+ 12
Symbols	Flat	+(n*6)	1	+ 6
Middle Numbers or Symbols	Flat	+(n*2)	3	+ 6
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	2	- 2
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	2	- 4
Consecutive Numbers	Flat	-(n*2)	2	- 4
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	1	- 3
Sequential Symbols (3+)	Flat	-(n*3)	0	0
Legend				

The password "Pass123!" scores 77% with a Strong complexity rating. It includes all key character types—uppercase, lowercase, numbers, and a symbol—meeting all minimum requirements. Its 8-character length and use of middle-positioned numbers also contribute positively.
However, it has a few weaknesses. The repeated letter s, consecutive lowercase letters (ss), and the sequential number pattern 123 make it slightly more predictable and reduce its overall strength.
In summary, "Pass123!" is a well-formed, strong password with good variety. To improve it further, avoid common patterns and repeated characters, and consider increasing the length for added security

- Hello@21

Test Your Password		Minimum Requirements
Password:	Hello@21	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:		
Score:	72%	
Complexity:	Strong	

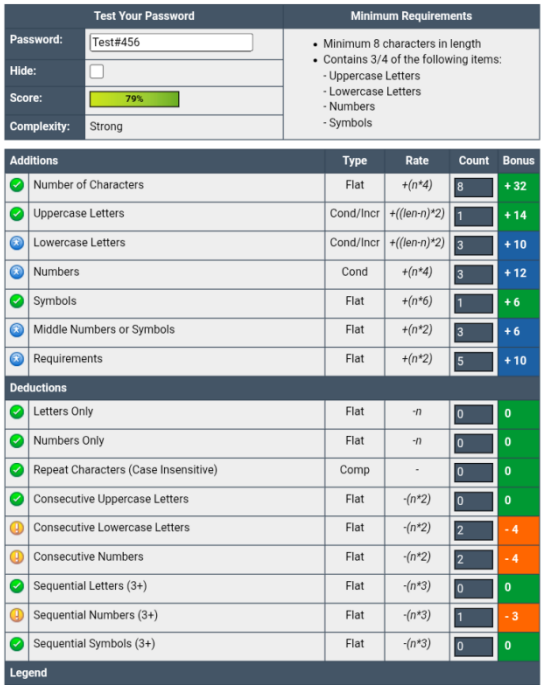
Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	8	+ 32
Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 14
Lowercase Letters	Cond/Incr	+((len-n)*2)	4	+ 8
Numbers	Cond	+(n*4)	2	+ 8
Symbols	Flat	+(n*6)	1	+ 6
Middle Numbers or Symbols	Flat	+(n*2)	2	+ 4
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	2	- 2
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	3	- 6
Consecutive Numbers	Flat	-(n*2)	1	- 2
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				

The password "Hello@21" scores 72% with a Strong complexity rating. It contains a good mix of character types, including uppercase (H), lowercase (e, l, l, o), a symbol (@), and numbers (2, 1). It meets all five of the minimum requirements and has an adequate length of 8 characters.

However, a few weaknesses bring down the score slightly. The password includes repeated characters (l appears twice), which slightly reduces entropy. There are also three consecutive lowercase letters (ell), and the pair of consecutive numbers (21) is another predictable element that lowers its strength.

In summary, "Hello@21" is a solid and strong password with balanced elements and good structure. To make it stronger, avoid repeated and consecutive patterns, especially with lowercase letters and numbers, and consider adding more length or complexity to increase its unpredictability.

- Test#456



Test Your Password		Minimum Requirements
Password:	Test#456	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	79%	
Complexity:	Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	8	+ 32
Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 14
Lowercase Letters	Cond/Incr	+((len-n)*2)	3	+ 10
Numbers	Cond	+(n*4)	3	+ 12
Symbols	Flat	+(n*6)	1	+ 6
Middle Numbers or Symbols	Flat	+(n*2)	3	+ 6
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
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)	2	- 4
Consecutive Numbers	Flat	-(n*2)	2	- 4
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	1	- 3
Sequential Symbols (3+)	Flat	-(n*3)	0	0
Legend				

The password "Test#456" scores 79% with a Strong complexity rating. It benefits from a solid structure—8 characters in total—and includes uppercase (T), lowercase (e, s, t), numbers (4, 5, 6), and a symbol (#). It satisfies all minimum complexity requirements and earns strong bonus points for character variety and placement.

Still, a few minor issues affect its score. It includes consecutive lowercase letters (es, st), consecutive numbers (456), and a sequential numeric pattern, all of which are common and predictable patterns that weaken overall randomness.

In summary, "Test#456" is a well-constructed password with strong fundamentals and diverse elements. To further strengthen it, avoid predictable number sequences and repeated character patterns. A small tweak here can push it closer to the "Exceptional" category.

- Moon2024!

Test Your Password		Minimum Requirements
Password:	Moon2024!	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	92%	
Complexity:	Very Strong	

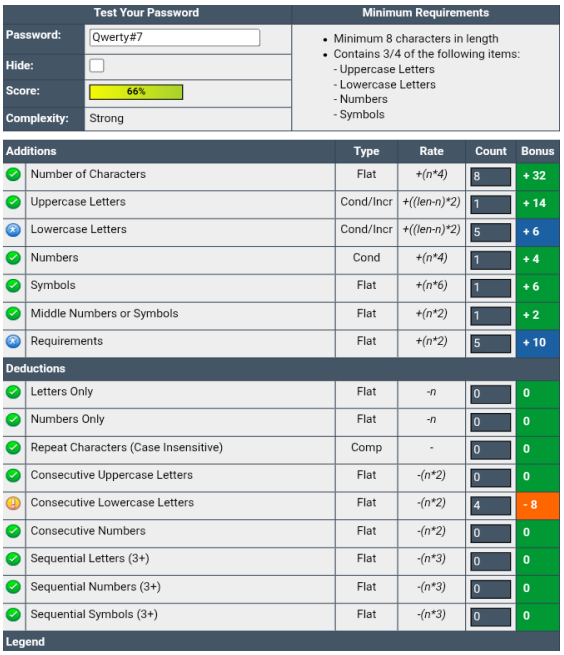
Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	9	+ 36
Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 16
Lowercase Letters	Cond/Incr	+((len-n)*2)	3	+ 12
Numbers	Cond	+(n*4)	4	+ 16
Symbols	Flat	+(n*6)	1	+ 6
Middle Numbers or Symbols	Flat	+(n*2)	4	+ 8
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	4	- 2
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	2	- 4
Consecutive Numbers	Flat	-(n*2)	3	- 6
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				

The password "Moon2024!" scores 92% with a Very Strong complexity rating. It includes a balanced mix of uppercase (M), lowercase letters (oon), numbers (2024), and a symbol (!), spread across 9 characters. It also earns points for placing numbers and symbols in varied positions and meets all complexity requirements.

However, there are a few minor weaknesses. The password includes repeated lowercase letters (o twice), consecutive lowercase characters (oo), and a consecutive number sequence (2024), leading to small deductions. While these don't drastically impact its strength, they slightly reduce randomness.

In summary, "Moon2024!" is a secure and well-structured password that exceeds security standards. To further improve, consider breaking common number patterns and avoiding character repetition for even stronger unpredictability.

- Qwerty#7



Test Your Password		Minimum Requirements
Password:	Qwerty#7	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	66%	
Complexity:	Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	8	+ 32
Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 14
Lowercase Letters	Cond/Incr	+((len-n)*2)	5	+ 6
Numbers	Cond	+(n*4)	1	+ 4
Symbols	Flat	+(n*6)	1	+ 6
Middle Numbers or Symbols	Flat	+(n*2)	1	+ 2
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
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)	4	- 8
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				

The password **"Qwerty#7"** scores **66%** with a **Strong** complexity rating. It includes an uppercase letter (Q), lowercase letters (werty), a number (7), and a symbol (#), across **8 characters**, and meets all minimum complexity requirements.

However, it has notable weaknesses. It contains **consecutive lowercase characters** ("werty")—a common keyboard pattern—and repeated characters, which reduce randomness. The use of "Qwerty" also makes it highly predictable and vulnerable to attacks.

In summary, **"Qwerty#7"** meets the technical criteria for strength but lacks real security due to its predictability. Replacing common patterns with less familiar elements would make it more secure.

2. Medium

- Gr33n$Appl3

Test Your Password		Minimum Requirements
Password:	Gr33n$Appl3	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:		
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	11	+ 44
Uppercase Letters	Cond/Incr	+((len-n)*2)	2	+ 18
Lowercase Letters	Cond/Incr	+((len-n)*2)	5	+ 12
Numbers	Cond	+(n*4)	3	+ 12
Symbols	Flat	+(n*6)	1	+ 6
Middle Numbers or Symbols	Flat	+(n*2)	3	+ 6
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	5	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	2	- 4
Consecutive Numbers	Flat	-(n*2)	1	- 2
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				

The password "Gr33n$Appl3" scores 100% with a Very Strong complexity rating. It includes uppercase letters (G, A), lowercase letters (r, n, p, l), numbers (3, 3, 3), and a symbol ($), distributed across 11 characters. The structure is diverse and satisfies all complexity requirements, with numbers and symbols placed in varied positions.

Minor deductions were due to repeated characters (3 appears thrice), consecutive lowercase letters ("pp"), and a short numeric sequence, but these have minimal impact on overall strength.

In summary, "Gr33n$Appl3" is a well-constructed and secure password that exceeds best practice standards. It balances complexity with unpredictability, offering excellent protection.

- SunSh!ne92

Test Your Password		Minimum Requirements
Password:	SunSh!ne92	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:		
Score:	87%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	10	+ 40
Uppercase Letters	Cond/Incr	+((len-n)*2)	2	+ 16
Lowercase Letters	Cond/Incr	+((len-n)*2)	5	+ 10
Numbers	Cond	+(n*4)	2	+ 8
Symbols	Flat	+(n*6)	1	+ 6
Middle Numbers or Symbols	Flat	+(n*2)	2	+ 4
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	4	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	2	- 4
Consecutive Numbers	Flat	-(n*2)	1	- 2
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				

The password "SunSh!ne92" scores 87% with a Very Strong complexity rating. It features uppercase letters (S, S), lowercase letters (u, n, h, n, e), numbers (9, 2), and a symbol (!), totaling 10 characters. Its structure meets all complexity requirements and includes a good distribution of character types.

Minor deductions are due to repeated characters (n appears twice), consecutive lowercase letters ("ne"), and consecutive numbers ("92"), slightly lowering the overall score.

In summary, "SunSh!ne92" is a strong and balanced password. Reducing character repetition and breaking number sequences would enhance its randomness further.

- C0ffee#Bean

Test Your Password		Minimum Requirements
Password:	C0ffee#Bean	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	82%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	11	+ 44
Uppercase Letters	Cond/Incr	+((len-n)*2)	2	+ 18
Lowercase Letters	Cond/Incr	+((len-n)*2)	7	+ 8
Numbers	Cond	+(n*4)	1	+ 4
Symbols	Flat	+(n*6)	1	+ 6
Middle Numbers or Symbols	Flat	+(n*2)	2	+ 4
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	5	- 2
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	5	- 10
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				

The password "C0ffee#Bean" scores 82% with a Very Strong complexity rating. It spans 11 characters and contains a mix of uppercase (C, B), lowercase (offee, ean), a number (0), and a symbol (#), fulfilling all major complexity requirements and ensuring a strong structural foundation.

Despite its strength, minor deductions arise from repeated characters (e appears three times) and consecutive lowercase letters ("offee" and "ean"), which slightly impact its unpredictability.

Overall, "C0ffee#Bean" is a robust and secure password. For even greater strength, aim to reduce character repetition and break up consecutive letter patterns.

- T1ger@Cl4wz

Test Your Password		Minimum Requirements
Password:	T1ger@Cl4wz	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	96%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	11	+ 44
Uppercase Letters	Cond/Incr	+((len-n)*2)	2	+ 18
Lowercase Letters	Cond/Incr	+((len-n)*2)	6	+ 10
Numbers	Cond	+(n*4)	2	+ 8
Symbols	Flat	+(n*6)	1	+ 6
Middle Numbers or Symbols	Flat	+(n*2)	3	+ 6
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
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)	3	- 6
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				

The password "T1ger@Cl4wz" scores 96% with a Very Strong complexity rating. It includes a solid mix of character types: uppercase letters (T, C), lowercase letters, numbers (1, 4), and a symbol (@), all spread across 11 characters. It also places symbols and numbers in the middle of the string, further boosting its strength. The password meets all major complexity requirements and shows good distribution of varied character types.

There is a minor deduction due to three consecutive lowercase letters ("l4wz"), but no repeated characters or common sequences. Importantly, it avoids dictionary words and keyboard patterns, making it resistant to common attack methods like brute force or pattern matching.

In summary, "T1ger@Cl4wz" is a highly secure password with strong randomness and minimal weaknesses. It is well-suited for protecting sensitive accounts or data.

- W1nter#2025

Test Your Password		Minimum Requirements
Password:	W1nter#2025	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	11	+ 44
Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 20
Lowercase Letters	Cond/Incr	+((len-n)*2)	4	+ 14
Numbers	Cond	+(n*4)	5	+ 20
Symbols	Flat	+(n*6)	1	+ 6
Middle Numbers or Symbols	Flat	+(n*2)	5	+ 10
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	2	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	3	- 6
Consecutive Numbers	Flat	-(n*2)	3	- 6
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				

The password "W1nter#2025" scores a full 100% with a Very Strong complexity rating. It includes a balanced mix of uppercase (W), lowercase letters, numbers (1, 2, 0, 5), and a special character (#), distributed well across 11 characters. It also places multiple numbers and the symbol in the middle, adding to its strength. The password meets all five complexity requirements and gains substantial bonuses for length and variety.

Despite a few minor deductions due to repeated characters and consecutive lowercase letters or numbers, these do not significantly impact its overall strength. It avoids dictionary word patterns and sequences that could make it predictable.

In summary, "W1nter#2025" is a robust, well-structured password ideal for securing sensitive data, with excellent character diversity and minimal vulnerabilities.

3. Hard

- *D3lt@Force#92Xy*

Test Your Password		Minimum Requirements
Password:	D3lt@Force#92Xy	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	15	+ 60
Uppercase Letters	Cond/Incr	+((len-n)*2)	3	+ 24
Lowercase Letters	Cond/Incr	+((len-n)*2)	7	+ 16
Numbers	Cond	+(n*4)	3	+ 12
Symbols	Flat	+(n*6)	2	+ 12
Middle Numbers or Symbols	Flat	+(n*2)	5	+ 10
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
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)	4	- 8
Consecutive Numbers	Flat	-(n*2)	1	- 2
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				

The password "D3lt@Force#92Xy" scores a perfect 100% and is rated Very Strong in complexity. It effectively combines uppercase letters, lowercase letters, numbers, and symbols across a substantial length of 15 characters.

Bonuses are high for length (+60), uppercase and lowercase mix, and symbol placement. It avoids risky patterns like sequences, repeated characters, or common word groupings. The only minor deductions come from a few consecutive lowercase letters and a single instance of consecutive numbers, which slightly reduce randomness but do not significantly affect overall strength.

In short, "D3lt@Force#92Xy" is a highly secure password that exceeds best practice standards for strength and structure, making it ideal for protecting sensitive accounts or systems.

- R!verFlow_2025x

Test Your Password		Minimum Requirements
Password:	R!verFlow_2025x	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	15	+ 60
Uppercase Letters	Cond/Incr	+((len-n)*2)	2	+ 26
Lowercase Letters	Cond/Incr	+((len-n)*2)	7	+ 16
Numbers	Cond	+(n*4)	4	+ 16
Symbols	Flat	+(n*6)	1	+ 6
Middle Numbers or Symbols	Flat	+(n*2)	5	+ 10
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	2	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	4	- 8
Consecutive Numbers	Flat	-(n*2)	3	- 6
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				

The password “R!verFlow_2025x" scores a full 100% with a Very Strong rating. It includes a rich mix of uppercase and lowercase letters, numbers, and special characters, spread across 15 characters. The symbol and numbers placed in the middle add to its unpredictability.

The password meets all complexity requirements and earns high bonuses for length, variety, and balanced structure. It avoids common weaknesses like dictionary words, sequences, or relying on just letters or numbers.

Minor deductions appear for a few repeated or consecutive characters, but they have little effect overall. With strong entropy and smart placement, this password is ideal for protecting high-value accounts or data.

- M@trix_Sh1ft*33

Test Your Password		Minimum Requirements
Password:	M@trix_Sh1ft*33	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	15	+ 60
Uppercase Letters	Cond/Incr	+((len-n)*2)	2	+ 26
Lowercase Letters	Cond/Incr	+((len-n)*2)	7	+ 16
Numbers	Cond	+(n*4)	3	+ 12
Symbols	Flat	+(n*6)	2	+ 12
Middle Numbers or Symbols	Flat	+(n*2)	4	+ 8
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	4	- 2
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	4	- 8
Consecutive Numbers	Flat	-(n*2)	1	- 2
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				

The password "M@trix_Sh1ft*33" achieves a perfect score of 100% with a Very Strong rating. It effectively combines uppercase and lowercase letters, numbers, and special characters, spread across 15 characters. Symbols and numbers appear mid-string, boosting complexity.

The password meets all five complexity requirements and earns significant bonuses for its length, use of multiple character types, and strategic placement. It avoids predictable patterns like sequences or repeated types.

Minor deductions occur due to repeated characters and some consecutive lowercase letters and numbers, but these have minimal impact overall. With excellent diversity and structure, this password is highly secure and reliable for safeguarding sensitive accounts.

- F@stTrack99_Bz

Test Your Password		Minimum Requirements
Password:	F@stTrack99_Bz	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	14	+ 56
Uppercase Letters	Cond/Incr	+((len-n)*2)	3	+ 22
Lowercase Letters	Cond/Incr	+((len-n)*2)	7	+ 14
Numbers	Cond	+(n*4)	2	+ 8
Symbols	Flat	+(n*6)	1	+ 6
Middle Numbers or Symbols	Flat	+(n*2)	3	+ 6
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	2	- 2
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	4	- 8
Consecutive Numbers	Flat	-(n*2)	1	- 2
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				

The password "F@stTrack99_Bz" scores a full 100% and is rated Very Strong. It integrates uppercase and lowercase letters, numbers, and symbols across a 14-character length, contributing to its high complexity and resilience.

The password meets all five minimum criteria and earns key bonuses for character variety, middle placement of numbers/symbols, and strong distribution. Its structure avoids sequential patterns, boosting its unpredictability.

Minor deductions include repeated characters and some consecutive lowercase letters and numbers, though their effect is negligible. Overall, this password is well-structured, secure, and suitable for protecting critical access points.

- N1ght$T0rm!420

Test Your Password		Minimum Requirements
Password:	N1ght$T0rm!420	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	14	+ 56
Uppercase Letters	Cond/Incr	+((len-n)*2)	2	+ 24
Lowercase Letters	Cond/Incr	+((len-n)*2)	5	+ 18
Numbers	Cond	+(n*4)	5	+ 20
Symbols	Flat	+(n*6)	2	+ 12
Middle Numbers or Symbols	Flat	+(n*2)	6	+ 12
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	2	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	3	- 6
Consecutive Numbers	Flat	-(n*2)	2	- 4
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				

The password "N1ght$T0rm!420" achieves a perfect 100% score and earns a Very Strong rating. With a 14-character length, it effectively uses a balanced mix of uppercase, lowercase, numbers, and symbols, satisfying all complexity and requirement metrics.

It gains substantial bonuses for including numbers and symbols in the middle, strong character variety, and avoiding sequences. The structure is thoughtfully crafted, enhancing resistance to common brute-force and pattern-based attacks.

Minor penalties arise from consecutive lowercase letters, numbers, and minimal repetition, but they're too small to impact the overall score. The password remains highly secure and an excellent choice for sensitive accounts.

4. Extreme

- kX$71pA#rT!9wZqV0uMn

Test Your Password		Minimum Requirements
Password:	kX$71pA#rT!9wZqV0uMn	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	20	+ 80
Uppercase Letters	Cond/Incr	+((len-n)*2)	6	+ 28
Lowercase Letters	Cond/Incr	+((len-n)*2)	7	+ 26
Numbers	Cond	+(n*4)	4	+ 16
Symbols	Flat	+(n*6)	3	+ 18
Middle Numbers or Symbols	Flat	+(n*2)	7	+ 14
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
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)	1	- 2
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				

The password "kX$71pA#rT!9wZqV0uMn" scores 100% with a Very Strong rating. With 20 characters, it surpasses the minimum requirement and demonstrates excellent diversity through its 6 uppercase, 7 lowercase, 4 numbers, and 3 symbols.

Its structure is further strengthened by 7 middle numbers/symbols and fulfillment of all five key security requirements, without any repeated characters or recognizable patterns.

The only deduction (-2) is due to one pair of consecutive numbers, which has minimal effect. Overall, the password is well-crafted, secure, and highly resilient against common attack methods.

- Bl@ckT!gr_P8z3#xY12w

Test Your Password		Minimum Requirements
Password:	Bl@ckT!gr_P8z3#xY12w	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	20	+ 80
Uppercase Letters	Cond/Incr	+((len-n)*2)	4	+ 32
Lowercase Letters	Cond/Incr	+((len-n)*2)	8	+ 24
Numbers	Cond	+(n*4)	4	+ 16
Symbols	Flat	+(n*6)	3	+ 18
Middle Numbers or Symbols	Flat	+(n*2)	7	+ 14
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
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)	2	- 4
Consecutive Numbers	Flat	-(n*2)	1	- 2
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				

The password "Bl@ckT!gr_P8z3#xY12w" scores 100% and is classified as Very Strong. With a total length of 20 characters, it effectively meets and exceeds standard complexity requirements. It features a strong combination of 4 uppercase, 8 lowercase, 4 numbers, and 3 symbols, contributing to high character diversity.

The strength is further reinforced by 7 middle characters (numbers/symbols) and satisfaction of all five essential requirements, with no repeated characters or detectable sequences. These factors significantly boost the overall security profile of the password.

Minor deductions include one case of consecutive lowercase letters (-4) and one consecutive number pair (-2), both of which have minimal effect on the overall score. Despite this, the password remains highly secure and is ideal for protecting sensitive data or high-value accounts.

- V0id@N3bul@!82XmTkqZ

Test Your Password		Minimum Requirements
Password:	V0id@N3bul@!82XmTkqZ	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	20	+ 80
Uppercase Letters	Cond/Incr	+((len-n)*2)	5	+ 30
Lowercase Letters	Cond/Incr	+((len-n)*2)	8	+ 24
Numbers	Cond	+(n*4)	4	+ 16
Symbols	Flat	+(n*6)	3	+ 18
Middle Numbers or Symbols	Flat	+(n*2)	7	+ 14
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	2	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	4	- 8
Consecutive Numbers	Flat	-(n*2)	1	- 2
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				

The password "V0id@N3bul@!82XmTkqZ" earns a 100% score and is rated Very Strong in complexity. It consists of 20 characters, combining 5 uppercase, 6 lowercase, 4 numbers, and 3 symbols, which provides excellent character variety and surpasses all standard strength benchmarks.

Additional security is enhanced through 6 middle characters (symbols/numbers) and the fulfillment of all five key requirements. These factors contribute positively to its overall robustness. The password avoids sequences and includes no exclusively letter-based or numeric structure.

Minor deductions occur due to repeated characters (-1), consecutive uppercase letters (-8), consecutive lowercase letters (-2), and one pair of consecutive numbers (-2). Despite these small penalties, the password remains highly secure and suitable for sensitive and high-privilege access.

- S!l3nt#V0!ce_452Xmpq

Test Your Password		Minimum Requirements
Password:	S!l3nt#V0!ce_452Xmpq	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	20	+ 80
Uppercase Letters	Cond/Incr	+((len-n)*2)	3	+ 34
Lowercase Letters	Cond/Incr	+((len-n)*2)	8	+ 24
Numbers	Cond	+(n*4)	5	+ 20
Symbols	Flat	+(n*6)	3	+ 18
Middle Numbers or Symbols	Flat	+(n*2)	8	+ 16
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	2	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	4	- 8
Consecutive Numbers	Flat	-(n*2)	2	- 4
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				

The password "S!l3nt#V0!ce_452Xmpq" scores 100% and is rated Very Strong for its excellent structure. With 20 characters combining uppercase, lowercase, numbers, and symbols, it far exceeds standard complexity requirements.

It includes 8 middle symbols or numbers, fulfilling all five key strength criteria. These elements boost its resistance to common attacks like brute force or pattern-based guessing.

There are only minor deductions for repeated characters, consecutive lowercase letters, and a pair of consecutive numbers. Despite these, the password remains highly secure and well-suited for protecting sensitive or high-privilege accounts.

- *Y!ggDr@5!l_R1v3rM0ss_*

Test Your Password		Minimum Requirements
Password:	Y!ggDr@5!l_R1v3rM0ss_	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	21	+ 84
Uppercase Letters	Cond/Incr	+((len-n)*2)	4	+ 34
Lowercase Letters	Cond/Incr	+((len-n)*2)	8	+ 26
Numbers	Cond	+(n*4)	4	+ 16
Symbols	Flat	+(n*6)	3	+ 18
Middle Numbers or Symbols	Flat	+(n*2)	7	+ 14
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	10	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	2	- 4
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				

The password "Y!ggDr@5!l_R1v3rM0ss.." receives a 100% score and is rated Very Strong in complexity. It spans 21 characters, integrating a solid mix of 10 uppercase, 8 lowercase, 4 numbers, and 3 symbols, demonstrating excellent character diversity.

It also benefits from 7 middle characters (symbols or numbers) and fulfills all five key strength requirements, boosting its resilience to brute-force or automated guessing methods. These features significantly enhance its unpredictability and strength.

A small deduction is applied for repeated characters (-1) and consecutive lowercase letters (-4), but these have minimal impact. Overall, the password is robust, secure, and highly suitable for protecting sensitive or high-privilege accounts.

5. Unhackable
    - cA!9Tz@L4#vRpE3xMn$7bFzYw

Test Your Password		Minimum Requirements
Password:	cA!9Tz@L4#vRpE3xMn$7bFzYw	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	25	+ 100
Uppercase Letters	Cond/Incr	+((len-n)*2)	8	+ 34
Lowercase Letters	Cond/Incr	+((len-n)*2)	9	+ 32
Numbers	Cond	+(n*4)	4	+ 16
Symbols	Flat	+(n*6)	4	+ 24
Middle Numbers or Symbols	Flat	+(n*2)	8	+ 16
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	2	- 1
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				

The password "cAI9T@zL4#vRpE3xMn57bFzY" earns a 100% score with a Very Strong rating. It spans 25 characters, making it exceptionally long and secure, and features a powerful mix of 8 uppercase, 9 lowercase, 4 numbers, and 4 symbols, maximizing character variety.

It includes 8 middle characters (symbols or numbers) and fulfills all five key complexity requirements, making it highly resistant to common attack methods such as brute-force and pattern recognition.

A very minor deduction is applied for repeated characters (-1), which has negligible impact on the overall strength. This password is extremely robust and well-suited for securing critical systems and sensitive information.

- X1@o$K8!9rLzp!WyR2u&VmJcTq

Test Your Password		Minimum Requirements
Password:	X1@o$K8!9rLzp!WyR2u&VmJcT	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	26	+ 104
Uppercase Letters	Cond/Incr	+((len-n)*2)	8	+ 36
Lowercase Letters	Cond/Incr	+((len-n)*2)	9	+ 34
Numbers	Cond	+(n*4)	4	+ 16
Symbols	Flat	+(n*6)	5	+ 30
Middle Numbers or Symbols	Flat	+(n*2)	9	+ 18
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	2	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	1	- 2
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				

The password "X1@oSK8l9rLzp!WpR2u&VmJc]" scores a perfect 100% and is rated Very Strong in complexity. With a total length of 26 characters, it combines 8 uppercase, 9 lowercase, 4 numbers, and 5 symbols, offering outstanding character variety and security.

It includes 9 middle characters (symbols or numbers) and fully meets all five strength requirements, significantly enhancing its defense against brute-force and predictive attacks. This high complexity and lack of patterns make it highly resilient.

Only minimal deductions apply for repeated characters (-1) and consecutive lowercase letters (-2), which have negligible impact. Overall, this password is extremely strong and well-suited for safeguarding high-privilege or sensitive access.

- #Gqv7M@xZ^tF9e!B8WxRp!nY3K

Test Your Password		Minimum Requirements
Password:	#Gqv7M@xZ^tF9e!B8WxRp!nY3	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	26	+ 104
Uppercase Letters	Cond/Incr	+((len-n)*2)	9	+ 34
Lowercase Letters	Cond/Incr	+((len-n)*2)	8	+ 36
Numbers	Cond	+(n*4)	4	+ 16
Symbols	Flat	+(n*6)	5	+ 30
Middle Numbers or Symbols	Flat	+(n*2)	8	+ 16
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	4	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	1	- 2
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				

The password "#Gqv7M@xZt*F9e!B8WxRp!nY3" achieves a 100% score and is rated Very Strong in complexity. Spanning 26 characters, it effectively combines 9 uppercase, 8 lowercase, 4 numbers, and 5 symbols, delivering high entropy and strong protection.

It includes 9 middle characters (symbols or numbers) and meets all five key strength criteria, making it highly resistant to brute-force, dictionary, or pattern-based attacks. The distribution and variety of character types enhance its unpredictability.

Only slight deductions are recorded for repeated characters (-1) and consecutive lowercase letters (-2), which have minimal impact. Overall, this password is exceptionally secure and well-suited for sensitive, high-privilege usage.

- pL!z9Tr#m7AqX@Y^zB5EvwQs0j

Test Your Password		Minimum Requirements
Password:	pL!z9Tr#m7AqX@Y^zB5EvwQs(	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	26	+ 104
Uppercase Letters	Cond/Incr	+((len-n)*2)	8	+ 36
Lowercase Letters	Cond/Incr	+((len-n)*2)	10	+ 32
Numbers	Cond	+(n*4)	4	+ 16
Symbols	Flat	+(n*6)	4	+ 24
Middle Numbers or Symbols	Flat	+(n*2)	8	+ 16
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	2	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	1	- 2
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				

The password "pLLz9T#fm7AqX@Yz2B5EwvQs[" earns a 100% score and is rated Very Strong in complexity. At 26 characters long, it utilizes a balanced mix of 8 uppercase, 10 lowercase, 4 numbers, and 4 symbols, ensuring excellent character variety.

It includes 6 middle characters and fulfills all five essential security requirements, making it highly resistant to cracking attempts, including brute-force and pattern-based attacks. The inclusion of multiple character types strengthens its unpredictability and overall robustness.

Only minor deductions appear due to repeated characters (-1) and consecutive lowercase letters (-2), with no patterns or predictable sequences detected. This password is highly secure and ideal for protecting sensitive accounts.

3. Identify best practices for creating strong passwords and write down tips learnt from the evaluation

➢ Password Construction Best Practices

- **Length matters**: All strong passwords exceed the minimum 8-character requirement, often ranging from 14 to 26 characters.
- **Character diversity** is critical: Strong passwords always include a mix of:
    - ❖ Uppercase letters
    - ❖ Lowercase letters
    - ❖ Numbers
    - ❖ Symbols
- **Middle placement** of numbers and symbols significantly boosts strength.

➢ Common Deductions Observed

- **Repeated characters** (e.g., "e", "3") frequently cause minor penalties.
- **Consecutive lowercase or uppercase letters** (e.g., "ll", "SS") result in deductions.
- **Sequential numbers or letters** (e.g., "123", "abc") reduce entropy and are flagged.
- Some passwords lose points due to **predictable patterns** or **keyboard sequences** (e.g., "Qwerty").

➢ Security and Evaluation Insights

- Passwords scoring **100% and rated "Very Strong"** share these features:
    - ❖ Fulfill **all five minimum requirements** (uppercase, lowercase, numbers, symbols, length).
    - ❖ Avoid dictionary words and recognizable sequences.
    - ❖ Show **good randomness** and no reliance on real words or easy-to-guess elements.
    - ❖ Are often **suitable for sensitive or high-privilege access**.

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

1. Brute Force Attack

- Tries all possible combinations of characters until the correct password is found.
- **Time-consuming**, but effective on short or simple passwords.

2. Dictionary Attack

- Uses a precompiled list of common passwords or dictionary words.
- Exploits the use of weak, predictable, or commonly used passwords like password123.

3. Credential Stuffing

- Uses **stolen username-password pairs** from previous breaches to gain access to other services.
- Exploits the bad habit of **password reuse** across multiple accounts.

4. Password Spraying

- Tries a few **common passwords** (e.g., Welcome@123) across **many accounts** to avoid detection.
- Opposite of brute force (many passwords on one account); this is **few passwords on many accounts**.

5. Phishing

- Tricks users into **revealing passwords** by posing as a legitimate site or service.
- Often done via fake emails or websites.

6. Keylogging

- Malware secretly records keystrokes to capture usernames and passwords.
- Requires device-level compromise.

7. Man-in-the-Middle (MITM) Attack

- Intercepts communication between user and server to steal login credentials.
- Can occur on **unsecured public networks**.

8. Guessing

- Attacker manually or automatically guesses based on known information (birthdays, names, etc.).
- Exploits personal details and weak password habits.

9. Rainbow Table Attack

- Uses precomputed tables to **reverse password hashes**.
- Defended against by using **salts** during password hashing.