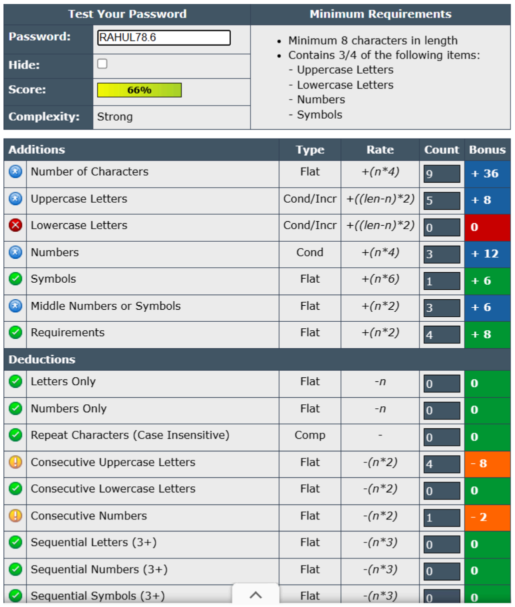
Weak and Strong Passwords & Common Password Attacks

Weak Passwords

Weak passwords are usually short, simple, and predictable. They often include easy-to-guess patterns like ‘123456’, ‘password’, or someone’s name. Because of this, they are highly vulnerable to brute force and dictionary attacks.

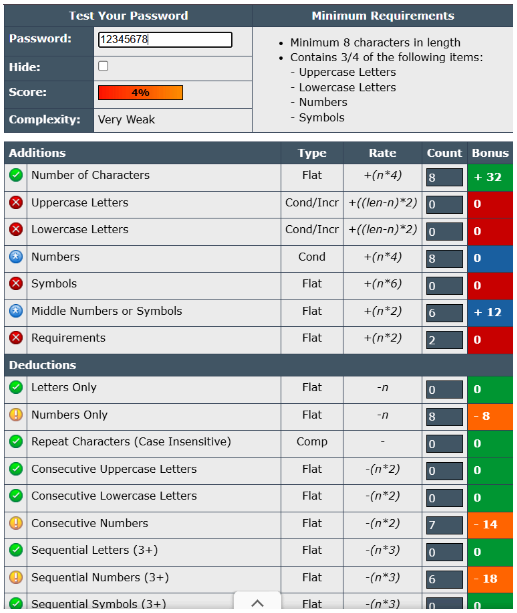


Test Your Password	
Password:	RAHUL78.6
Hide:	□
Score:	66%
Complexity:	Strong

Minimum Requirements

- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

	Additions	Type	Rate	Count	Bonus
★	Number of Characters	Flat	+(n*4)	9	+ 36
★	Uppercase Letters	Cond/Incr	+((len-n)*2)	5	+ 8
✗	Lowercase Letters	Cond/Incr	+((len-n)*2)	0	0
★	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)	4	+ 8
	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)	4	- 8
✓	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

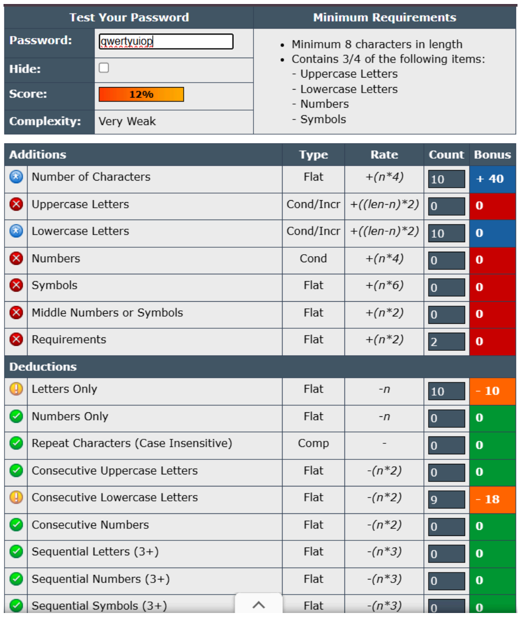


Test Your Password	
Password:	12345678
Hide:	□
Score:	4%
Complexity:	Very Weak

Minimum Requirements

- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

	Additions	Type	Rate	Count	Bonus
✓	Number of Characters	Flat	+(n*4)	8	+ 32
✗	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
✗	Lowercase Letters	Cond/Incr	+((len-n)*2)	0	0
★	Numbers	Cond	+(n*4)	8	0
✗	Symbols	Flat	+(n*6)	0	0
★	Middle Numbers or Symbols	Flat	+(n*2)	6	+ 12
✗	Requirements	Flat	+(n*2)	2	0
	Deductions				
✓	Letters Only	Flat	-n	0	0
!	Numbers Only	Flat	-n	8	- 8
✓	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)	7	- 14
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
!	Sequential Numbers (3+)	Flat	-(n*3)	6	- 18
✓	Sequential Symbols (3+)	Flat	-(n*3)	0	0

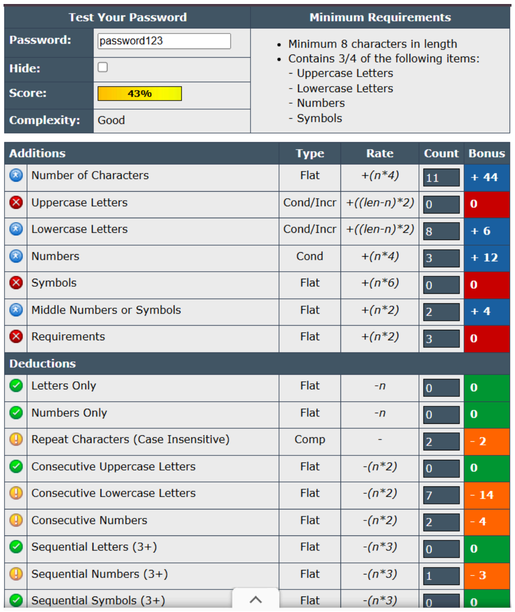


Test Your Password	
Password:	qwertyuiop
Hide:	□
Score:	12%
Complexity:	Very Weak

Minimum Requirements

- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

	Additions	Type	Rate	Count	Bonus
★	Number of Characters	Flat	+(n*4)	10	+ 40
✗	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	10	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)	2	0
	Deductions				
!	Letters Only	Flat	-n	10	- 10
✓	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)	9	- 18
✓	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



Test Your Password	
Password:	password123
Hide:	□
Score:	43%
Complexity:	Good

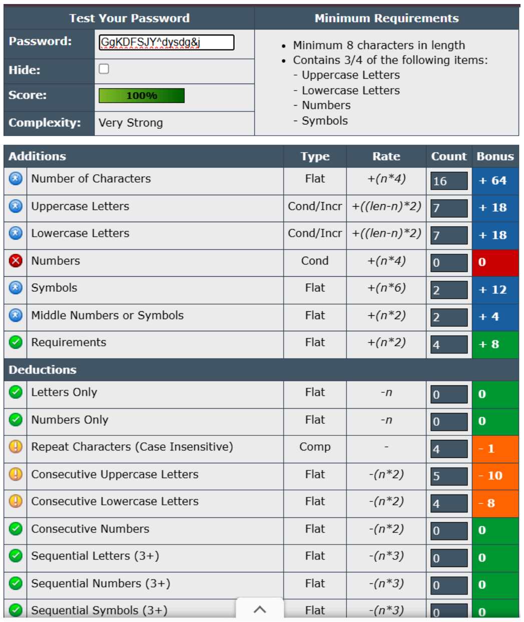
Minimum Requirements

- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

	Additions	Type	Rate	Count	Bonus
★	Number of Characters	Flat	+(n*4)	11	+ 44
✗	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	8	+ 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)	3	0
	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)	7	- 14
!	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

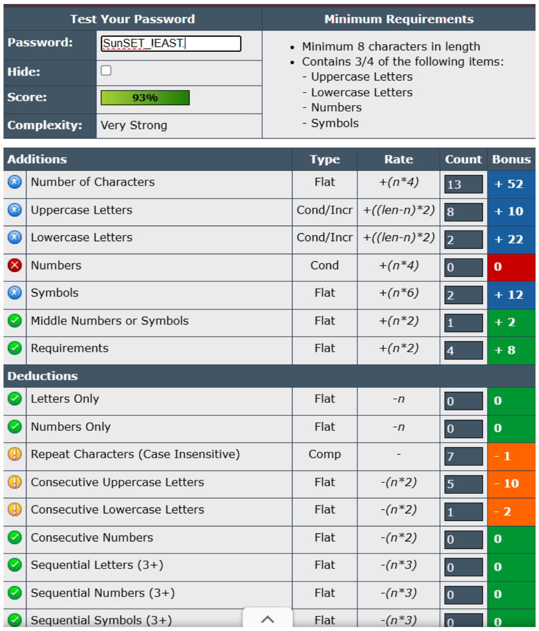
Strong Passwords

Strong passwords are long, unique, and complex. They are typically at least 12 characters long and use a mix of uppercase and lowercase letters, numbers, and special characters. Strong passwords are harder for hackers to crack and provide stronger security, especially when combined with two-factor authentication.



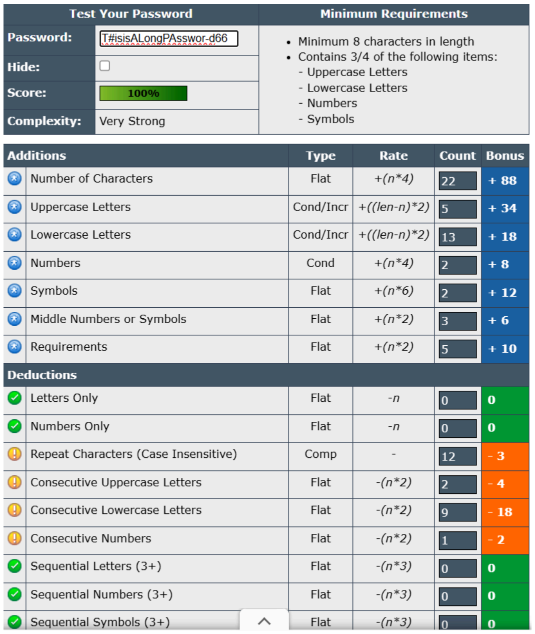
Test Your Password		Minimum Requirements
Password:	GgKDFSJY^dysdg&j	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	□	
Score:	100%	
Complexity:	Very Strong	

	Additions	Type	Rate	Count	Bonus
★	Number of Characters	Flat	+(n*4)	16	+ 64
★	Uppercase Letters	Cond/Incr	+((len-n)*2)	7	+ 18
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	7	+ 18
✗	Numbers	Cond	+(n*4)	0	0
★	Symbols	Flat	+(n*6)	2	+ 12
★	Middle Numbers or Symbols	Flat	+(n*2)	2	+ 4
✓	Requirements	Flat	+(n*2)	4	+ 8
	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)	5	- 10
!	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



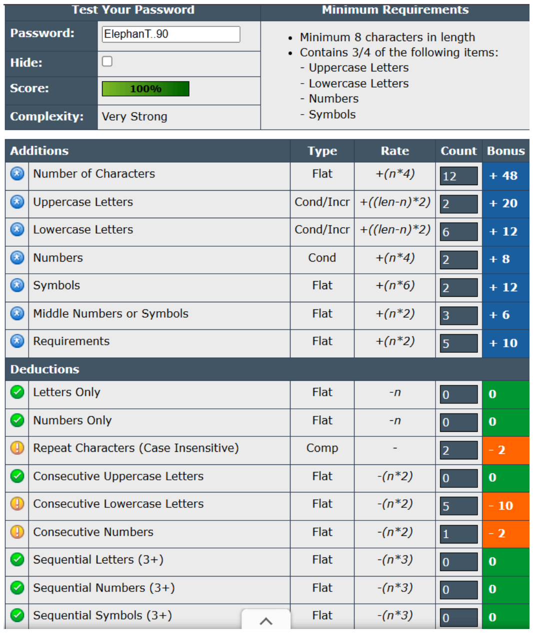
Test Your Password		Minimum Requirements
Password:	SunSET_!EAST	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	□	
Score:	93%	
Complexity:	Very Strong	

	Additions	Type	Rate	Count	Bonus
★	Number of Characters	Flat	+(n*4)	13	+ 52
★	Uppercase Letters	Cond/Incr	+((len-n)*2)	8	+ 10
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	2	+ 22
✗	Numbers	Cond	+(n*4)	0	0
★	Symbols	Flat	+(n*6)	2	+ 12
✓	Middle Numbers or Symbols	Flat	+(n*2)	1	+ 2
✓	Requirements	Flat	+(n*2)	4	+ 8
	Deductions				
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
!	Repeat Characters (Case Insensitive)	Comp	-	7	- 1
!	Consecutive Uppercase Letters	Flat	-(n*2)	5	- 10
!	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



Test Your Password		Minimum Requirements
Password:	T#isisALongPAsswor-d66	• 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)	22	+ 88
★	Uppercase Letters	Cond/Incr	+((len-n)*2)	5	+ 34
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	13	+ 18
★	Numbers	Cond	+(n*4)	2	+ 8
★	Symbols	Flat	+(n*6)	2	+ 12
★	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	-	12	- 3
!	Consecutive Uppercase Letters	Flat	-(n*2)	2	- 4
!	Consecutive Lowercase Letters	Flat	-(n*2)	9	- 18
!	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



Test Your Password		Minimum Requirements
Password:	ElephanT..90	• 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)	12	+ 48
★	Uppercase Letters	Cond/Incr	+((len-n)*2)	2	+ 20
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	6	+ 12
★	Numbers	Cond	+(n*4)	2	+ 8
★	Symbols	Flat	+(n*6)	2	+ 12
★	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)	5	- 10
!	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

Weak vs Strong Passwords (Points)

🔴 Weak Passwords:

- Usually short and simple (e.g., ‘123456’, ‘password’).

- Often based on predictable patterns like names, birthdays, or keyboard sequences.

- Easy for hackers to crack using brute force or dictionary attacks.

🟢 Strong Passwords:

- At least 12 characters long for better security.

- Includes a mix of uppercase, lowercase, numbers, and special symbols.

- Unpredictable and not reused across different accounts.

- Much harder to crack, even with automated attack tools.

Common Password Attacks

1. Brute Force Attack

- Attacker tries all possible combinations of characters until the correct password is found.

- Very effective against short or simple passwords.

- Can be slowed down with rate limiting, account lockouts, and longer passwords.

2. Dictionary Attack

- Uses a list of common words, names, or leaked passwords instead of random guesses.

- Much faster than brute force because it skips unlikely combinations.

- Prevented by using random, complex, non-dictionary-based passwords.

3. Credential Stuffing

- Attackers use previously leaked username-password pairs from breaches.

- Exploits the fact that many people reuse the same password across accounts.

- Prevented with unique passwords per site and two-factor authentication (2FA).

4. Phishing

- Trick users into revealing their password via fake websites, emails, or messages.

- Relies on social engineering rather than technical cracking.

- Countered with user awareness, checking URLs, and multi-factor authentication.

5. Keylogging

- Malware records keystrokes typed on a device, capturing passwords directly.

- Often installed via malicious downloads, email attachments, or USB drives.

- Prevented with antivirus software, OS updates, and avoiding suspicious links/files.