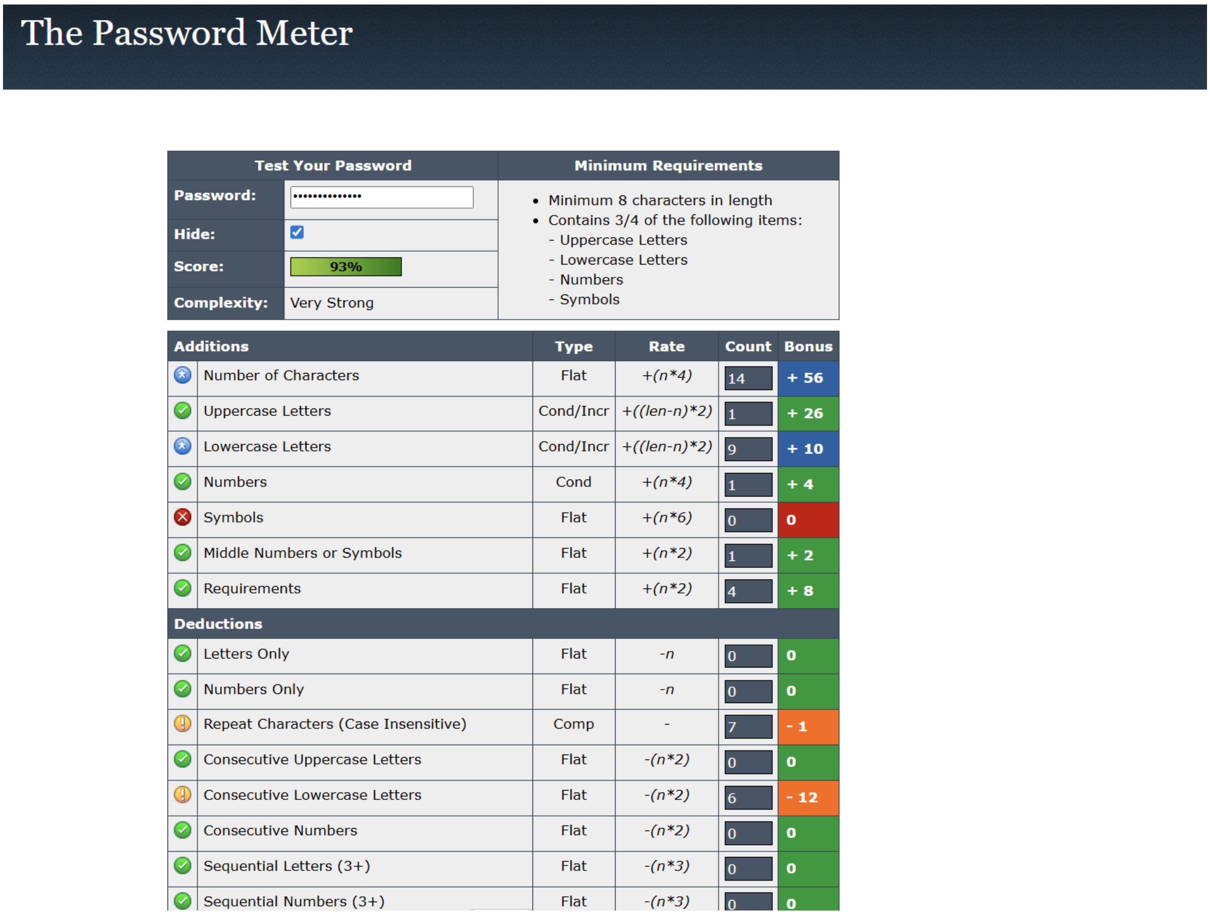
Task 6 : Create a Strong Password and Evaluate Its Strength.

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

Utilizing complex passwords ,Implementing multi-factor authentication , **Enact account lock ,Use of upper case, lower case, numbers , symbols, Para-phrase , and its length makes the password strong and difficult to crack.**

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

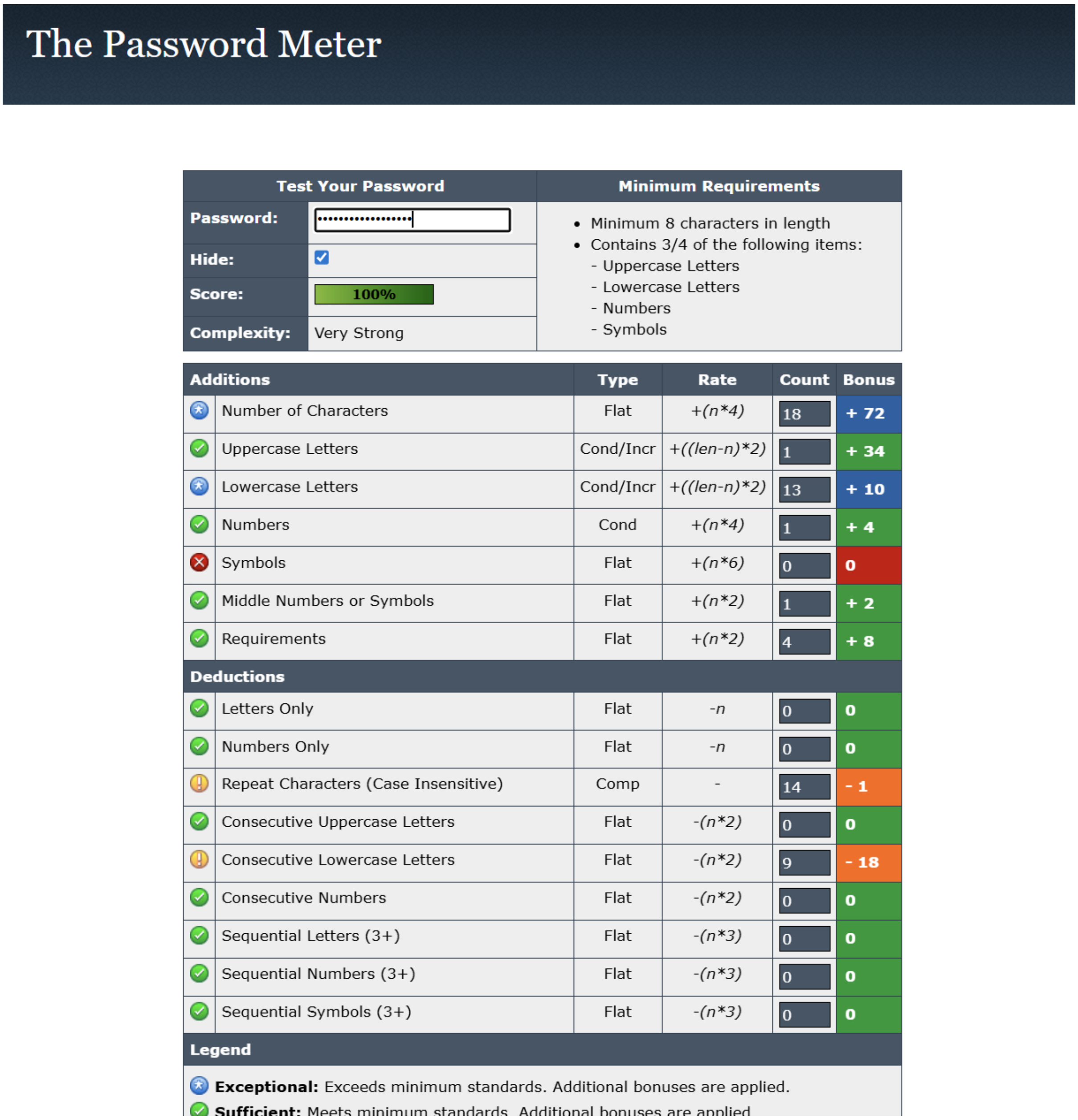
Deliverables: password with minimum 8 -character length, upper case, lowercase, numbers, symbols, use of para-phrase makes it strong as observed in this task.



The Password Meter

Test Your Password		Minimum Requirements
Password:	••••••••••••••	- 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)	14	+ 56
✓	Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 26
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	9	+ 10
✓	Numbers	Cond	+(n*4)	1	+ 4
✗	Symbols	Flat	+(n*6)	0	0
✓	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)	0	0
!	Consecutive Lowercase Letters	Flat	-(n*2)	6	- 12
✓	Consecutive Numbers	Flat	-(n*2)	0	0
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
✓	Sequential Numbers (3+)	Flat	-(n*3)	0	0



The Password Meter

Test Your Password	
Password:	••••••••••••••••••
Hide:	☑
Score:	100%
Complexity:	Very Strong

Minimum Requirements

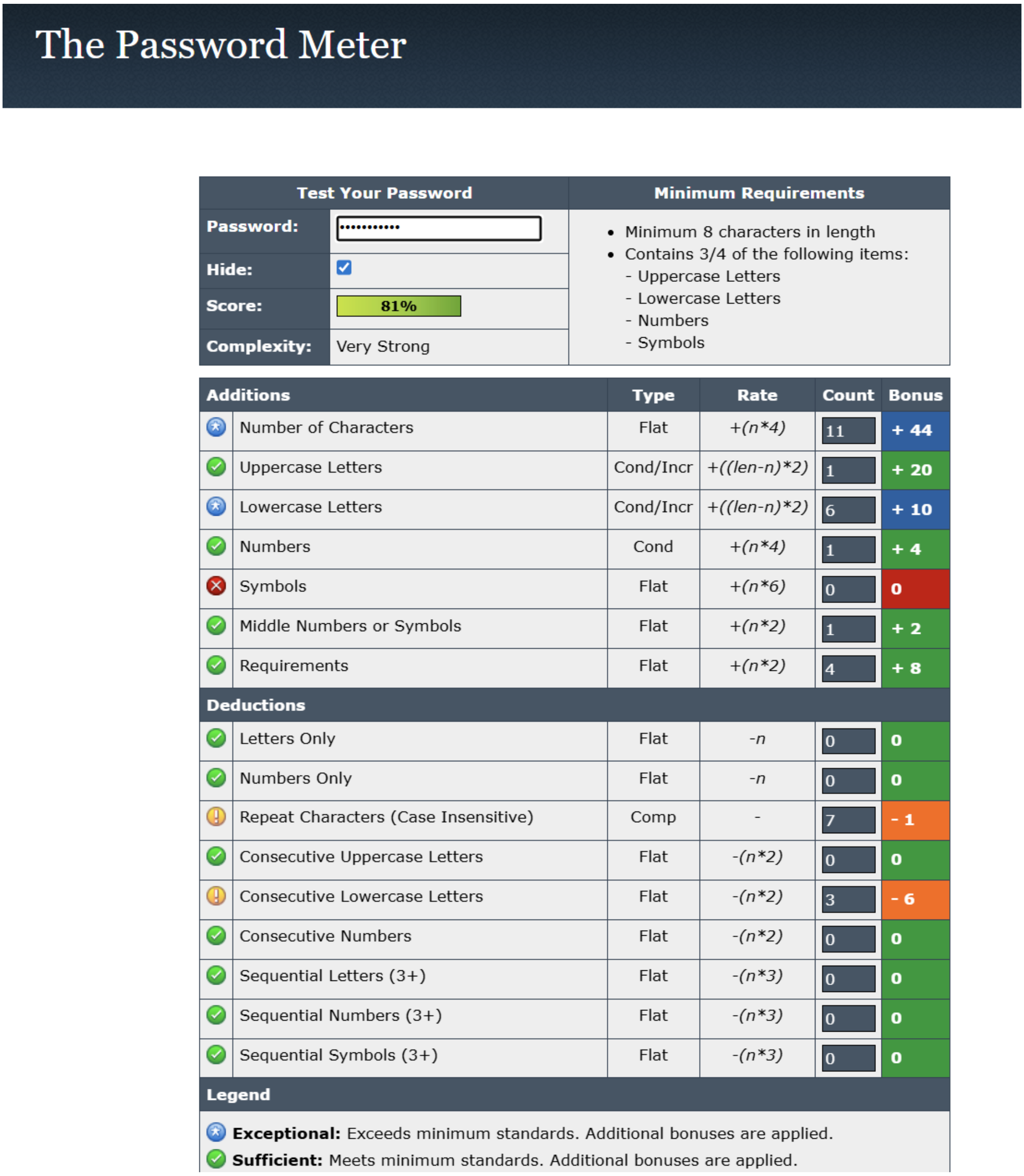
- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

	Additions	Type	Rate	Count	Bonus
★	Number of Characters	Flat	+(n*4)	18	+ 72
✓	Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 34
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	13	+ 10
✓	Numbers	Cond	+(n*4)	1	+ 4
✗	Symbols	Flat	+(n*6)	0	0
✓	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	-	14	- 1
✓	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

Legend

★ **Exceptional:** Exceeds minimum standards. Additional bonuses are applied.

✓ **Sufficient:** Meets minimum standards. Additional bonuses are applied.



The Password Meter

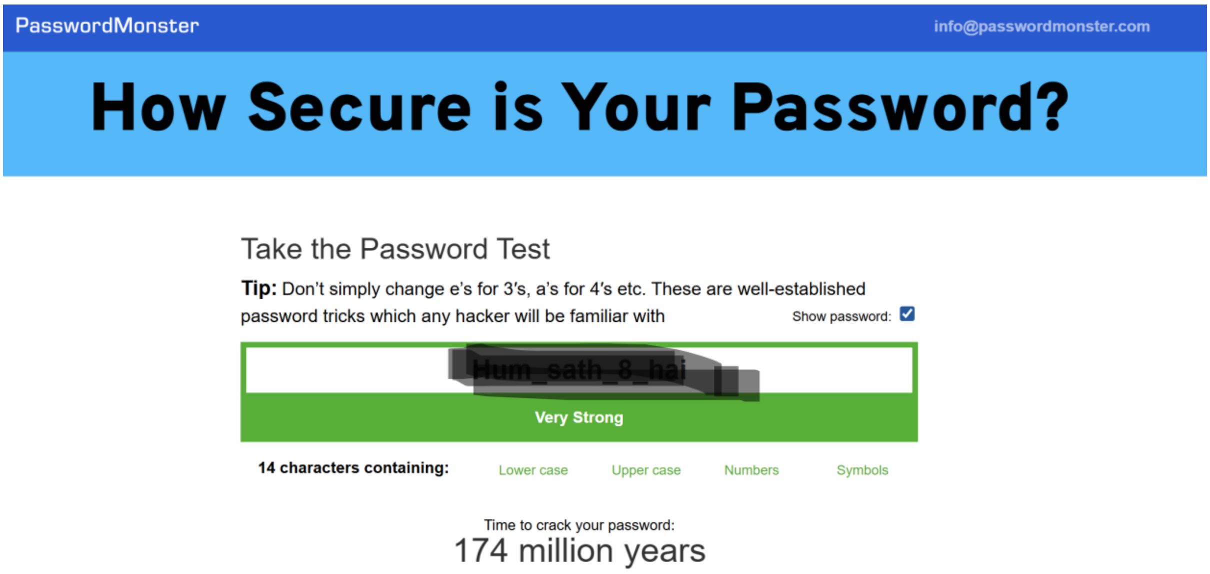
Test Your Password		Minimum Requirements
Password:	•••••••••••	- Minimum 8 characters in length - Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☑	
Score:	81%	
Complexity:	Very Strong	

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)	6	+ 10
✓	Numbers	Cond	+(n*4)	1	+ 4
✗	Symbols	Flat	+(n*6)	0	0
✓	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)	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

★ **Exceptional:** Exceeds minimum standards. Additional bonuses are applied.

✓ **Sufficient:** Meets minimum standards. Additional bonuses are applied.



PasswordMonster info@passwordmonster.com

How Secure is Your Password?

Take the Password Test

Tip: Don’t simply change e’s for 3’s, a’s for 4’s etc. These are well-established password tricks which any hacker will be familiar with

Show password: ☑

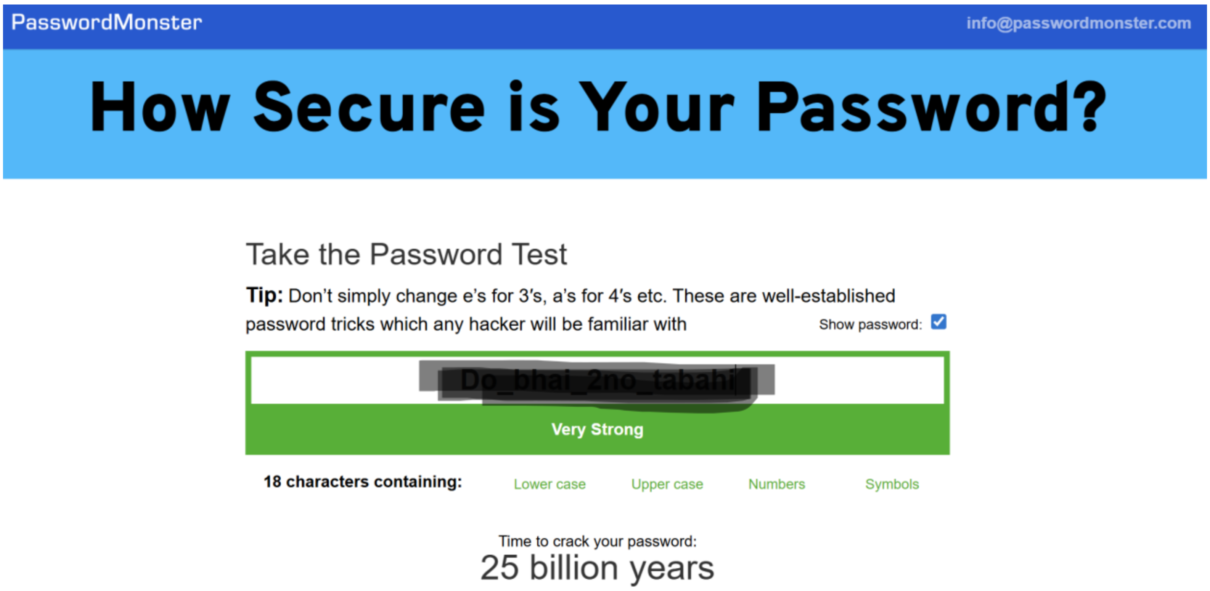
[redacted]

Very Strong

14 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:

174 million years



PasswordMonster info@passwordmonster.com

How Secure is Your Password?

Take the Password Test

Tip: Don’t simply change e’s for 3’s, a’s for 4’s etc. These are well-established password tricks which any hacker will be familiar with

Show password: ☑

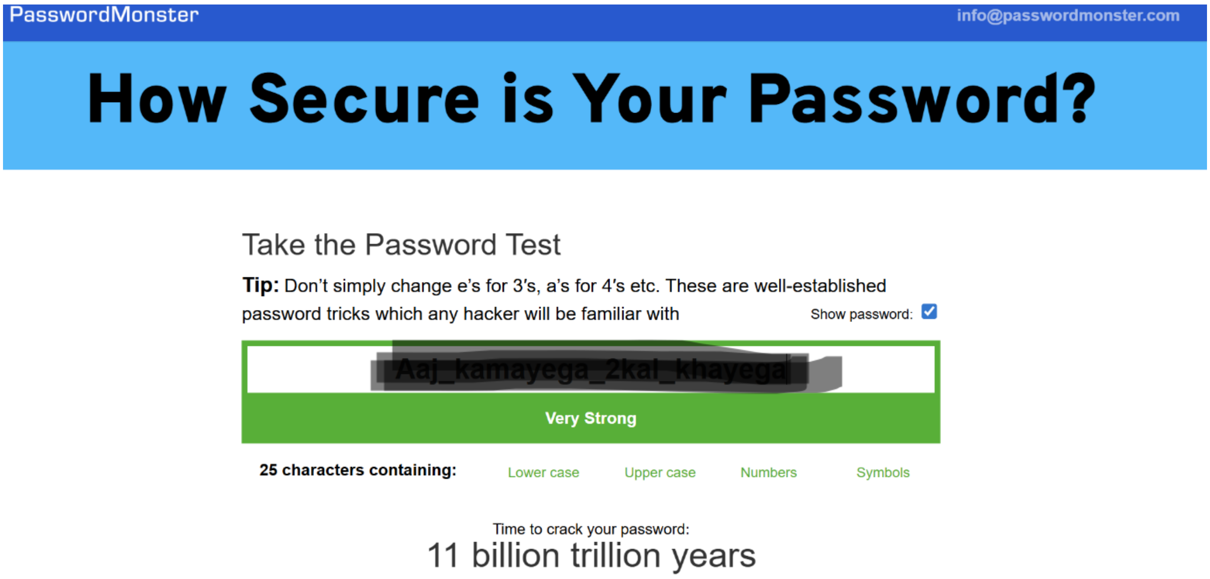
[redacted]

Very Strong

18 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:

25 billion years



PasswordMonster info@passwordmonster.com

How Secure is Your Password?

Take the Password Test

Tip: Don't simply change e's for 3's, a's for 4's etc. These are well-established password tricks which any hacker will be familiar with

Show password: ☑

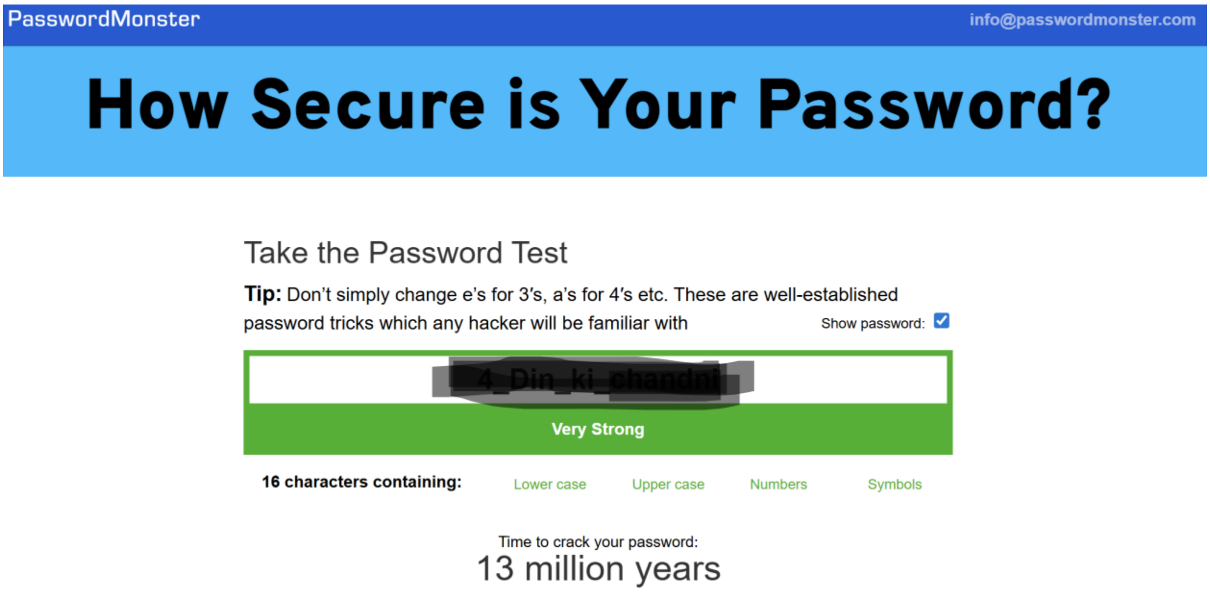
[redacted]

Very Strong

25 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:

11 billion trillion years



PasswordMonster info@passwordmonster.com

How Secure is Your Password?

Take the Password Test

Tip: Don't simply change e's for 3's, a's for 4's etc. These are well-established password tricks which any hacker will be familiar with

Show password: ☑

[redacted]

Very Strong

16 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:

13 million years

Research common password attacks (brute force, dictionary).

the 8 Most Prominent Password Attacks

Brute-Force

The simplest and slowest form of password attack is the brute-force method. Automated systems manually attempt several million, billion, or trillion combinations of letters and numbers in the hope of accidentally stumbling on an account password.

Dictionary

Dictionary attacks try words from a predetermined list in attempt to brute-force an account’s password. These dictionaries, while including fewer overall words, will often focus on “common” passwords compiled by hackers over the years. The lists can also include terms from actual dictionaries, common names, or combinations of dates and locations.

Keyloggers

Keyloggers are types of software that monitor keystrokes on the host system and copy that information into a text file. These types of software can come from some other kind of hack, like an infected email attachment or something installed locally on the machine. A keylogger will expose any passwords typed by the user.

Credential Stuffing

It’s common for a hacker, upon hacking one account, to attempt using those credentials on several other accounts. Similarly, hackers who steal passwords (through, for example, a database breach) will wait and, over time, attempt to use those credentials again, both in other systems and within the same system again.

This approach assumes that at least some users will fail to update passwords after a breach and that more users will not change an identical username and password on a different system.

Password Spraying

Password spraying tries to attack multiple accounts at once in search of weak passwords.

A spraying attack will take a handful of common passwords (like a dictionary attack) but rely on regular patterns, like well-known defaults, birthdates, or simple phrases like combinations of numbers and the word “password,” and attempt to brute-force multiple accounts at the same time.

This “spray approach” will not have the same success rate as a dedicated dictionary attack. Instead, it counts on a numbers game: across hundreds of accounts, at least one of them is using weak password security.

Phishing

Phishing has been one of the most prominent forms of cyberattack. It counts on users’ ignorance of modern security threats and their trust in official-seeming emails by spoofing these emails to request user passwords.

No one is invulnerable to these attacks, and phishing has been the source of some of the most significant cybersecurity events in modern history—massive spear phishing attempts have cost enterprises billions of dollars in stolen funds.

Summarize how password complexity affects security.

In today’s digital world, our online accounts are more exposed than ever before. As cyber threats evolve, so must the ways we protect ourselves. One critical area that has seen a shift is password security. For years, people were told to change their passwords often. But this method has not kept up with modern threats.

Instead of relying on constant password changes, the emphasis has shifted to complexity. A strong password today needs to be more than just different. It needs to be complex, random, and difficult to guess. Frequent changes can be tiring and confusing. Complexity offers better, lasting protection.

That is why understanding password complexity is essential. It guards against common attacks and lowers the risk of breaches. Also, it offers a better solution than strategies that are no longer effective. In this article, we will explore what makes a password truly strong. We will discuss why complexity is better than rotation. Then, we’ll look at how you can start securing your digital life today.

THANK YOU