Password Strength Evaluation Report

Objective:

To understand the elements that make a password strong and evaluate different passwords using online strength checkers.

Step-by-Step Process

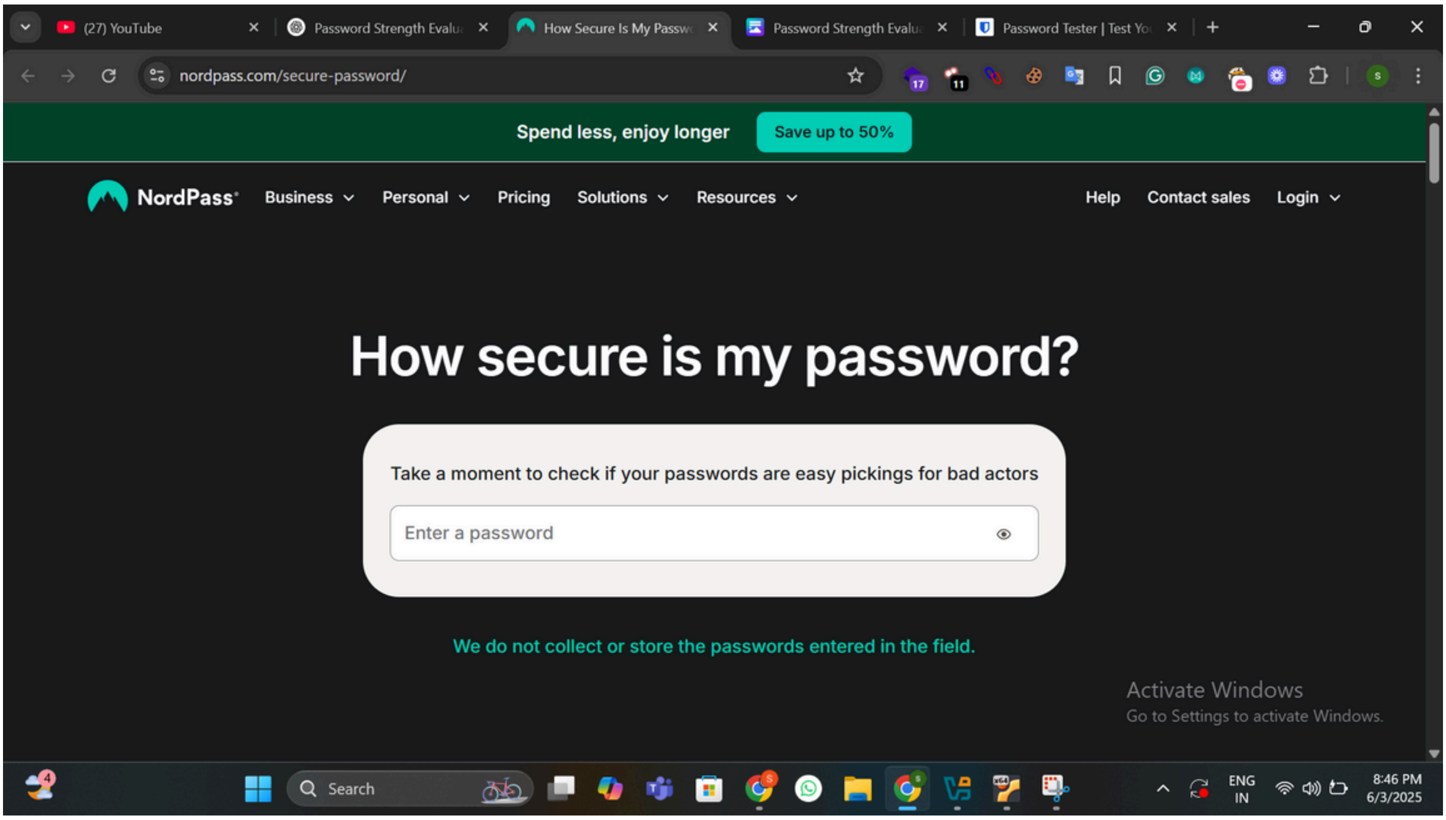
Step 1: Create Multiple Passwords with Varying Complexity

Password Example	Type/Category
12345678	Very Weak – Numbers only
password	Very Weak – Dictionary word
apple123	Weak – Lowercase + numbers
Apple2025	Moderate – Uppercase + numbers
Apple@2025	Good – Mixed case + symbol
ApP!e#2025$	Strong – Random, symbols, mixed case
correcthorsebatterystaple	Strong – Long passphrase
Th1s1sMy$3cureP@ss	Very Strong – Complex, readable

Step 2: Testing Tools Used

Used the following password strength checkers:

1. Bitwarden Password Strength Tester
2. Kaspersky Password Checker
3. NordPass Password Checker



Spend less, enjoy longer

Save up to 50%

How secure is my password?

Take a moment to check if your passwords are easy pickings for bad actors

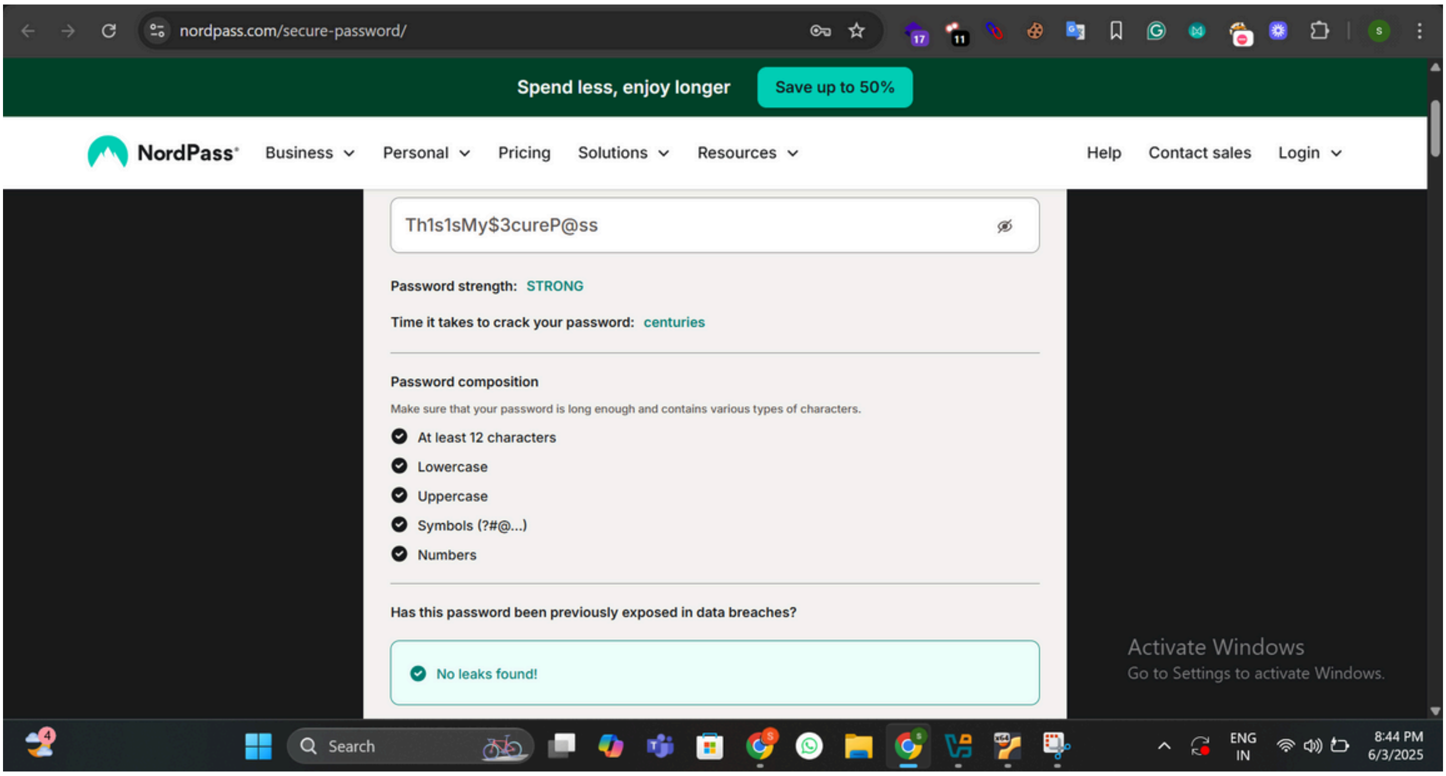
Enter a password

We do not collect or store the passwords entered in the field.

Activate Windows
Go to Settings to activate Windows.

Step 3: Evaluation Results

Password	Bitwarden Score	Kaspersky Rating	Time to Crack Estimate
12345678	Very Weak	Extremely Weak	Less than 1 second
password	Very Weak	Extremely Weak	Less than 1 second
apple123	Weak	Weak	Seconds
Apple2025	Medium	Medium	A few minutes
Apple@2025	Good	Strong	Several hours
ApP!e#2025$	Strong	Very Strong	Months
correcthorsebatterystaple	Very Strong	Strong	Centuries (due to length)
Th1s1sMy$3cureP@ss	Very Strong	Very Strong	63+ years



Th1s1sMy$3cureP@ss

Password strength: STRONG

Time it takes to crack your password: centuries

Password composition

Make sure that your password is long enough and contains various types of characters.

- ✓ At least 12 characters
- ✓ Lowercase
- ✓ Uppercase
- ✓ Symbols (?#@...)
- ✓ Numbers

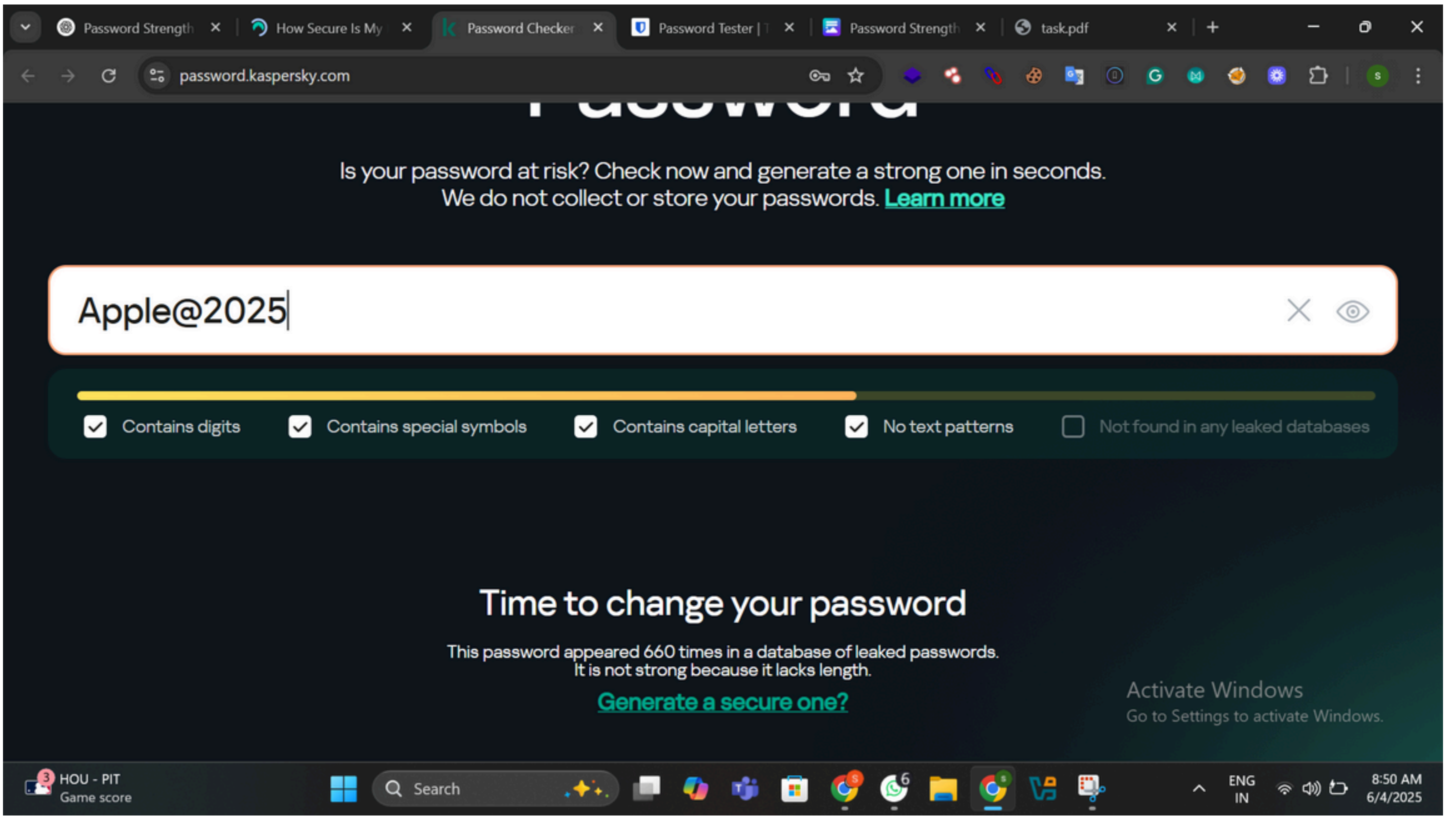
Has this password been previously exposed in data breaches?

✓ No leaks found!

Step 4: Identify Best Practices for Creating Strong Passwords

- Use a **minimum of 12 characters**.
- Include a mix of **uppercase**, **lowercase**, **numbers**, and **symbols**.
- Avoid **dictionary words** or common patterns.
- Don’t reuse passwords across multiple accounts.
- Use a **passphrase** or sentence that’s easy for you but hard for others.
- Use a **password manager** to store complex passwords.

Moderate Password:



Is your password at risk? Check now and generate a strong one in seconds.
We do not collect or store your passwords. Learn more

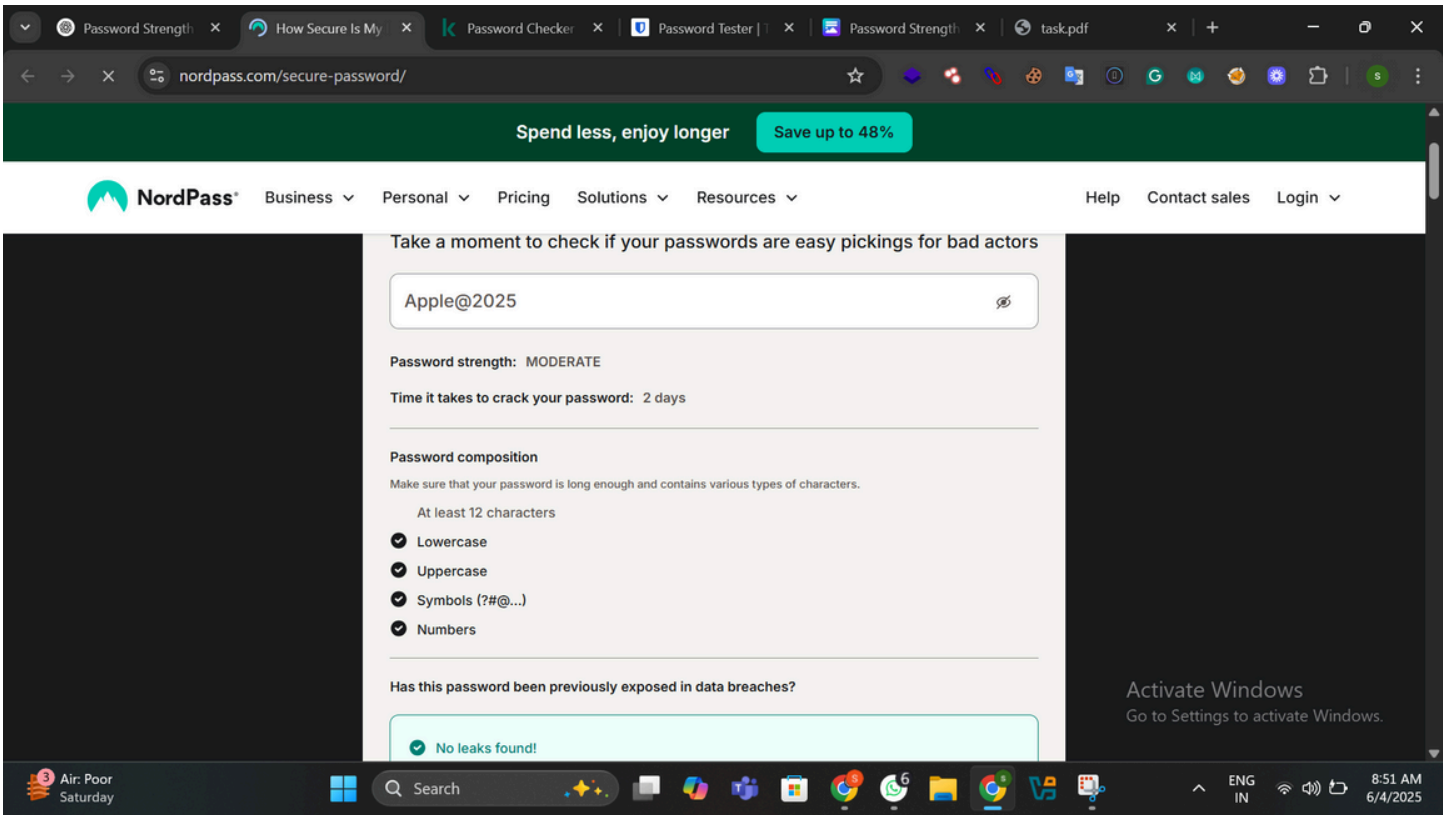
Apple@2025

☑ Contains digits ☑ Contains special symbols ☑ Contains capital letters ☑ No text patterns □ Not found in any leaked databases

Time to change your password

This password appeared 660 times in a database of leaked passwords.
It is not strong because it lacks length.

Generate a secure one?



Take a moment to check if your passwords are easy pickings for bad actors

Apple@2025

Password strength: MODERATE

Time it takes to crack your password: 2 days

Password composition

Make sure that your password is long enough and contains various types of characters.

At least 12 characters

✓ Lowercase

✓ Uppercase

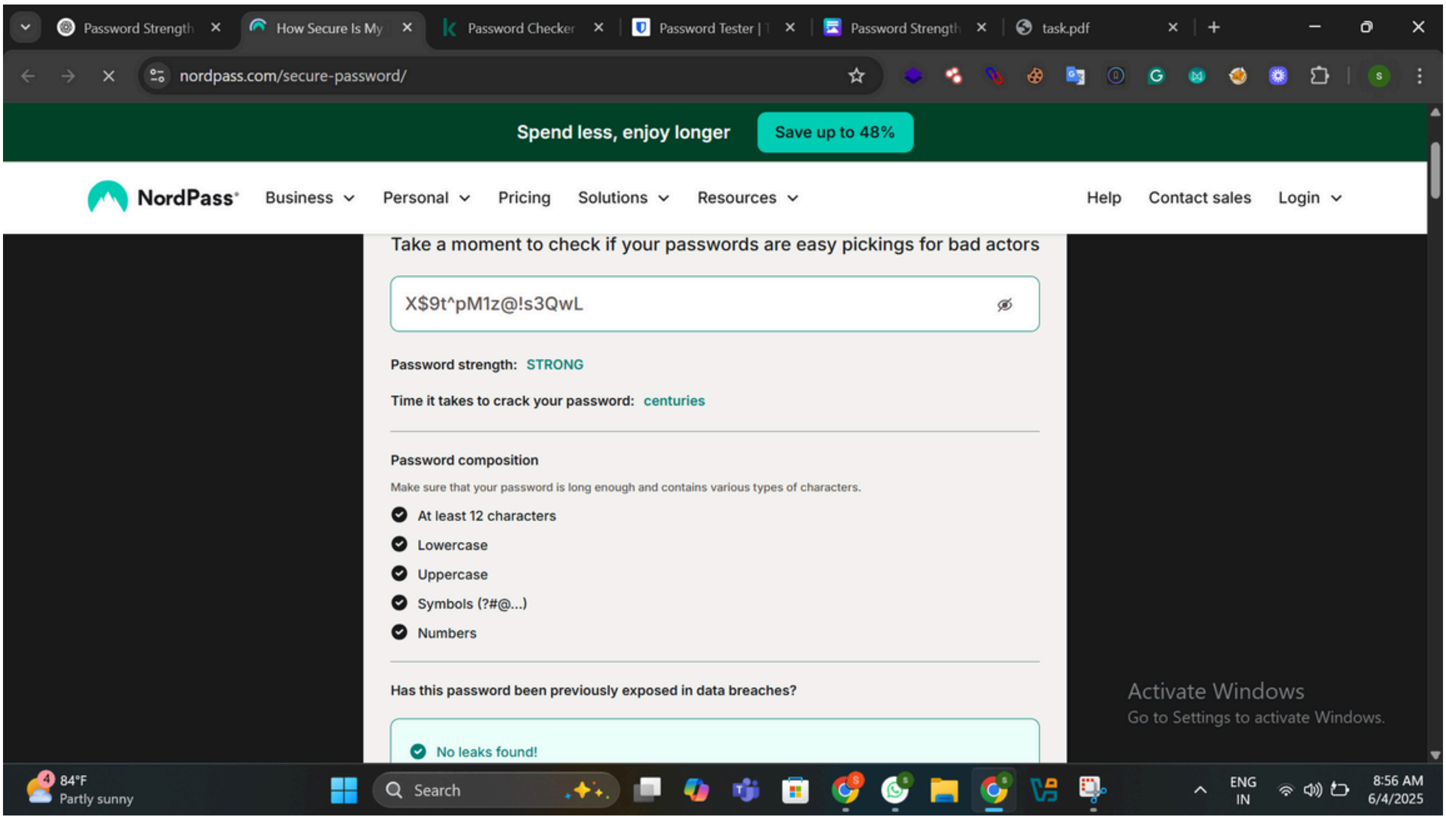
✓ Symbols (?#@...)

✓ Numbers

Has this password been previously exposed in data breaches?

✓ No leaks found!

Very Strong Password:



Take a moment to check if your passwords are easy pickings for bad actors

X$9t^pM1z@!s3QwL

Password strength: STRONG

Time it takes to crack your password: centuries

Password composition

Make sure that your password is long enough and contains various types of characters.

✓ At least 12 characters

✓ Lowercase

✓ Uppercase

✓ Symbols (?#@...)

✓ Numbers

Has this password been previously exposed in data breaches?

✓ No leaks found!

Step 5: Tips Learned from the Evaluation

- **Length matters**: Longer passwords significantly increase strength.
- **Diversity helps**: Adding symbols and mixing cases drastically improves security.
- **Avoid simplicity**: Common words and number combinations are weak.
- **Tools help**: Online tools provide useful insights and should be used regularly.

Step 6: Research on Common Password Attacks

🔍 Common Password Attacks:

1. **Brute Force Attack**
   - Tries all possible combinations.
   - Longer and more complex passwords are resistant.
2. **Dictionary Attack**
   - Uses common words and variations.
   - Avoid real words and predictable combinations.
3. **Phishing**
   - Tricking users to reveal passwords.
   - No technical crack involved but common.
4. **Credential Stuffing**
   - Re-using leaked passwords on other sites.
   - Unique passwords for each site help prevent this.

Step 7: Summary – How Password Complexity Affects Security

Factor	Impact on Security
Length	Exponentially increases resistance to brute force
Symbols	Adds variability and unpredictability
Case Variety	Makes dictionary and pattern attacks harder
Uniqueness	Prevents reuse exploitation (credential stuffing)

Conclusion: The more unpredictable and lengthy your password, the harder it is to crack. Complexity protects against both brute force and dictionary attacks.