

Task 6: Create a Strong Password and Evaluate Its Strength

1. Introduction & Objective

The objective of this task was to understand what makes a password strong and evaluate its strength using an online password strength checker (NordPass). By testing multiple passwords with varying complexity, we aimed to analyze their resistance against brute-force and dictionary attacks, and learn best practices for creating secure passwords.

2. Methodology

1. Created multiple passwords with different combinations of uppercase letters, lowercase letters, numbers, and special characters.
2. Tested each password using NordPass password checker.
3. Recorded password strength, estimated time to crack, and data breach status.
4. Analyzed the results to identify patterns and understand the impact of complexity on password strength.

3. Results

| Password | Strength | Time to Crack | Composition | Data Breach Status |
|-------------------------|----------|---------------|--|-----------------------|
| hello123 | WEAK | 3 seconds | Lowercase, Numbers | Exposed 4 times |
| Hello@123 | MODERATE | 7 minutes | Lowercase, Uppercase, Symbols, Numbers | Exposed 189,272 times |
| H3ll0@W0rld | STRONG | 19 days | Lowercase, Uppercase, Symbols, Numbers | No leaks found |
| #G%a9Qw7*Lz | STRONG | 4 months | Lowercase, Uppercase, Symbols, Numbers | No leaks found |
| ILoveCyberSecurity2025! | STRONG | Centuries | Lowercase, Uppercase, Symbols, Numbers | No leaks found |

4. Screenshots

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

hello123

Password strength: **WEAK**

Time it takes to crack your password: **3 seconds**

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?

Number of times this password has been exposed: 4

powered by haveibeenpwned.com

Spend less, enjoy longer Save up to 50%

NordPass Business Personal Pricing Solutions Resources Help Login Get a Quote

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

Hello@123

Password strength: **MODERATE**

Time it takes to crack your password: **7 minutes**

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?

Number of times this password has been exposed: 189,272

powered by haveibeenpwned.com

Spend less, enjoy longer Save up to 50%

NordPass Business Personal Pricing Solutions Resources Help Login Get a Quote

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

H3ll0@W0rld!

Password strength: **STRONG**

Time it takes to crack your password: **10 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!

powered by haveibeenpwned.com

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

ILoveCyberSecurity2025!

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!

powered by haveibeenpwned.com

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

#G%a9Qw7+Lz

Password strength: **STRONG**

Time it takes to crack your password: **4 months**

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!

powered by haveibeenpwned.com

5. Best Practices for Strong Passwords

- Use at least 12–16 characters.
- Include uppercase, lowercase, numbers, and special characters.
- Avoid dictionary words or common phrases.
- Never reuse passwords across accounts.
- Use passphrases for better memorability and strength.
- Consider using a password manager.
- Enable Multi-Factor Authentication (MFA) wherever possible.

6. Conclusion

This exercise demonstrated that password complexity and length significantly impact security. Simple passwords are easily cracked within seconds or minutes, while strong passwords can take months or centuries to break. Adopting strong password creation habits and using tools like password managers can greatly enhance overall account security.