**PASSWORD STRENGTH EVALUATION REPORT**

Best Practices:

1.Longer passwords are stronger. Aim for at least 12-16 characters.

2.Mix character types:

* Uppercase & Lowercase
* Numbers
* Symbols

3. Avoid:

* Dictionary words (e.g., sunshine, dragon)
* Personal info (e.g., birthdate, name)
* Repeating characters or sequences (aaa111)

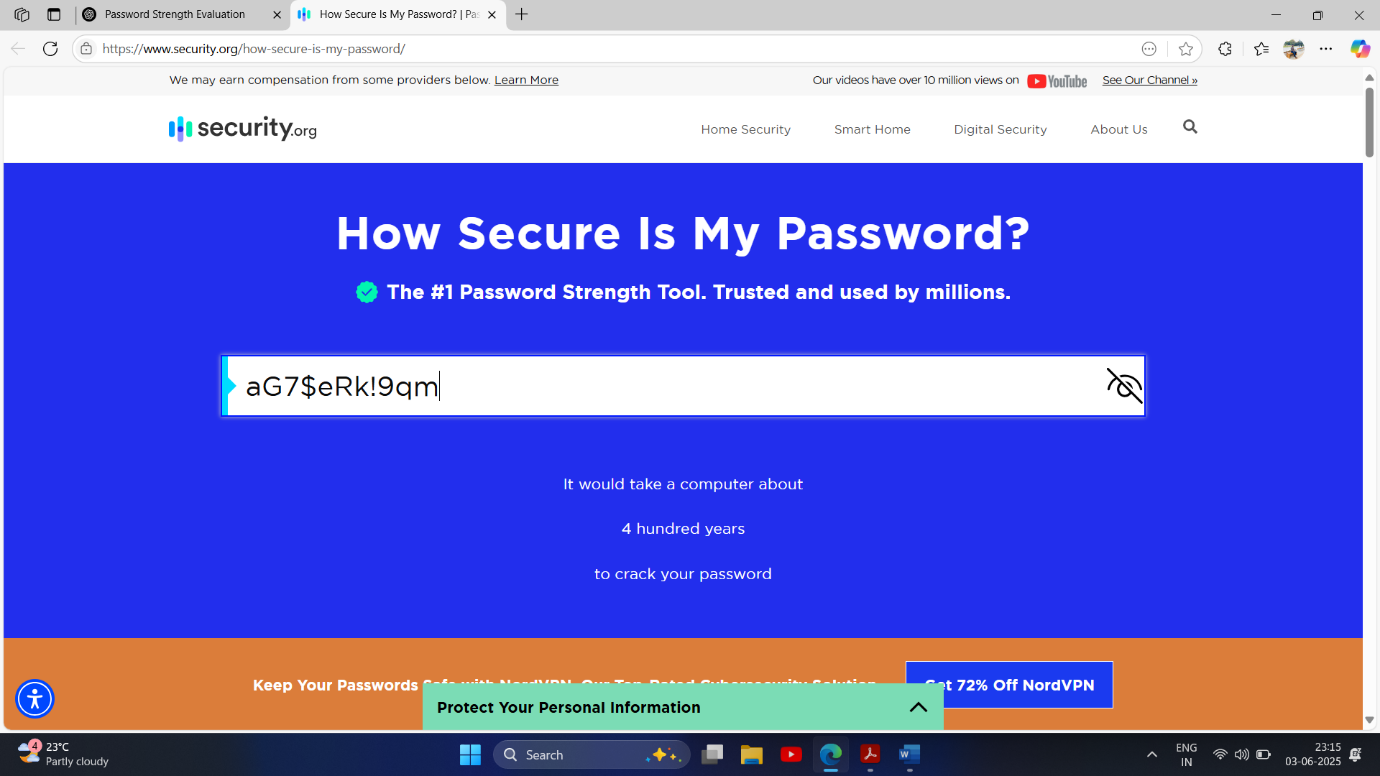
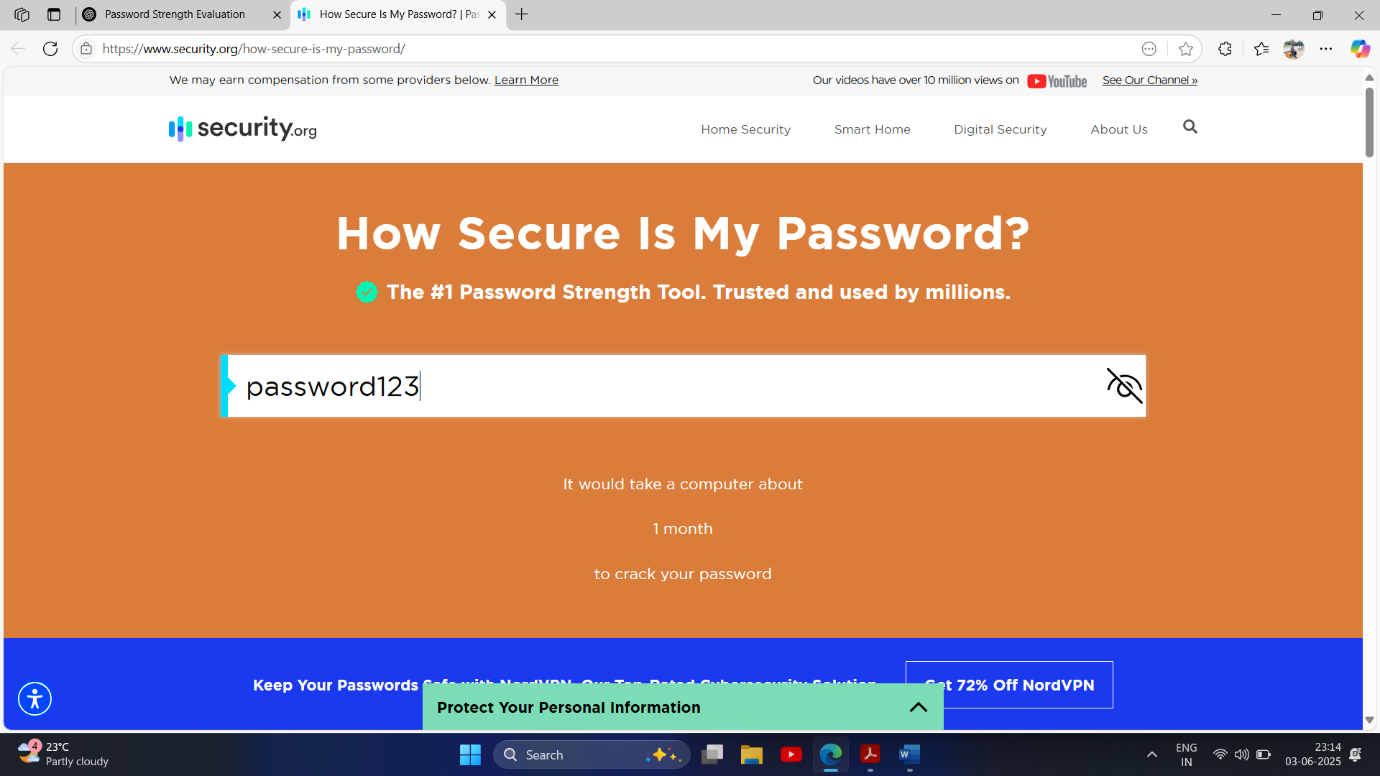
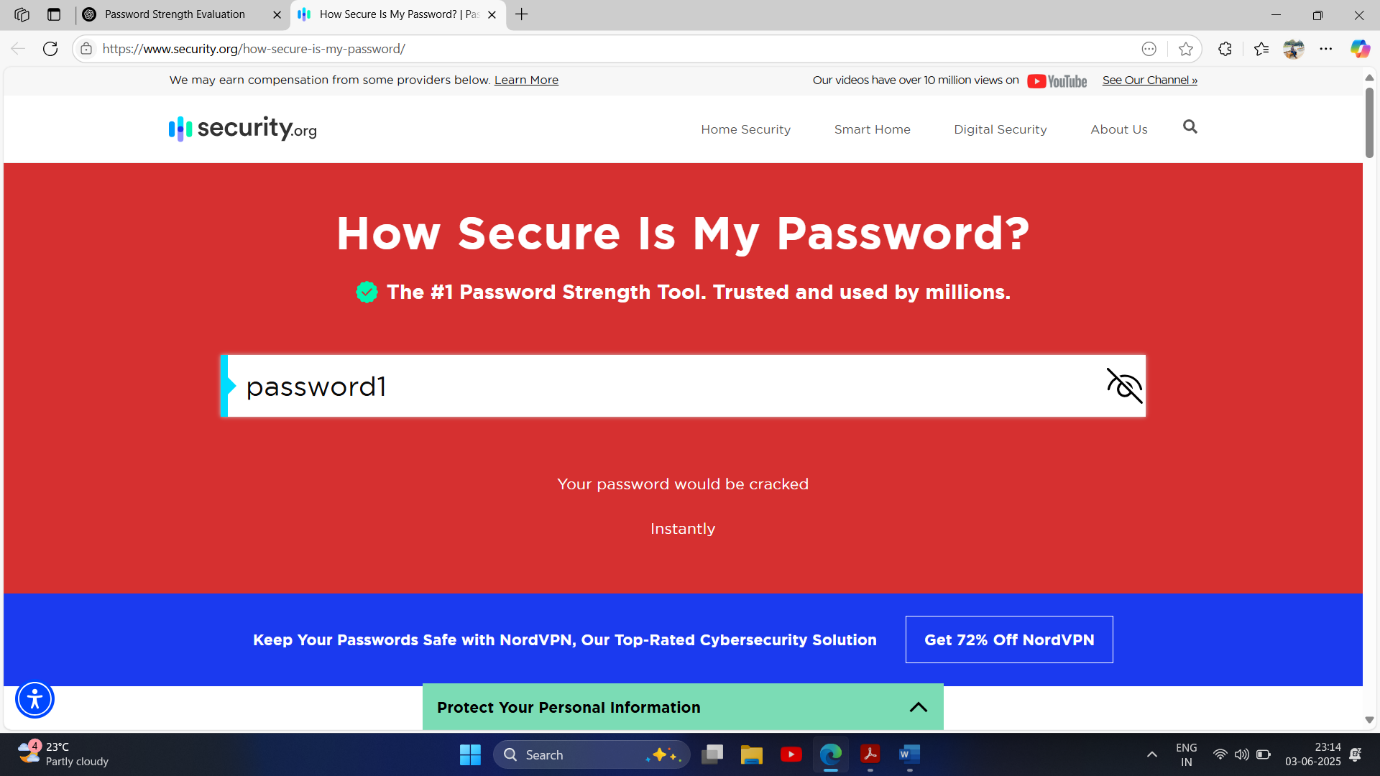
4. Use passphrases combining unrelated words with symbols (e.g., Demon!zfonkey$Chair7).

**Common Password Attacks**

| Attack Type | Description | Impact |
| --- | --- | --- |
| Brute Force | Tries every possible combination | Time-consuming for long, complex passwords |
| Dictionary Attack | Uses common wordlists | Easily breaks weak or common passwords |
| Credential Stuffing | Uses stolen credentials from other breaches | Reused passwords are at high risk |

Password Test Cases:

| **Password** | **Components Used** | **Length** | **Score (%)** | **Feedback** |
| --- | --- | --- | --- | --- |
| password123 | Lowercase, Numbers | 11 | 26% | Too common, lacks complexity |
| P@ssw0rd! | Uppercase, Lowercase, Number, Symbol | 9 | 64% | Better, but still predictable |
| G7$eRk!9qm | Uppercase, Lowercase, Numbers, Symbols | 10 | 96% | Strong password |
| 12345678 | Numbers only | 8 | 8% | Very weak, common pattern |
| iloveyou | Lowercase only | 8 | 10% | Very common phrase |



Tips Learned from Evaluation

* Use a password manager to create and store complex passwords.
* Don't reuse passwords across multiple sites.
* Regularly update passwords, especially for sensitive accounts.
* Enable multi-factor authentication (MFA) where possible

Summary: How Password Complexity Affects Security

* Simple passwords (short, common, predictable) are vulnerable to both brute force and dictionary attacks.
* Complex passwords with high entropy take exponentially longer to crack.
* Password complexity, when combined with length and uniqueness, significantly increases resistance to attacks.

**Outcome**

By testing various passwords and analyzing their strength, we confirmed that:

* Complexity (character variety + length) directly boosts password security.
* Weak passwords can be cracked in seconds.
* Strong passwords last centuries or more under brute-force attacks.
* Applying strong password practices and awareness of attack methods is key to maintaining security.