**TASK 6: CREATE A STRONG PASSWORD AND EVALUATE ITS STRENGTH.**

**Objective:**

To understand the importance of strong passwords by creating, testing, and analyzing them, and learning how complexity affects security.

**Procedure:**

**Step 1.** Create Multiple Passwords

Generate at least 6 different passwords with varying complexity levels:

* + asdf1234
  + Qwer!1234
  + . zxcG0192
  + ZpMQ^09125
  + mlpokn+5786
  + /ZpMQ;lkhj^09125

**Step 2.** Vary Password Characteristics

Use combinations of the following in each password:

* + Uppercase letters (A–Z)
  + Lowercase letters (a–z)
  + Numbers (0–9)
  + Symbols (! @, #, etc.)
  + Length variation (from 6 to 16+ characters)

**Step 3.** Test Passwords Using Online Strength Checker

Websites for testing passwords:

* + <https://password.kaspersky.com>
  + <https://www.security.org/how-secure-is-my-password/>

Enter each password and record the feedback and strength rating.

**Password Test Results:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Password** | **Strength Score** | **Time to Crack** | **Feedback** |
| asdf1234 | Very Weak | Instantly | Lacks symbols, uppercase, length |
| Qwer!1234 | Weak | Three Weaks | Lacks length |
| . zxcG0192 | Strong | Nine Years | Lacks length |
| ZpMQ^09125 | Moderate | Five Years | Lacks length |
| mlpokn+5786 | Moderate | Four Years | Lacks uppercase, length |
| /ZpMQ;lkhj^09125 | Very Strong | 41 Trillion Years | Difficult to crack |

**Tips for strong passwords:**

* 1. Use 12+ characters.
  2. Include uppercase, lowercase, numbers, and symbols.
  3. Avoid personal info like names or birthdates.
  4. Use passphrases (e.g., Gr8!Time2Learn@AI).
  5. Don’t reuse passwords across sites.
  6. Don’t use dictionary phrases or predictable patterns.

**Common Password Attacks:**

**1. Brute Force Attack**

* Tries all possible combinations of characters until the correct password is found.
* Time-consuming but guaranteed to work if no limits are in place.
* **Defense**: Use long, complex passwords and account lockouts after failed attempts.

**2. Dictionary Attack**

* Uses a precompiled list of common words, phrases, and passwords (like password123, qwerty, admin, etc.).
* Faster than brute force.
* **Defense**: Avoid using real words or common patterns in passwords.

**3. Credential Stuffing**

* Uses stolen usernames and passwords from past data breaches to try logging into other websites.
* Based on the assumption that users reuse passwords.
* **Defense**: Use unique passwords for every account and enable two-factor authentication (2FA).

**4. Phishing**

* Tricks the user into revealing their password through fake websites, emails, or messages.
* Doesn’t require guessing the password.
* **Defense**: Don’t click on suspicious links and always verify the sender/source.

**5. Keylogging**

* Malicious software records every keystroke, including typed passwords.
* **Defense**: Use antivirus software and avoid downloading unknown programs.

**6. Rainbow Table Attack**

* Uses precomputed hash values of passwords to crack encrypted password databases.
* Faster than brute force if the password is not salted.
* **Defense**: Use strong password hashing algorithms with salts.

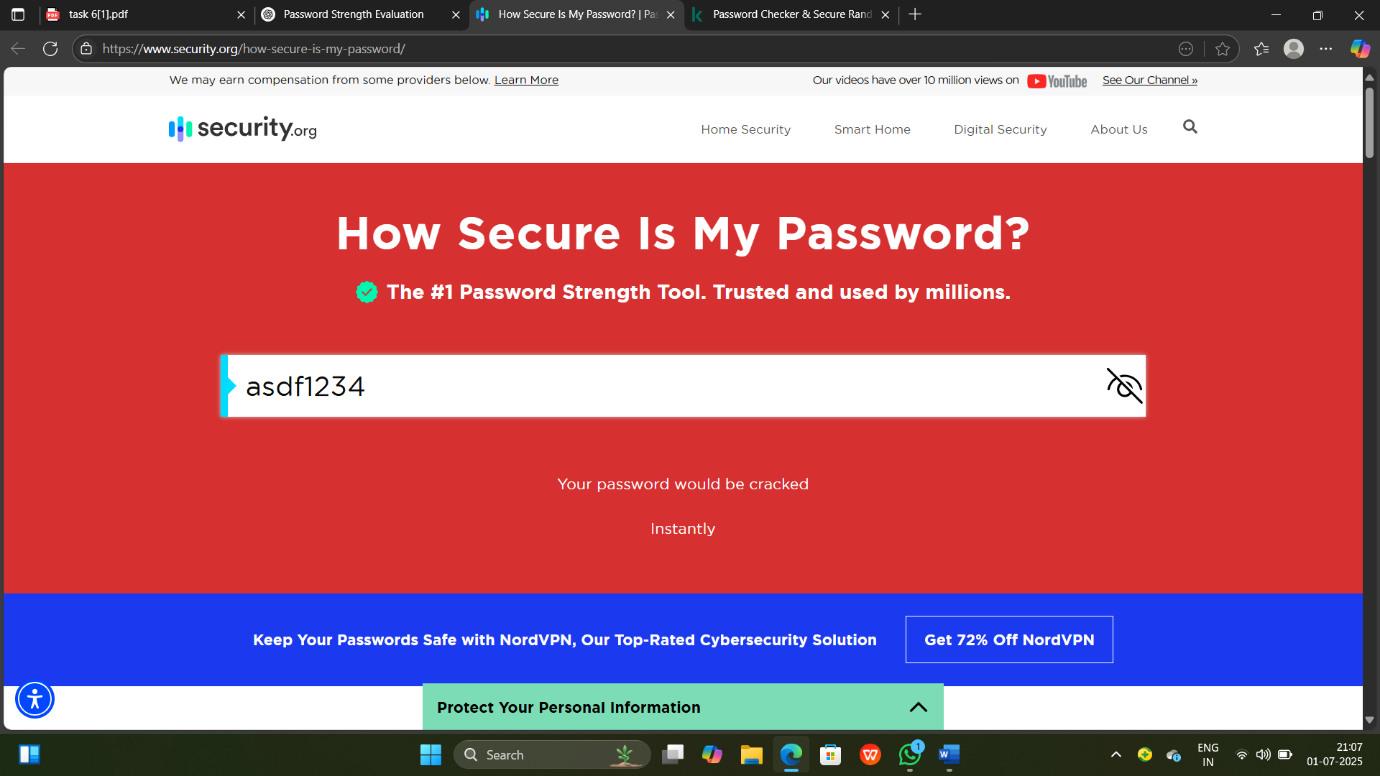
**7. Shoulder Surfing**

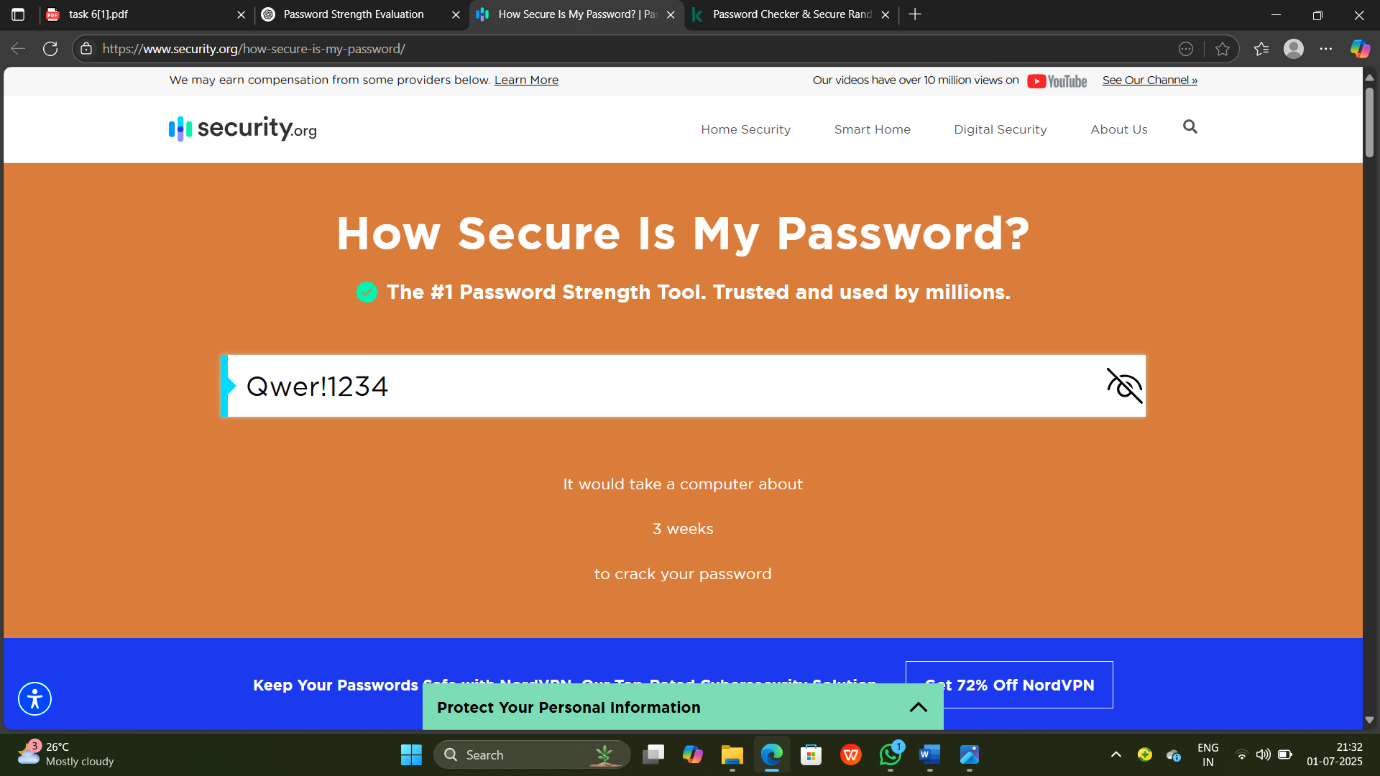
* Physically observing someone typing their password.
* Common in public or shared spaces.
* **Defense**: Be aware of your surroundings; use privacy screens.

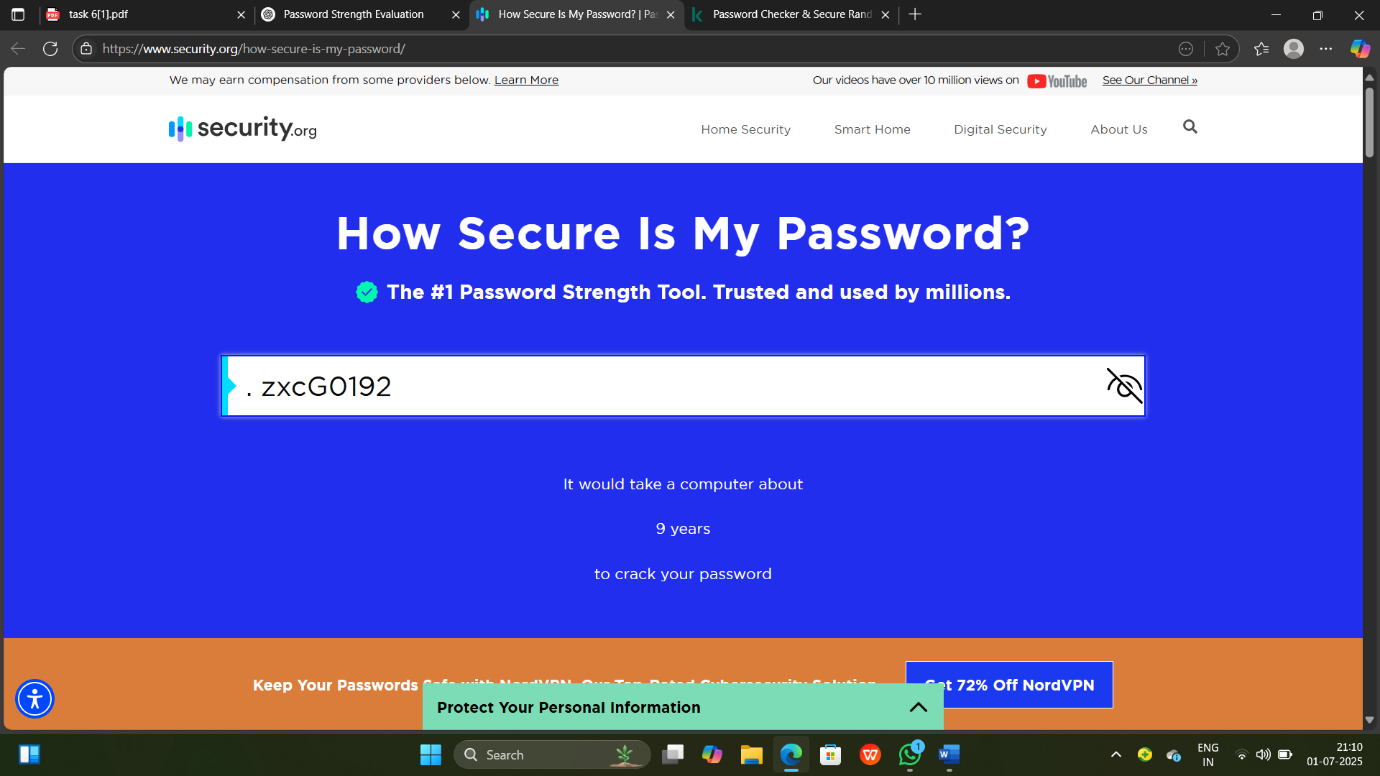
**8. Man-in-the-Middle (MitM) Attack**

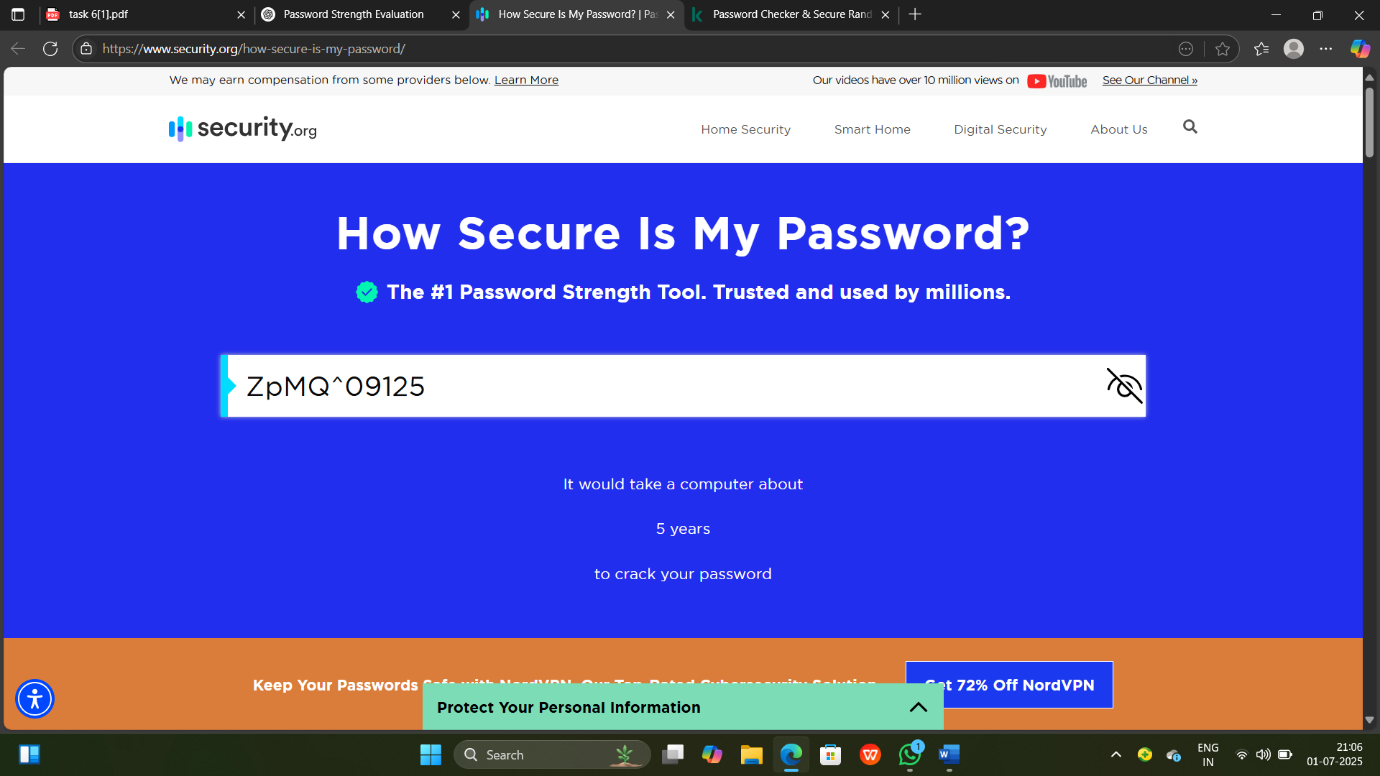
* Attacker intercepts data between user and server, including passwords if not encrypted.
* **Defense**: Use HTTPS and secure networks.

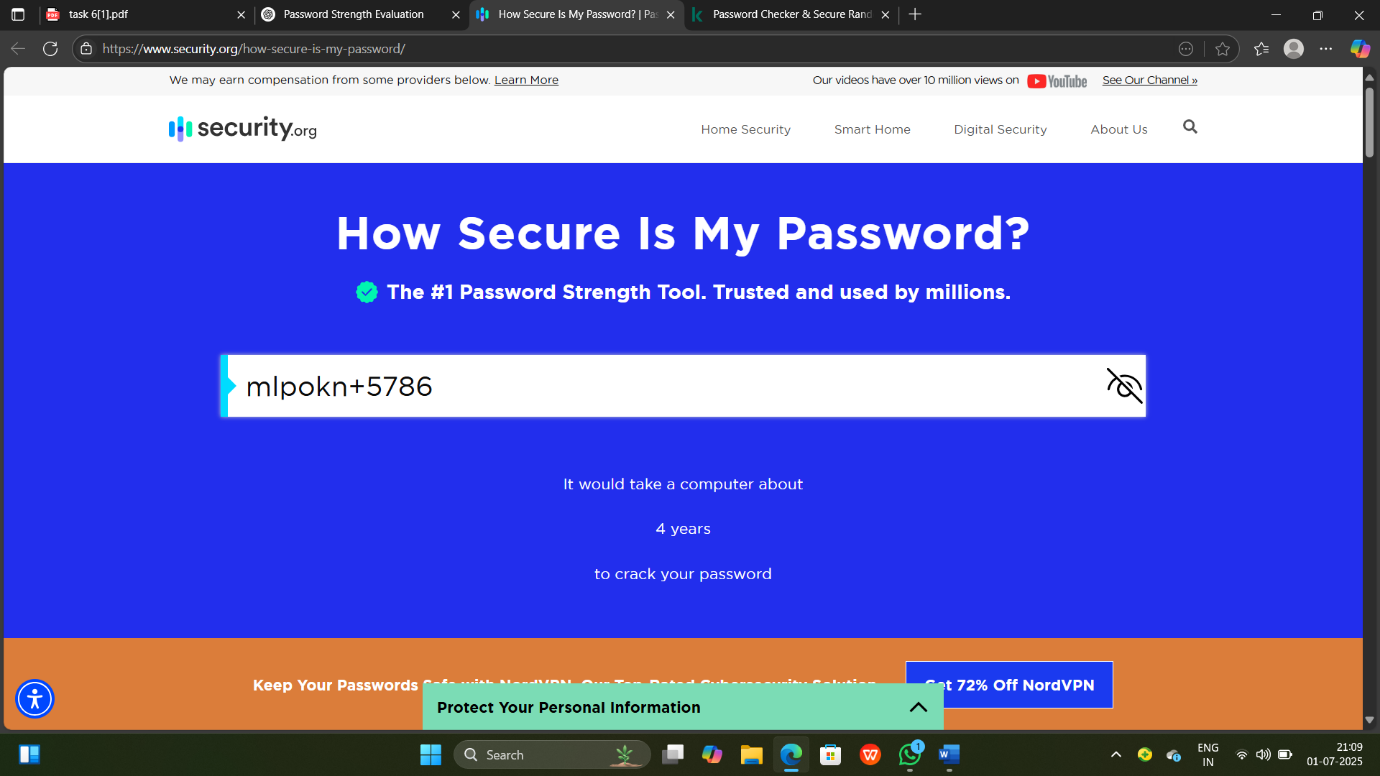
**Screenshots:**

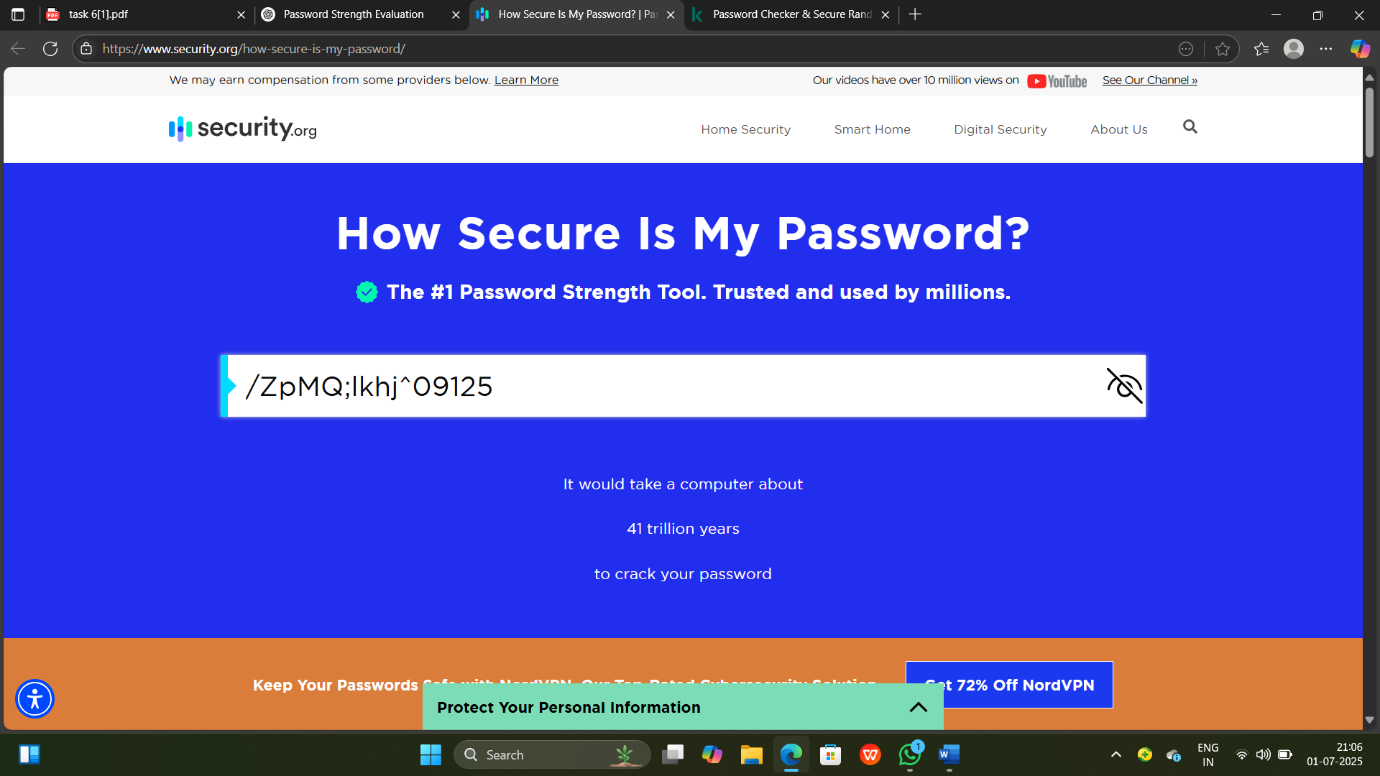
****

****

****

****

****

****

**Conclusion:**

Strong passwords are very important for protecting our accounts and personal information. Passwords that are long and use a mix of uppercase, lowercase, numbers, and symbols are much harder to guess or hack. Weak passwords can be cracked in seconds, while strong ones can take years.