# Create a Strong Password and Evaluate its Strength

## Objective:

To understand what makes a password strong and test it using online password strength checkers.

## Tools Used:

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

## Password Strength Test Results:

|  |  |  |  |
| --- | --- | --- | --- |
| **Password** | **Score** | **Complexity** | **Time-to-crack** |
| password | 8% | Very Weak | Instantly |
| qwertyuiop | 12% | Very Weak | Instantly |
| lisa456 | 37% | Weak | 1 sec |
| Lisa123 | 53% | Good | 1 min |
| l1sa@987 | 71% | Strong | 19 min |
| Li$@234 | 77% | Strong | 6 min |
| /\_1$@Mm34!# | 100% | Very Strong | 5 thousand years |

## Best Practices for Creating Strong Passwords

* Use at least 12 characters in your password.
* Include uppercase, lowercase, numbers, and special characters.
* Avoid using dictionary words, names, or personal information.
* Do not reuse passwords across multiple accounts.
* Update your passwords regularly, especially for critical accounts.
* Do not use keyboard pattern passwords like “qwertyuiop” or “123456789”

## Tips learned from Evaluation:

* Length significantly improves password strength.
* Replacing letters with numbers/symbols (e.g., ‘A’ with ‘@’ , ‘S’ with ‘$’) improves complexity.
* Mixed character types make passwords harder to crack.
* Short or predictable passwords like ‘hello’ or ‘password’ are rated very poorly.

## Common Password Attacks

1. **Brute Force Attacks:**

* This method systematically tries **all possible combinations** of characters until the correct one is found.
* The longer and more complex a password, the more time it takes to crack via brute force.
* Example: Trying ‘aaaa’, ‘aaab’, ‘aaac’ until the right match is found.
* **Prevention:** Use long passwords with varied character types (uppercase, lowercase, numbers, symbols).

1. **Dictionary Attacks:**

* Instead of trying all combinations, attackers use a **predefined list of common words or passwords,** like "password", "123456", or "qwerty".
* These are fast because they target known weak passwords first.
* **Prevention:** Avoid using real words or predictable patterns. Don’t use common names, dates, or phrases.

1. **Credential Stuffing:**

* Attackers use **leaked username-password pairs** from past data breaches and try them on other websites.
* Based on the fact that many people **reuse passwords** across multiple platforms.
* **Prevention:** Use unique passwords for each account. Enable two-factor authentication (2FA).

1. **Phishing Attacks:**

* Tricking users into giving away their passwords by mimicking legitimate websites or services.
* Often done via fake emails, SMS, or malicious links.
* **Prevention:** Never click on suspicious links. Always verify the URL before entering login info.

1. **Keylogging:**

* Malicious software records keystrokes to capture your password as you type.
* Can be installed through infected files or email attachments.
* **Prevention:** Keep antivirus software updated and avoid downloading unknown files.

## Summary

Password complexity plays a critical role in protecting digital accounts. Simple passwords are easily compromised through brute force or dictionary attacks. Creating long passwords with a mix of character types increases resistance against automated cracking tools. Regularly updating passwords and avoiding reuse enhances overall security hygiene.