

Step 1: Create 5 Different Passwords:

1. butterfly
2. butterfly55
3. bu!!er4ly@55
4. ASD@fgh\$jkl789^
5. Mydream@556

Step 2: Test Them on a Password Strength Checker:

<https://howsecureismypassword.net/>

1. butterfly :

The screenshot shows a web browser window with the URL password.kaspersky.com. The page title is "kaspersky password checker". The main heading is "Check and Improve Your Password". Below the heading, it says "Is your password at risk? Check now and generate a strong one in seconds. We do not collect or store your passwords. [Learn more](#)".

The password "butterfly" is entered into the input field. Below the input field, there are four checkboxes indicating password requirements: "Digits [0-9]", "Symbols [!@#]", "Uppercase [A-Z]", and "No leaks found". All four checkboxes are currently unchecked.

Below the checkboxes, there is a section titled "Don't wait - change your password now". It states: "This password appeared 336823 times in a database of leaked passwords. It is not strong because it lacks digits, special symbols, capital letters, proper length." Below this text is a link that says "Generate a secure one?".

The browser's taskbar is visible at the bottom, showing various application icons and the system clock displaying 19:07 on 28-10-2025.

2. butterfly55:

The screenshot shows the Kaspersky Password Checker website. The browser address bar displays 'password.kaspersky.com'. The page title is 'kaspersky password checker'. The main heading is 'Check and Improve Your Password'. Below the heading, a message states: 'Is your password at risk? Check now and generate a strong one in seconds. We do not collect or store your passwords. [Learn more](#)'. The password input field contains 'butterfly55'. Below the input field, a progress bar shows the password's strength: 'Digits [0-9]' is checked, 'Symbols [!@#]' is unchecked, 'Uppercase [A-Z]' is unchecked, and 'No leaks found' is unchecked. A red bar indicates the password is weak. Below the progress bar, a message says: 'Don't wait - change your password now'. Below this, a note states: 'This password appeared 718 times in a database of leaked passwords. It is not strong because it lacks special symbols, capital letters, proper length.' A green link 'Generate a secure one?' is visible. The Windows taskbar at the bottom shows the search bar and various application icons.

3. bu!!er4ly@55:

The screenshot shows the Kaspersky Password Checker website. The browser address bar displays 'password.kaspersky.com'. The page title is 'kaspersky password checker'. The main heading is 'Check and Improve Your Password'. Below the heading, a message states: 'Is your password at risk? Check now and generate a strong one in seconds. We do not collect or store your passwords. [Learn more](#)'. The password input field contains 'bu!!er4ly@55'. Below the input field, a progress bar shows the password's strength: 'Digits [0-9]' is checked, 'Symbols [!@#]' is checked, 'Uppercase [A-Z]' is unchecked, and 'No leaks found' is checked. A yellow bar indicates the password is strong. Below the progress bar, a message says: 'Time to change your password'. Below this, a note states: 'Your password does not appear in any databases of leaked passwords. It is not strong because it lacks capital letters, proper length.' A green link 'Generate a secure one?' is visible. The Windows taskbar at the bottom shows the search bar and various application icons.

4. ASD@fgh\$jkl789^ :

The screenshot shows the Kaspersky Password Checker website. The browser address bar displays 'password.kaspersky.com'. The page title is 'kaspersky password checker'. The main heading is 'Check and Improve Your Password'. Below it, a subheading reads: 'Is your password at risk? Check now and generate a strong one in seconds. We do not collect or store your passwords. [Learn more](#)'. A password input field contains 'ASD@fgh\$jkl789^'. Below the input field, a progress bar shows four criteria: 'Digits [0-9]', 'Symbols [!@#]', 'Uppercase [A-Z]', and 'No leaks found', all of which are checked. A message states: 'Don't wait - change your password now'. Below this, it says: 'Your password does not appear in any databases of leaked passwords. It is not strong because it lacks proper length.' A button labeled 'Generate a secure one?' is visible. The Windows taskbar at the bottom shows the search bar and various application icons.

5. Mydream@556 :

The screenshot shows the Kaspersky Password Checker website. The browser address bar displays 'password.kaspersky.com'. The page title is 'kaspersky password checker'. The main heading is 'Check and Improve Your Password'. Below it, a subheading reads: 'Is your password at risk? Check now and generate a strong one in seconds. We do not collect or store your passwords. [Learn more](#)'. A password input field contains 'Mydream@556'. Below the input field, a progress bar shows four criteria: 'Digits [0-9]', 'Symbols [!@#]', 'Uppercase [A-Z]', and 'No leaks found', all of which are checked. A message states: 'Time to change your password'. Below this, it says: 'Your password does not appear in any databases of leaked passwords. It is not strong because it lacks proper length.' A button labeled 'Generate a secure one?' is visible. The Windows taskbar at the bottom shows the search bar and various application icons.

Step 3: Record the Results :

#	Password	Strength Rating	Estimated Time to Crack (rough)	Feedback / Notes
1	butterfly	Very Weak	< 1 second — seconds (dictionary attack)	Common dictionary word, only lowercase, short. Will be found almost instantly by dictionary attacks.
2	butterfly55	Weak	Seconds → minutes (dictionary + common digit suffix)	Same base word plus a common two-digit suffix — slightly better but still highly predictable and vulnerable to targeted/dictionary lists.
3	bu!!er4ly@55	Medium → Strong	Hours → years (depends on attacker resources & rules)	Uses symbol substitutions and numbers which raises entropy. However it's clearly derived from a single dictionary word (butterfly) so advanced rule-based cracking (substitutions) reduces effective strength. Better than 1–2, but not ideal.
4	ASD@fgh\$jk1789^	Strong → Very Strong	Decades → centuries (large search space)	Long and includes upper/lower, symbols, and digits. But it appears to follow keyboard-row patterns (ASD fgh jkl) which are somewhat predictable — still quite strong due to length and mixed characters. Randomize more to maximize strength.
5	Mydream@556	Medium	Years → decades	Passphrase-like (word + symbol + digits). Better than short single words, but mydream is a phrase that could appear in targeted guesses; repeated digits (556) reduce entropy relative to fully random digits.

Step 4: Observe & Identify Patterns

You'll notice:

- Longer and more random = stronger passwords.
- Words found in the dictionary or with numbers like "123" = weak.
- Mixed symbols, letters, and case = much stronger.

Step 5: Write Down Best Practices

- Minimum 12–16 characters.
- Use uppercase, lowercase, numbers, and symbols.
- Avoid personal info (birthday, name, etc.)
- Use a password manager.
- Enable 2FA for extra protection.

Step 6: Research & Note Attacks:

Common Attacks:

- **Brute Force:** Tries every possible combination.
- **Dictionary Attack:** Uses a list of common passwords.
- **Phishing:** Tricks you to reveal password.

Example:

If your password is sunflower, a dictionary attack will guess it instantly.

If your password is Tg\$9eR!2m@x#8, brute force might take **millions of years**.