**1-2. Create Multiple Passwords with Varying Complexity**

| **Password** | **Composition** |
| --- | --- |
| apple123 | Lowercase + Numbers |
| AppleTree1 | Uppercase + Lowercase + Number |
| P@ssw0rd! | Uppercase + Lowercase + Number + Symbol |
| 1qaz2wsx | Common Pattern |
| X!9rT&7#mL$ | Complex: All elements + long |
| banana | Simple lowercase word |
| Summer2025 | Seasonal + Year |
| B@sk3tB@ll#23 | Passphrase style + Symbols + Numbers |
| qwerty | Very common weak password |
| Z5\*rE8!tY3@v | Random, high entropy |

**3–4. Test Passwords on Strength Checkers**

**Tools Used:**

* Kaspersky Password Checker
* NordPass Strength Checker
* [HowSecureIsMyPassword.net](https://howsecureismypassword.net/)

| **Password** | **Est. Crack Time** | **Strength (Feedback Summary)** |
| --- | --- | --- |
| apple123 | < 1 second | **Very weak** – common pattern |
| AppleTree1 | Few hours | **Weak** – predictable format |
| P@ssw0rd! | Few minutes – 1 hour | **Moderate** – uses common substitutions |
| 1qaz2wsx | < 1 second | **Very weak** – keyboard pattern |
| X!9rT&7#mL$ | Centuries | **Very strong** – high entropy |
| banana | < 1 second | **Very weak** – dictionary word |
| Summer2025 | Minutes | **Weak** – predictable date |
| B@sk3tB@ll#23 | Years | **Strong** – long, with mixed types |
| qwerty | < 1 second | **Very weak** – common password |
| Z5\*rE8!tY3@v | Centuries | **Very strong** – randomized |

**5. Identify Best Practices for Creating Strong Passwords**

* **Length matters**: Longer passwords (12+ characters) are exponentially stronger.
* **Avoid common words and patterns**: No dictionary words, keyboard sequences, or dates.
* **Mix character types**: Use uppercase, lowercase, numbers, and symbols.
* **Unpredictability**: Randomness makes passwords significantly harder to crack.
* **Avoid substitutions of common passwords**: e.g., P@ssw0rd is still weak despite symbols.

**6. Tips Learned from Evaluation**

* Use passphrases with added complexity, like Sun#Ri$eD@wn2025!
* Don't reuse passwords across accounts.
* Password managers can generate/store complex passwords securely.
* Change passwords regularly if exposed in breaches.
* Avoid personal info (birthdays, names, pets).

**7. Common Password Attacks**

**Brute Force**:

* Tries all possible combinations.
* Defeated by long, complex passwords.

**Dictionary Attack**:

* Uses a list of known words/passwords.
* Defeated by avoiding real words and adding randomness.

**Credential Stuffing**:

* Uses stolen username/password combos.
* Mitigated by using unique passwords per account.

**Phishing**:

* Tricks user into giving up passwords.
* Defeated by vigilance and 2FA.

**8. How Password Complexity Affects Security**

* **Increased complexity = increased resistance** to automated cracking.
* **Short and simple passwords** can be cracked in seconds.
* **Unique and complex passwords** significantly reduce the risk of account compromise.
* **Randomization adds entropy**, making each guess exponentially harder for attackers