Create a Strong Password and Evaluate Its Strength.

1. Password Examples with Varying Complexity

* Weak: hello123, password
* Medium: Hello@123, Summer2025
* Strong: H@ck3r!ntern$2025, Xy#9rT!8qL$1v

2. Variations Used

* Lowercase only → Weak
* Uppercase + numbers → Better
* Symbols + length ≥ 12 → Strong
* Randomized characters, no dictionary words → Very Strong

3. Password Strength Testing (Sample Results)

* hello123 → Weak (cracked <1 sec)
* Hello@123 → Medium (hours)
* H@ck3r!ntern$2025 → Strong (years)
* Xy#9rT!8qL$1v → Very Strong (centuries)

4. Feedback from Tools

* Weak → Too short, predictable
* Medium → Pattern-based (capital first, ends with 123)
* Strong → Good mix, long, harder to guess
* Very Strong → Randomized, lengthy

5. Best Practices for Strong Passwords

* Use 12–16+ characters
* Mix uppercase, lowercase, numbers, symbols
* Avoid dictionary words, names, birthdays
* Prefer passphrases or random generator
* Use password manager
* Enable multi-factor authentication (MFA)

6. Tips Learned

* Length matters more than just complexity
* Attackers try common passwords first
* Random & unique passwords reduce risks
* Update passwords, don’t reuse

7. Common Password Attacks

* Brute Force → Tries all combinations
* Dictionary Attack → Uses wordlists
* Credential Stuffing → Reuses stolen passwords
* Phishing → Tricks users into revealing
* Keylogging → Records keystrokes

8. Summary – How Complexity Affects Security

* Simple → Easily cracked
* Moderate → Still vulnerable
* Strong & long → Hard to break
* Best defense → Strong + MFA + password manager