Password Security Evaluation Report

1 & 2. Created Passwords with Varying Complexity

Weak	hello123
Medium	Hello1234
Strong	H3ll0!2025
Very Strong	T!mE$@2025_S#cur3

3 & 4. Password Strength Test Results

Password	Strength Feedback
hello123	Very Weak – cracked instantly
Hello1234	Weak – cracked in hours
H3ll0!2025	Strong – cracked in years
T!mE$@2025_S#cur3	Very Strong – centuries to crack

5. Best Practices for Creating Strong Passwords

- Use at least 12–16 characters.
- Mix uppercase, lowercase, numbers, and symbols.
- Avoid dictionary words and personal information.
- Use passphrases (e.g., B3tter_Security#2025!).
- Do not reuse passwords across multiple accounts.

6. Tips Learned from Evaluation

- Short/simple passwords are broken instantly.
- Adding numbers improves slightly, but not enough.
- Special symbols + longer length make passwords much stronger.
- Random combinations are best and least predictable.

7. Common Password Attacks

- Brute Force: Tries all possible combinations.
- Dictionary Attack: Uses a list of common words.
- Credential Stuffing: Uses leaked username-password pairs.
- Hybrid Attack: Mixes dictionary words with variations.

8. Summary: How Password Complexity Affects Security

Password complexity directly increases security. Low complexity passwords are easily cracked within seconds or minutes. Medium complexity passwords can take hours to days, but still remain vulnerable. High complexity passwords (16+ characters, with mixed uppercase, lowercase, numbers, and symbols) may take centuries or longer to crack using brute force. Strong password complexity makes common attacks ineffective, forcing attackers to use alternative methods such as phishing.