■ Password Strength Evaluation and Security Analysis Report

1. Objective

The purpose of this report is to evaluate the security impact of password length, character mix, and randomness. Using simulated password strength scoring, this report categorizes different complexity tiers, demonstrates their security implications, and highlights best practices for strong password creation.

2. Evaluation Data Sheet: Complexity, Strength, and Defense

Tier	Sample Password Type	Length Range	Criteria Met	Simulated Score	Estimated Crack Time	Primary Defens
Weak	Dictionary words, simple patterns, short.	8–10	Lowercase, numbers, simple caps.	Poor (1/4)	Instant (<1 sec)	N/A
Medium	Simple mix, predictable placement of symbols.	10–12	Upper, Lower, Number, Symbol	Fair–Good (2–3/4)	Minutes → Weeks	Added Complexi
rong (Random)	Fully random, high-entropy strings.	16–18	All character types, random	Excellent (4/4)	Hundreds of Years	Extreme Length
trong (Phrase)	Long, nonsensical, easy-to-remember phrase.	18–20	Long phrase, substitutions	Excellent (4/4)	Decades → Centuries	Extreme Length

3. Sample Password Sets (10 per Tier)

Weak Passwords

```
summer2025
Asdf1234
password!
iloveyou
Dragon12
11223344
football1
secretkey
MyDogName
QWERTY99
```

Medium Passwords

```
F0xjump$
Gr8day!!
River#Flow1
SecureWeb8
Book%Shelf5
J@nu@ry24
Pa$$word!2
H!ghw@y
BigCat$25
L@ptop1020
```

Strong Passwords

```
W#2aL7p%4jB0x!9t
2H!P$M6v^L8qZ1yR
1T%qZ&H3r;@5c0mJ
BlueMoonR!sesSlowly
Pa$$w0rdIsT00L0ng!
Th3L@zyD0gSleeps!
P!nkF0xJumpsOver3
G%5aB#9t^K4fJ2eL
```

```
9*eN4d&r;(S8t2F7L0
7bV$H1jY@3gT0dP%
```

4. Best Practices for Strong Passwords

- Prioritize Length: Crack times rise exponentially when length increases (12 → 16+ characters).
- Maximize Randomness (Entropy): Avoid dictionary words, names, or predictable sequences.
- Ensure Uniqueness: Reuse of even a strong password exposes multiple accounts.

5. Tips Learned from Evaluation

■ Avoid Sub-12 Passwords: Too weak for modern cracking speeds.

■ Embrace Passphrases: Long, nonsensical passphrases are both strong and memorable.

■ Use Password Managers: For generating and storing high-entropy 16+ character passwords.

6. Research Summary: Password Complexity & Security

Complexity Component	Security Impact	Defense Summary
Length (16+ chars)	Exponentially increases total combinations.	Best defense vs. Brute-Force.
Randomness (No words/patterns)	Prevents inclusion in attack lists/dictionaries.	Defense vs. Dictionary Attacks.
Character Mix (Upper/Lower/Num/Sym)	Expands character set and combinations.	Enhances Brute-Force defense.

7. Common Password Attacks

Brute-Force Attack: Tries all possible combinations systematically. Defense → Password Length.

Dictionary Attack: Uses precompiled lists of words & substitutions. Defense → Randomness.

8. Final Conclusion

The strongest security posture is achieved when a password is:

- Unique (not reused anywhere else)
- Long (16+ characters minimum)
- Randomly generated (maximized entropy)

Such passwords remain resilient against both dictionary attacks and brute-force methods for centuries.