Task 6: Create a Strong Password and Evaluate Its Strength

Objective

The objective of this task is to understand the elements of a strong password, test sample passwords against strength checkers, and learn best practices for password security.

Password Strength Evaluation (as per "passwordmeter.com")

Password	Composition	Score (Example)	Feedback / Weaknesses
password123	Lowercase + numbers	Weak (43%)	Too common, predictable, dictionary word
Pass@2024	Uppercase + lowercase + number + symbol	Strong (92%)	Some complexity, but still short
S3cur3!Life#2025	Uppercase + lowercase + numbers + symbols + 14 chars	Very Strong (100%)	Long, complex, not in dictionary
qwerty!	Lowercase + symbol, short	Weak (26%)	Common pattern, too short
Tr0ub4dor&3Horse$Battery	Very long passphrase with substitutions	Very Strong (100%)	Hard to crack, highly resistant to attacks

Test Your Password		Minimum Requirements
Password:	password123	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	43%	
Complexity:	Good	

Test Your Password		Minimum Requirements
Password:	Pass@2024	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	92%	
Complexity:	Very Strong	

Test Your Password		Minimum Requirements
Password:	S3cur3!Life#2025	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Test Your Password		Minimum Requirements
Password:	qwerty!	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	26%	
Complexity:	Weak	

Test Your Password		Minimum Requirements
Password:	Tr0ub4dor&3Horse$Battery	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Best Practices Learned

- Use a mix of uppercase, lowercase, numbers, and special characters.

- Ensure length is at least 12–16 characters.
- Avoid dictionary words, common sequences (123, qwerty), or personal info.
- Use passphrases made of multiple random words.
- Enable multi-factor authentication (MFA) for additional security.
- Change passwords periodically and don't reuse across accounts.

Password Complexity Table

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years

Common Password Attacks

1. Brute Force Attack

Attacker tries every possible combination until success.
Mitigation: Long and complex passwords greatly increase time to crack.

2. Dictionary Attack

Attacker uses a list of common words/passwords.
Mitigation: Avoid common words, use symbols and randomness.

3. Credential Stuffing

Using leaked username-password pairs across multiple sites.
Mitigation: Unique passwords for each service.

Summary

Password complexity directly impacts resistance against brute force and dictionary attacks.
- Strong passwords are long, unique, and random, not based on predictable patterns.
- Passphrases can be both secure and memorable.
- Combined with MFA, strong passwords provide a robust defense against unauthorized access.