Task 6: Create a Strong Password and Evaluate Its Strength

Tool Used: Bitwarden & passwordmonster.com Password Checkers

Introduction

For this task, I explored how to create strong passwords and tested different examples using online tools to see how long it would take a hacker to crack them. I learned how certain patterns (like using dictionary words or numbers only) make passwords easier to break.

Step 1: Password Samples

I came up with five different passwords with varying complexity and checked how long it would take to crack each one.

Password	Estimated Time to Crack	Notes
`mumbai123`	Less than 2 seconds	Simple, lowercase + numbers only
`Mumbai@2025`	Around 3 hours	Moderate—includes capital + symbol
`#Aq8%vZ!r1`	More than 26 trillion years	Very strong—random, long, complex
`12345678`	Instant (common password)	Extremely weak—commonly used
`BlueMoon`	A few seconds	Weak—dictionary-based, too short

Step 2: Observations

- The more complex and random a password is, the harder it is to crack.
- Common or predictable passwords (like `12345678`) are broken instantly.
- Just capitalizing a letter or adding a symbol helps but still isn't enough on its own.

- Longer passwords are much stronger, especially when they avoid real words.

Step 3: Common Password Attacks

While researching, I came across these attack methods:

- **Brute Force:** Tries every possible combination—time-consuming for strong passwords.
- **Dictionary Attack:** Uses common passwords and wordlists.
- **Phishing:** Tricks people into giving up passwords by pretending to be legit sites.
- **Credential Stuffing:** Reuses stolen passwords from data breaches.

Step 4: Tips for Strong Passwords

Here's what I learned about creating strong passwords:

- Use at least **12–16 characters**.
- Mix **uppercase, lowercase, numbers, and special symbols**.
- **Avoid dictionary words**, birthdays, or personal information.
- Consider using **a passphrase** or a **password manager** to store secure, unique passwords.

Final Thoughts

This activity helped me realize how easy it is to crack weak passwords. I used to think adding a number was enough, but now I understand why password managers and random generation are important. Going forward, I'll be more careful about choosing strong, secure passwords for all my accounts.

Time it takes a hacker to brute force your password in 2025

Hardware: 12 x RTX 5090 | Password hash: bcrypt (10)

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

Hive Systems

Read more and download at
hivesystems.com/password