Task 6: Creating and Testing Strong Passwords

# Objective

The goal of this task was to learn what makes a password strong, try out different examples, test them with an online password checker, and then understand how complexity protects against attacks.

# Step 1: Trying Out Passwords

I created a few different passwords, starting from simple ones and then gradually making them more complex. I tested each of them on passwordmeter.com, and here’s what I found:

|  |  |  |
| --- | --- | --- |
| Password | My Intention | Tool’s Feedback |
| abcd1234 | Just a simple mix of letters and numbers | Weak – too short and predictable |
| Abcd@123 | Added uppercase and a symbol | Medium – better, but still not strong enough |
| AbcD@2025! | Longer with more variety | Strong – much harder to crack |
| S3cUr3!Pa$$w0rD2025 | A mix of everything | Very Strong – good length and randomness |
| Qw!9rT#zL@7yP$2uB\*5 | A totally random string | Extremely Strong – almost impossible to guess |

# Step 2: What I Learned

* Length is powerful → Short passwords fail quickly, while longer ones are much safer.
* Mix everything → A good mix of uppercase, lowercase, numbers, and symbols makes a huge difference.
* Avoid common words → Anything like “password123” or “qwerty” is a big no.
* Randomness helps → The less predictable the pattern, the stronger the password.
* Passphrases work well → A sentence-like password such as Blue$TigerRuns7Fast! can be both strong and easier to remember than random gibberish.

# Step 3: How Hackers Attack Passwords

* Brute Force → Tries every possible combination. Long and complex passwords make this extremely slow.
* Dictionary Attack → Uses common words and password lists. Randomness and symbols protect against this.
* Hybrid Attack → A mix of both, like guessing “Password123!”. Strong unique passwords defeat this too.

# Final Thoughts

This task showed me clearly that password strength is not just about adding a symbol at the end—it’s about length, complexity, and unpredictability. A strong password makes it very expensive and time-consuming for attackers to break in.  
  
I also realized it’s impossible to remember super-random strings for every account, so using a password manager or creating memorable passphrases is the best balance between security and usability.  
  
Conclusion: The stronger and more unique the password, the safer the account.