Task 6 Report: Create and Evaluate Strong Passwords

# Objective

To understand what makes a password strong, create various password types, evaluate their strength using online tools, and learn best practices for password security.

# Passwords Created & Evaluated

|  |  |  |  |
| --- | --- | --- | --- |
| Password | Complexity Level | Score (PasswordMeter) | Feedback Summary |
| password123 | Weak | 25% | Too common, lacks symbols, easy to guess |
| Passw0rd! | Medium | 55% | Better—uses symbol and number, but still guessable |
| S@feC0de2025 | Strong | 78% | Good mix of chars, numbers, symbol, decent length |
| tR7$Wq!v9xZ&uF#4 | Very Strong | 100% | High entropy, random, complex, ideal password |

# Tips Learned for Creating Strong Passwords

* Use at least 12–16 characters.
* Include a mix of uppercase & lowercase letters, numbers, and special symbols (e.g., @, !, #, $).
* Avoid common words (e.g., password, 123456, qwerty).
* Don’t reuse old passwords.
* Use a password manager to store complex passwords.

# Common Password Attack Methods

|  |  |
| --- | --- |
| Attack Type | Description |
| Brute Force | Tries all possible combinations until it finds the right one. |
| Dictionary Attack | Uses a list of commonly used passwords and words to guess the password. |
| Phishing | Tricks the user into revealing their password (via fake websites or emails). |

# How Password Complexity Improves Security

* Longer passwords increase the number of possible combinations exponentially.
* Symbols and mixed case add more variations than just lowercase letters.
* Random passwords are harder to guess than ones with patterns or dictionary words.
* A strong password takes years to crack with brute force, whereas a weak one can be cracked in seconds.

# Conclusion

Using password strength tools like PasswordMeter.com, it's clear that randomness, length, and variety are key to strong passwords. Users should adopt these practices and stay informed about common threats.