Task 6: Create a Strong Password and Evaluate Its Strength

Objective

Understand the characteristics of strong passwords and assess their robustness using online password strength checkers.

Tools Used

- PasswordMeter

Password Creation and Evaluation

I created five passwords with varying complexities and tested them using the tools mentioned above. Here is a summary of the results:

Password	Composition Details	Password Meter Score	Bitwarden Crack Time	Security.org Crack Time	NordPass Crack Time
`sunshine123`	Lowercase + Numbers (10 chars)	Weak	<1 second	<1 second	<1 second
`Sunshine@123`	Mixed Case + Numbers + Symbol (12 chars)	Moderate	~1 minute	~2 minutes	~2 minutes
`S@f3P@ssw0rd!`	Mixed Case + Numbers + Symbols (13 chars)	Strong	~1 hour	~1 hour	~1 hour
`Tr0ub4dor&3`	Mixed Case + Numbers + Symbol (11 chars)	Strong	~3 hours	~4 hours	~4 hours
`C0mpl3x!P@ss#2025`	Mixed Case + Numbers + Multiple Symbols (16 chars)	Very Strong	34,000 years	46 million years	5 million years

Analysis of Results

- **Length Matters**: Longer passwords significantly increase the time required to crack them. For instance, rising from 10 to 16 characters can shift crack time from seconds to millions of years.
- **Complexity Enhances Security**: Incorporating uppercase letters, numbers, and symbols adds layers of complexity, making passwords harder to guess.
- **Avoid Common Patterns**: Simple and commonly used passwords like `sunshine123` are extremely vulnerable, often cracked in less than a second.

Best Practices for Creating Strong Passwords

1. **Use a Mix of Character Types**: Combine uppercase and lowercase letters, numbers, and special symbols.
2. **Increase Length**: Aim for passwords that are at least 14 characters long.
3. **Avoid Predictable Patterns**: Refrain from using easily guessable information like names, birthdays, or common words.
4. **Utilize Passphrases**: Create a sequence of random words or a sentence that's easy to remember but hard to guess.
5. **Regularly Update Passwords**: Change passwords periodically and avoid reusing them across different platforms.
6. **Employ Password Managers**: Tools like Bitwarden or NordPass can generate and store complex passwords securely.

Password Attacks

Understanding common attack methods emphasizes the importance of strong passwords:

- **Brute Force Attacks**: Systematically trying all possible combinations. Longer and more complex passwords exponentially increase the time required to crack them.
- **Dictionary Attacks**: Using a list of common words and phrases to guess passwords. Avoiding real words and common phrases mitigates this risk.

Conclusion

Creating strong, unique passwords is a fundamental step in safeguarding your digital presence. By understanding the elements that contribute to password strength and the methods attackers use, you can better protect your accounts and personal information.