Password Strength Analysis and Cybersecurity Assessment Report

**Task 6 Create a Strong Password and Evaluate Its Strength Cybersecurity Internship Project**

**Submitted by Sankabathula Abhishek**

# Executive Summary

This report presents a comprehensive analysis of password strength evaluation using the [PasswordMeter.com](http://passwordmeter.com/) online testing tool. Three passwords of varying complexity were tested to understand the relationship between password characteristics and security strength. The analysis reveals critical insights about password security fundamentals, attack resistance, and best practices for creating robust authentication credentials.

**Key Findings:**

 Password length is the most critical factor determining strength

 Character diversity across all four types (uppercase, lowercase, numbers, symbols) significantly improves security

 Consecutive patterns and predictable sequences substantially reduce password effectiveness

 A 13-character password with mixed character types achieved maximum security rating

# Testing Methodology

**Tool Selection:** [PasswordMeter.com](http://passwordmeter.com/)

[PasswordMeter.com](http://passwordmeter.com/) was selected for this analysis based on its comprehensive scoring system that evaluates multiple password characteristics:

 **Scoring Range**: 0 100% with color-coded strength indicators

 **Character Analysis**: Detailed breakdown of uppercase, lowercase, numbers, and symbols  **Pattern Recognition**: Detection of consecutive sequences and repetitive patterns

 **Improvement Feedback**: Specific recommendations for password enhancement  **Real-time Analysis**: Immediate scoring updates as passwords are modified

# Test Password Selection

Three passwords were systematically designed to demonstrate different strength levels:

**abc123#** 7 characters) - Basic complexity password

**Temp$2024** 9 characters) - Moderate strength with dictionary word

**SecStr0ng#2024** 13 characters) - Advanced strength password

# Detailed Test Results Analysis

# 

**Password 1 "abc123#" - Score: 44% Good**

**Character Composition:**

 Length: 7 characters

 Lowercase letters: 3 (abc)  Numbers: 3 123

 Symbols: 1 (#)

 Missing: Uppercase letters

**Scoring Breakdown:**

 **Additions**: 28 (characters) 6 (lowercase) 8 (numbers) 6 (symbols) 4 (middle symbols)

8 (requirements)

 **Deductions**: 6 (consecutive lowercase) 2 (consecutive numbers)  **Final Score**: 44%

**Security Assessment:**

 **Brute Force Resistance**: Approximately 2 hours to crack

 **Dictionary Vulnerability**: High due to predictable patterns

 **Overall Rating**: Poor - vulnerable to multiple attack methods

**Critical Weaknesses:**

 Insufficient length for modern security standards

 Contains obvious consecutive sequences (abc, 123  Missing uppercase letter character type

 Highly predictable pattern structure

**Password 2 "Temp$2024" - Score: 70% Strong**

**A screenshot of a computer

AI-generated content may be incorrect.**

**Character Composition:**

 Length: 9 characters

 Uppercase letters: 1 T

 Lowercase letters: 4 (emp)  Numbers: 4 2024

 Symbols: 1 $

**Scoring Breakdown:**

**Additions**: 36 (characters) 10 (uppercase) 6 (lowercase) 16 (numbers) 6 (symbols) 8 (middle symbols) 8 (requirements)

**Deductions**: 2 (repeat characters) 6 (consecutive lowercase) 6 (consecutive numbers)

 **Final Score**: 70%

**Security Assessment:**

 **Brute Force Resistance**: Approximately 3 years to crack

 **Dictionary Vulnerability**: Medium due to "Temp" dictionary word

 **Overall Rating**: Fair - resistant to brute force but vulnerable to dictionary attacks

**Notable Improvements:**

 Uses all four character types

 Better length than previous password

 Strategic symbol placement in middle position

**Remaining Weaknesses:**

 Contains common dictionary word "Temp"  Predictable year pattern "2024"

 Consecutive character sequences still present

**Password 3 "SecStr0ng#2024" - Score: 100% Very Strong)**

**A screenshot of a computer

AI-generated content may be incorrect.**

**Character Composition:**

 Length: 13 characters

 Uppercase letters: 3 S, S

 Lowercase letters: 6 (ectrng)  Numbers: 4 0, 2024

 Symbols: 1 (#)

**Scoring Breakdown:**

 **Additions**: 44 (characters) 18 (uppercase) 10 (lowercase) 32 (numbers) 6 (symbols)

16 (middle symbols) 8 (requirements)

 **Deductions**: 3 (repeat characters) 2 (consecutive uppercase) 14 (consecutive numbers)  **Final Score**: 100%

**Security Assessment:**

 **Brute Force Resistance**: Approximately 150,000 years to crack

 **Dictionary Vulnerability**: Low-Medium due to modified word patterns  **Overall Rating**: Good - strong resistance to most attack methods

**Strengths:**

Excellent length exceeding minimum requirements Maximum character diversity utilization

High entropy providing strong randomness Achieves optimal scoring thresh

**Minor Areas for Improvement:**

 Still contains recognizable word patterns  Year-based elements remain predictable

 Could benefit from complete randomization

# Comparative Analysis Strength Progression Insights

The three passwords demonstrate a clear progression in security effectiveness:

**Length Impact**: Moving from 7 to 13 characters increased the score by 56 percentage points

**Character Diversity**: Adding all four character types improved scoring significantly

**Pattern Avoidance**: Reducing consecutive sequences enhanced overall strength

# Attack Resistance Comparison

|  |  |  |  |
| --- | --- | --- | --- |
| Password | Brute Force Time | Dictionary Risk | Overall Security |
| abc123# | 2 hours | High | Poor |
| Temp$2024 | 3 years | Medium | Fair |
| SecStr0ng#2024 | 150,000 years | Low-Medium | Good |

**Password Attack Methods and Defense Strategies Common Attack Vectors**

1. **Brute Force Attacks**

 Systematic attempt of all possible character combinations

 Effectiveness decreases exponentially with password length

 Defense: Use passwords with 12+ characters and high character diversity

1. **Dictionary Attacks**

 Utilization of common word lists and predictable patterns

 Targets passwords based on real words and common substitutions  Defense: Avoid dictionary words and predictable modifications

1. **Hybrid Attacks**

 Combination of dictionary and brute force methodologies  Focuses on common words with number/symbol additions

 Defense: Use random character combinations rather than modified words

1. **Credential Stuffing**

 Exploitation of password reuse across multiple accounts  Uses breached credentials from other security incidents  Defense: Maintain unique passwords for each account

# Security Recommendations Based on Test Results

**Immediate Implementation Guidelines**

**Minimum Length Standard**: Establish 12-character minimum for all passwords

**Character Diversity Requirement**: Mandate use of all four character types

**Pattern Avoidance**: Eliminate consecutive sequences and predictable patterns

**Dictionary Word Restriction**: Avoid common words and their simple modifications

**Regular Testing Protocol**: Implement routine password strength validation

# Advanced Security Measures

**Password Manager Integration**: Utilize automated password generation and storage

**Multi-Factor Authentication**: Deploy additional security layers beyond passwords

**Passphrase Methodology**: Consider random word combinations for memorable security

**Breach Monitoring**: Implement continuous monitoring for compromised credentials

**Security Awareness Training**: Regular education on password best practices

# Contemporary Security Standards and Guidelines NIST 2025 Password Guidelines Alignment

The test results align with current National Institute of Standards and Technology recommendations:

 **Length Priority**: Emphasis on character count over complexity requirements  **Complexity Balance**: Character diversity important but secondary to length  **Expiration Policy**: Password changes only when compromise is detected

 **Blocklist Implementation**: Protection against commonly breached passwords

# Industry Best Practices Integration

Modern cybersecurity frameworks emphasize:

**Usability Focus**: Balancing security with user experience **Risk-Based Approach**: Tailoring requirements to threat levels

**Technology Integration**: Leveraging password managers and automated tools **Continuous Improvement**: Regular policy updates based on emerging threats

# Lessons Learned and Implementation Strategy

**Critical Success Factors**

**Length Dominance**: Password length provides the greatest security improvement

**Tool Utilization**: Strength testing tools provide valuable optimization feedback

**Pattern Recognition**: Understanding common weaknesses enables better password creation

**Holistic Approach**: Combining multiple security measures maximizes protection

# Organizational Implementation Roadmap

**Phase 1 Foundation Immediate)**

 Deploy password strength testing requirements  Establish minimum security standards

 Provide user education and training materials

**Phase 2 Enhancement 3 6 months)**

 Implement password manager solutions

 Enable multi-factor authentication systems  Develop breach monitoring capabilities

**Phase 3 Optimization 6 12 months)**

 Conduct regular security audits and assessments  Refine policies based on emerging threats

 Explore passwordless authentication technologies

# Conclusion

This comprehensive password strength analysis demonstrates the critical importance of systematic security evaluation using professional testing tools. The progression from a basic 44% strength password to a maximum 100% strength password illustrates how strategic character selection, length optimization, and pattern avoidance dramatically improve security effectiveness.