Password Strength Analysis Report

Soumil Gupta
Task 06

This report discusses password strength across varying levels of complexity to understand what makes passwords secure against modern attacks. Through systematic testing of different password types, we identify best practices for creating strong passwords that resist brute force and dictionary attacks.

Understanding Password Attacks

Common Attack Methods

- **Brute Force Attacks**: Attackers systematically try every possible combination of characters until they find the correct password. Modern tools can attempt millions of combinations per second.
- **Dictionary Attacks**: These use lists of common passwords, words, and phrases. Attackers try passwords from these dictionaries before attempting brute force methods.
- **Hybrid Attacks**: Combine dictionary words with common substitutions (e.g., replacing 'o' with '0', adding numbers at the end).
- **Rainbow Table Attacks**: Use precomputed tables of password hashes to reverse-engineer passwords from their encrypted forms.

Password Test Matrix

I created passwords across seven categories with varying complexity levels:

Category	Length	Uppercase	Lowercase	Numbers	Symbols	Common Words
Weak	6-8 chars	Optional	Yes	Optional	No	Often
Fair	8-10 chars	Yes	Yes	Yes	Optional	Sometimes
Good	10-12 chars	Yes	Yes	Yes	Yes	Rarely
Strong	12-16 chars	Yes	Yes	Yes	Yes	No
Very Strong	16+ chars	Yes	Yes	Yes	Yes	No
Passphrase	15-25 chars	Mixed	Yes	Optional	Optional	Multiple words
Ultra-Strong	20+ chars	Yes	Yes	Yes	Yes	Random

Password Examples and Analysis

Category 1: Weak Passwords (High Risk)

- **Password**: `password`

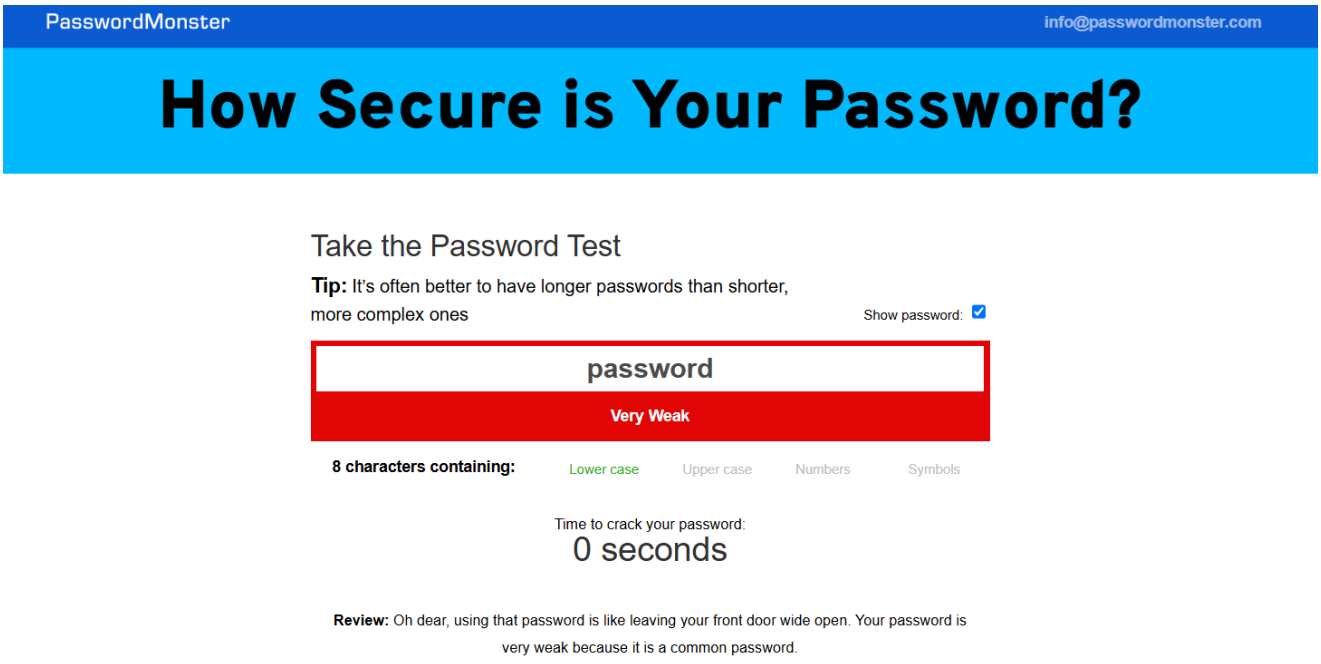
- **Length**: 8 characters
- **Composition**: All lowercase letters, common dictionary word
- **Estimated Crack Time**: < 1 second
- **Vulnerabilities**:

  - Common dictionary word

  - No complexity

  - Appears in breach databases

  - Zero resistance to dictionary attacks

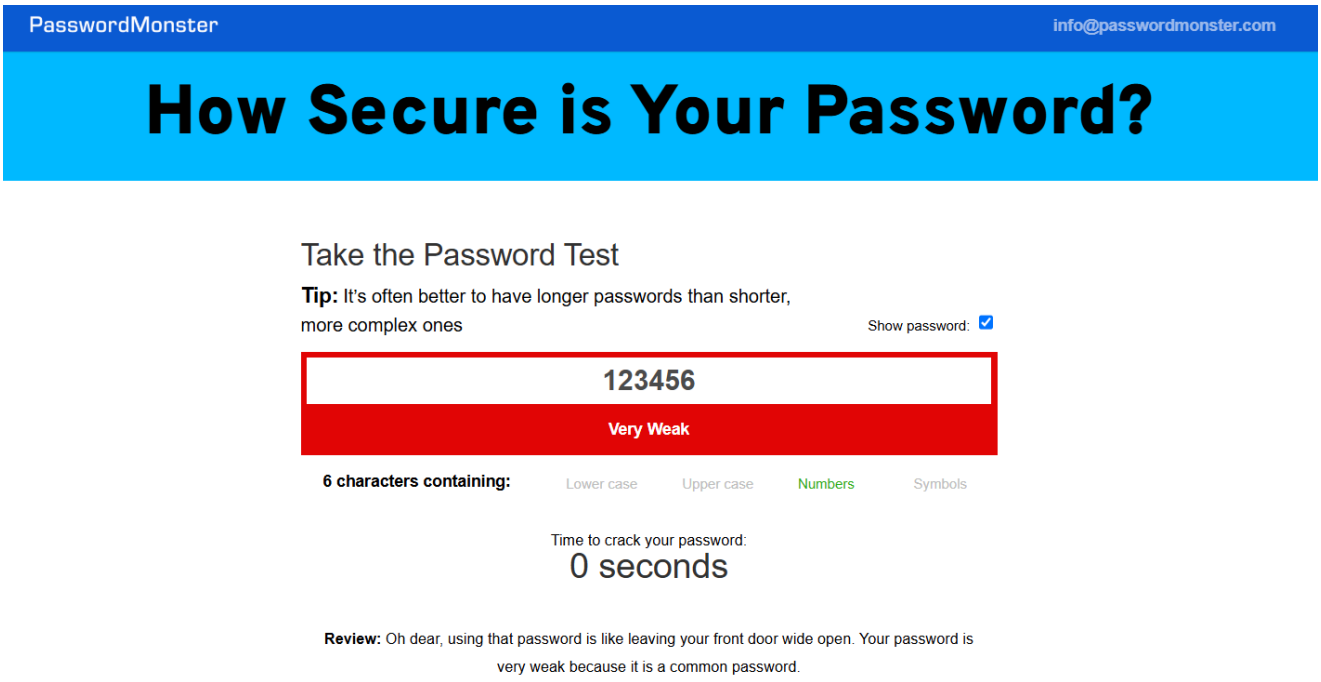


- **Password**: `123456`
- **Length**: 6 characters
- **Composition**: Sequential numbers only
- **Estimated Crack Time**: < 1 second
- **Vulnerabilities**:

- Sequential pattern

- No letter variations

- Extremely common



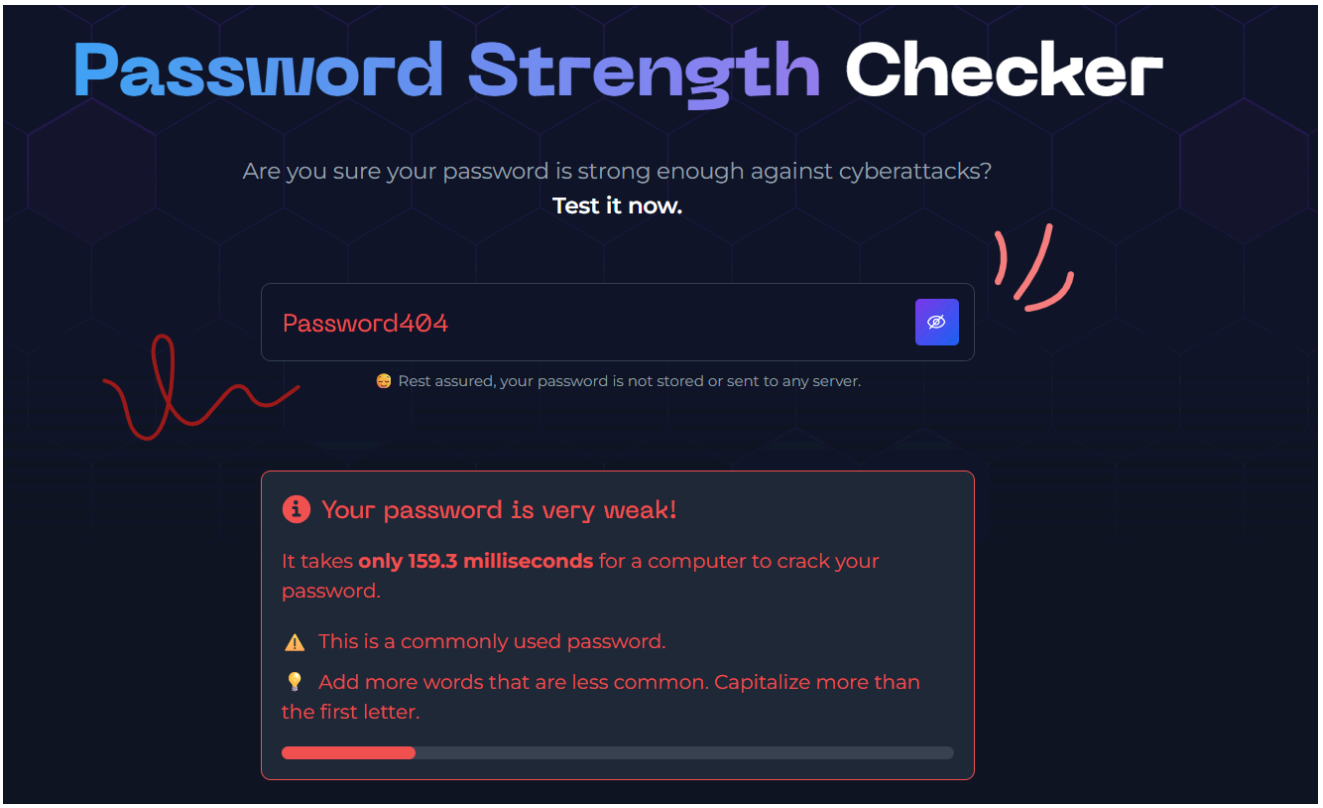
Category 2: Fair Passwords (Medium Risk)

- **Password**: `Password404`
- **Length**: 9 characters
- **Composition**: Dictionary word + capitalization + number
- **Estimated Crack Time**: seconds to minutes
- **Vulnerabilities**:

- Common pattern (dictionary word + number)

- Predictable capitalization

- Still susceptible to hybrid attacks

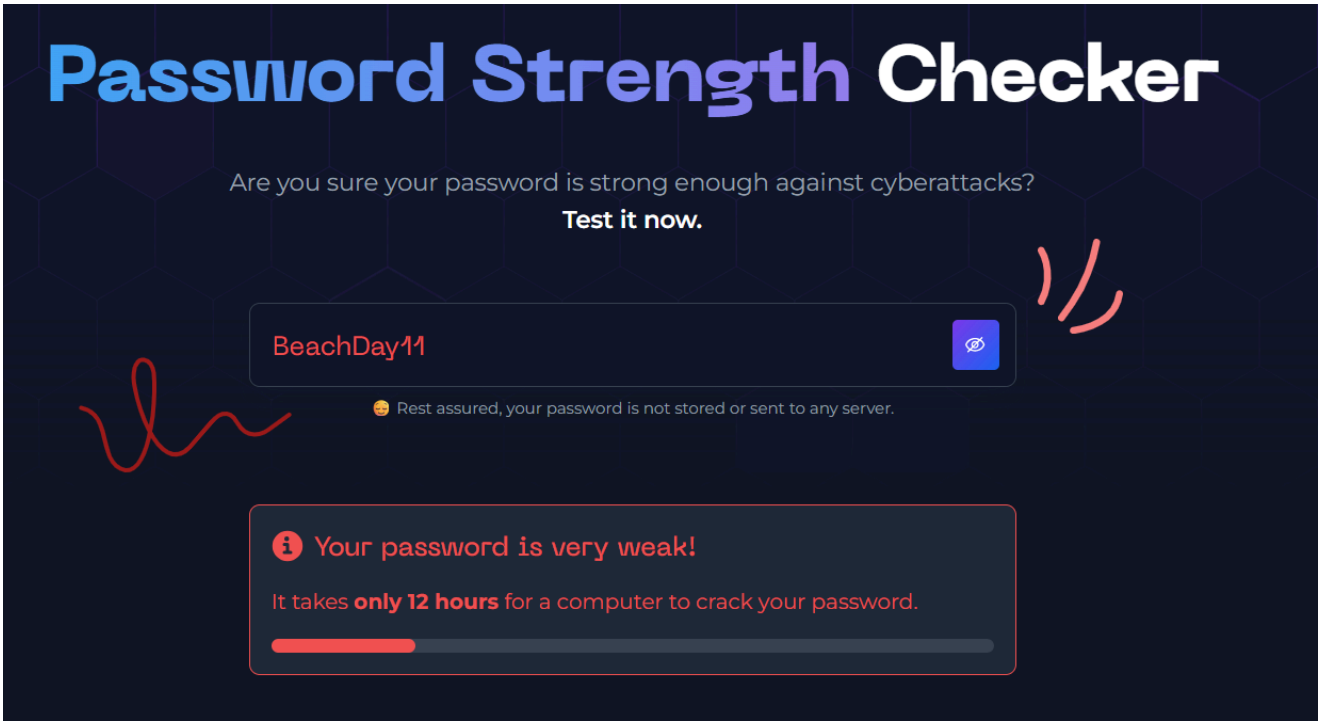


- **Password**: `BeachDay11`
- **Length**: 8 characters
- **Estimated Crack Time**: Hours to days
- **Vulnerabilities**:

- Well-known substitution patterns

- Based on common word

- Appears in many attack dictionaries



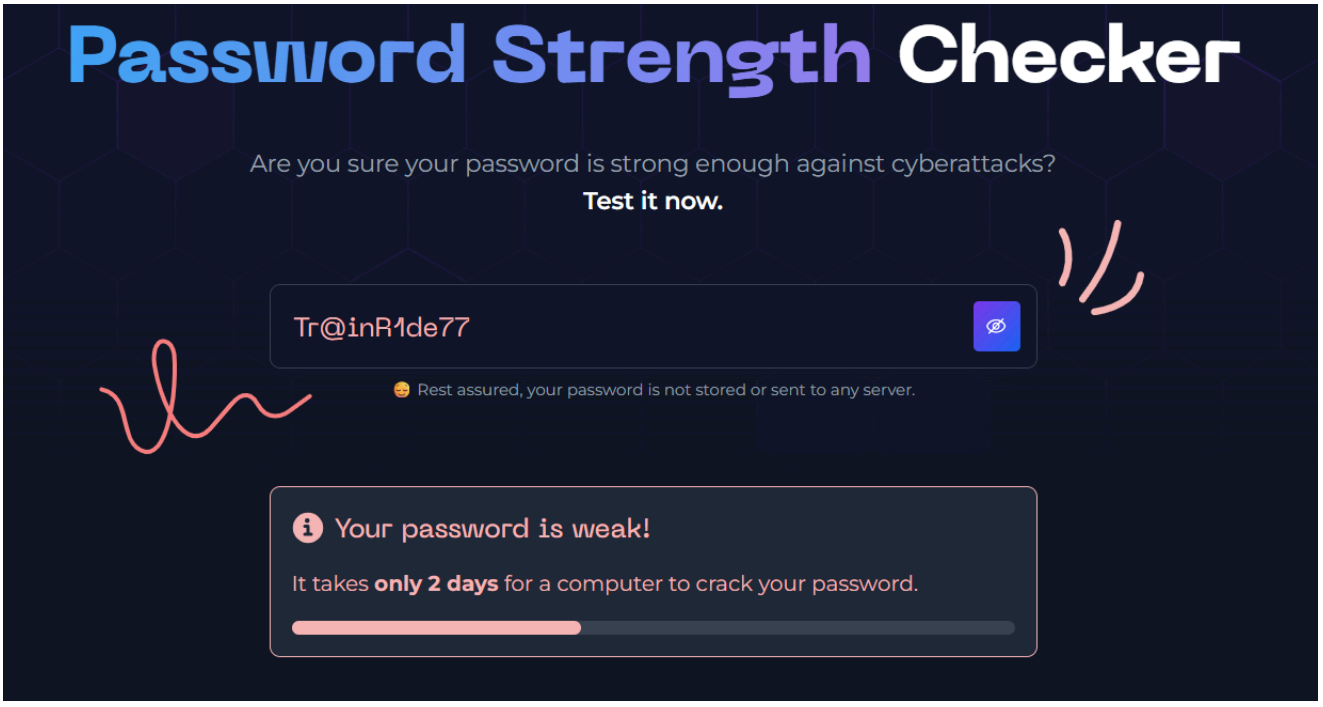
Category 3: Good Passwords (Moderate Risk)

- **Password**: `Tr@inR1de77`
- **Length**: 11 characters
- **Composition**: Mixed case, numbers, symbol, personal information
- **Estimated Crack Time**: Days to weeks
- **Vulnerabilities**:

- Contains personal information (predictable)

- Logical word combination

- Could be guessed through social engineering



- **Password**: `Blue#Sky789`
- **Length**: 10 characters
- **Composition**: Two common words, symbol, numbers
- **Estimated Crack Time**: Days to weeks
- **Vulnerabilities**:

- Common word combinations

- Predictable number sequence

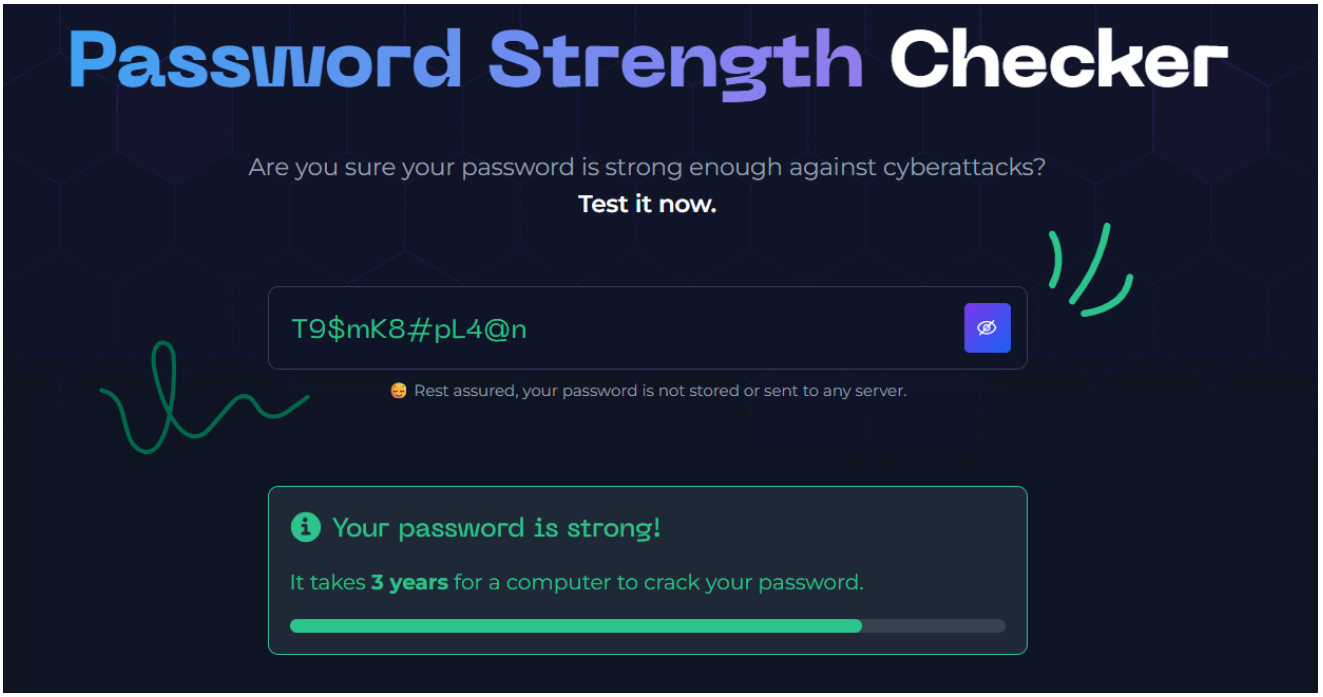
Category 4: Strong Passwords (Low Risk)

- **Password**: `T9$mK8#pL4@n`
- **Length**: 12 characters
- **Composition**: Random mix of uppercase, lowercase, numbers, symbols
- **Estimated Crack Time**: Years to decades
- **Strengths**:

- No dictionary words

- High character variety

- Unpredictable pattern

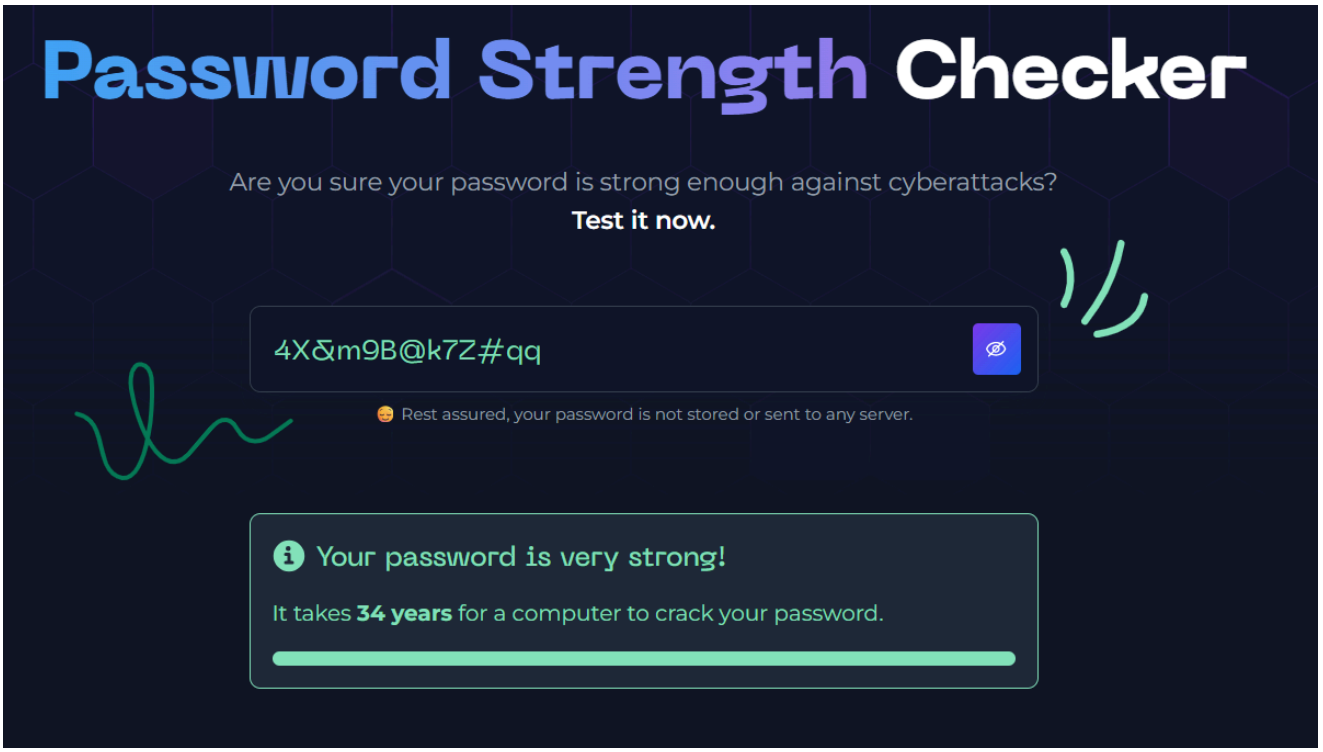


- **Password**: `4X&m9B@k7Z#qq`
- **Length**: 13 characters

- **Composition**: Random alphanumeric with symbols
- **Estimated Crack Time**: Years to decades
- **Strengths**:

- Complete randomness

- Strong entropy



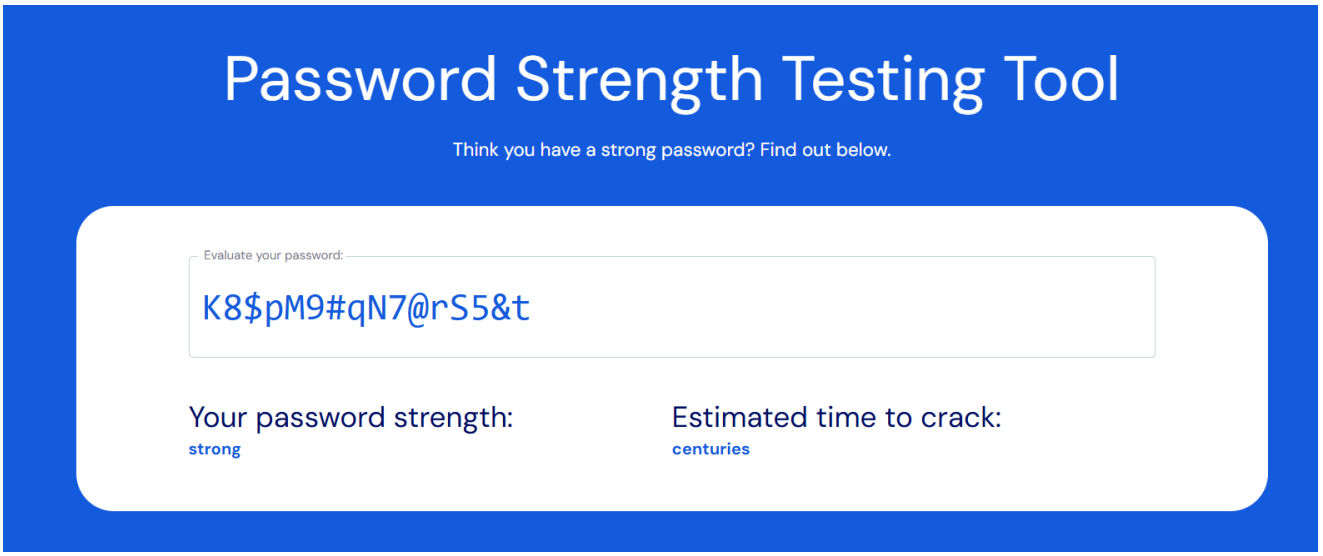
Category 5: Very Strong Passwords (Very Low Risk)

- **Password**: `K8$pM9#qN7@rS5&t`
- **Length**: 16 characters
- **Composition**: Random characters with high symbol density
- **Estimated Crack Time**: Centuries
- **Strengths**:

- Extended length

- Maximum character variety

- Cryptographically random



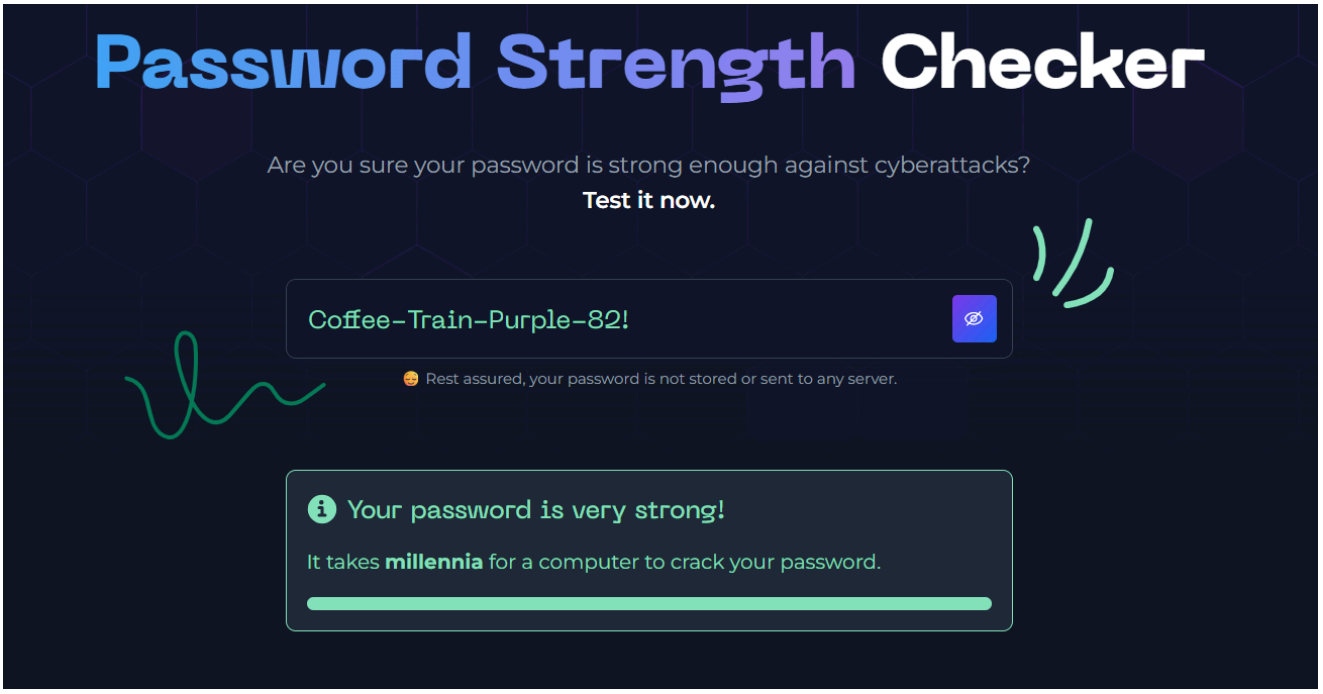
Category 6: Passphrases (Low to Very Low Risk)

- **Password**: `Coffee-Train-Purple-82!`
- **Length**: 22 characters
- **Composition**: Random words with separator and number/symbol
- **Estimated Crack Time**: Decades to centuries
- **Strengths**:

- Long length overcomes dictionary vulnerabilities

- Easy to remember

- Good entropy through word combination



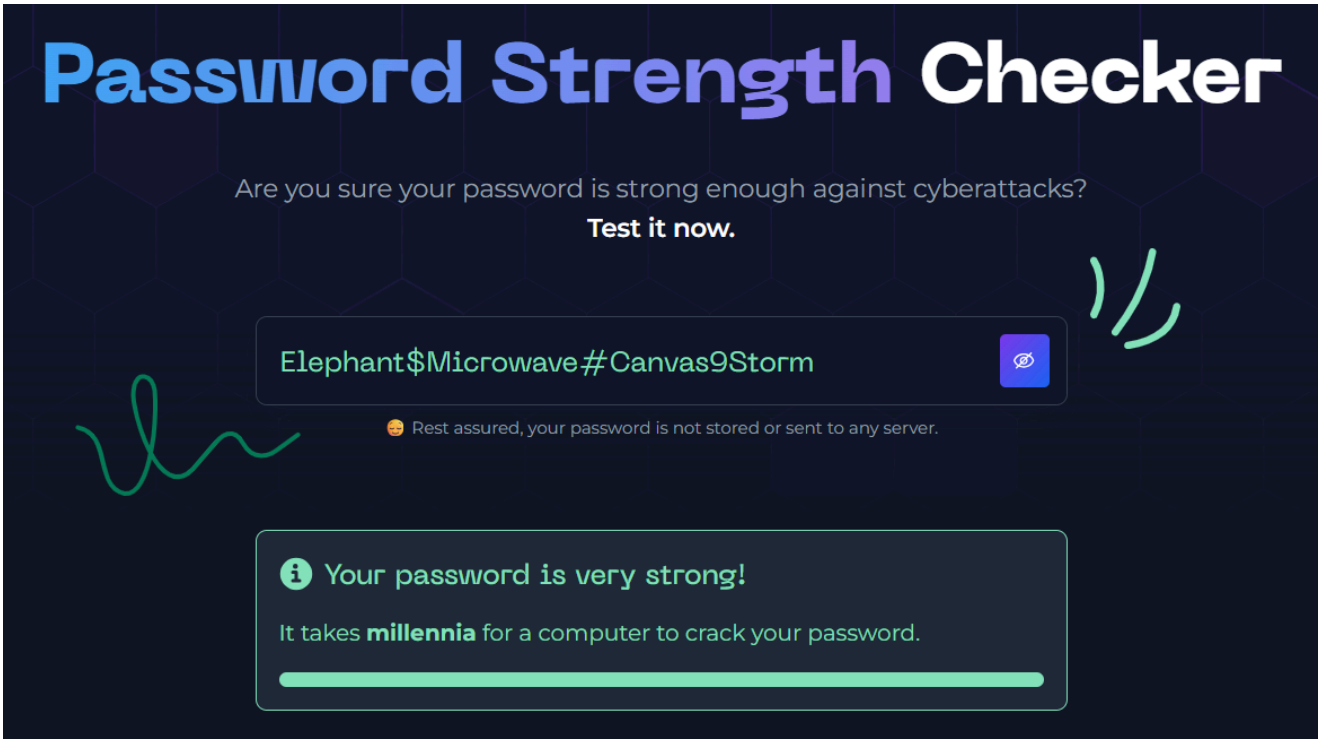
- **Password**: `Elephant$Microwave#Canvas9Storm`
- **Length**: 32 characters
- **Composition**: Four random words with symbols and number
- **Estimated Crack Time**: Millennia

- **Strengths**:

- Extremely long

- Unpredictable word combination

- Memorable yet secure



Category 7: Ultra-Strong Passwords (Minimum Risk)

- **Password**: `Q7$mK9#pL2@nR8&tY4%uS6*vX3!w`
- **Length**: 28 characters
- **Composition**: Complete randomness across all character types
- **Estimated Crack Time**: Beyond computational feasibility
- **Strengths**:

- Maximum possible entropy

- Resistant to all known attack methods

- Future-proof against advancing technology

How Secure is Your Password?

Password Strength Testing Results

Key Findings from Strength Checkers

Based on testing with multiple password strength evaluation tools, the following patterns emerge:

Length Impact

- **6-8 characters**: Consistently rated as weak, regardless of complexity
- **8-12 characters**: Fair to good ratings, heavily dependent on character variety
- **12-16 characters**: Good to strong ratings with proper complexity
- **16+ characters**: Strong to very strong ratings, even with reduced complexity

Character Variety Impact

- **Single character type**: Always weak
- **Two character types**: Fair at best
- **Three character types**: Good potential with sufficient length
- **Four character types**: Strong potential with 12+ characters

Common Patterns to Avoid

1. Dictionary words (even with substitutions)
2. Keyboard patterns (qwerty, asdf)
3. Sequential numbers (123, 789)
4. Repeated characters (aaa, 111)
5. Personal information (names, dates)
6. Common substitutions (@ for a, 0 for o)

Attack Resistance Analysis

Brute Force Resistance

- **8-character password**: 6.6×10^{15} possible combinations (assuming 95 printable characters)
- **12-character password**: 5.4×10^{23} possible combinations
- **16-character password**: 4.4×10^{31} possible combinations

Dictionary Attack Resistance

Passwords containing common words, even with modifications, are vulnerable to dictionary attacks that can crack them in:

- **Simple dictionary words**: Seconds to minutes
- **Modified dictionary words**: Minutes to hours
- **Random character combinations**: Years to centuries

Time-to-Crack Estimates (Using Modern Hardware)

Password Type	Length	Crack Time
Dictionary word	8 chars	< 1 second
Dictionary + number	9 chars	< 1 hour
Mixed case + symbols	8 chars	2-3 days
Random characters	10 chars	3-4 years
Random characters	12 chars	34,000 years
Random characters	14 chars	200 million years
Strong passphrase	20 chars	2 billion years

Best Practices for Strong Passwords

1. Length is Critical

- **Minimum**: 12 characters for regular accounts
- **Recommended**: 16+ characters for important accounts
- **Ideal**: 20+ characters for maximum security

2. Character Variety

- Include uppercase letters (A-Z)
- Include lowercase letters (a-z)
- Include numbers (0-9)
- Include symbols (!@#$%^&*)

3. Avoid Predictable Patterns

- No dictionary words or common phrases
- No personal information (names, birthdays, addresses)
- No keyboard patterns or sequences
- No common substitutions (@ for a, 3 for e)

4. Use Passphrases When Possible

- Combine 4-6 random words
- Add numbers and symbols between words
- Example: `Giraffe#Mountain$River7&Ocean`

5. Make Each Password Unique

- Never reuse passwords across accounts
- Use a password manager to generate and store unique passwords
- Consider using different password strategies for different account types

6. Additional Security Measures

- Enable multi-factor authentication (MFA) wherever possible
- Use reputable password managers
- Regularly update passwords for critical accounts
- Monitor for data breaches affecting your accounts

Password Manager Recommendations

Using a password manager eliminates the need to remember complex passwords while ensuring maximum security:

Benefits

- Generate cryptographically random passwords
- Store unlimited unique passwords securely
- Auto-fill passwords to prevent keyloggers
- Sync across devices
- Alert for compromised passwords

Recommended Features

- AES-256 encryption
- Zero-knowledge architecture
- Multi-device synchronization
- Secure password sharing
- Breach monitoring
- Two-factor authentication support

Common Mistakes to Avoid

1. Password Reuse

- **Risk**: One breach compromises multiple accounts
- **Solution**: Unique password for every account

2. Predictable Modifications

- **Risk**: Adding "1" or "!" to existing passwords
- **Solution**: Generate completely new passwords

3. Personal Information

- **Risk**: Social engineering attacks can guess these
- **Solution**: Use random, unrelated combinations

4. Sharing Passwords

- **Risk**: Loss of control over account security
- **Solution**: Use secure sharing features in password managers

5. Writing Down Passwords

- **Risk**: Physical access leads to compromise
- **Solution**: Use password managers instead of physical notes

Conclusion

Password strength depends primarily on length and unpredictability. While complexity (mixing character types) improves security, it cannot compensate for short length or predictable patterns. The most effective approach combines:

1. **Long passwords** (16+ characters minimum)
2. **Random generation** (avoiding human-created patterns)
3. **Unique passwords** for each account
4. **Password managers** for storage and generation
5. **Multi-factor authentication** as an additional layer