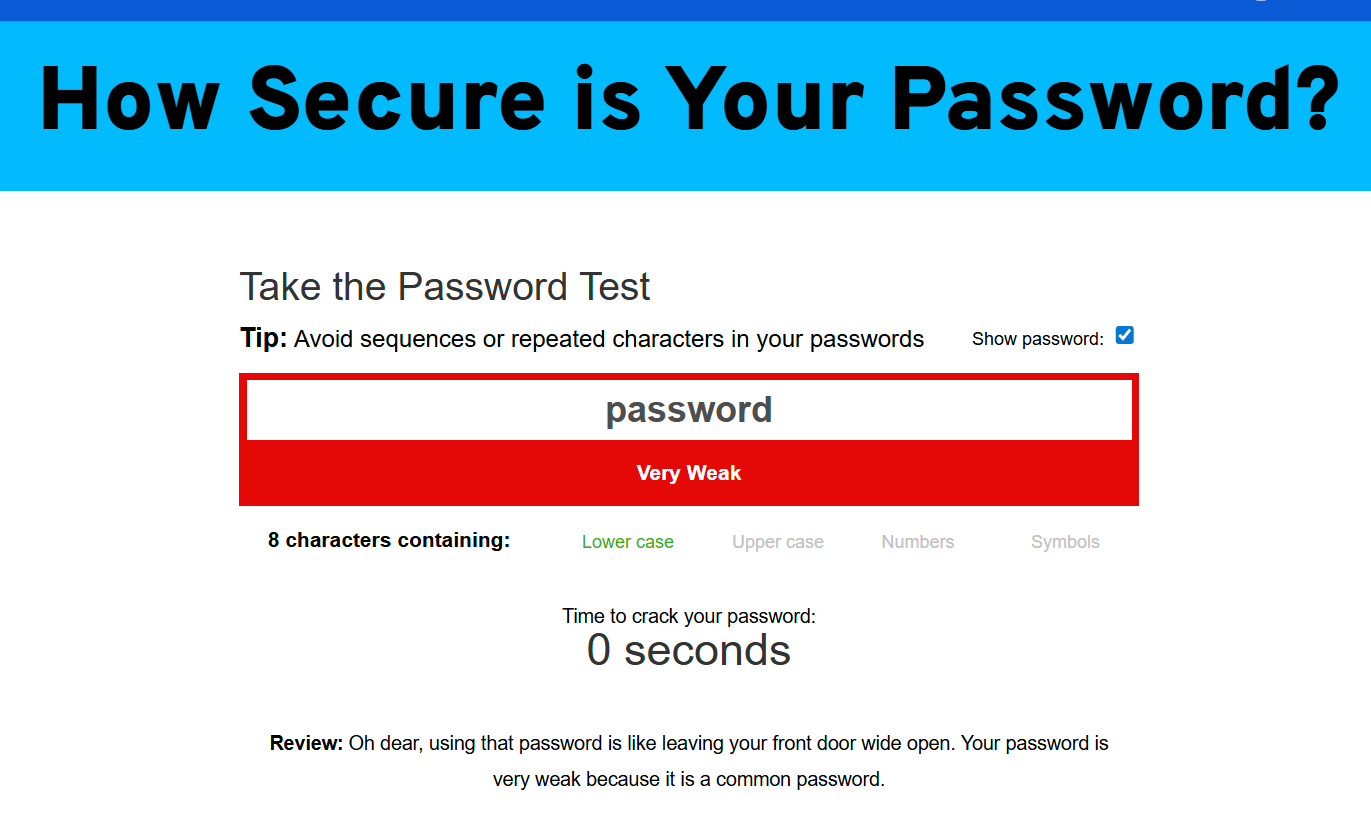
TASK –6

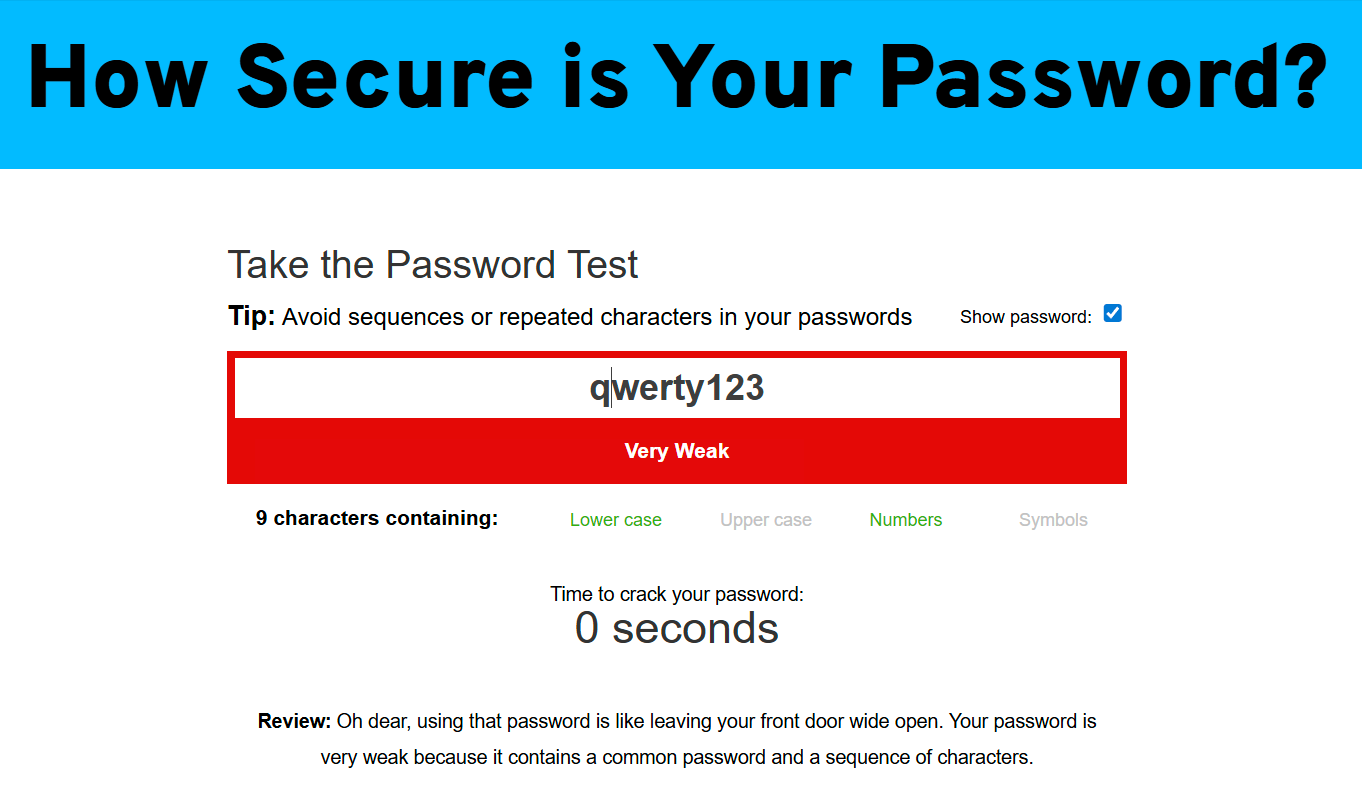
Analysis of Password Strength



The image is a report from a password strength checker after testing the password (password).

* **Password Tested:** password
* **Strength Rating:** **Very Weak**
* **Estimated Time to Crack:** **0 seconds**
* **Password Characteristics:** 8 characters, containing only lowercase letters.
* **Detailed Review:** "Oh dear, using that password is like leaving your front door wide open. Your password is very weak because it is a common password."

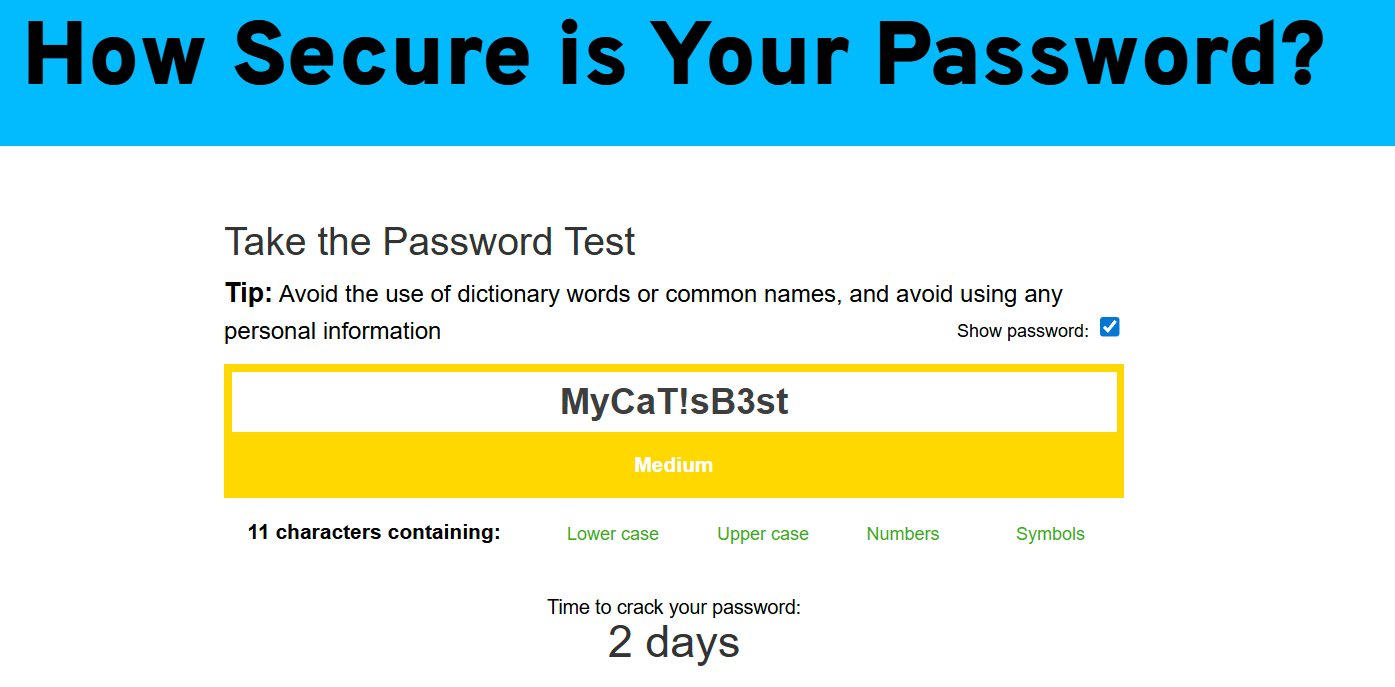
**In summary, the tool reports that the password (password) offers no security because it is one of the most common passwords in the world and can be guessed instantly by any attacker.**



The provided image shows the results from the password strength checker for the password qwerty123.

* **Password Tested:** qwerty123
* **Strength Rating:** **Very Weak**
* **Estimated Time to Crack:** **0 seconds**
* **Password Characteristics:** 9 characters, containing lowercase letters and numbers.
* **Detailed Review:** "Oh dear, using that password is like leaving your front door wide open. Your password is very weak because it contains a common password and a sequence of characters."

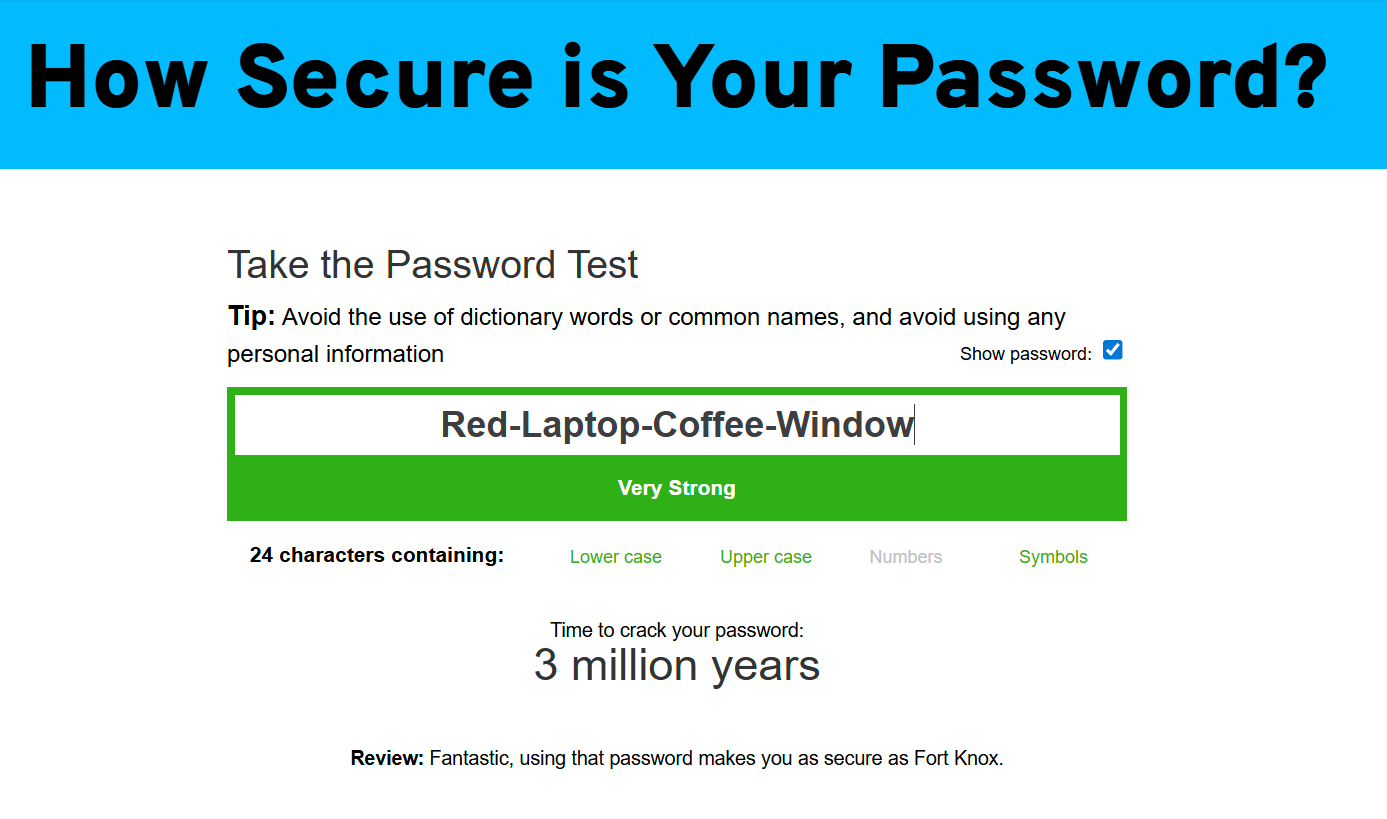
**In summary, the tool reports that the password qwerty123 is extremely insecure because it is based on a predictable keyboard sequence, making it one of the first things an attacker's software would try.**



This image provides the security analysis for the password MyCaT!sB3st.

* **Password Tested:** MyCaT!sB3st
* **Strength Rating:** **Medium**
* **Estimated Time to Crack:** **2 days**
* **Password Characteristics:** 11 characters, containing lowercase letters, uppercase letters, numbers, and symbols.

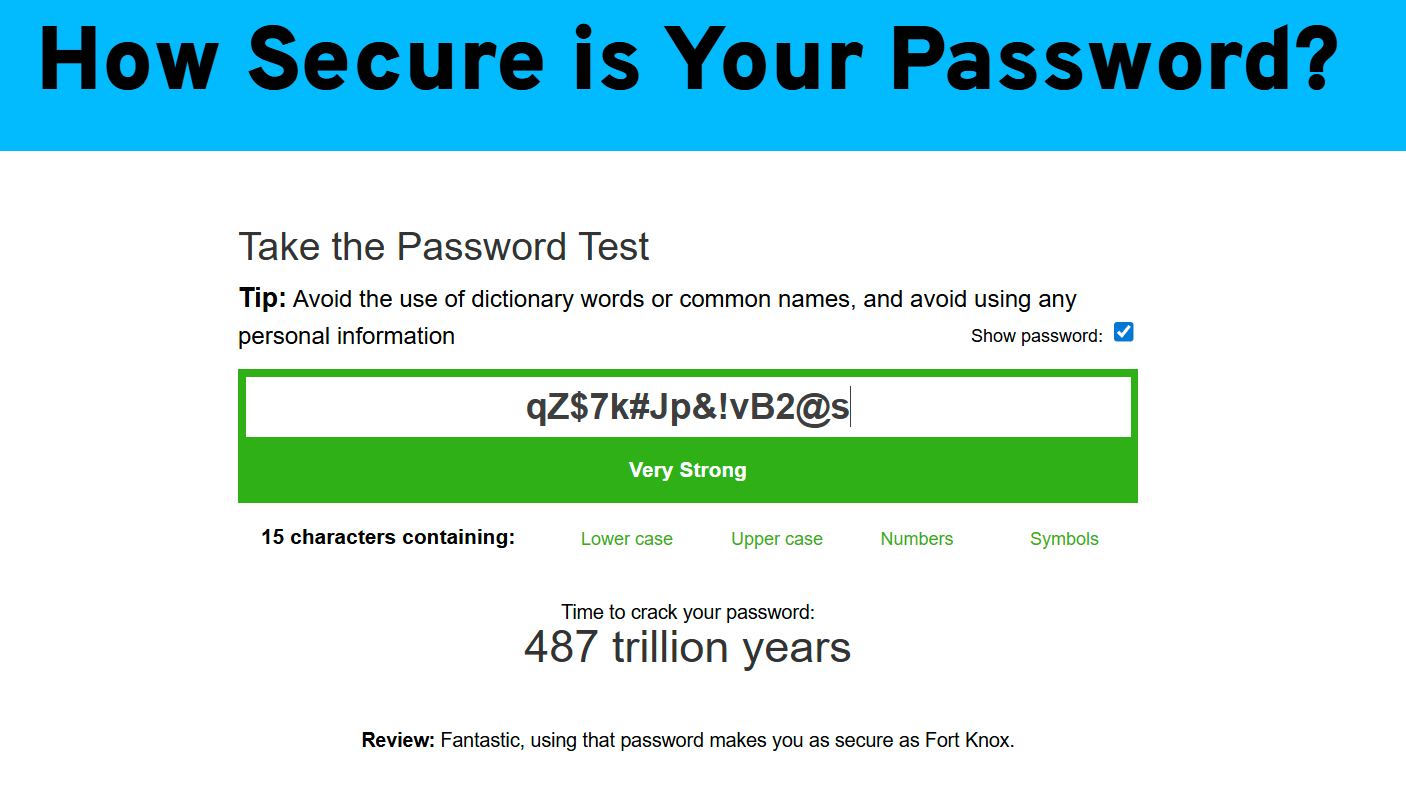
**In summary, the tool rates this password as "Medium." While it is significantly better than the previous examples because it uses a mix of all character types, its underlying pattern ("My cat is best") and common substitutions (like ! for i and 3 for e) make it vulnerable to more advanced cracking techniques, hence the relatively short crack time of 2 days.**



Here is the information from the security analysis of the passphrase Red-Laptop-Coffee-Window.

* **Password Tested:** Red-Laptop-Coffee-Window
* **Strength Rating:** **Very Strong**
* **Estimated Time to Crack:** **3 million years**
* **Password Characteristics:** 24 characters, containing lowercase and uppercase letters.
* **Detailed Review:** "Fantastic, using that password makes you as secure as Fort Knox."

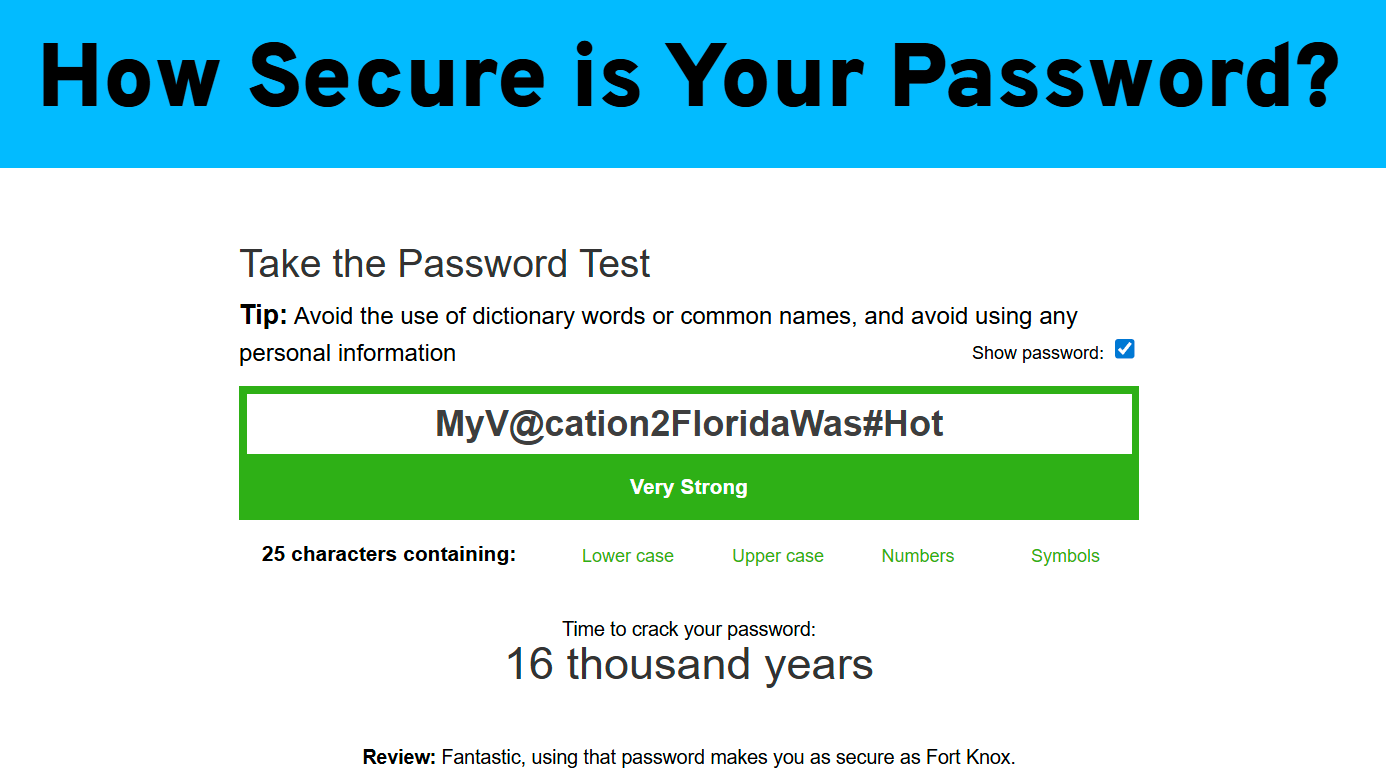
**In summary, this result powerfully demonstrates the security of using a long passphrase. The password's exceptional strength comes almost entirely from its extreme length (24 characters), which makes it computationally impossible for an attacker to guess using brute-force methods.**



Here is the security analysis from your series, for the password qZ$7k#Jp&!vB2@s.

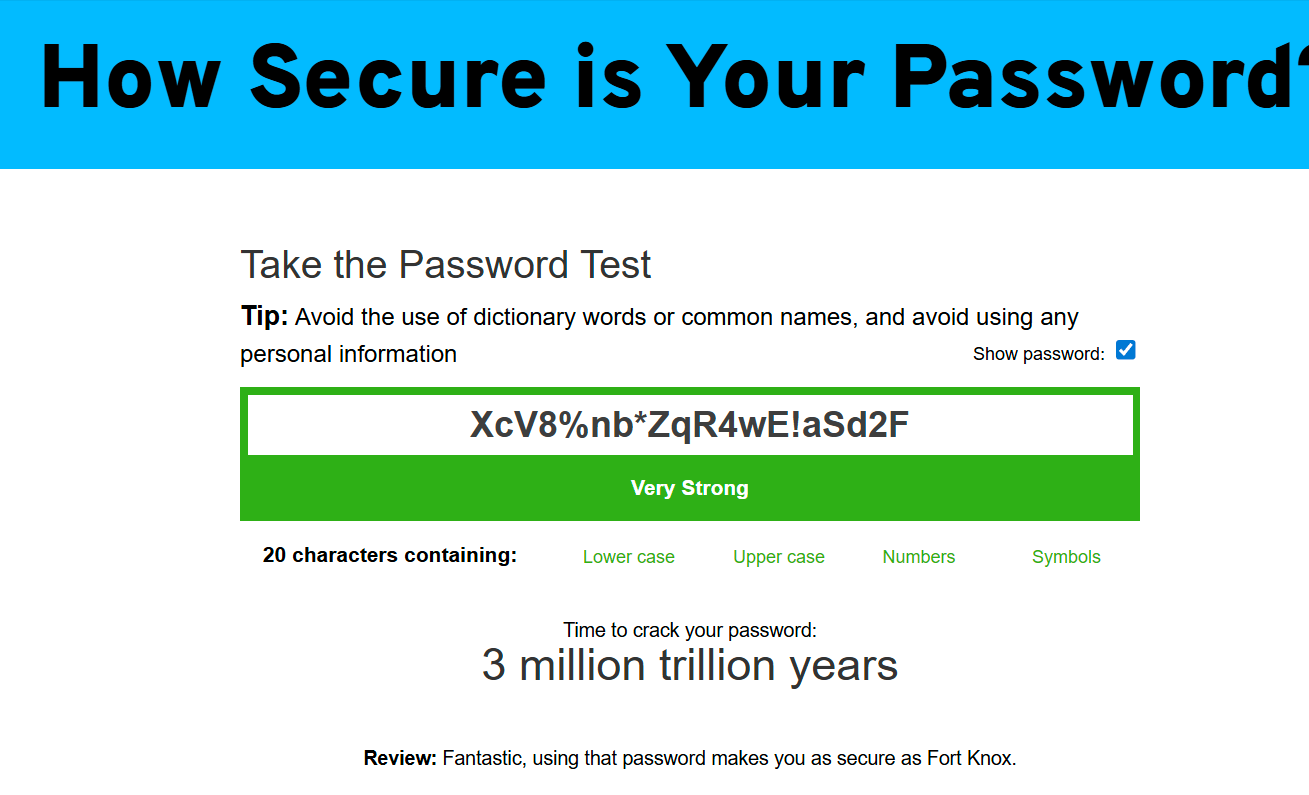
* **Password Tested:** qZ$7k#Jp&!vB2@s
* **Strength Rating:** **Very Strong**
* **Estimated Time to Crack:** **487 trillion years**
* **Password Characteristics:** 15 characters, containing lowercase letters, uppercase letters, numbers, and symbols.
* **Detailed Review:** "Fantastic, using that password makes you as secure as Fort Knox."

**In summary, this password achieves the highest level of security. Its strength comes from the ideal combination of great length (15 characters) and true randomness using all four character types. This makes it invulnerable to dictionary, pattern-based, and brute-force attacks.**

 Here is the information from the security analysis of the password MyV@cation2FloridaWas#Hot.

* **Password Tested:** MyV@cation2FloridaWas#Hot
* **Strength Rating:** **Very Strong**
* **Estimated Time to Crack:** **16 thousand years**
* **Password Characteristics:** 25 characters, containing lowercase letters, uppercase letters, numbers, and symbols.
* **Detailed Review:** "Fantastic, using that password makes you as secure as Fort Knox."

**In summary, this password is rated as very strong because it effectively combines the great length of a passphrase with embedded, unpredictable complexity (@, 2, #). This hybrid approach makes it highly resistant to all common forms of password attacks.**

 Here is the security analysis from the screenshot for the randomly generated password XcV8%nb\*ZqR4wE!aSd2F.

* **Password Tested:** XcV8%nb\*ZqR4wE!aSd2F
* **Strength Rating:** **Very Strong**
* **Estimated Time to Crack:** **3 million trillion years**
* **Password Characteristics:** 20 characters, containing lowercase letters, uppercase letters, numbers, and symbols.
* **Detailed Review:** "Fantastic, using that password makes you as secure as Fort Knox."

**In summary, this password receives an exceptionally high rating due to its two main strengths: its long length (20 characters) and its complete randomness. The use of all four character types in an unpredictable sequence maximizes its security, making it invulnerable to all modern password cracking techniques.**

**Identify best practices for creating strong passwords.**

**Example Best Practices you might identify:**

* **Length is Key:** As seen with the passphrase, a longer password is significantly stronger, even if it's made of simple words.
* **Complexity Matters:** A mix of uppercase letters, lowercase letters, numbers, and symbols drastically increases strength.
* **Avoid Predictability:** Passwords based on common words (password), keyboard patterns (qwerty), or simple substitutions (P@ssword1) are weak because attackers' tools specifically look for these.
* **Use Passphrases:** A sequence of 4-5 unrelated words is often easier to remember than a complex 12-character password and can be much more secure due to its length.

### **Key Lessons Learned from the Evaluation**

* I learned that a very long password made of simple words (a passphrase) can be much stronger than a short, complex one, because length is the most important factor for security.
* I realized that simply capitalizing the first letter and adding "123!" at the end is a common and predictable pattern that doesn't add as much security as I thought.
* I was surprised that even password like (MyCaT!sB3st) offers limited protection, as modern hacking tools are programmed to check for these common substitutions.
* I learned that the weakest passwords are cracked instantly because they are on a pre-made list. A strong password's main job is to be unique enough to not be on any list.
* I learned that a "Medium" strength rating can be misleading. A password that can be cracked in a few days is not safe for important accounts, so I will always aim for a "Strong" or "Very Strong" rating.
* I realized there are two valid paths to top-tier security: a long passphrase for memorable passwords (like a master password) and a shorter, completely random string for everything else.
* My key takeaway is that using a random password generator and a password manager is the best and most practical option for security, as it's impossible to remember dozens of truly strong passwords.

Of course. Here is a comprehensive list that includes the explanations for Brute-Force and Dictionary attacks you mentioned, followed by the additional common attacks.

### **Common Password Attacks**

This section provides context for *why* password strength is so important by explaining the methods attackers use to compromise accounts.

#### **1. Brute-Force Attack**

* **What It Is:** An attack where an attacker's software tries every single possible combination of characters until it finds the correct password.
* **How It Works:** This is the digital equivalent of trying every key on a giant keychain. The software starts with "a", then "b", then "c", continuing through "aa", "ab", and so on, until it guesses the correct combination. While simple, it can be effective against short passwords.
* **How Complexity Helps:** A longer password with more character types (lowercase, uppercase, numbers, symbols) exponentially increases the total number of possible combinations. The number of possibilities is calculated as CL, where L is the password length and C is the number of characters in the set (e.g., 26 for lowercase, ~90 with all types). A long, complex password makes a brute-force attack take too long to be practical (e.g., thousands or millions of years).

#### **2. Dictionary Attack**

* **What It Is:** A more targeted attack where the software tries words from a pre-compiled list, or "dictionary."
* **How It Works:** Instead of trying every combination, this attack uses a list containing millions of common passwords, real words, names, and simple patterns. Advanced dictionary attacks will also try common substitutions (e.g., o -> 0, e -> 3) and add common endings like 123 or !. This is why password and Password123! are cracked instantly.
* **How Complexity Helps:** Using truly random characters and avoiding real words (like in qZ$7k#Jp&!vB2@s) makes your password immune to a dictionary attack, as it simply won't be on the attacker's list.

#### **3. Credential Stuffing**

* **What It Is:** An attack where usernames and passwords stolen from one data breach are used to gain access to other unrelated services.
* **How It Works:** Attackers obtain large lists of leaked email/password pairs from data breaches. They then use automated bots to "stuff" these credentials into high-value targets like banking and email sites, knowing that many people reuse the same password everywhere.
* **How to Defend Against It:**
  + **Use a unique password for every single account.** This is the most crucial defense.
  + Enable Multi-Factor Authentication (MFA) wherever possible.

#### **4. Phishing**

* **What It Is:** A social engineering attack where a user is tricked into voluntarily revealing their password.
* **How It Works:** An attacker sends a deceptive email that looks like it's from a legitimate source (e.g., your bank). The message creates a sense of urgency ("Your account is locked!") and includes a link to a fake login page. When the user enters their credentials, the attacker captures them.
* **How to Defend Against It:**
  + Be suspicious of unsolicited emails. Check the sender's address carefully.
  + Never click links in suspicious emails; go to the website directly by typing its address.

#### **5. Password Spraying**

* **What It Is:** An attack that tries a small list of common passwords against a large number of user accounts.
* **How It Works:** Instead of trying 10,000 passwords for one user (which would cause a lockout), the attacker tries one common password, like Winter2025!, against *every* user in a company. This slow approach avoids detection and finds the weakest links in an organization.
* **How to Defend Against It:**
  + Avoid using weak, common, or seasonal passwords.
  + Enforce strong password policies that ban common passwords.

**Summarize how password complexity affects security.**

Password complexity is the most critical measure of its strength, determining how long an attacker would need to guess it. A complex password builds layers of defense by making the total number of possible combinations astronomically large. This is achieved through three key elements.

### **Length: The Exponential Defender**

**Length** is the single most important factor. Each character you add doesn't just add to the password's strength; it multiplies it exponentially. This is the primary defense against **brute-force attacks**, where a computer tries every possible combination.

* An 8-character password might be cracked in hours.
* A 12-character password can take centuries.
* A 16+ character password can take trillions of years.

Think of it like a combination lock: a 3-digit lock has 1,000 possibilities. A 6-digit lock has 1,000,000 possibilities—a thousand times harder to crack, despite being only twice as long.

### **Character Variety: Multiplying the Possibilities**

Using a wide **variety of characters**—uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols (!@#$)—makes a password significantly stronger. It increases the pool of options for each character slot from 26 (just lowercase) to over 90. This forces an attacker's computer to do much more work for every single guess.

### **Unpredictability: Avoiding Shortcuts**

**Unpredictability** is the defense against intelligent attacks, like **dictionary attacks**. These attacks use pre-made lists of common words, phrases, and leaked passwords. By avoiding real words, keyboard patterns (like qwerty), and predictable substitutions (like P@ssw0rd), you make these lists useless. True randomness forces an attacker to rely on the much slower brute-force method, which has already been made impossible by your password's length and character variety.

In short, a secure password combines all three elements: it is **long**, uses **varied character types**, and is **unpredictable**. A failure in any one of these areas creates a vulnerability an attacker can exploit. The most effective way to achieve this trifecta is by using a **password manager** to generate and store strong, random passwords for all your accounts.