## Password Security Workshop (Deep Detail with Examples)

### ****Create Multiple Passwords with Varying Complexity****

| **Password** | **Description** |
| --- | --- |
| **apple123** | **Simple, predictable** |
| **App1e$2024** | **Mixed case, digits, symbol, year** |
| **G@l@xy!Drive#998** | **Complex, symbols & uncommon words** |
| **2^TmB&R8pzK@wz9** | **Randomized, high entropy** |
| **Summer#Vacation2025** | **Human-readable but lengthy** |

### ****Use Character and Length Variations****

**To improve security, use:**

* **Uppercase letters: A-Z**
* **Lowercase letters: a-z**
* **Numbers: 0-9**
* **Symbols: !@#$%^&\*()\_+**
* **Length: ≥ 12 characters recommended**

**Combine: T1m3$hift2025! is better than timetime2025.**

### ****Test on a Password Strength Checker****

**Use tools like:**

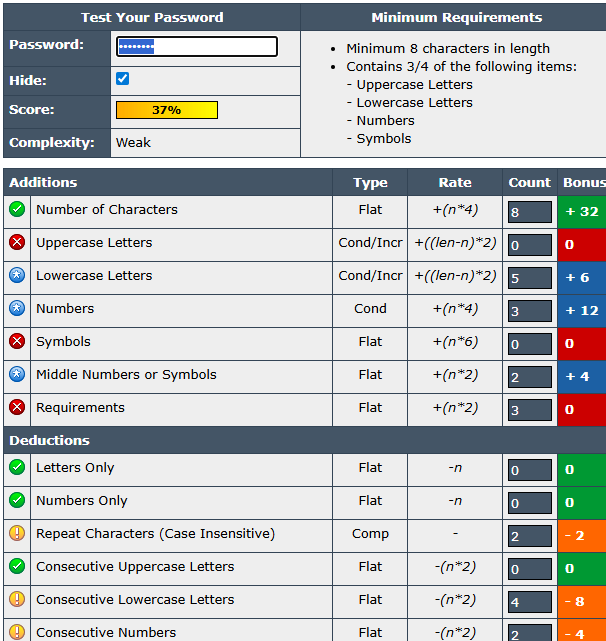
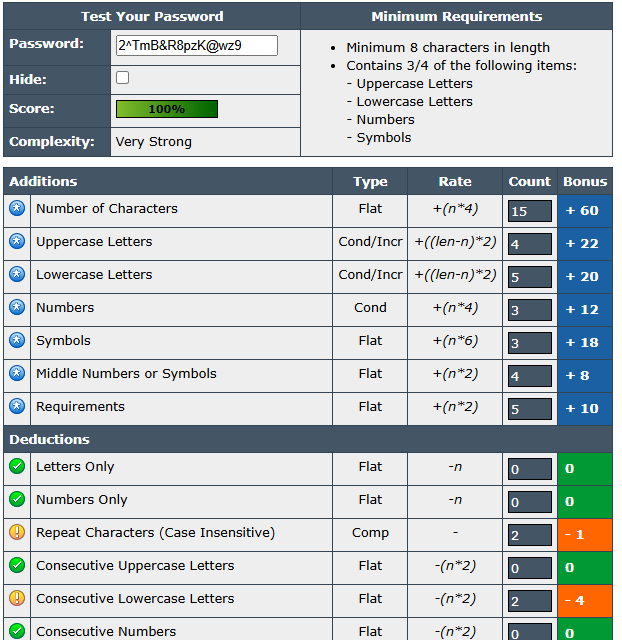
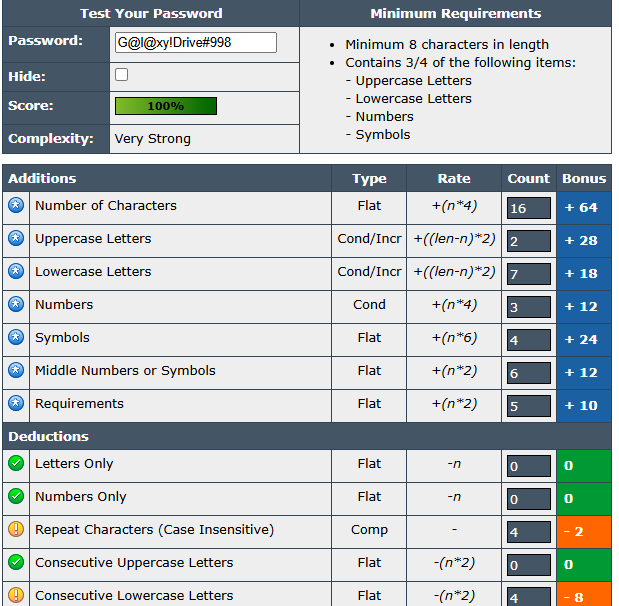
**Kaspersky Password Checker**

**Have I Been Pwned**

**NordPass Strength Meter**

**Local zxcvbn (by Dropbox): entropy-based strength checker**

**Results Example:**



| **Password** | **Strength (score)** | | **Time to Crack** |
| --- | --- | --- | --- |
| **apple123** | | **Weak (1/5)** | **<1 second (dictionary)** |
| **App1e$2024** | **Moderate (3/5)** | | **~2 hours (offline brute)** |
| **G@l@xy!Drive#998** | **Strong (4/5)** | | **Months (GPU brute-force)** |
| **2^TmB&R8pzK@wz9** | **Very Strong (5/5)** | | **Billions of years** |

### ****Note Scores and Feedback****

**"Avoid dictionary words"**

**"Add more symbols"**

**"Increase length"**

**"Avoid personal info or repeated patterns"**

### ****Identify Best Practices for Strong Passwords****

* **At least 14 characters**
* **Avoid dictionary words, names, or birthdates**
* **Use passphrases: Sw1m!ng\_@Moonlight**
* **Never reuse passwords across accounts**
* **Use password managers to generate/store passwords**

### ****Write Down Tips Learned from Evaluation****

### Tips:

* **Length > complexity: thisisaverylongpassword > P@$$w0rd**
* **Add non-obvious substitutions (e.g., not just @ for a)**
* **Entropy matters: Random characters ≠ guessable patterns**
* **Use multi-word passphrases with symbols: "Eagle!Mountain\_2025"**

### ****Research Common Password Attacks****

1. **Brute Force:**
   * **Tries all combinations.**
   * **Countered by length, complexity, and rate-limiting.**
2. **Dictionary Attacks:**
   * **Uses common passwords, names, phrases.**
   * **Defeated by avoiding real words.**
3. **Credential Stuffing:**
   * **Uses leaked passwords from breaches.**
   * **Mitigation: never reuse passwords.**
4. **Phishing & Keylogging:**
   * **Steals passwords via social engineering or malware.**
   * **Use MFA and endpoint protection.**
5. **Rainbow Table Attacks:**
   * **Precomputed hashes.**
   * **Salted hashing makes this ineffective.**
6. **Hybrid Attacks:**
   * **Mix dictionary + brute force (e.g., "admin1234").**

### ****How Password Complexity Affects Security****

| **Password Type** | **Vulnerability Level** | **Example** | **Crack Time** |
| --- | --- | --- | --- |
| **Simple Dictionary** | **Very High** | **password123** | **<1 second** |
| **Basic Complexity** | **Moderate** | **P@ssword2024** | **Minutes–hours** |
| **Random Complex** | **Low** | **cY$7!e%9Q@L2** | **Years–centuries** |
| **Long Passphrase** | **Low** | **Sunset\_Bridge!2025** | **Decades** |

**Complexity increases entropy, which drastically increases cracking time. But length is often more effective than adding just one more symbol.**

## ****Outcome: Key Takeaways****

| **Element** | **Good Practice** |
| --- | --- |
| **Length** | **Aim for 14+ characters** |
| **Complexity** | **Mix letters, digits, symbols** |
| **Predictability** | **Avoid names, dictionary words** |
| **Reusability** | **Use unique passwords per site** |
| **Storage** | **Use password managers (Bitwarden, 1Password)** |
| **MFA** | **Enable for all critical accounts** |
| **Periodic Rotation** | **Rotate only when compromised or required** |

## Expert Tip: Use passphrases + padding

**Instead of K@!rT4w, use:**

**Correct\_Horse\_Stable\_2025!**

**Human memorable**

**High entropy**

**Avoids dictionary-only weakness**