Password Strength Analyzer Non-Technical

Password Analyzer is a beginner-friendly cybersecurity tool that demonstrates how modern systems evaluate password strength—and why weak passwords are still one of the easiest ways attackers gain access.

This project is designed as an educational demo, not a real password checker. Users should never enter real passwords.

What the Project Does

The Password Analyzer simulates how a system evaluates password security:

- **User Input**
  Enter a *test password* (for learning purposes only).

- **Strength Scoring**
  The tool assigns a score from 0 to 4, similar to a report card:

  - 0 = Very Weak

  - 4 = Strong

- **Crack Time Estimation**
  Estimates how long a computer might take to crack the password—ranging from seconds to centuries—based on length and complexity.

- **Weakness Detection**
  Identifies common problems such as:

  - Short length

  - Lack of character variety

  - Predictable or common patterns

- **Improvement Suggestions**
  Provides actionable tips and suggests stronger alternatives using memorable passphrases, such as:

BlueHorseBattery2026

- **Plain-English AI Explanation**
  An AI assistant explains the results in simple terms, helping users understand *why* a password is weak or strong and how to improve it.

Why This Matters

- Weak passwords remain one of the top attack vectors in real-world breaches.

- This project helps users learn how to:

    o Think like an attacker

    o Create stronger passwords without making them impossible to remember

- It demonstrates how automation and AI can support security awareness—not just enforcement.

Technologies & Concepts Demonstrated

- Python-based password analysis

- Entropy and pattern checking

- Estimated brute-force cracking time

- Human-readable security explanations via AI

- Secure design principles (no password storage)

Portfolio Context

This project is part of a larger Cybersecurity Portfolio, a collection of hands-on demos exploring real-world security concepts through practical tools and clear explanations.

Author

Created by Robert Gravelle
January 2026
Educational & portfolio use