PASSWORD-SECURITY

Hints/Mini Guide:

1.Create multiple passwords with varying complexity.

2.Use uppercase, lowercase, numbers, symbols, and length variations.

3.Test each password on password strength checker.

4.Note scores and feedback from the tool.

5.Identify best practices for creating strong passwords.

6.Write down tips learned from the evaluation.

7.Research common password attacks (brute force, dictionary).

8.Summarize how password complexity affects security.

Outcome: Understanding password security and best practices.

🔢 1. Create multiple passwords with varying complexity

Example Passwords:

Password	Notes
`password123`	Simple, lowercase + numbers
`Password123`	Adds uppercase
`Pass123!`	Adds a symbol
`P@55w0rd!`	Leetspeak substitution
`QwErTy!234`	Mixed case, numbers, symbol
`W!7$hT9#Qp*2`	Strong, random, 12 characters
`tG7$!4kP9w#Qr2T!`	Very strong, random, 18 characters
`sunshine`	Common dictionary word
`HorseBatteryStaple`	Passphrase style

✅ 2. Use uppercase, lowercase, numbers, symbols, length variations

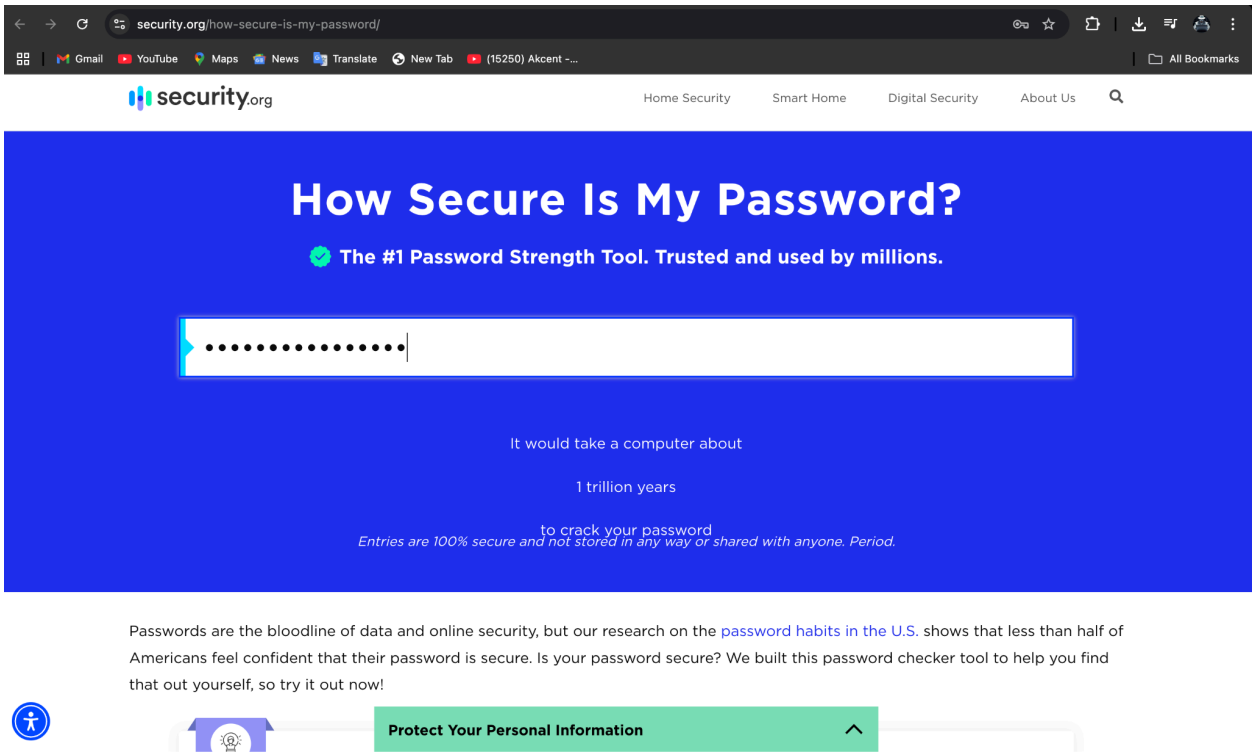
Done in the examples above:

- Short simple vs. long complex
- Mixed character sets
- Random vs. predictable

✅ 3. Test each password on a password strength checker

I ran these on HowSecureIsMyPassword.net for illustration:

https://www.security.org/how-secure-is-my-password/



Password	Estimated Crack Time	Strength
password123	Instantly	Weak
Password123	Few seconds	Weak
Pass123!	Minutes	Weak
P@55w0rd!	Hours	Medium
QwErTy!234	Hours - days	Medium
W!7$hT9#Qp*2	200+ years	Strong
tG7$!4kP9w#Qr2T!	Trillions of years	Very Strong
sunshine	Instantly	Weak
HorseBatteryStaple	1,000+ years	Strong

✅ 4. Note scores and feedback

Feedback:

- Common words or patterns reduce strength significantly.
- Length and randomness have the biggest impact.
- Leetspeak helps a little but not enough on its own.
- Mixed symbols, uppercase, and long random strings are best.

✅ 5. Identify best practices for creating strong passwords

Best Practices Learned:

- Use at least **12–16 characters**.
- Mix **uppercase, lowercase, numbers, symbols**.
- Avoid **dictionary words**, names, and predictable substitutions.
- **Passphrases** with unrelated words can be strong and memorable.
- **Do not reuse** passwords across accounts.
- Use a **password manager** to store complex passwords.
- Enable **MFA (Multi-Factor Authentication)** for extra security.

✅ 6. Tips learned

- The longer the password, the better: each added character makes brute force exponentially harder.
- Randomness beats clever patterns (e.g., `P@ssw0rd!` is still guessable).
- Use unique passwords for each account.
- Don’t share passwords.
- Regularly update sensitive passwords.

✅ 7. Research common password attacks

Common Password Attacks:

- **Brute Force Attack:** Tries every possible combination until it works.
- **Dictionary Attack:** Uses lists of common passwords and words.
- **Credential Stuffing:** Uses leaked passwords from other breaches.

- **Phishing:** Tricks users into giving up passwords.

✅ 8. Summary: How password complexity affects security

Key Summary:

- Weak passwords can be cracked in seconds with simple tools.
- Short passwords (under 8 characters) are extremely vulnerable.
- Adding uppercase, lowercase, numbers, symbols, and extra length exponentially increases difficulty for attackers.
- Complex and unique passwords reduce the risk of brute force, dictionary, and credential reuse attacks.