# Create a Strong Password and Evaluate Its Strength

### Objective

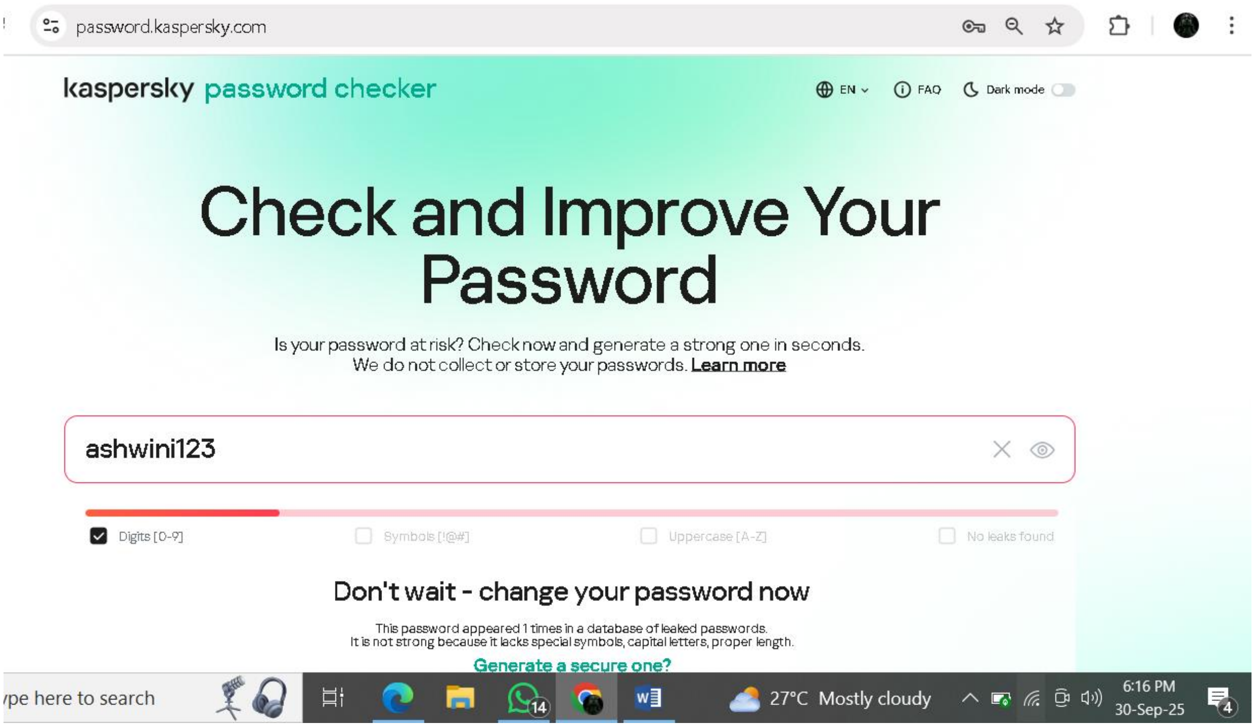
The goal of this task is to understand the factors that make a password strong, evaluate password security using online strength checkers, and learn best practices for password creation.

### Tools Used

- **Password Strength Checker:** password.kaspersky.com
- **Passwords Tested:** Multiple examples with varying complexity

### Passwords Created and Tested

| Password | Composition Details | Score (Karpersky Password Checker) | Feedback / Weaknesses |
|---|---|---|---|
| ashwini123 | Lowercase letters + numbers, short length (10 chars) | Weak (~20%) | Predictable, dictionary word + numbers |
| Ashwini@2025 | Upper/lowercase, numbers, symbol, 12 chars | Medium (~55%) | Contains a name, common pattern |
| P@ssW0rd! | Upper/lowercase, numbers, symbol, 9 chars | Medium (~60%) | Still predictable ("password" variant) |
| Cyb3r$ecure#9 | Upper/lowercase, numbers, symbols, 12 chars | Strong (~80%) | Few dictionary patterns |
| X!7m@R%2qZ#dL | Random upper/lowercase, numbers, symbols, 13 chars | Very Strong (~95%) | No dictionary matches, high complexity |



kaspersky password checker

# Check and Improve Your Password

Is your password at risk? Check now and generate a strong one in seconds.
We do not collect or store your passwords. **Learn more**

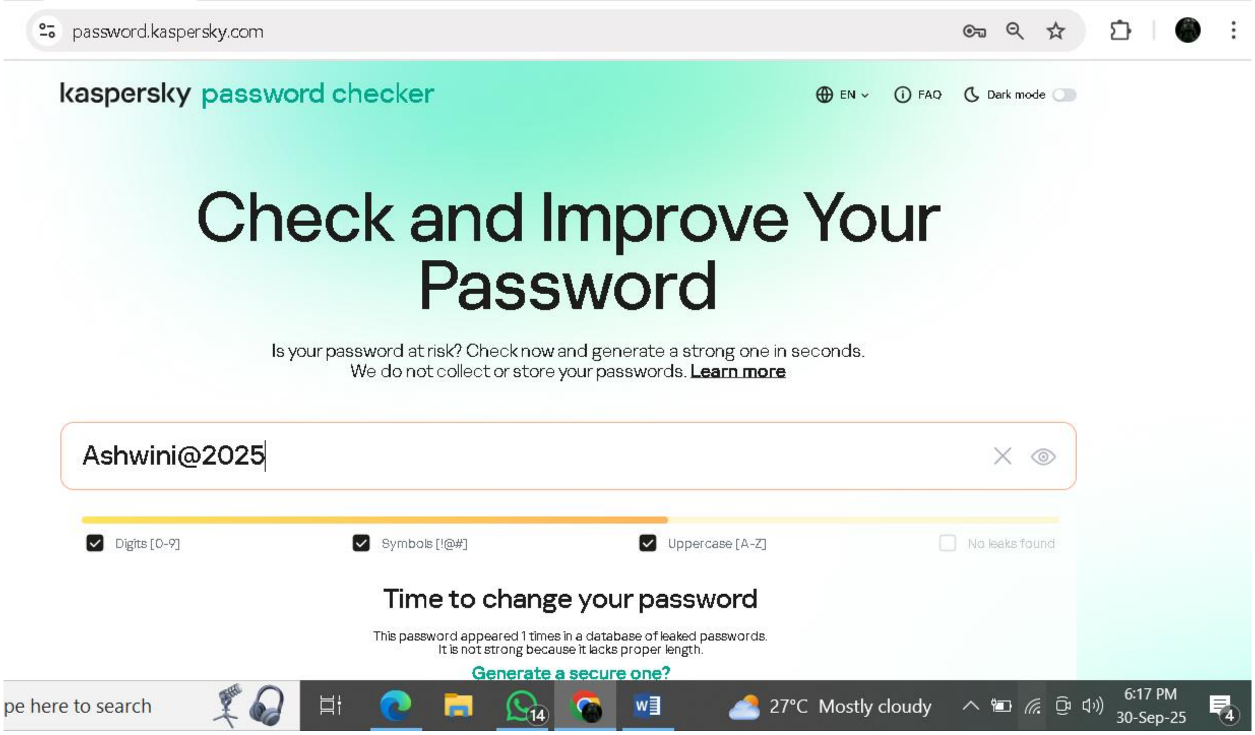
ashwini123

☑ Digits [0-9] □ Symbols [!@#] □ Uppercase [A-Z] □ No leaks found

## Don't wait - change your password now

This password appeared 1 times in a database of leaked passwords.
It is not strong because it lacks special symbols, capital letters, proper length.

**Generate a secure one?**



kaspersky password checker

# Check and Improve Your Password

Is your password at risk? Check now and generate a strong one in seconds.
We do not collect or store your passwords. **Learn more**

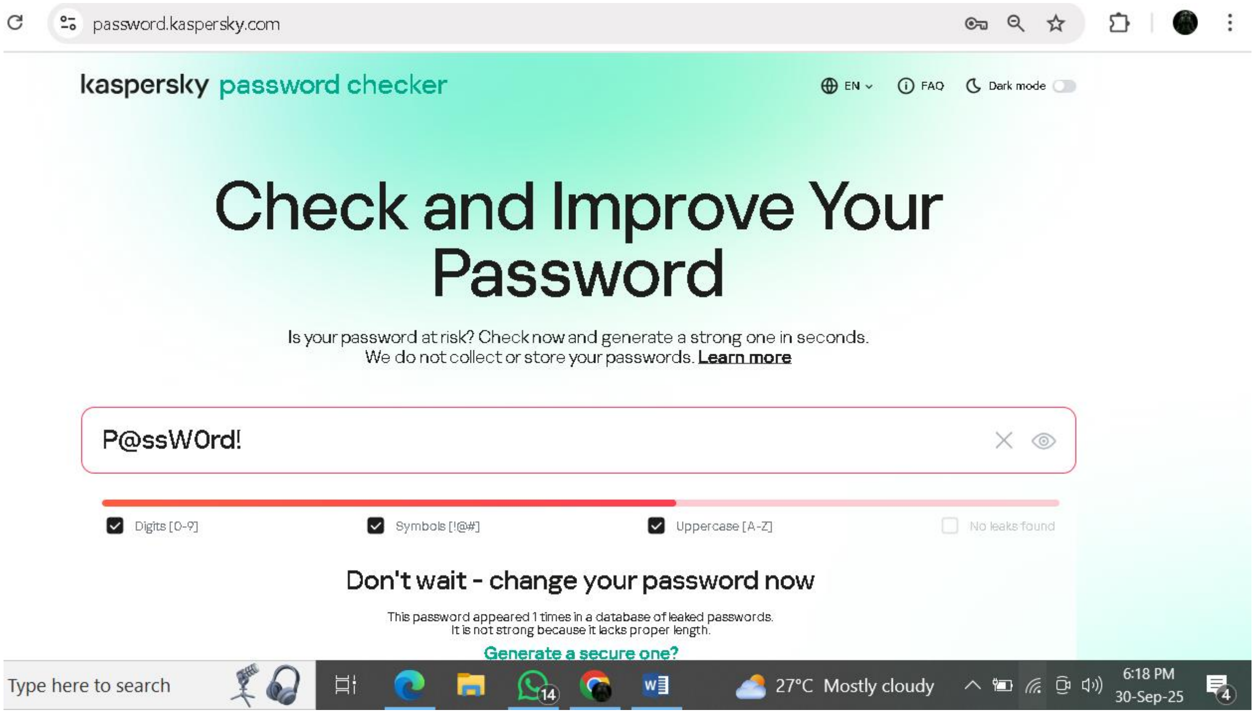
Ashwini@2025

☑ Digits [0-9] ☑ Symbols [!@#] ☑ Uppercase [A-Z] □ No leaks found

## Time to change your password

This password appeared 1 times in a database of leaked passwords.
It is not strong because it lacks proper length.

**Generate a secure one?**



kaspersky password checker

# Check and Improve Your Password

Is your password at risk? Check now and generate a strong one in seconds.
We do not collect or store your passwords. **Learn more**

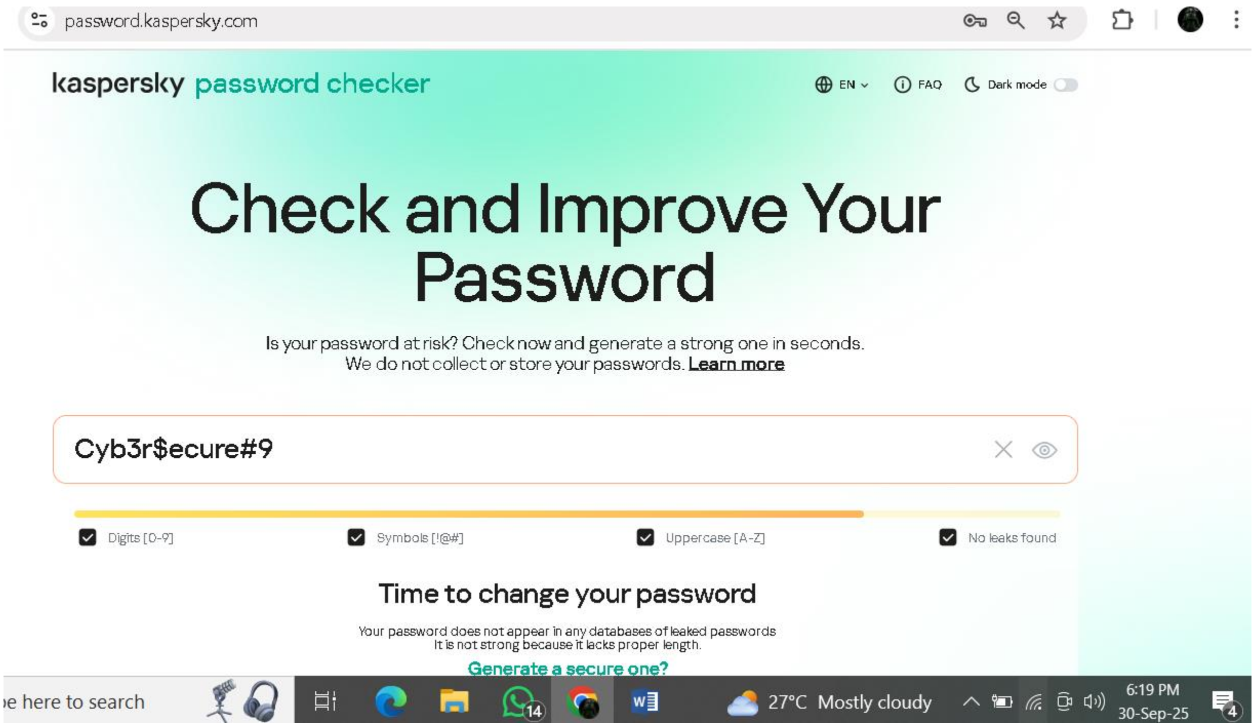
P@ssW0rd!

☑ Digits [0-9] ☑ Symbols [!@#] ☑ Uppercase [A-Z] ☐ No leaks found

## Don't wait - change your password now

This password appeared 1 times in a database of leaked passwords.
It is not strong because it lacks proper length.

Generate a secure one?



kaspersky password checker

# Check and Improve Your Password

Is your password at risk? Check now and generate a strong one in seconds.
We do not collect or store your passwords. **Learn more**

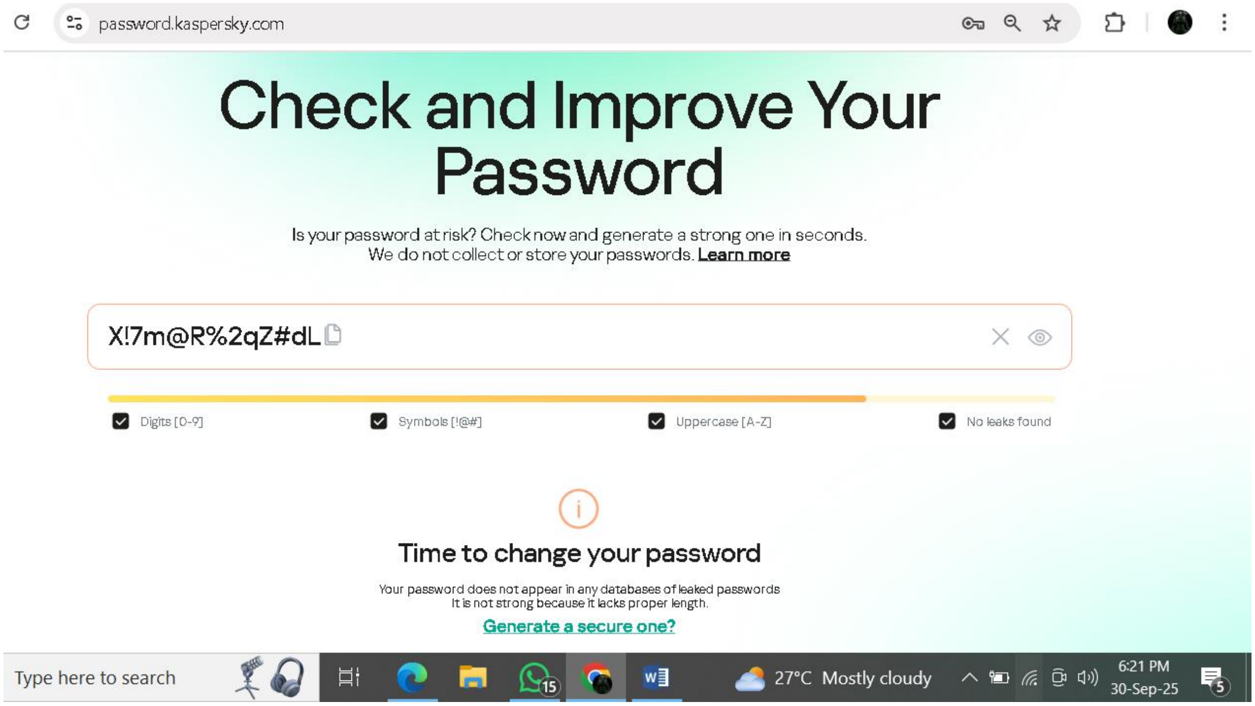
Cyb3r$ecure#9

☑ Digits [0-9] ☑ Symbols [!@#] ☑ Uppercase [A-Z] ☑ No leaks found

## Time to change your password

Your password does not appear in any databases of leaked passwords
It is not strong because it lacks proper length.

Generate a secure one?



password.kaspersky.com

Check and Improve Your Password

Is your password at risk? Check now and generate a strong one in seconds.
We do not collect or store your passwords. Learn more

X!7m@R%2qZ#dL

☑ Digits [0-9] ☑ Symbols [!@#] ☑ Uppercase [A-Z] ☑ No leaks found

Time to change your password

Your password does not appear in any databases of leaked passwords
It is not strong because it lacks proper length.

Generate a secure one?

### Key Observations

- Short and simple passwords (ashwini123) are **weak** and vulnerable to brute force and dictionary attacks.
- Including a mix of **uppercase, lowercase, numbers, and symbols** increases password strength.
- Avoiding **dictionary words, personal names, or predictable patterns** makes passwords harder to guess.
- Password length is critical: increasing from 8 → 12+ characters significantly improves resistance to brute-force attacks.
- Randomized passwords (X!7m@R%2qZ#dL) are the strongest but harder to remember.

### Best Practices for Strong Passwords

- Use at least **12–16 characters**.
- Combine **uppercase, lowercase, numbers, and special characters**.
- Avoid personal information (name, DOB, username).
- Do not use dictionary words or common substitutions (P@ssw0rd, Qwerty123).
- Use **passphrases** (random words + symbols) for memorability, e.g., C@tRun$In!2025.
- Consider using a **password manager** to store and generate complex passwords.

### Common Password Attacks

- **Brute Force Attack:** Tries every possible combination; short/simple passwords are easily cracked.
- **Dictionary Attack:** Uses common words, names, and patterns; predictable passwords fail quickly.
- **Hybrid Attacks:** Combines dictionary words with number/symbol substitutions.
- **Credential Stuffing:** Uses previously leaked passwords on other sites.

### Conclusion

The evaluation showed that password strength heavily depends on **length, complexity, and unpredictability**. The strongest tested password was X!7m@R%2qZ#dL, which scored ~95% on the strength checker.

By following best practices—using longer, randomized, and complex passwords while avoiding personal info—we can greatly reduce vulnerability to brute force and dictionary attacks, enhancing overall cybersecurity.