**Step 5 – Identify best practices for creating strong passwords**

* Long passwords are much harder to crack.
* Mixed characters (upper, lower, numbers, symbols) increase strength.
* Randomness is key — avoid dictionary words and personal info.
* Passphrases can be both secure and memorable.

**Step 6 – Write down tips learned from the evaluation**

1. Make passwords **at least 12 characters** long.
2. Use a **mix of character types**.
3. Avoid predictable patterns (123, abc, dates).
4. Don’t use personal info (name, birthday, etc.).
5. Use passphrases for memorability without sacrificing security.
6. Store passwords in a password manager instead of remembering all.

**Step 7 – Research common password attacks**

* **Brute Force:** Trying all possible combinations until one works.
* **Dictionary Attack:** Using a list of common passwords/words to guess.
* **Credential Stuffing:** Using stolen credentials from breaches on other sites.
* **Phishing:** Tricking users into revealing passwords.

**Step 8 – Summarize how password complexity affects security**

**Example Summary:**  
Password complexity greatly increases resistance against brute force and dictionary attacks. Longer passwords exponentially increase the number of possible combinations, making them harder to crack. Including uppercase letters, numbers, and special characters further diversifies possibilities. However, complexity should be balanced with memorability to ensure users do not reuse or write down insecure copies of passwords.