**TASK 6**

Best practices for creating strong passwords :

* A password should be at least 12 characters long containing combination of upper and lower case letters or characters, numbers and special symbols.
* Common password related research found that 50% of users use passwords of 8 characters or less, which aren’t secure as longer passwords.
* A password shouldn’t include any of your personal information, as identity theft and data breaches can compromise such information.

Sample passwords that are reviews by online password strength checkers

1. S@h#e2e4l1a : this is a 11 characters of strong complexity password that score 99% and takes time of approximately 550 years to crack.
2. C[h9a%n5d+el : this is a 12 characters of very strong complex password that score 100% and takes time of 4billion years of cracking, this secure as fort Knox.
3. D]e7e^o0ak : 1million years takes to crack this, and scores 100 percent containing of 10 characters.
4. Ch8?a$w3l8a : 12 characters of complex passwords containing various characters takes time of 31 thousand of cracking.
5. Y7!eg5it9=a/ : it’s a 13 characters of very strong password that scores 98%, takes time of 5 million years of cracking

Tips for secure password

* Number of characters, combination and uniqueness
* Only change password when needed
* Use password manager and antivirus software to compromise identity theft protection

Common password attacks like brute force

A bruteforceattack is where an attacker tries allpossiblecombinations of passwords, or login credentials until the correct one is found. It’s one of the simplest forms of cyberattacks, but it can be effective if systems have week credentials.

### HowItWorks

The attacker uses a program that:

1. Generatesaguess .
2. Triesit to log in or decrypt data.
3. If it fails, moves to the next guess.
4. Repeats until it succeeds or is blocked.

Types of Brute Force Attacks

1. SimpleBruteForce  
   Tries everypossiblecombination .
2. DictionaryAttack  
   Uses a list of commonpasswords instead of every possible one.
3. HybridAttack  
   Combines dictionary words with common patterns (e.g., “Password123”).
4. CredentialStuffing  
   Uses known username-password pairs (from leaked databases) to access other accounts.

How password complexity affects security?

* after gaining access to a user’s credentials, many hackers will log into their accounts to steal more of their personally identifiable information

they will use this information either to steal money from the user directly or to steal their identity.

* A hacker breaking into your accounts due to a week password can compromise your privacy. For e.g. If you don’t change the default password of your IP security cameras, hackers may be able to log into your user account and watch you in your own home.
* For businesses, hackers can start disinformation campaigns against companies, sharing their data with competitors and storing it for a ransom.