**Password Management**

A password is a secret word or phrase or code that you need to know in order to have access to a place or system. In technical terms, it is a series of letters or numbers that you must type into a computer or computer system in order to be able to use it.  A password is a real-life implementation of challenge-response authentication (a set of protocols to protect digital assets and data).

*A string of characters i.e letters, numbers, or special characters, used to verify the identity of a user during the authentication process is known as a password.*

### Password Management:

Since passwords are meant to keep the files and data secret and safe so it is prevented the unauthorized access, password management refers to the practices and set of rules or principles or standards that out must follow or at least try to seek help from in order to be a good/strong password and along with its storage and management for the future requirements.

### Issues Related to Managing Passwords:

The main problem with password management is that it is not safe to use the same password for multiple sites, therefore having different passwords for different sites and on top of that remembering them is quite difficult. As per the statistics, more than 65% of people reuse passwords across accounts and the majority do not change them, even after a known breach. Meanwhile, 25% reset their passwords once a month or more because they forgot them.

To escape from this situation people often tend to use password managers (A password manager is a computer program that allows users to store, generate, and manage their passwords for local applications and online services.). Password managers to a certain extent reduce the problem by having to remember only one “master password” instead of having to remember multiple passwords. The only problem with having a master password is that once it is out or known to an attacker, the rest of all the passwords become available.

The main issues related to managing passwords are as follows:

* Login spoofing
* Sniffing attack
* [Brute force attack](https://www.geeksforgeeks.org/brute-force-attack/)
* [Shoulder surfing attack](https://www.geeksforgeeks.org/what-is-shoulder-surfing-in-cyber-security/)
* Data breach

### Methods to Manage Password:

There are a lot of good practices that we can follow to generate a strong password and also the ways to manage them.

* **Strong and long passwords:** A minimum length of 8 to 12 characters long, also  it should contain at least three different character sets (e.g., uppercase characters, lowercase characters, numbers, or symbols)
* **Password Encryption:** Using irreversible end-to-end encryption is recommended. In this way, the password remains safe even if it ends up in the hands of cybercriminals.
* **Multi-factor Authentication (MFA):** Adding some security questions and a phone number that would be used to confirm that it is indeed you who is trying to log in will enhance the security of your password.
* **Make the password pass the test:**Yes, put your password through some testing tools that you might find online in order to ensure that it falls under the strong and safe password category.
* **Avoid updating passwords frequently:** Though it is advised or even made mandatory to update or change your password as frequently as in 60 or 90 days.