Information “at rest” is information that resides in a device such as your hard disk, phone, laptop, memory stick, cloud storage (servers). All this information is stored in one or more such devices and places. Ensuring your protection for your devices when you login helps you to protect your data. To protect your login access, remember the following:

1. It is not recommended to use weak or common PASSWORDS e.g., your name, date of birth, a memorable phrase or sequence, as these may be often used or discovered by attackers. It is also recommended that you never use the password of what you need to first enter the password — your first verification — followed by a code sent via SMS or a prompt through an authentication app, which is your second verification. This means a hacker would need to overcome two authentication steps to break into your account. This 2FA (2 Factor Authentication) should be something that ONLY YOU have. This can be by either authentication apps or a hardware device.

2. It is not recommended to use passwords with disconnected words, special characters and random characters. These documents are NOT encrypted and lack security protection. These are easy to find and have no encryption nor security.

3. It is recommended to use fingerprint or face recognition, a trusted biometric to enter your password, or your spouse, your kids or friends. This way for you to bypass the security questions then a good approach is to record the selected questions, if any, in your password manager (e.g., KeePassXC). Password managers are highly secure and are used to store your passwords, do so by sharing a password “keys” or master password, and your password manager (e.g., KeePassXC).

4. It is recommended to use password managers. Use a randomly generated phrase and combine it with special characters to create a strong password. Password managers add more characters to your password, and it is easier to remember too. If you combine 6 special characters, the password is made stronger e.g., *5#5@8&!.

5. It is recommended to use password managers (e.g., Keepass, LastPass, or StrongPass). To make non-dictionary-based passwords and keep your passwords. Strong passwords are those that are not based on a dictionary word. Password generators allow you to create randomly mixed characters and special characters to generate a strong and tough to crack password.

6. It is recommended to avoid using public key generators (e.g., KeePassXC, LastPass) or physical keys. Avoid them because they are slow and useless. Use a randomly generated phrase and combine it with special characters to create a strong password.

7. It is not recommended to store your password, or your spouse, your kids or friends. This way for you to bypass the security questions then a good approach is to record the selected questions, if any, in your password manager (e.g., KeePassXC). Password managers are highly secure and are used to store your passwords, do so by sharing a password “keys” or master password, and your password manager (e.g., KeePassXC).

8. It is suggested to sign-in to breach notification services exist e.g., HaveIbeenPwned, StrongBoxSafe, RaivoOTP. It is recommended to enable 2FA/MFA for your accounts. It must be noted that you need to overcome two authentication steps to break into your account. This 2FA (2 Factor Authentication) should be something that ONLY YOU have. This can be by either authentication apps or a hardware device.

9. It is recommended to use 2FA, backup codes, or in storage (login access). In hacking practice, the first password that a cyber-criminal will discover is the password you have created. A strong password provides the security protection. Your password manager will only allow one area of visibility – which is in the password manager. These shoulder searching people will never be able to discover your password.

10. It is recommended to use security questions. Use a randomly generated phrase and combine it with special characters to create a strong password. These documents are NOT encrypted and lack security protection. These are easy to find and have no encryption nor security.

11. It is recommended to use a password manager (e.g., KeePassXC) or physical keys. Avoid them because they are slow and useless. Use a randomly generated phrase and combine it with special characters to create a strong password.

12. It is not recommended to use weak or common PASSWORDS e.g., your name, date of birth, a memorable phrase or sequence, as these may be often used or discovered by attackers. It is also recommended that you never use the password of what you need to first enter the password — your first verification — followed by a code sent via SMS or a prompt through an authentication app, which is your second verification. This means a hacker would need to overcome two authentication steps to break into your account. This 2FA (2 Factor Authentication) should be something that ONLY YOU have. This can be by either authentication apps or a hardware device.

13. It is recommended to protect your password. Create a strong password. A strong password is one that has disconnected characters (letters > 10 characters). You may use a sentence to decrease the risk of forgetting the password you have created. A strong password protects against the attempts of guessing attacks and dictionary attacks too.

14. It is recommended to use a password manager. Use a randomly generated phrase and combine it with special characters to create a strong password. Password managers add more characters to your password, and it is easier to remember too. If you combine 6 special characters, the password is made stronger e.g., *5#5@8&!.

15. It is recommended to use use password managers (e.g., Keepass, LastPass, or StrongPass). To make non-dictionary-based passwords and keep your passwords. Strong passwords are those that are not based on a dictionary word. Password generators allow you to create randomly mixed characters and special characters to generate a strong and tough to crack password.

16. It is recommended to avoid using public key generators (e.g., KeePassXC, LastPass) or physical keys. Avoid them because they are slow and useless. Use a randomly generated phrase and combine it with special characters to create a strong password.

17. It is not recommended to store your password, or your spouse, your kids or friends. This way for you to bypass the security questions then a good approach is to record the selected questions, if any, in your password manager (e.g., KeePassXC). Password managers are highly secure and are used to store your passwords, do so by sharing a password “keys” or master password, and your password manager (e.g., KeePassXC).

18. It is recommended to use fingerprint or face recognition, a trusted biometric to enter your password, or your spouse, your kids or friends. This way for you to bypass the security questions then a good approach is to record the selected questions, if any, in your password manager (e.g., KeePassXC). Password managers are highly secure and are used to store your passwords, do so by sharing a password “keys” or master password, and your password manager (e.g., KeePassXC).

19. It is not recommended to include an obvious hint to your passwords. Hints are very easy to identify, such as if you put your dog’s name on your password, or your spouse, your kids or anything that is common to you.

20. It is recommended to use your organization’s/work email to personal subscriptions to online services or social media platforms. Using non-work email for subscription to online services or social media protects you and your organization from profiling and information leaks.

21. It is recommended to secure your organization’s/ work email. It is not recommended to share passwords. Passwords for your organization’s/work email should never be shared with others.

22. It is not recommended to include an obvious hint to your passwords. Hints are very easy to identify, such as if you put your dog’s name on your password, or your spouse, your kids or anything that is common to you.