SECURE YOUR PASSWORDS WITH A PASSWORD MANAGER

Many believe that Password Managers are unsafe and make you more susceptible to a breach.
This myth is untrue because passwords are encrypted and typically require MFA.
Password Managers are flexible, easy, and make accessing strong passwords quicker, saving your time

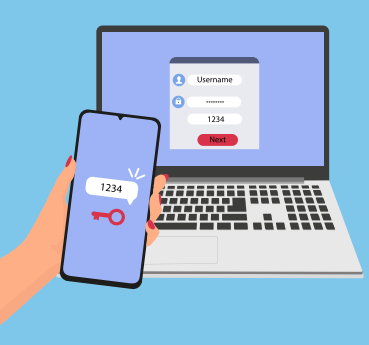
ENCRYPTED

Quality password managers will encrypt all passwords stored on the platform. This makes it almost impossible for a hacker to decode your passwords and protects them from a breach. The only access to your Password Manager vault is through your single, private, login password

EASY, BUT SAFE

In the Cyber realm, there are almost always trade-offs between ease-of-use and security. Password Managers are both easy and low-risk to you. The platform itself and company do not actually know your passwords. This is because decryption keys are not stored. Once logged in, many Password Managers offer auto-fill and other ease-of-use features

MFA



Strong Password Managers utilize Multi-Factor Authentication to make your vault secure. MFA makes it nearly impossible for an outsider to access your vault lacking valid credentials. MFA methods include: facial recognition, biometrics, additional authentication apps, and inputting an SMS code

PROTECT YOUR PASSWORDS IN MINUTES WITH LOGMEONCE MANAGER

-AEH and SHA-512 Encyption
-Enables MFA
-IOS and Android Compatible
-Access Anywhere through Cloud Technology