Best Practices for Using a Password Manager Program

September 2023 - By Corey K

I believe that the security gained from using a Password Manager program far outweighs the risk of keeping your passwords in one place (even using the Cloud). I think it is the only way to maintain long, unique, random passwords. However, as we saw evidenced from the breach of LastPass in the fall of 2022, hackers will target all password manager companies. So, we must use our Password Manager securely (as presented here).

Note: Cybersecurity is a journey! All your passwords should be strong and unique (especially important ones like financial accounts, email [since it is often used for changing other passwords!], shopping, etc.). Now is a great time to change some passwords to long, unique, random ones. But you don't have to do it overnight! Maybe update a weaker password each time you use one or choose one per day/week to change.

Best Practices:

1) **Use a Password Manager from a company whose main business is providing password management**, not from a company who just packages a password manager with other services.
   a) There may be times to use a Password Manager from a generalized security company like one who provides antivirus, but that would be the exception.
      i) We will have to see about Proton Pass, but it is too new to recommend at this point.
   b) I would recommend password managers from 1Password, Dashlane, Bitwarden, NordPass, Keeper, or LastPass; or the free offline password manager from Keepass.
      i) The best free online password manager would be Bitwarden.
      ii) If you download Keepass, be careful to get it from the official website; there are hacked versions offered on the Internet.
2) **Strong Security of Program Architecture and of Company:**
   a) Use a Password Manager that has a "zero-knowledge architecture" – i.e. the company itself can't get to your passwords without your master password. All the ones listed above have some level of zero-trust.
   b) Password Manager company needs to have secure operational procedures:
      i) Auditing (& Pen Testing) by third-party; results shared.
      ii) All security practices and programs that are required for protecting sensitive information.
3) **Practices for whatever password manager you choose**:
   a) You must have a very long and unique master password for your password manager (20+ characters long with words/passphrase).
      i) Try using a unique passphrase that you can easily remember and maybe one that is fairly easy to type on the keyboard, but is difficult for a hacker to guess or crack.
   b) Turn on Multifactor Authentication (MFA/2FA) for accessing your Password Manager (at least for the first time it is accessed from a new browser or installation).
   c) You should have strong, unique passwords for ALL important accounts (16+ random characters; or 20+ characters in words/passphrase).
      i) Consider letting your password manager create a long, random password for you.
   d) You should use MFA for all important accounts! Even if someone cracks your master password, it is very challenging (but not 100% impossible) to get through MFA into your accounts.
      i) There are basically three different types/strengths of MFA:
         (1) Weakest: Using SMS/text message.
         (2) Strong (best for most people): Authenticator application, such as Google Authenticator, or Microsoft Authenticator.
         (3) Strongest: Hardware token [e.g. Yubikey] - Maybe challenging for most people, but suggested for people who would be highly targeted.
   e) Practice good cyber hygiene: e.g. apply security patches, learn about and resist social engineering scams, have good antivirus program, use VPN when appropriate, etc. (See www.ComputerSecurityNW.com)