Steps for Implementing a Password Manager (PM) Program

Introduction:

Cybersecurity is a journey. If you don't take steps on the journey to protect your identity and become more secure online, you will never reach your desired goal. One of the four foundational and critical items for cybersecurity (for both individuals and businesses) is implementing long, unique passwords for every online account. The only way to do this is to use a Password Manager (PM) program.

Besides the strong security benefits you get from using a PM, one major advantage (and the reason I first started using one) was to **share passwords** with my wife. I realized that if I passed away, she wouldn't be able to get to many of our financial and other accounts. So, I chose a PM that synchronizes all our passwords through the Cloud.

However, I admit that embarking on the journey to use a PM program can be **intimidating (if not a little terrifying!)**, especially if you are not comfortable with technology and you have been using a method that has apparently worked for you. But, believe me, using a password manager program is a critical step on your security journey; your digital life will be much more secure if you commit to using one! I created this document to help ease that process (with clear directions). I strongly encourage you to take this step now.

People often ask, "**What about passwords I have already created?**" Answer: The good news is that your current passwords can be imported into your new secure Password Manager! (Please see details in the "Exporting/Importing any existing passwords" section below.) -- If your passwords are stored on your computer [in a note, Word doc, or Excel spreadsheet], then please move to a password manager today!! That is very insecure and is a potential disaster waiting to happen.)

Important Note: Built into every browser is the function to remember passwords, personal information, credit cards, etc. **Please don't allow your web-browser to remember your passwords!** It is a terrible idea since these passwords are not encrypted. Your browser is the program that interacts with websites and tends to be insecure; those passwords can be stolen just by visiting a legitimate (but hijacked) website. And that's beside the fact that anyone who gets ahold of your computer can get to those passwords. (The one exception to this is if you use Apple iPhone and Mac computers, please the discussion on "Apple Keychain" in the "Choosing the Right Password Manager Program" document.)

Step 1 – Choosing a Password Manager Program

See the other document, "**Choosing the Right Password Manager Program**."

Step 2 – Installing Your Password Manager Program

Initial Installation:

1) **Master Password/Passphrase**: Before installing your password manager, you need to create/decide on a Master Passphrase. This is the passphrase (password) you will enter every time you open your PM. (Not exactly true, since it can be unlocked with facial recognition on your smartphone, and you can allow your browser extension to stay logged in.) In any case, please realize you will have to type in this master passphrase often. (It gets easier over time as your fingers get accustomed to typing it.)
   a) This Master Password/Passphrase needs to be **long**! Maybe 16 to 20 characters.
   b) So, go ahead and make it a **passphrase** (a sentence or words strung together, with substitutions of letters and the addition of special characters and numbers). Using a passphrase makes it easier to remember something longer than a random password.

c) **Don't use a password/passphrase that you have used in any account before!** Otherwise, a password breach could expose this master passphrase.
d) **Don't lose it!** If you lose your Master Passphrase after making this transition, you will not be able to get back to your passwords!! This is a substantial risk and must be addressed!
   i) **NOTE:** Please note that this Master Password/Passphrase is not like other passwords to online accounts. It is used to encrypt your passwords before they ever leave your computer (to be stored in the cloud). **If you lose this Master Password it cannot be reset or recovered. Password Manager companies do NOT offer an option to "reset your password."** Although this removes the risk of someone stealing your Password Manager account, it means you must not forget this Master Passphrase!
e) So, I suggest you **write it down on a piece of paper** and keep it locked in a desk drawer or in a safe at home. (Don't keep this master password stored anywhere on your computer!!)

2) Only after having a strong master passphrase written down, then **install your PM**.
   a) Many of the newer PM programs don't have a stand-alone program to install, but instead only install as an **Extension (plug-in)** to your web-browser (e.g. Microsoft Edge, Google Chrome, Firefox, Apple Safari). Even if there is a standalone program, the real convenience of PM is that it will automatically fill in passwords; so go ahead and install the browser extension.
   b) You install the extension by going to the specific browser extension store (like the Chrome Web Store or Microsoft Edge Add-ons). Search for the extension and click: Add to browser. (Don't just download from a random website.)
   c) Suggestion/Hint: I use **multiple web-browsers** on my computer.
      i) I have my PM installed for one browser (e.g. MS Edge) and use that browser exclusively for logging into my bank accounts and other online accounts.
      ii) I use a different browser (e.g. Firefox) for research and general use. I can delete all cookies and browsing history at any time without causing account login difficulties (like reauthenticating with 2FA/MFA).
      iii) Decide if this might work best for you and implement that now.

3) **Exporting/Importing any existing passwords**:
   a) If you currently store passwords in your web-browser (or an older PM), then you should **export** them and save them in a .csv file. (Your new password manager may prompt you to do this and provide directions for doing so.)
      i) Make sure you know where this file is saved on disk, such as on your Desktop.
      ii) **Important Note**: This file will contain an unencrypted copy of all your current passwords! After you finish this process, this file must be securely deleted; see step below.
   b) **Import** this .csv file of existing passwords into your newly installed PM. Your PM program may prompt you to import them.
   c) After importing, **delete the .csv file** and **empty your trash** (so your existing passwords stored in this file can't be recovered if someone gets access or hacks into your computer).

Step 3 – Making the Switch!

Transition Phase and Goal Setting:

You need to become comfortable using your new PM. Make a **firm decision and commitment** to work through this **uncomfortable learning phase**, and **overcome any issues** you run into, until you know your PM well and have fully transitioned to using it daily. I suggest you take some time to transition completely over to the PM before deleting your previous method for remembering passwords. Commit to these steps now:

1) **First**: If applicable, turn off "auto-saving" of passwords in your web-browser (but you don't need to delete them immediately).
2) **Then**: Stop using your old method now! Make a commitment to transition to your new PM as soon as possible.
3) **After One Week**: Use your new PM for a week or maybe two weeks. Assuming all is working well, it is critical to go back and delete the previously used copy of your passwords stored in your web-browser or in a document or spreadsheet. If you don't delete these, then you have left a big hole in your security settings!
4) **Important Note** – If you are transitioning from a different PM program or web-browser:
   a) Make sure all details have been transferred to the new PM program before deleting your old PM program and its data. The transfer through a .csv file always seems to transfer websites, usernames, and passwords, but may not transfer all other details, such as the Notes field. No need to check every item; just pick a few records to confirm the process worked as expected.
   b) Be sure to go back and **delete that old PM program** or **web-browser data** (besides that .csv transfer file). If you don't delete your account with a previous password manager, then you are leaving your passwords in a place you are no longer monitoring.

Protecting Your Password Manager from Hacking:

Obviously, your PM program holds the keys to all your accounts, so it is critical to protect access to it.

1) **Turn on 2FA/MFA** (2-Factor/Multi-Factor Authentication) for accessing your Password Manager program. This will be in the PM settings. Even if someone might guess/hack your master passphrase and attempt to get access to your passwords, they won't be able to without the one-time code generated by your 2FA method.
   a) You most likely will only need to enter this code the first time you access the PM on a new computer or browser. There may be options for how often this 2FA code is required.
   b) If you can use a YubiKey or an Authenticator app (e.g. Google or Microsoft Authenticator) I suggest you use this as your 2FA device as they are more hack-proof than traditional SMS-based 2FA (via text message). If not, then you can use your phone number as SMS-based 2FA.
   c) **Important**: When you implement 2FA, you will most likely be presented with a list of One Time Codes that can be used instead of your normal 2FA method. It is best to print these to paper and keep them in a physical safe or other secure location. You can use these to access your PM program if you lose access to your normal 2FA method. Don't lose them but keep them protected!

Step 4 – Strengthening Weak Passwords:

Change Weak Passwords:

Now that you have a secure way to create and use strong passwords, it is critical that you change all your weak passwords to strong ones, especially on your most important online accounts.

1) **Getting Comfortable**: Just so you learn the process of using your PM, choose a password for an online service that you would like to change. It can be one that is not so important as you are using it to learn the process.
   a) You need to use the "**Change Password**" function of whatever website or program you are using. When it comes to entering a new password, then use the **password generator function** built into the PM to create a long password for you.
      i) If needed, you can customize your passwords to be a certain length, with symbols, digits, etc. Consider choosing a default password length of 16 to 20 characters.

ii) Remember, you no longer need to remember these passwords since your PM program will do that for you! So, let's make it long and difficult!

b) Your PM should offer to remember this new password, replacing the old one previously used.

c) Now **logout** of that online account and **log back in using your PM** to fill in the necessary account information.

d) Congratulations! You have now accelerated your Security Journey. Even if you had to fight through complications and learnings to get this password changed, you did it! It only becomes easier with use!

2) **Now**: Choose one of your **more important accounts** and change its password with your PM.
   a) Please note that **you must change the password on all your most critical accounts**, like your financial accounts, Apple ID and/or Google access, your email (since your email account is often used to reset passwords!), online shopping, social media, etc.
3) **Make a commitment** to change weak passwords or passwords you have re-used on multiple websites.
   a) Commit to spend 15 minutes/day (or one hour a week) until you have changed/strengthened all important passwords. (Consider putting this down on your calendar.)
4) **Set a goal** of when you will be completed with your transition to the password manager and have changed all previous passwords. Consider 2 months, or whatever seems appropriate for your situation.
5) Note: Occasionally when you are changing a password, the one generated by your PM program will not be accepted by the website/service you are logging into. They may have a restriction on password length or limit special characters allowed. If that is the case, you can generate a shorter password, or take the one given to you and edit it in Notepad (or a text editor) to meet the required specifications. Once you paste it into the password field, your PM will offer to remember it for you.

Step 5 – Maintaining Access (Disaster Recovery)

Long-Term Access & Account Recovery:

As with all Password Managers, if you forget your Master Passphrase, there may be no way to recover all your passwords. You must ensure that you maintain access to your PM, even in unusually or rare circumstances. Consider the following circumstances and practices; prepare for this NOW. (This is not an optional step that you might eventually address in the future.)

1) **Write Down Master Password and Store Securely**: So that you don't lose access to your PM or forget your Master Password, keep a written copy of your Master Password in a locked location.
   a) I have seen people only access their password manager on their smartphone that uses facial recognition, so they never had to type in their Master Password. When they went to move to a new phone, they could not access their PM since they had forgotten their Master Password!
2) **Consider**: Make a way for loved ones to get access to your passwords if you pass away or are incapacitated. Use the built-in features of the PM program if that option is available.
   a) If no legacy sharing options are available, then you could seal the master passphrase in an envelope, give it to a trusted family member to store in their safe, and get them a One Time Code that can be used instead of your normal 2FA method (since they may not have access to your normal 2FA method). Make sure they store this information securely, in a locked location.

Step 6 – Continuing the Password Journey:

1) Password Health Report:

a) You were encouraged above to create strong passwords on any important account. If you have not done that, please do that now, or within a week. (See Part 4 above.)

b) However, it may be too much work to change all weak passwords immediately. To help with this, most of the paid versions of PMs listed above have some form of audit report as to whether your passwords are considered strong, and/or whether they are reused on multiple accounts. You should continue your cybersecurity journey by making a commitment to changing all weak passwords.
c) Use the list of weak or reused passwords provided to you by your password manager as a list to work through over the course of a couple months.

2) Dark Web Monitoring Alerts:

a) Many of the paid versions of PMs listed above monitor the Dark Web to see if your username and passwords have been compromised and are being sold to hackers. Make sure to monitor these alerts and change the password on any account highlighted there.
b) The fact that your password was compromised and is for sale on the Dark Web does not mean someone else has already logged into your account, but it does mean that you should change your password before they do!

Optional Resources for Further Research:

- CISA Password Recommendations: www.cisa.gov/news-events/news/choosing-and-protecting-passwords
- Understanding Password Managers: www.security.org/password-manager/