



PASSWORD MANAGEMENT RESOURCES:

Here are some great links for websites to help you to choose, manage and monitor your website usernames/passwords. Please spend some time becoming familiar with them, and bookmarking them for future reference.

- <https://www.wired.com/story/best-password-managers/>
- Again, one of **THE** most important things you can do **RIGHT** now, to keep yourself secure online, is to use a password manager. It creates new secure (i.e. long) passwords for you to use on new websites, it keeps all of your passwords in an encrypted vault, and it even syncs them across devices. They are quite easy to use as well. Please choose one for your PC, Mac, Android, iPhone, and web browsers.
 - Also LastPass has recently starting persuading users who use their Free product to upgrade to the Premium. The Free still works just as good, but now won't allow you to sync your passwords between devices. If you don't like this, other solutions such as 1Password and BitWarden still offer these free syncing services
- <https://howsecureismypassword.net/>
 - This website will inform you how long it might take a hacker to crack your chosen password
- <https://haveibeenpwned.com/>
 - An amazing website that will let you know, and warn you in the future, if either your email address or password have been discovered stolen anywhere on the Internet!
- <https://haveibeenpwned.com/passwords>

- Here you check specifically for passwords you have used that may already be compromised by the bad guys
- <https://monitor.firefox.com/>
 - Mozilla Firefox's equivalent service to Have I Been Powned
- <https://chrome.google.com/webstore/detail/password-checkup/pncab-npcffmalkkjpajodfhijclecjno>
 - Google has a new Chrome extension that will check and warn you if you're using a password that has already been detected as stolen on the Dark Web
- <https://www.themooltipass.com/>
 - **Mooltipass** is an actual hardware password manager you carry in your pocket. Pretty cool!