

**Summer VTC Questions & Answers**  
**Solve Your Password Management Problems**  
**Kenneth Tubaugh, Educational Services Director & Program**  
**Coordinator - Columbus Computer Society**

**Question:** I do not understand why password managers do not usually offer to store data on a local PC and then use local sync by local Wi-Fi or Bluetooth.

**Answer:** Bitwarden offers local hosting. Most password managers do not. Here is a link to the Bitwarden article covering "On-Premises Hosting:" <https://bitwarden.com/help/hosting/>

**Question:** What about using "[howsecureismypassword.net](https://howsecureismypassword.net)" to test time to crack?

**Answer:** This is a great resource to test your password complexity. However, it cannot test the randomness. For example, I entered a phrase that is easily crackable yet met the complexity requirements. I used a variation on the phrase "To be or not to be. That is the question." A simple quote to remember for a human. A hacker will crack this dictionary password in no time. This tool is a good frame of reference but provides false security.

**Question:** How do you keep the "password" for the password manager safe?

**Answer:** The safest method is to create a randomly generated password using a password manager and memorize it. If you need to write it down for a while, digital storage methods like notes, a text document, a spreadsheet, and so on are **NOT** a good idea. I have my parent's master password stored in **MY** password vault. This is secure, but not convenient for them. A handwritten note would likely be more secure. You just have to keep it locked up somewhere safe... like a safe or safety deposit box. Memorization is best! Remember, you only need to remember one password now (other than the password to log into your computer).

**Question:** If you already have a list of passwordS on a thumb drive on an excel spreadsheet, can you import all your passwords into Bitwarden?

**Answer:** Yes. This is an easy process for Bitwarden to handle. Export a copy of the Excel spreadsheet into a \*.csv file. Here is an article explaining the import process using numerous methods: <https://bitwarden.com/help/article/import-data/>

**Question:** Is KeePass any good? I've been using it for years.

**Answer:** KeePass seems to be fine. It's free and open-source like Bitwarden. In my limited experience with KeePass, I found Bitwarden to be more modern and easier to use. KeePass has been around longer than Bitwarden.

**Question:** I keep it in DropBox which is web accessible . . . .so it's ok?

**Answer:** I'm not exactly sure what "it" is referring to in this context. It might have made more sense to me during the presentation, so my apologies. I will answer this question in two ways:

(1) If you are keeping your passwords in a file on Dropbox, then I would be very worried. Dropbox doesn't encrypt your data by default. Un-encrypted data is readable by anyone on the Internet with basic computer hacking skills.

(2) If you are syncing your password manager's vault using Dropbox than you might be okay. All is well if your password manager encrypts the vault before saving it to your Dropbox folder. If it saves in un-encrypted, then you should immediately seek out a different password manager.

**Question:** I use DuckDuckGo, problem?

**Answer:** DuckDuckGo is an alternative to searching for things on the Internet. It takes a more ethical approach to searching (not sharing personal data and so on).

DuckDuckGo does offer a built-in password generator service. This is a small part of the password management process. The next step is securely saving that information. Here is an article discussing this feature: <https://dev.iachieved.it/iachievedit/creating-strong-passwords-with-duckduckgo/>

I have a feeling your browser (Chrome, Edge, Firefox, Internet Explorer, or Safari) is saving your passwords. This is not a good password manager. It's a convenient solution that sacrifices security. A password manager is much more secure.

**Question:** What about username/passwords for standalone programs like Steam?

**Answer:** You can still use a password manager. You save the login information in your password manager application. When you need that information, launch the app and copy/paste the password into the Steam login window (CTRL+C and CTRL+V).

**Question:** I'm currently using LastPass free, planning to go to the paid version. Can you import LastPass passwords to Bitwarden?

**Answer:** Yes. Here is an article explaining the import process using numerous methods: <https://bitwarden.com/help/article/import-data/>

**Question:** So, I'm assuming you can keep all the same passwords from LastPass to Bitwarden for your websites.

**Answer:** Yes, there is no need to change the passwords if they were randomly generated using industry standards. If you used LastPass to generate them, you are good to go.

If you would like to switch to Bitwarden, here is an article explaining the import process using numerous methods: <https://bitwarden.com/help/article/import-data/>

**Question:** Do you think a passphrase for a password manager login is too simple? eg correct horse battery staple.

**Answer:** Yes, it's too simple. Passphrases are best used for security questions, not passwords (for example "mother's maiden name"). Remember, you are not fighting a human, you are fighting a computer. Dictionary words are easy to crack.

**Question:** Could you talk about 2-factor authentication?

**Answer:** That is a whole other topic in and of itself. My humble opinion is this: two-factor authentication is great for security. It adds another layer to the login process if your password is hacked. However, there is an exception. Authentication codes sent via text to a mobile number is NOT very secure. Mobile numbers can be easily hijacked. A better option is an Authenticator app.

**Question:** Do password managers sync with computers, tablets, and phones?

**Answer:** Yes, most do. Bitwarden syncs with all of these and is also accessible via a web browser.

**Question:** Can you tell us briefly what it is that you don't like about other password managers (other than not working on all platforms)?

**Answer:** I'm only familiar with a few.

1Password is actually my favorite password manager. Consumer Reports ranks it number one. I moved away from it because I needed a password manager to work on Linux. 1Password does not. If I were being picky, I'd say that it's not open source and it's pricey compared to Bitwarden. The interface was also dated when I moved to Bitwarden.

**Question:** How secure is the password company. Can they get hacked?

**Answer:** Yes, they can be hacked. However, I trust LastPass and Bitwarden's security practices. Both were hacked and the data was useless to the criminals. It was encrypted.

**Question:** Once Bitwarden is installed, do I have to go it to get the password every time I open a program like Google on my phone?

**Answer:** It depends on the app. My email app caches (saves) the password for future use. I've only entered it once into this app. Other apps might require a login every time you open it. Most apps don't behave this way.

**Question:** If one uses a laptop, iPhone and desktop, is accessibility possible to all three if Bitwarden is download on only one of the devices.

**Answer:** Yes. You can use your web browser to access your passwords.

**Question:** Is there an export feature... I want to print out my passwords stored in the Bitwarden and place that in my Safe Deposit Box

**Answer:** Yes. Here is an article that discusses exporting: <https://bitwarden.com/help/article/export-your-data/>

**Question:** Do password managers remain accessible with new operating systems?

**Answer:** Yes, as long as the password manager's parent company keeps the app updated. I used 1Password for nearly a decade without a single hiccup.

**Question:** Where is the database for Bitwarden stored?

**Answer:** Either on Bitwarden's servers or your server. Bitwarden encrypts the data on their servers. You need to do the same if you decide to host on your server.

**Question:** When you first start doing the password manager, do you have to enter in all your accounts all at one time?

**Answer:** No. Slow and steady is best. If you rush it, you might make a mistake.