Password Managers (beginning)

Learning Objectives

Learners will:

- Understand that a master password is used to open a password manager vault.
- Be able to give examples of when one can use a password manager (to remember passwords, notes, and even randomly-generated answers to security questions).
- Understand the difference between a stand-alone and a browser-based password manager.

Prerequisites

- Learners should understand how to choose a good master password.

GOTCHAS AND PROBLEMS YOU MIGHT HIT

The user flow for a password manager may feel unfamiliar to many participants, unless they have had prior exposure to a similar tool. Participants will likely need to see how to do a given task within the password manager interface a few times, and will need some time to practice and demonstrate their mastery of the task on their own machines.

When making a new password for a critical service, such as to decrypt a password manager vault, there may be a few participants who will forget their new passwords. If people have changed the passwords for critical accounts or for their devices without memorizing their passwords, this activity may cause more harm than good. Consider suggesting people write down their passwords (on paper or in password managers). For those who write down their passwords, remind them to watch out for others peeking at their papers, and to keep these papers in a safe place!

It is also worth looking into memory retention techniques for those who have trouble remembering their passwords, like mnemonics, creating illustrations or imagery to accompany the password in the course of their memorization, creating a funny story around the password, and so on.

Lesson Content

WARMUP

Asking, “How many of you here have ever reused a password on more than one account?” is a good way to engage the audience as well as allowing you to get a good gauge of technical proficiency. You can follow up with a variant of that question that highlights another way in which passwords can be reused: “How many of you have used minor variations on the same password between accounts?”

Follow these questions with something along the lines of, “That’s okay. With the number of sites we are forced to log into, it’s only natural we would want a simple way to remember them all. But reusing the same password on different websites is the number one cause of account compromise. Password managers can help!” It makes your audience feel like they haven’t been playing the fool all this time, and that they have the opportunity now to fix the problem.

KNOWLEDGE SHARE

Different password managers will have different time commitments and characteristics. The two basic types of password managers are:

Browser-based password managers: You access them via a website, and can download them as a browser extension for your computer and an app for your phone. They are able to sync across devices. Most importantly, browser-based password managers are very good for defeating phishing attempts. While it can be hard for a human to differentiate a bogus sign-in page from a legitimate one based on visual cues, a password manager uses technical cues to tell them apart. If a browser-based password manager does not recognize a login page, that can be a sign to the user that something is off.

Standalone password managers: These often exist as separate files on your device and require you to copy-paste login information from the password manager to a given log-in

screen. While this makes it harder to reliably sync across devices, standalone password managers can be good for users who would like to keep their passwords on a separate, offline device like a thumb drive. This can especially apply for people who use shared devices.

Generally, teaching browser-based tools like 1Password and LastPass is easier and more intuitive than a separate password manager program. (Of course, these two have also had their share of vulnerabilities.) They're also easier and take less time overall to install. For most users, the vast majority of the time they spend on their computer is in a browser window.

Dedicated programs such as KeePassXC are powerful tools for advanced users. Users can increase their security level in "database settings" to protect against brute force attacks. These are all great features for the advanced user, but may be unintuitive and hard to teach to a novice audience.

If you don't have time to do hands-on training for this tool, consider using a visual aid to drive home the key concepts, such as our imaginary password manager.

ANTICIPATED QUESTIONS & ANSWERS

Q: What if my password manager company gets compromised? Why should I trust them when I know that there's no such thing as perfect software or perfect security?
A: This is a fantastic question, and shows that the person who asked it is thinking with a security mindset. Any security tool will involve compromises and tradeoffs, and password managers are no exception. The ultimate question may be: How does trusting a password manager compare to my password practices without one? For most people, a password manager protects against a relatively likely cause of account compromise (using the same password across accounts) for the tradeoff of exposing you to the less-likely risk of the password manager company itself being breached. Password managers such as 1Password and LastPass also store your passwords in a file that is encrypted with a key that only you have, so even if someone broke into the password manager company and stole your password file, they could not decrypt it.

Q: What if hackers break into my computer? Doesn't having a password manager mean that all they need to do is look at one file to see all my passwords?
A: If hackers have installed malware on your computer that allows them access to all of

your files, reading all of your passwords in one file is marginally faster than waiting for you to log into each of your accounts and enter your password manually.

Q: What if I forget my master password?
A: It's important to make a master password that is memorable. As is the case with other encrypted tools, knowing your password affects whether you can access the encrypted information behind it. Be sure to memorize your master password!

It might make sense to write down your password on a piece of paper and keep it in a safe place, and then destroy it when you have it memorized.

Diceware is a great way to create a password that is strong, random and easy to remember. If you find you're having trouble memorizing your master password, you can create a story around the words used, or create a mnemonic for yourself. For people with memory loss issues, sharing the password with a trusted friend or family member may make sense. Storing a hardcopy of the password in a safe or other secure place may also be an option.

Q: Are password managers right for everyone?
A: For some people, a password manager may not make sense. People in abusive relationships, for example, may find themselves in a position where someone could force them to unlock their password database, exposing a list of their online accounts and a rough record on their online activity. The same might apply for children, particularly LGBTQ youth or youth with religious or political beliefs that are stigmatized in their household or community.

The goal here is to make sure that people use long, hard-to-guess, unique passwords for each account. A password manager is one way to achieve that goal, but may not be the right choice if someone has physical security risks like the ones described above.