Bryan Jones
LFI Week 3
Teach two people about what you learned and write one page about your experience.

At work, we are in the process of rolling out a shared account of a popular online password manager. I used this opportunity to talk about diceware and KeepassX. Most of these folks are technology professionals. I will also share some of my experiences doing privacy workshops at my library with patrons.

Our use of a shared password manager brought up the need for us to have strong passphrases. To my surprise, no one had heard of diceware. They thought it was interesting. My feeling was, "Interesting, but I am never going to use this." A lot of them had devised there own ways of coming up with random passwords; e.g., the "book method." We discussed which methods were more random than others; e.g., using your zipcode as a cipher for which word to pick from which page of a book. We discussed that this gives you easy password recovery but is also less random than diceware. The size of the diceware word list was discussed and the amount of possible permutations. It was pointed out that was enough permutations for now, but in the future this would change. I mentioned that in the few years I've been doing workshops the minimal number of recommended words in a passphrase had gone up from five to six. When we finished a coworker asked me where to find the diceware word list.

I demonstrated KeepassX. This was more appealing to some than having passwords in the cloud. Most thought having to keep track of a local file to be a pain. We did not discuss the option of saving the database online, as we were focusing how Keepass as different that what the office had decided to go with. We discussed the pros and cons being responsible for a digital file (Keepass database) versus physical file (pen and paper). I surprised how many of my coworkers used some version of pen and paper. I mentioned that Rosalie's lecture was the first time I had heard a security professional be chill with pen and paper.

Mixed into all this conversation was the issue of two factor authentication. Our talk did cause some coworkers to reconsider what accounts they wanted to enable 2FA on.

My experience with patrons is not dissimilar. They understand the concept of diceware, or least the necessity of a long, random passphrase, but I don't know how much people utilize it. They also understand the functionality of password managers but convenience of online ones often outweigh security and/or ethical concerns about cloud computing and/or propriety software.

These are patrons that show up to something called “Online Privacy Workshop” on the library’s events calendar. Anyone that works at the public library knows there are way more patrons that really have zero tech knowledge and wouldn’t even show up for a class like that. The emergence of threat modeling outside network security circles is a positive development as it gets people thinking about how they are vulnerable and who would want to compromise them.

Some very small steps:

If patrons need passwords written down, the librarian might was well use something like diceware, or a password manager, to create a good password.

When helping patrons with library apps, or internet anything, encourage them to opt out and not sign up for “notifications” or offers. I try to get them to think about (without being pushy) the minimal amount of information needed to use a service and why a service is would want more than that.