Megan Kinney
Cohort - 2018
LFI - Week 5

I created a library instruction session around threat modeling in week three. In week three, I framed the session as part one of two. The first session would talk about some basic internet safety strategies, but would also ask students to think through how they use the internet, and who they might be concerned would see what they are doing. I would then use this example threat model below to start session #2, where I first show an example, and then have them map their responses from week 1 onto it.

My sample is based on something I see a lot in my community college libraries - students mixing both academic and personal work (in this example: navigating library resources for research, as well as completing a necessary FAFSA component). Students in my schools have been coached to use Chrome, because it is the browser that works best with the learning management system (Canvas).

What am I doing that is worth protecting?
Assets could include: sensitive topics being researched for class (like a psychology paper on substances - drug use), confidential/personal data (FAFSA includes personal financial info, SSN, parent financial info, etc), a personal Google account (many students log in DIRECTLY to the browser)

Who do I want to protect it from?
Adversaries could include: legal officials (in case they disclose anything incriminating in the paper), other patrons in the library (could be eavesdropping on the persona/financial information, or accidentally log into my accounts via the browser and see my email/assignments/etc). FAFSA is also an often spoofed site, so online predators could be hoping the student will enter personal information into a place they can access.

How likely is it that I will need to protect it?
Since people are constantly having their identity stolen (with SSNs and financial info), very! The content of their undergraduate research is probably harmless, but someone could take their paper on drug use and use it out of context/against them.

How bad are the consequences if I fail?
Their personal identity could be compromised, which could lead to financial ruin in various forms (financial aid not getting their application because they submitted it on a fake site, or identity information could be used by someone to rack up credit harm which can take years to fix).

How much trouble am I willing to go through to prevent these consequences?
(I would hope a lot!) The student would probably be best if they used an incognito window for all these things - since logging into the browser and forgetting to log out gives people direct access

to any feature they use with Google. They would also have to make sure the FAFSA site is .gov and https. They could check in with the librarian to check that they are in the right place. Visually, the computers are close together, so it is hard to totally hide what others might see, but there are privacy screens students can place over the monitor to try to mitigate the risk. (As far as me trying to protect them, I can ask IT to see if it is possible to install Chrome w/ a default of Incognito. I can educate them in the classroom about how easy it is for others to try to take their personal information if they're not careful. I can offer privacy screens and advocate for a different layout in the building as money becomes available. I can educate students on these issues, but when 40 are in use AND students don't want to show me what they are doing to keep it all private, it makes it difficult.)