Make a list. Where is your personal information digitally stored?
DO NOT share sensitive information.

List digital devices (phone, tablet, computer, smart tv…)	**Accounts (emails, online shopping, banking, etc.)**	**Items with Passwords (*not your passwords*)**	*What causes dependencies in your digital universe?*

Let's get messy! Map your digital universe here.

Pick an attacker: The Thief, The Con Artist, The Stalker, The Insider
The more you can specify your attacker's wants, the more you can test your own cybersecurity against their success. You can do this exercise for your own data OR for the data of someone you care about (e.g., a parent, a grandparent, children, teenage nieces and nephews, students…).

Who is your attacker?

What do they want from you?

What opportunities do they have to get their hands on the things in your digital universe?

What resources/knowledge do they have to achieve their goals?

EXERCISE 1: How much information can you find out about yourself online?
In this exercise, take the moment to search about yourself and your closest family members online to see if any of this information could be used to unlock security questions (e.g., confirming your identity on phone calls or security questions you choose on important online accounts).

Step 1: Have I been pawned? https://haveibeenpwned.com/

Step 2: Search engine your name.
Use an "incognito browser" or download the Brave browser to see learn what information is available about you online. Note below if any of this information could directly impact your personal security. Together, we'll discuss what steps you can take next.

EXERCISE 2: LOCATION TRACKING.
In this exercise, we'll look at what information can be learned from location tracking services your devices have about you. There are many reasons why your device may need your location (from maps, directions, to verifying your identity against a hacker). Let's see what kind of information can be learned by just looking at your saved locations.

Step 1: Make a list.
What programs and applications have your location saved? Go through your device and make a list. These may be programs like Google Maps, Yelp, Foursquare, etc.

Step 2: What's using my location tracking and when?
Check your device settings to see if there are any that use "location services" - note which ones are currently on and which ones you have control to turn on/off.

Step 3: What information can these locations say about me?
Discuss and critically assess just how someone can use your saved locations.

EXERCISE 3: How much money can someone spend on my phone right now?
In this exercise, we will assess which of your accounts and devices allow for easier purchasing. There are many reasons why we opt for the convenience of shopping quickly, but it's also worth understanding how easy cash flow can be so you can protect yourself from financial attacks.

Step 1: List the devices and accounts that have your banking information saved for purchase or money transfer reasons.

Step 2: What are the default spending limits and when am I notified of unusual activity?
Look up if the accounts you list above have spending limits. Many banks allow you to set when you get notifications for unusual (or usual) spending activity. Make note if any of these accounts are shared with other individuals or if perhaps you would like to change your personal settings in the future.