C L A S S O U T L I N E

Background	This is designed as a 75 minute Don't Cancel that Class workshop at Greenfield Community College. It isn't tied to specific course content, but can be tailored to a particular course and scaled to shorter or longer class sessions. It is designed as more of a theoretical, reflective introduction to concepts of privacy and security than as a nuts-and-bolts or tech heavy workshop. It could also be used as part 1 in a two-part workshop series in which the second focuses more on specific strategies/methods/software.	
Learning Outcomes	1. Students will reflect on the concepts of privacy and security as they relate to students' own lives. 2. Students will recognize privacy and security vulnerabilities in common app and software features. 3. Students will practice a method for creating strong passwords.	
ACRL information literacy frame	Information has value	
Introduction/Where do you fall on the privacy spectrum?	Hello, my name, background (librarian, LFI, interest in digital privacy and security). You'll see that there's a sign on one wall that says privacy vegan and on the other wall that says privacy nihilist. The privacy vegan would like to live off the grid, disconnected from the digital world. The privacy nihilist says they have nothing to hide and the NSA knows everything about all of us anyway. Imagine that the space between those two walls is a spectrum between those two extremes. I'd like you each to say your name and then move, to the extent you are able, to the space in the room that you feel best represents where you fit between privacy vegan and privacy nihilist. After everyone has introduced themselves and moved around the room, ask for a few volunteers to explain why they placed themselves where they did and explain that other people are welcome to move based on their classmates' arguments.	**Time** 15 min

So what are privacy and security?/ Goals of the day.	Invite people to sit back at the tables. Digital privacy and security issues are constantly in the news, from the Cambridge Analytica scandal to data breaches (Experian, Google+). The terms “privacy” and “security” are often used interchangeably, but they mean different things. What do these two words mean to you? What is privacy? What is security? [Solicit some definitions from the audience. Write them down if possible.] My definitions: *privacy* is the ability to decide who gets to know what about you. *Security* is the steps you take to protect important things or information. Today we’re going to look at some specific ways our privacy is affected by common software applications, and we’re going to look at one specific thing you can do to enhance your own digital security.	10 min

Activity: **The Rewards and Risks of Convenience**	[The purpose of this activity is to get people thinking about unintended consequences (or at least unintended on the consumer end) of popular features. The class is divided in two groups, facing each other, debate style. One side is pro, the other con, but they would flip half way through. The groups are given a list of different tech features, the pro side talks about why these are helpful/make life easier and specific places or apps where they've seen this used. The cons talk about ways that this has been or could be misused, and specific groups who could be/are put at risk by the feature. Have each of these—the points the pro and con sides should touch upon—written on the board. Alternate between pro side talking first and con side. Each side is given the same feature, on an index card, at the same time. Try to get through at least 3 features—can do more depending on time. The moderator (instructor) can suggest things during the debate if the sides are stumped or aren't talking.] Almost all of us use smart phones and social networking software to connect with people and make our lives easier. Some of the same features in apps that enhance the convenience for some people can also put other people at risk. For example, a person being stalked or experiencing intimate partner violence, or an undocumented immigrant, could have a very different risk profile than a wealthy citizen in a stable relationship. I'm going to give each side an index card with an app feature on it. You're going to have 2 minutes first to talk amongst your group members and decide what to say and then the two sides are going to debate. Features: • The ability to tag other people in photographs • Facial recognition technology that automatically scans photographs and suggests people in them • Ability to remotely turn on or off items in a home and check their usage • Map or GPS software/apps that store common travel patterns • Advertising customized to your interests, based on search and purchase history • Single sign-on to multiple websites or services (for example, linked to a social media account) • The ability to remotely turn on apps that can locate a device • Facial recognition-enabled, internet-linked CCTV cameras in high-crime areas • The ability to sign on to devices or access locations with biometrics (like fingerprints)	**Time** 25 min

Check-in	Ask for a few volunteers to share a question they're wondering about after the last activity. Talk through these as a group.	**Time** 5 min
Creating a diceware passphrase	During the debate we talked about some things that can compromise personal privacy and security. I want to give you a method you can use to protect your privacy: really good passwords. What advice have you heard about what makes a strong password? We know, based on tests of password cracking software, that long, random, unique passwords are strongest, we also know that 1) it's really hard to remember lots of different long strings of random characters and 2) humans are pretty bad at faking randomness. There's a method called diceware you can use to create a really good, strong, random passphrase—rather than a single password—that you can probably memorize. You have sets of 5 dice and a printout [or link to PDF, if it's in a computer lab] of a long, numbered wordlist. [Demo the steps below and give out a handout with the same instructions, link to the diceware word list, spaces for 6 5-digit numbers and their corresponding words, and a few lines for writing a mnemonic.] 1. Roll the five dice and write down the numbers that you roll, left to right. 2. Repeat this 5 more times, for a total of 6 5-digit numbers. 3. Using the wordlist, look up the word that corresponds to each number and write it down. Once you're found your passphrase, keep it to yourself. There's a space on your handout that you can use later on to create a story or mnemonic for yourself to help remember your passphrase. Now you have one good, strong passphrase. So what? You can use this as your master password with a password manager, and then use your password manager to generate and store random, unique passwords for everything else. I use a password manager and it's very convenient.	**Time** 15 min
Closing	Final thoughts or questions? If this class has brought up anything that you talk about more, or if you or someone you know is facing specific privacy or security concerns, I am always happy to sit down and talk with you individually. Give my contact info. Thanks all!	**Time** 5 min

Learning Assessment End of Class	Writing prompt assignment (at the professor's discretion): Write a 250-500 word reflection about today's workshop. What topics (if any) that you talked about felt most relevant to you? Are there any changes you think you will make based on things that you talked about today?
Deliverables	Two-sided handout, diceware passphrase worksheet on one side; some tips, things to think about, and list of resources with more information on the other side.
Things to Remember for Next Time	