Library Freedom Project mini-module facilitator guidance + deck notes

Student Privacy Series

Overview

- These mini-module sessions focus on risk assessment for students.
- Sessions are intentionally designed to be short and hands-on to help understand a single privacy topic and apply one solution.

Purpose

- To present privacy information to students, especially new/first-year students and key to how students today think (or don't think) about privacy.
- To improve habits in a privacy-minded (versus security conscious) way.
- To define risk assessment as key to all following sessions.
- To encourage agency and the willingness to push-back when asked for information (from platforms, their College/University, jobs, etc.) that can lead to data leaks, theft, etc.

Session topics

- Risk assessment
- Passwords
- Public Wifi/VPNs
- Browsing Privacy
- Malware

Mode

- live, in-person or online

Tools

- laptop or desktop
- presentation deck available in Canva, PowerPoint, Google Docs, .pdf, .jpg
- a facilitation guide that's adaptable to the facilitator's campus and context
- links to Google Form for quick evaluation

- date and sign up for next session

Session 1 - Risk Assessment

Copy of deck

- Canva: https://www.canva.com/design/DAGNXutbaZw/WgBYwXcjHtLNJoeH9WdAQQ/view
- PowerPoint
- Google Slides: https://docs.google.com/presentation/d/1_ejpuHDrwPi8a-72bj6twLkNJrQLMC4LjI0kMy8zlAE/edit?usp=drive_link

Slide 1

Facilitator offers…

- Welcome
- Topic intro
- Roadmap to the session
    - What is risk assessment and why is it important?

Slide 2

Facilitator asks:

- What info do you as students share to receive service and use tools offered by the school?
- People can share aloud or, if online, put them in the chat for facilitator to read aloud

Slide 3

Facilitator reviews checklist:

- Did we miss anything?
- Is there anything on this checklist that's unexpected?

- Which of these, at the moment, don't seem relevant to the platform or service you're signing up for?

Slide 4

Facilitator shares…

- Real-world, relatable but scaleable example of misuse of cell phone data, e.g. port-out fraud

Slide 5

Facilitator shares…

- Obfuscation as a tactic for using platforms, not giving them accurate information, but memorable info

Slide 6

Facilitator models…

- Use any example, for instance: in response to a security question asking for your pet's name, don't use your family pet's name. Instead think of a favorite movie animal, your uncle's pet, etc; then add digits for each subsequent question.
    - Pet name: Pantheress
    - Favorite vacation place: Pantheress002
    - First car: Patheress003
- Be sure to put the answers somewhere such as…a password protector.

Slide 7

Facilitator can offer…

- Resource list bespoke to campus, favorite privacy websites, etc.
    - Threat modeling zine by Kelly McElroy: http://tiny.cc/lfp-threat-modeling

- Concise deep dive on…*Obfuscation : a user's guide for privacy and protest* by Finn Brunton and Helene Nissenbaum: https://clio.columbia.edu/catalog/14614666

Slide 8

Facilitator shares…

- Contact info
- Link to sign up for next session on passwords
- Invitation to complete very short feedback survey: https://docs.google.com/forms/d/e/1FAIpQLSeI0LgJpBLU5V2PqBjFW31xRA7N3PRLMEElGFW1i6FWegjqzA/viewform

Session 2 - Passwords

- Canva: https://www.canva.com/design/DAGOB5LhCwA/M0jweAwyILdnVv-xogZ2QA/view
- PowerPoint
- Google Slides: https://docs.google.com/presentation/d/1VPXg4DHXYL2QsA6_sf7NbyZrQFCli1yHN6iLEAwIUZA/edit?usp=drive_link

Slide 1

Facilitator offers…

- Welcome
- Topic intro through The Fallacy of the Single Password
- Roadmap to the session

Slide 2

Facilitator empathizes with:

- Proliferation of passwords
- Difficulty of generating unique ones that match sometimes unlisted criteria

- Insecure ways we respond to demands for many passwords

Slide 3

Facilitator shares…

- Bitwarden as a free and robust password manager option
- Download it now
- [create in advance] Demo master password with an account set up specifically for this session

Slide 4

Facilitator offers

- Encouragement
- Walk people through set up/troubleshoot as time allows

Slide 5

Facilitator shares…

- URL to sign up for next session
- URL to complete brief evaluation of session: https://docs.google.com/forms/d/e/1FAIpQLSdhfdJcAE54ptOZquuuf3BEfsYw0VoKvAJhck_qmFhHHbWNVQ/viewform

Slide 6

Facilitator can offer…

- Resource list bespoke to campus, favorite privacy websites, etc.
    - Passwords zine by Kelly McElroy: http://tiny.cc/lfp-password-zine
    - Bonus: Want a privacy-minded way to manage two-step authorization? Check out TOFU for iOS (https://www.tofuauth.com/) or Authy for Android: (https://authy.com/features/)

Session 3 - Privacy on Public Wifi/VPNs

- Canva: https://www.canva.com/design/DAGOCy6_eLo/oNJsVJNo-5o_gBjSSx2WNg/view
- PowerPoint
- Google Slides: https://docs.google.com/presentation/d/1hzVY7DLyn4oagH9c1-BDxxXjITlFazid_UC-1VhmFKs/edit?usp=drive_link

Slide 1

Facilitator offers…

- Welcome
- Topic intro through theme of constant weighing of convenience versus privacy

Slide 2

Facilitator asks:

- Where do you use public wifi and why?
- What is urgent? What can wait until back on a secured network?

Slide 3

Facilitator shares…

- Risks of public wifi use, including unsolicited airdrops, intercepts of important details transmitted (e.g. passwords, banking info)

Slide 4

Facilitator encourages…

- Locking down iOS Airdrop and Android Nearby features
- Think about whether you need a VPN.[1]

[1] You shouldn't use a VPN if:
- You want to encrypt your traffic.

- Does a VPN foster a false sense of security?
- Can you use the VPN that's already installed on your phone?
- Help install and set up Proton VPN on device: https://protonvpn.com/

Slide 5

Facilitator shares…

- URL to sign up for next session
- URL to complete brief evaluation of session: https://docs.google.com/forms/d/e/1FAIpQLScqNOYWBq6qmZ3ML0mDouF7F-9h7oRQDq9oiSfe8ha5oBgkZQ/viewform

Slide 6

Facilitator can offer…

- Further resources and encourage attendees to see if there's an LFP Privacy Advocate in their home/community to share info with friends, family

---

Session 4 - Browsing Privacy

- Canva
- PowerPoint
- Google Slides:

Most of your traffic is already encrypted because most common sites support HTTPS. Encrypting your DNS queries is becoming standard too in web browsers. There's all kinds of other metadata in your network packets available to track you. Advanced actors can correlate them to track and discover your location. There are some cases where using a VPN does make sense though.
- You want to hide your identity.
- You want to mask your IP address.
- Circumventing IP blocks to watch Netflix
- Getting around national firewalls
- Bypassing download limits
- Performing offensive security assessments
- Conducting OSINT and research

https://docs.google.com/presentation/d/1zbKnhKguRotZFFyvfZCuf13TwtrRog-Y-WFnK3YYUWE/edit?usp=drive_link

Slide 1

Facilitator offers…

- Welcome
- Topic intro through theme of targeted ads
- Roadmap to the session
    - Why is this important: your phone likely isn't listening to you to target ads, but data brokers are tracking other device usage to sell your data.

Slide 2

Facilitator shares:

- Range of places our data is sold, e.g. LFP's "All about data brokers" flyer

Slide 3

Facilitator shares:

- Benefits of secure browsing using Tor, Firefox, and Opera as examples
- Ability to block trackers, disallow pop-ups, browse freely/uncensored

Slide 4

Facilitator shares:

- URL to sign up for next session
- URL to complete brief evaluation of session: https://docs.google.com/forms/d/e/1FAIpQLSfehFTwQwJeHXh6CH2YrMsiiZcHM62lDi9ggCMJ4y9y1VnYjg/viewform

Slide 5

Facilitator shares:

- Further resources to LFP site and Preventative Measures Against Doxxing and Online Harassment: http://tiny.cc/lfp-antidoxxing-guide

Session 5 - Malware

- Canva
- PowerPoint
- Google Slides: https://docs.google.com/presentation/d/1Bxp8IwUUZB_LtoWYNQrBc7sHdcAl3oU4ej52mF0XUq8/edit?usp=drive_link

Slide 1

Facilitator offers…

- Welcome
- Topic intro
- Roadmap to the session
    - Why is this important

Slide 2

Facilitator defines malware and asks:

- Who's experienced a malware attack or attempt to install (e.g. websites, phishing emails with bad actor .pdfs)

Slide 3

Facilitator asks:

- What's stored locally on your computer that you'd hate to lose?
- Archivist sidenote about LOCKSS (lots of copies keeps stuff safe) principle
- Auto-save, if saving locally

Slide 4

Facilitator shares…

- Role of blockers for pop-ups and trackers
- Install and look at Opera settings, note pros and cons (sometime slower, some sites refuse to work if blockers are detected)

Slide 5

Facilitator shares…

- Email contact
- Brief feedback online and request for other topics of interest: https://docs.google.com/forms/d/e/1FAIpQLScDHOOB33QelJYpQ_C1ZoEptKdtUdOL83Q50bcJ1dO_oOL5lQ/viewform