Teaching Privacy in Libraries: Strategies and tools

https://libraryfreedomproject.org/resources-01/privacytoolkit/

An Infopeople Webinar
Presented by Alison Macrina
March 29, 2018

Infopeople is dedicated to bringing you the best in practical library training and improving information access for the public by improving the skills of library workers. Infopeople, a grant project of the Califa Group, is supported in part by the Institute of Museum and Library Services under the provisions of the Library Services and Technology Act administered in California by the State Librarian. This material is covered by Creative Commons 4.0 Non-commercial Share Alike license. Any use of this material should credit the funding source.
About me

- Internet activist
- Former librarian
- Library Freedom Project
- Tor Project
Goals

- Learn how to assess risk
- Get familiar with basic digital privacy concepts and best practices
- Learn privacy tools to teach
- Get resources for teaching privacy
What we’ll cover

- Threat modeling/assessing risk
- Best practices and talking points
- Web browsing
- Other online activity
- More resources
- Questions
Threat modeling

- Assets
- Adversaries
- Capabilities
- Consequences
Threat modeling

- aka risk assessment
- What it is
- How you can use it
- Let’s try it together!
Who are the adversaries you identified?
What do we do?

- We need broad political and technical solutions.
- In the meantime, we can take steps to reduce harm.
Talking points

- How do you define privacy?
  - control
  - autonomy
  - Choice
- What are some anti-privacy arguments? (group activity)
  - eg “I have nothing to hide.”
• If data is collected or stored, it can be exploited
• If data is transmitted or stored insecurely, it can be exploited
• The longer data is kept, the more likely it is to be exploited
• Metadata and content are both important
• Proprietary software has risks that free and open source software does not (but no software is perfect)
Basic best practices

- Tell the machines less information
- Or feed them noise (eg AdNauseum)
- Desktop > mobile
- Software updates
- DeepFreeze or CleanSlate
- Data policies
- Chrome as default web browser
  - Settings → privacy → turn off tracking
Social media

• Can Facebook ever be used safely? Maybe not.
• Does Facebook need to know this about me?
• Privacy settings can’t be relied on
• Location services – always off
• Photos are risky
  – Who is in them and what is their threat model?
  – What’s in the background?
  – Did you remove the metadata (exif)?
• Don’t RSVP to events
Doxing

- Doxing is the practice of publishing PII without consent, in order to create chaos
- Remove information from data brokers
- Don’t give PII to social media
- Use strong passwords and endpoint security
Passwords

(the biggest vulnerability on the internet)

- Strong passwords are complex, random, and unique
- Use EFF dice method to create a master passphrase
- Use a password manager to store all other passwords
  - Lastpass
  - 1Password
- Use 2factor authentication
- Lie to security questions
- Use at least a six-digit pin on mobile
Browsing (more) safely

- Problems with web browsers
  - Best options: Chrome or Tor Browser
- Problems with search engines
- The business model of the internet
- Better alternatives exist for desktop than mobile
Your connection is not private

Attackers might be trying to steal your information from expired.badssl.com (for example, passwords, messages, or credit cards). NET:ERR_CERT_DATE_INVALID

Automatically report details of possible security incidents to Google. Privacy policy

Back to safety
The web without third-party trackers

Privacy Badger
Basic best practices

https://libraryfreedomproject.org
Welcome to Tor Browser
You are now free to browse the Internet anonymously.

Test Tor Network Settings

What Next?
Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

Tips On Staying Anonymous »

You Can Help!
There are many ways you can help make the Tor Network faster and stronger:
- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »
- Obscures your real IP
- Prevents cross-site correlation
- No one can see the websites you visit
- Blocks fingerprinting, cookies, scripts
- Writes nothing to disk
• Orbot and Orweb: free Tor for Android
• No officially supported Tor for iOS
• Onion Browser for iOS is functional if not official!
A more private search engine:
duckduckgo.com
Signal

- Please download it!
- Encrypted texting, calling, video chat
- Android, iOS, MacOS, Windows, Linux
- No stored metadata
- Totally free
- How does it compare to Whatsapp?

[Image of a Signal chat]

https://libraryfreedomproject.org
Resources

- EFF’s Security Education Companion
- Library Freedom Project: libraryfreedomproject.org/resources
- Tactical Technology Collective’s Security in a Box: tacticaltech.org/projects/security-in-a-box-key-project
- DIY Cybersecurity for Domestic Violence: hackblossom.org/domestic-violence/
Questions?

Alison Macrina
alison@libraryfreedomproject.org