WRITE THIS STUFF DOWN

@flexlibris
alison@libraryfreedomproject.org

libraryfreedomproject.org/resources/privacytoolkit

https://libraryfreedomproject.org
ADVERSARIES
FREE SOFTWARE (FOSS)

http://libraryfreedomproject.org
Firefox
- Easy to use
- Not secure by design
- Use when Tor Browser gets weird
- Many privacy extensions available

Tor Browser
- Patched version of Firefox
- Some usability barriers
- Very secure
- Use until it does something you don't understand
- Bundled with HTTPS Everywhere and NoScript extensions
- Don't add any more extensions!

https://libraryfreedomproject.org
When torproject.org is blocked...

- Getter robots
- Bridges
- LFP letter to convince IT/city to unblock Tor
- Yes, Tor will subvert library computer filters!
- Tor Browser will run from a flash drive

https://libraryfreedomproject.org
DELETE COOKIES?!
~28 bits of entropy

\[ 2^{28} = 3 \text{ days at } 1000 \text{ guesses/sec} \]

Plausible attack on a weak remote web service. Yes, cracking a stolen hash is faster, but it's not what the average user should worry about.

Difficulty to guess: EASY

Difficulty to remember: HARD

Was it trombone? No, troubador, and one of the Os was a zero?

And there was some symbol...

Through 20 years of effort, we've successfully trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess.

That's a battery staple. Correct!

Correct horse battery staple

~44 bits of entropy

\[ 2^{44} = 530 \text{ years at } 1000 \text{ guesses/sec} \]

Difficulty to guess: HARD

Difficulty to remember: You've already memorized it
MOBILE DEVICES

https://libraryfreedomproject.org
Signal: encrypted text and calls

Hey! I need to demonstrate Signal during my mobile privacy talk. Can you send me some innocuous messages so I can take a screencap?

Here's a picture to show that you can send pictures.

Hey that's a cool picture. Check out this one:

https://libraryfreedomproject.org
EMAIL 😱

who can read your email?

- your email service provider
- operators of intermediate network connections
- your intended recipient's email service provider
- anyone who accesses those servers
- worse if you're not using TLS connections
• PGP email encryption
  - setup is the hard part!

• safer email providers
  - pobox.com
  - riseup.net
  - mykolab
  - alumni email
  - a server you trust

https://libraryfreedomproject.org
VIRTUAL PRIVATE NETWORKS

https://libraryfreedomproject.org
PRIVACY BEST PRACTICES

Legal and consumer resources
- PrivacySOS (ACLUm): privacysos.org
- Electronic Frontier Foundation: eff.org
- Tor Project: blog.torproject.org
- Bruce Schneier’s blog on security: schneier.com

Vendor relationships and policies
- ALA Library Privacy Guidelines for E-book Lending and Digital Content Vendors

In-library policies and practices
- data minimization (data retention policies)
- data encryption
- law enforcement requests
- other privacy concerns

https://libraryfreedomproject.org
Advocacy groups
- American Civil Liberties Union: aclu.org
- Electronic Frontier Foundation: eff.org
- Tor Project: blog.torproject.org
- Freedom of the Press Foundation: freedom.press

Media sources
- The Intercept: theintercept.com
- ProPublica: propublica.org

Resources for action
- Cryptoparty: cryptoparty.is
- LFP resources: libraryfreedomproject.org/resources
- EFF Surveillance Self-Defense: ssd.eff.org
- Bruce Schneier’s blog on security: schneier.com

https://libraryfreedomproject.org