

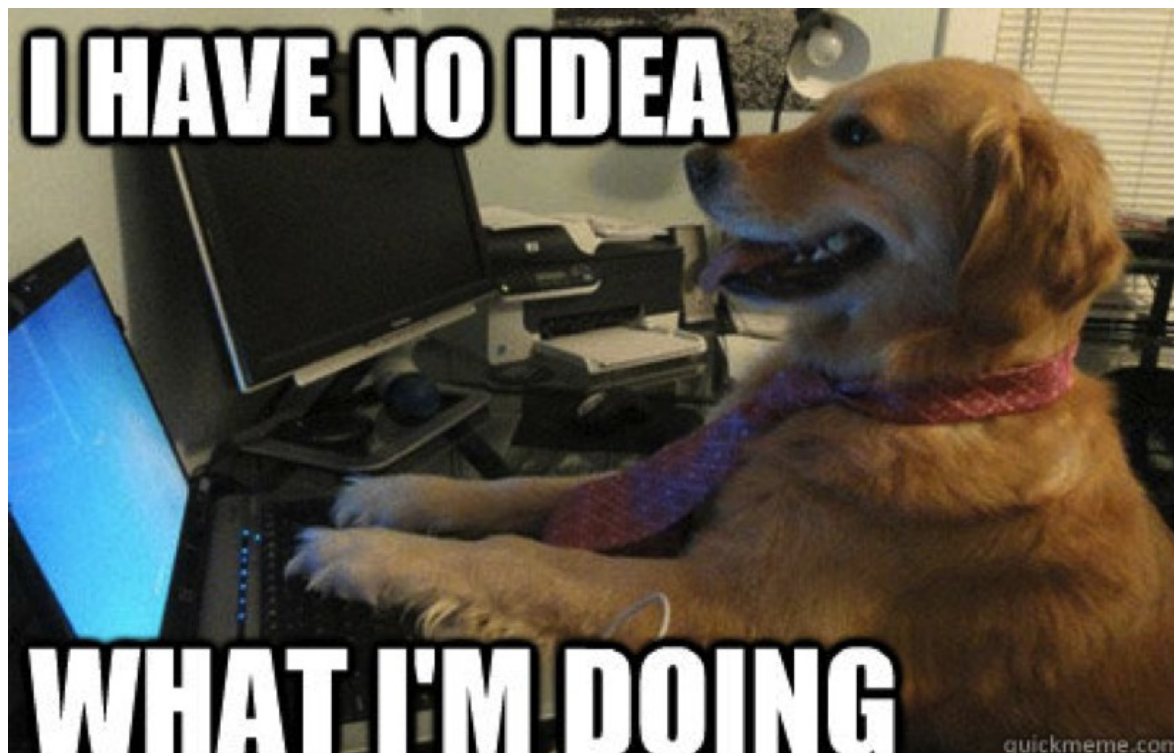
ONLINE PRIVACY WITHOUT TEARS



Alison Macrina

alison@libraryfreedomproject.org

libraryfreedomproject.org

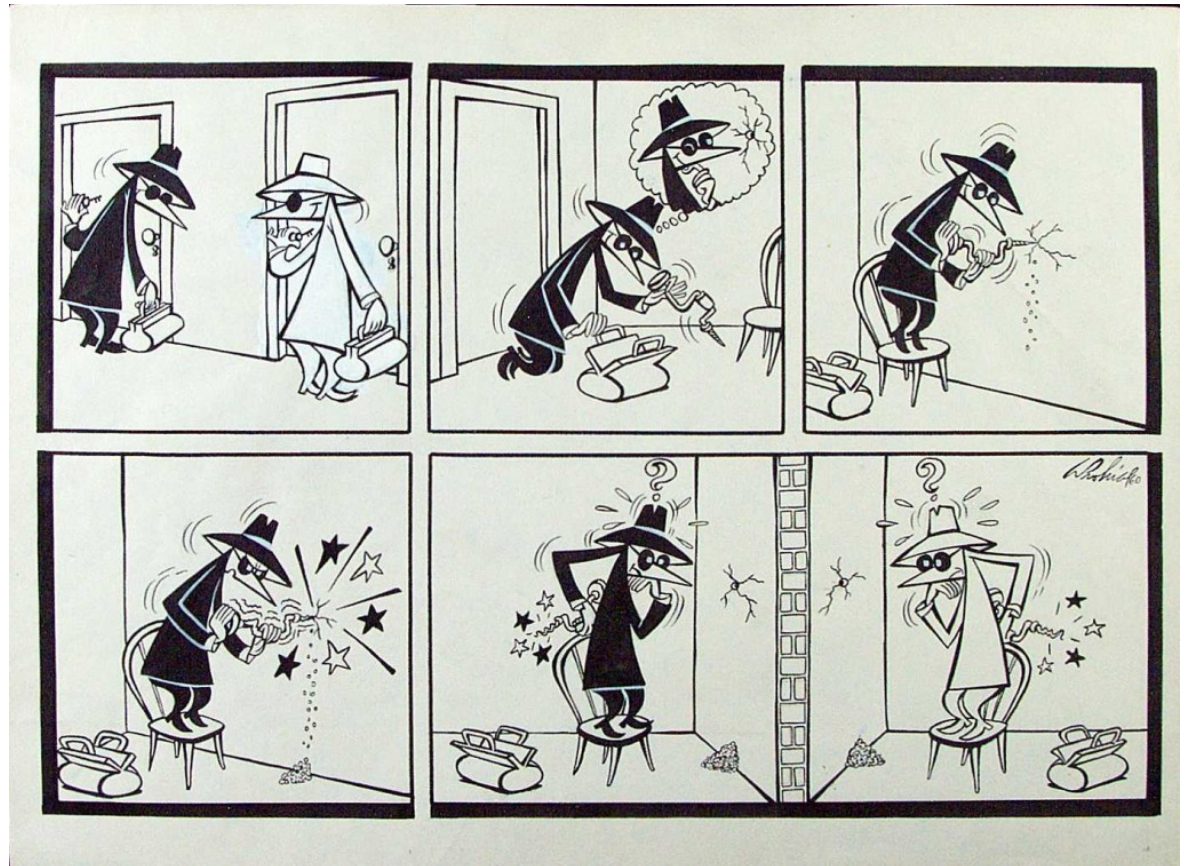


[https://libraryfreedomproject.org/
resources/onlineprivacybasics/](https://libraryfreedomproject.org/resources/onlineprivacybasics/)

The only link you need!

THREAT MODELING

- assets
- adversaries
- capabilities
- consequences



FREE SOFTWARE

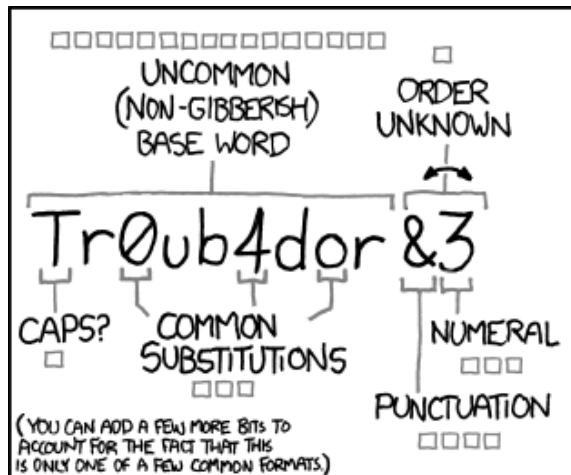
the freedom to run, copy, distribute, study,
change and improve the software
(gnu.org)

- vs. proprietary software
- why does this matter for privacy?
- most of these tools are free software

SOFTWARE UPDATES



PASSWORDS



~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.)

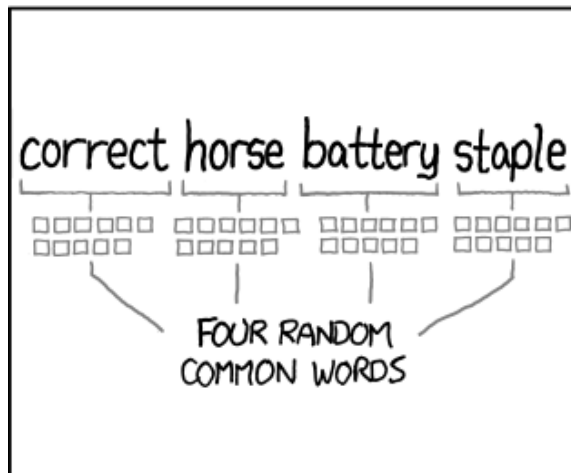
DIFFICULTY TO GUESS:
EASY

WAS IT TROMBONE? NO,
TROUBADOR. AND ONE OF
THE 0s WAS A ZERO?

AND THERE WAS
SOME SYMBOL...



DIFFICULTY TO REMEMBER:
HARD



~44 BITS OF ENTROPY

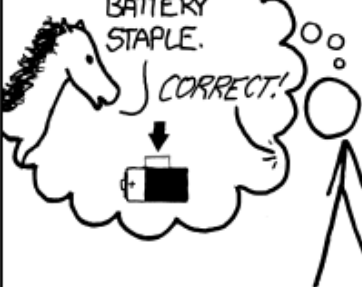
□□□□□□□□□□
□□□□□□□□□□
□□□□□□□□□□
□□□□□□□□□□

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS:
HARD

THAT'S A
BATTERY
STAPLE.

CORRECT!



DIFFICULTY TO REMEMBER:
YOU'VE ALREADY
MEMORIZED IT

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.

Your passwords are bad.
So are everyone else's.

–high entropy

COMPLEXITY! LENGTH!

NO PATTERNS!

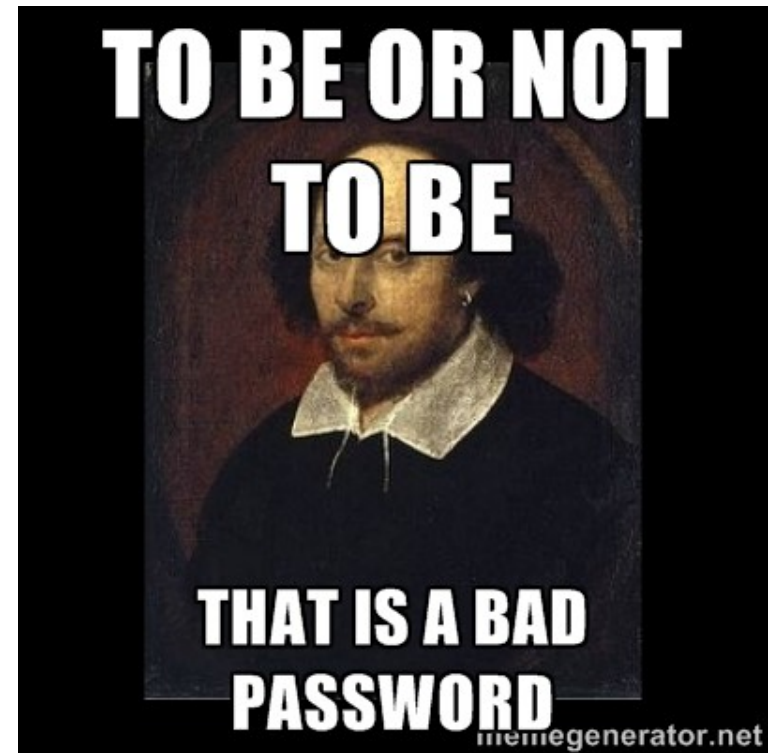
–password managers

KeePassX

KeePass

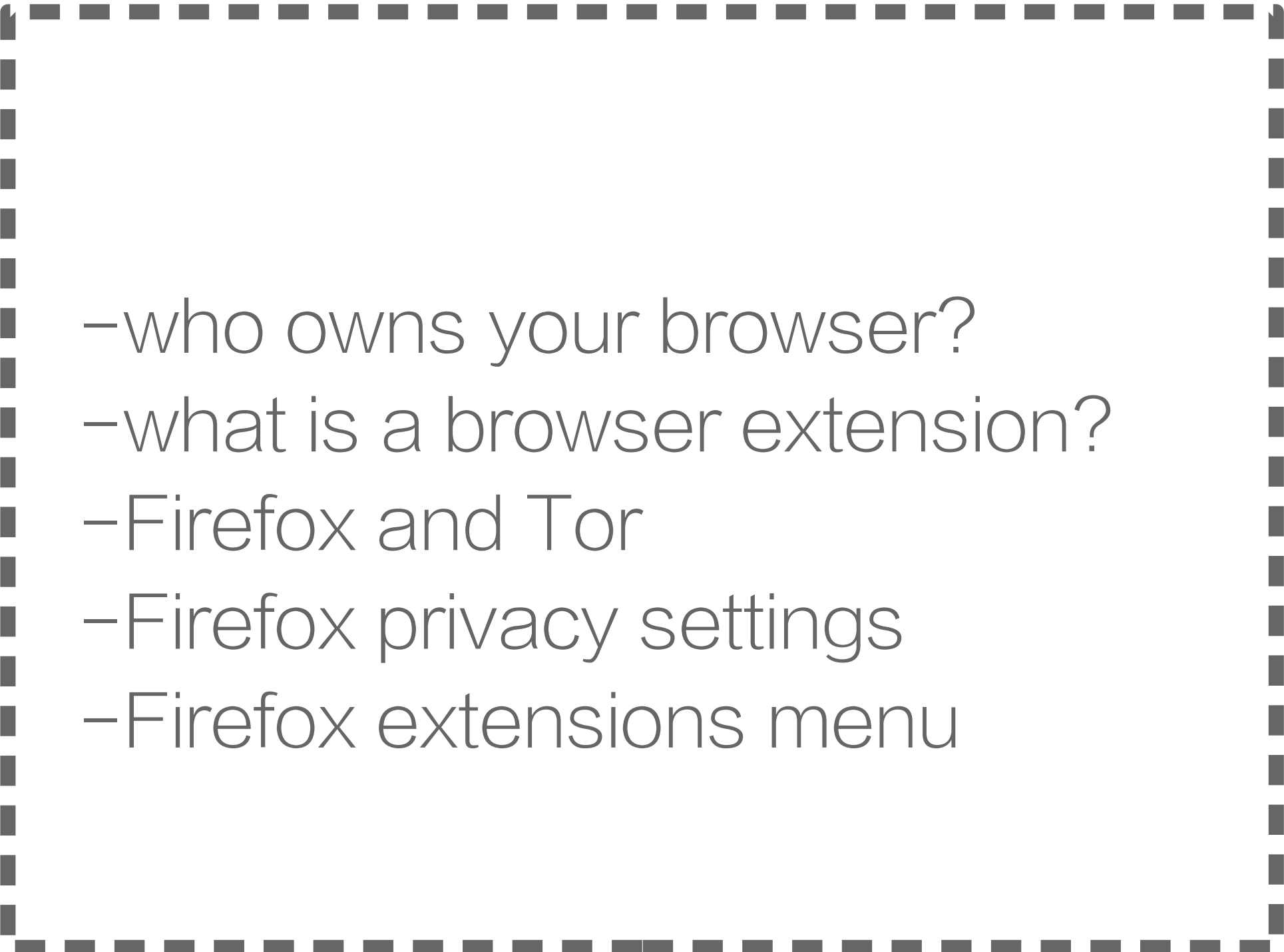
1Password

–diceware list and die





FIREFOX + EXTENSIONS

- 
- who owns your browser?
 - what is a browser extension?
 - Firefox and Tor
 - Firefox privacy settings
 - Firefox extensions menu

- behavioral analytics
- cookies
- analytics
- other unique identifiers
- Privacy Badger
- uBlock Origin
- DuckDuckGo search engine



This is a real image from an online marketing company.

- what is encryption?
- 1. confidentiality
- 2. authenticity
- 3. integrity
 - http vs https
 - HTTPS Everywhere





TOR BROWSER

Tor is the most secure browser available.



- Tor vs. Firefox
- Tor extensions: HTTPS Everywhere and NoScript
- Tor best practices
- more with Tor (mobile, proxies)



LOCAL FILE MAINTENANCE

Cleans system and
protects privacy:

- trash
- logs
- recent places
- cache
- session data and more



CCleaner – Windows and Mac OSX, not FOSS

*Windows users, do not ever use the registry cleaner!

Bleachbit – Windows and Linux, FOSS



DISK ENCRYPTION



- What does disk encryption do?
- Make sure to back up all files first!!!
- OS X: Filevault
- Windows: Bitlocker
- Linux: LUKS
- Alternative: Veracrypt



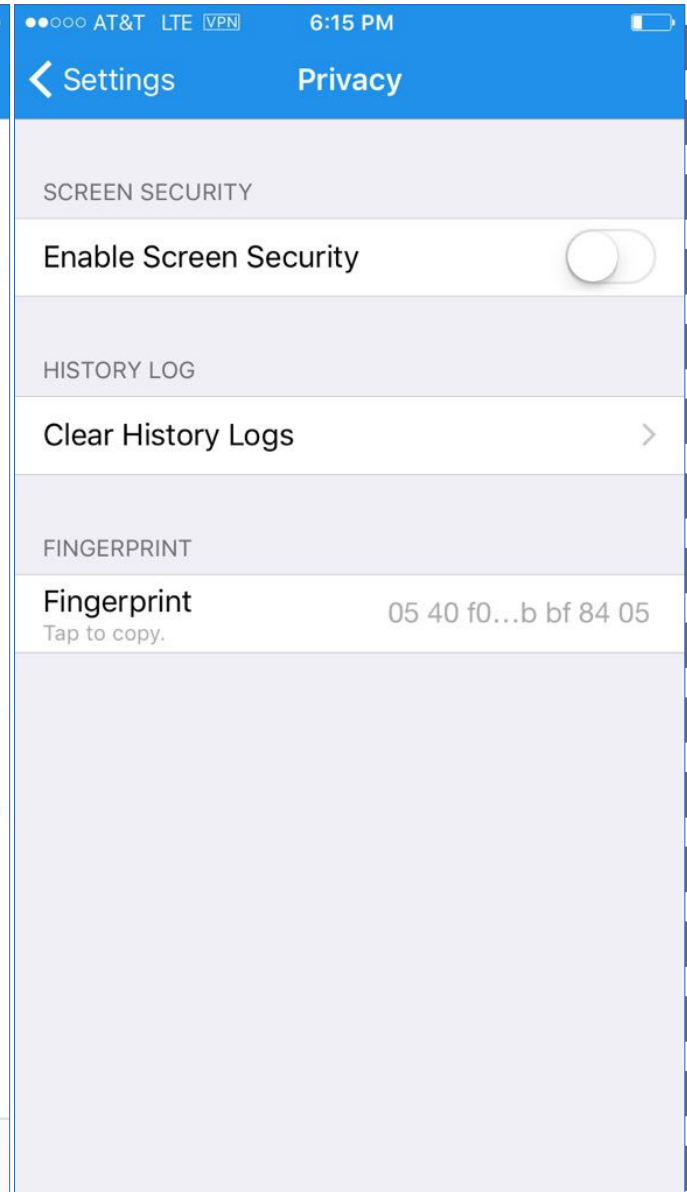
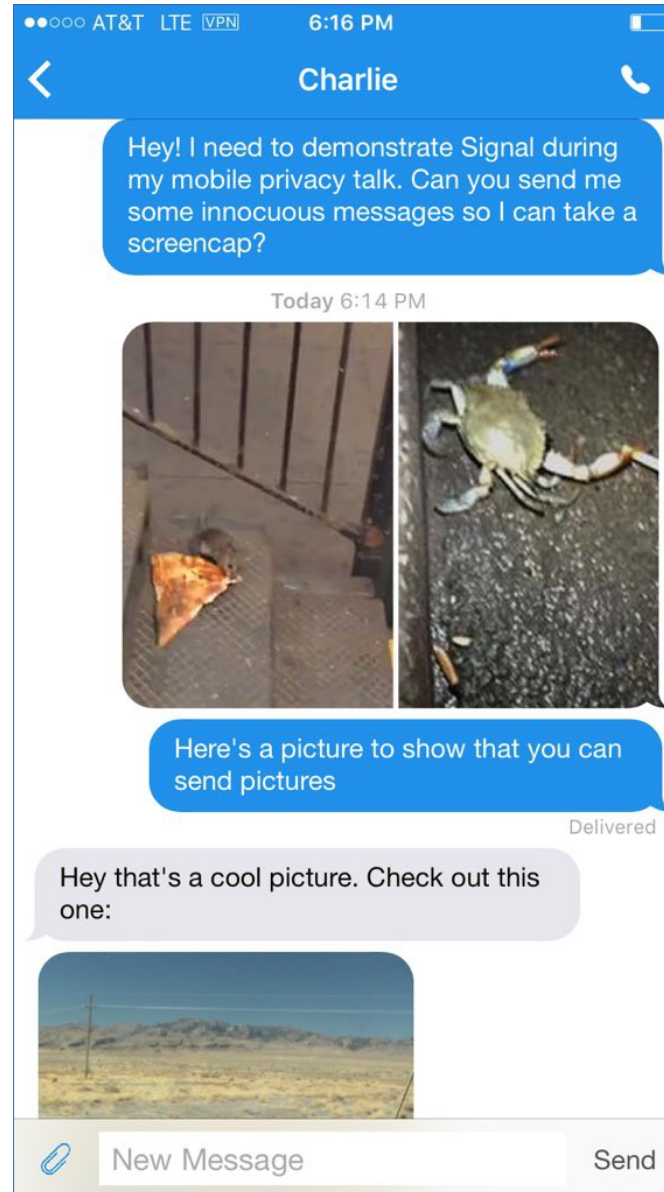
MOBILE DEVICES

-LFP's mobile privacy toolkit

-Android vs iOS

-The Guardian Project (Android)

-Encrypted texts and calls with Signal (iOS and Android)





VIRUSES AND MALWARE

DON'T GET SCAMMED! BE SAFE!

- phishing, script kiddies, malicious links, malicious attachments, and other scams
- differences between viruses and malware
- relationship to privacy
- good practices

antivirus: ClamAV

antimalware: MalwareBytes (Windows only, free vs pro)



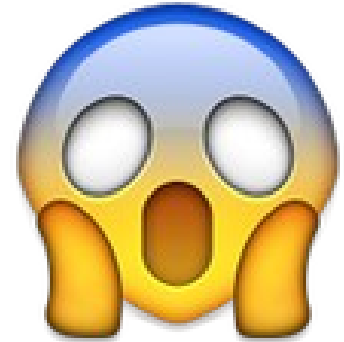
we're almost finished!



time for some difficult stuff!



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

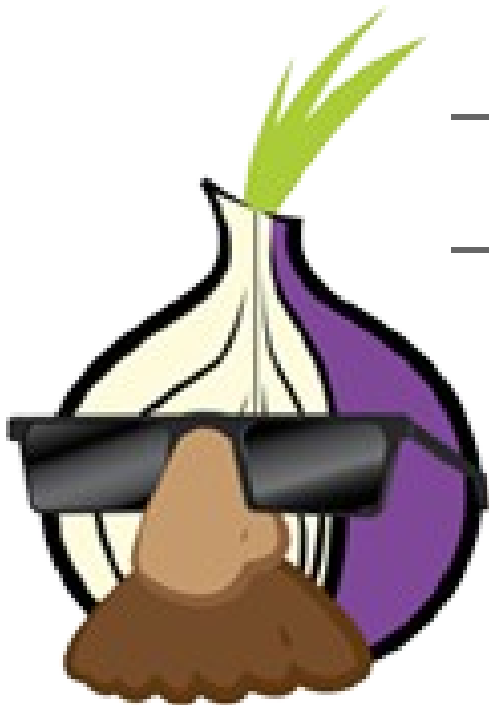
PGP encryption

- email self-defense from FSF email providers

- pobox.com

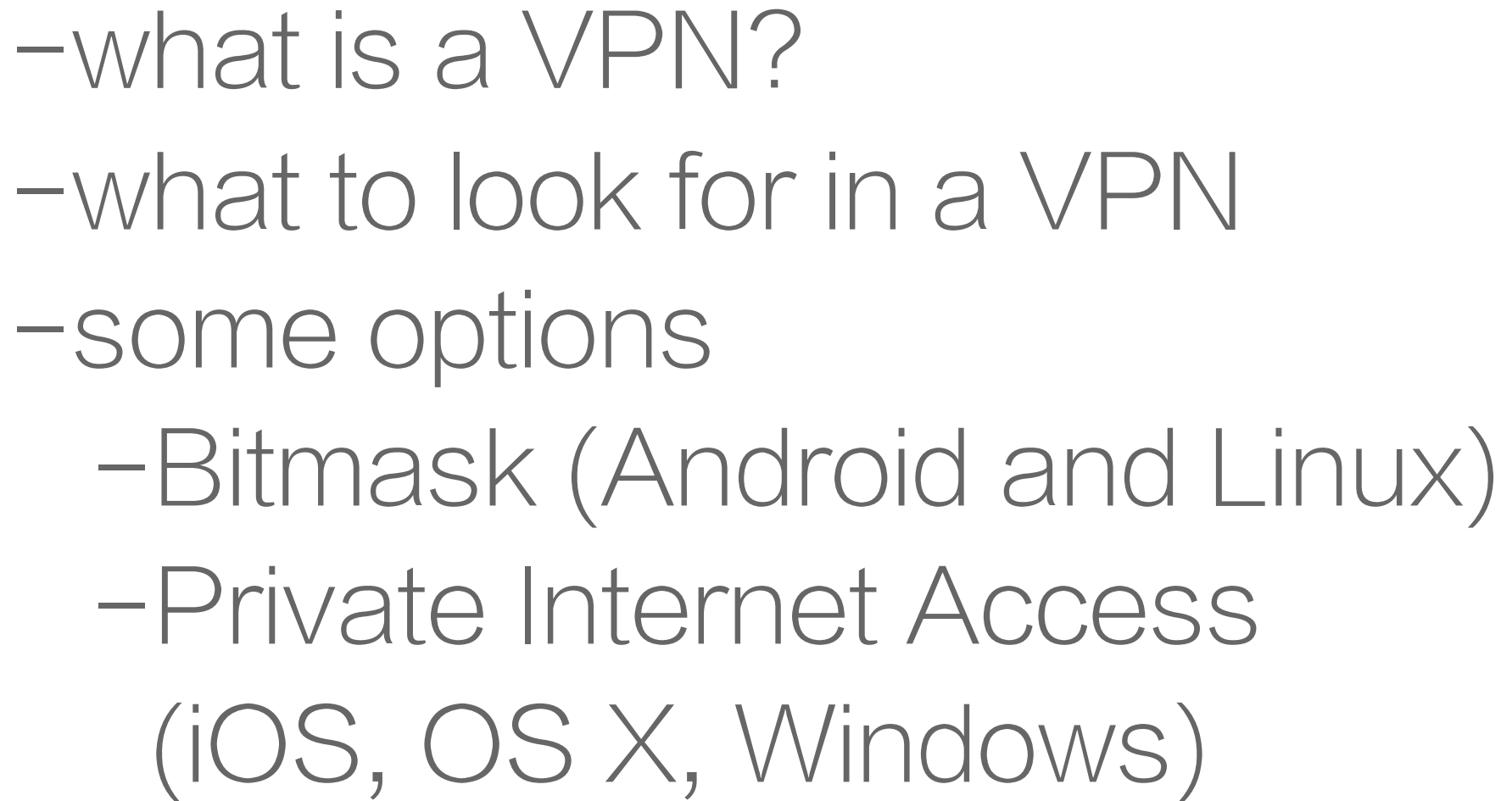
- alumni email

- a server you trust





VPN

- 
- what is a VPN?
 - what to look for in a VPN
 - some options
 - Bitmask (Android and Linux)
 - Private Internet Access
(iOS, OS X, Windows)

EXTRA CREDIT

- PRISM Break
- Surveillance Self-Defense (EFF)
- Schneier's blog
- Cryptoparties
- LFP resources

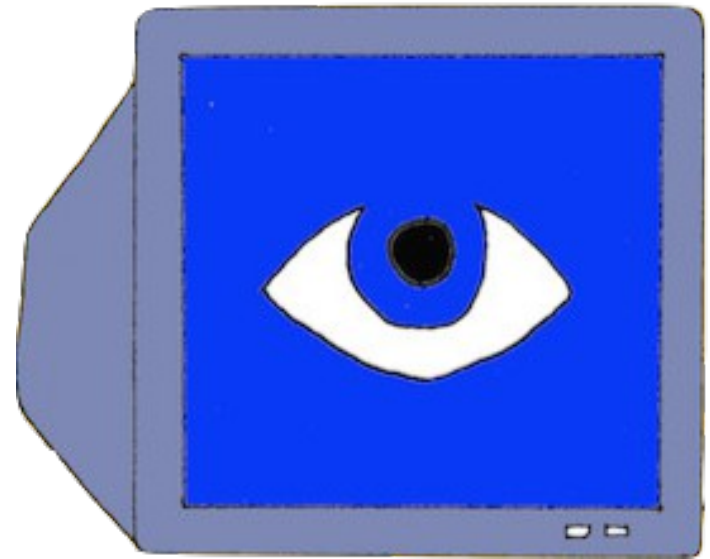


alison@libraryfreedomproject.org

@flexlibris

@libraryfreedom

libraryfreedomproject.org



Attribution-ShareAlike 4.0 International
www.creativecommons.org