

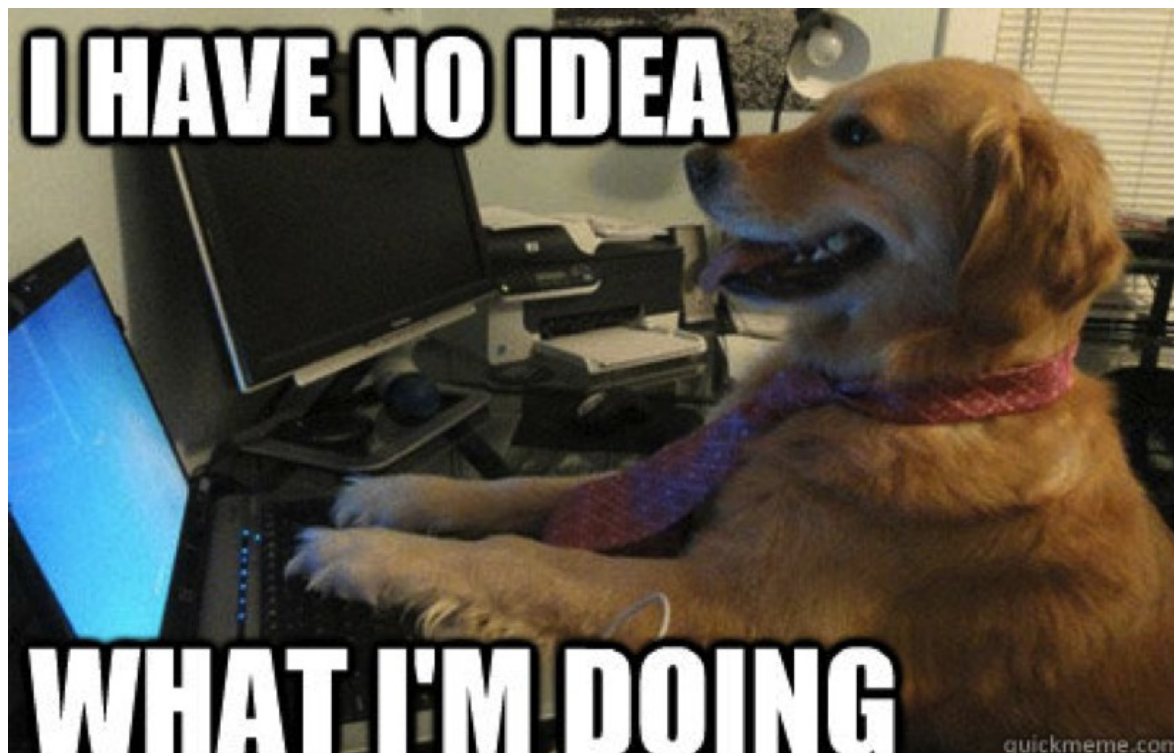
# ONLINE PRIVACY WITHOUT TEARS



Alison Macrina

[alison@libraryfreedomproject.org](mailto:alison@libraryfreedomproject.org)

[libraryfreedomproject.org](http://libraryfreedomproject.org)



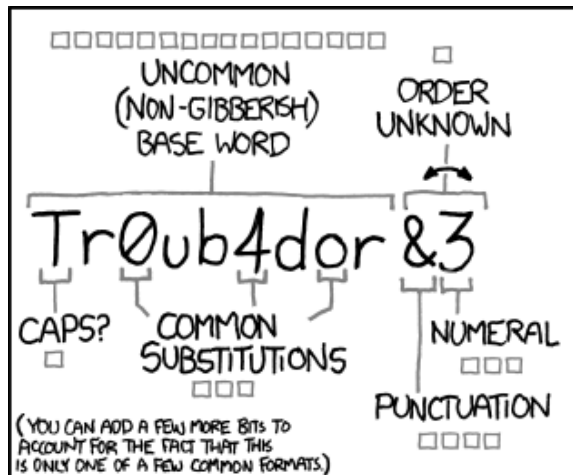
[https://libraryfreedomproject.org/  
resources/onlineprivacybasics/](https://libraryfreedomproject.org/resources/onlineprivacybasics/)

The only link you need!

# THE PROBLEM



# PASSWORDS



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

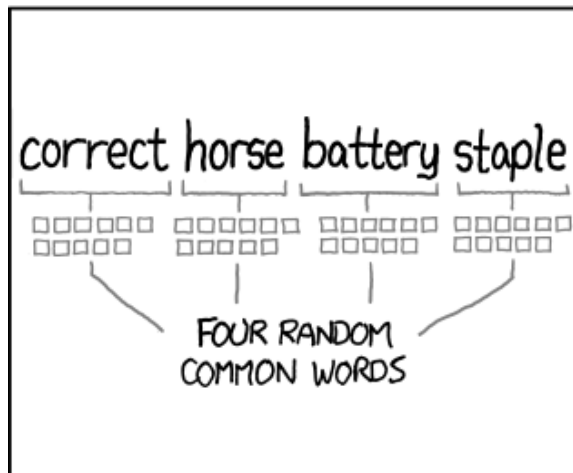
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

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.

- high entropy

COMPLEXITY! LENGTH!

NO PATTERNS!

- master passphrase  
with diceware

- password manager

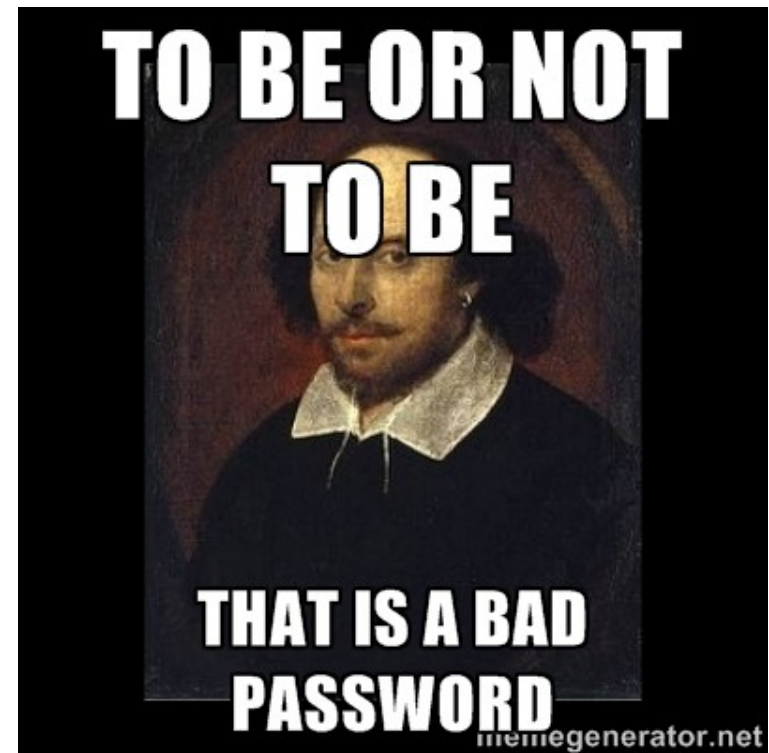
  - 1Password (very good, \$)

  - LastPass (kind of good, free)

  - KeePassX (very good, free, difficult!)

- 2factor authentication

- mobile passwords

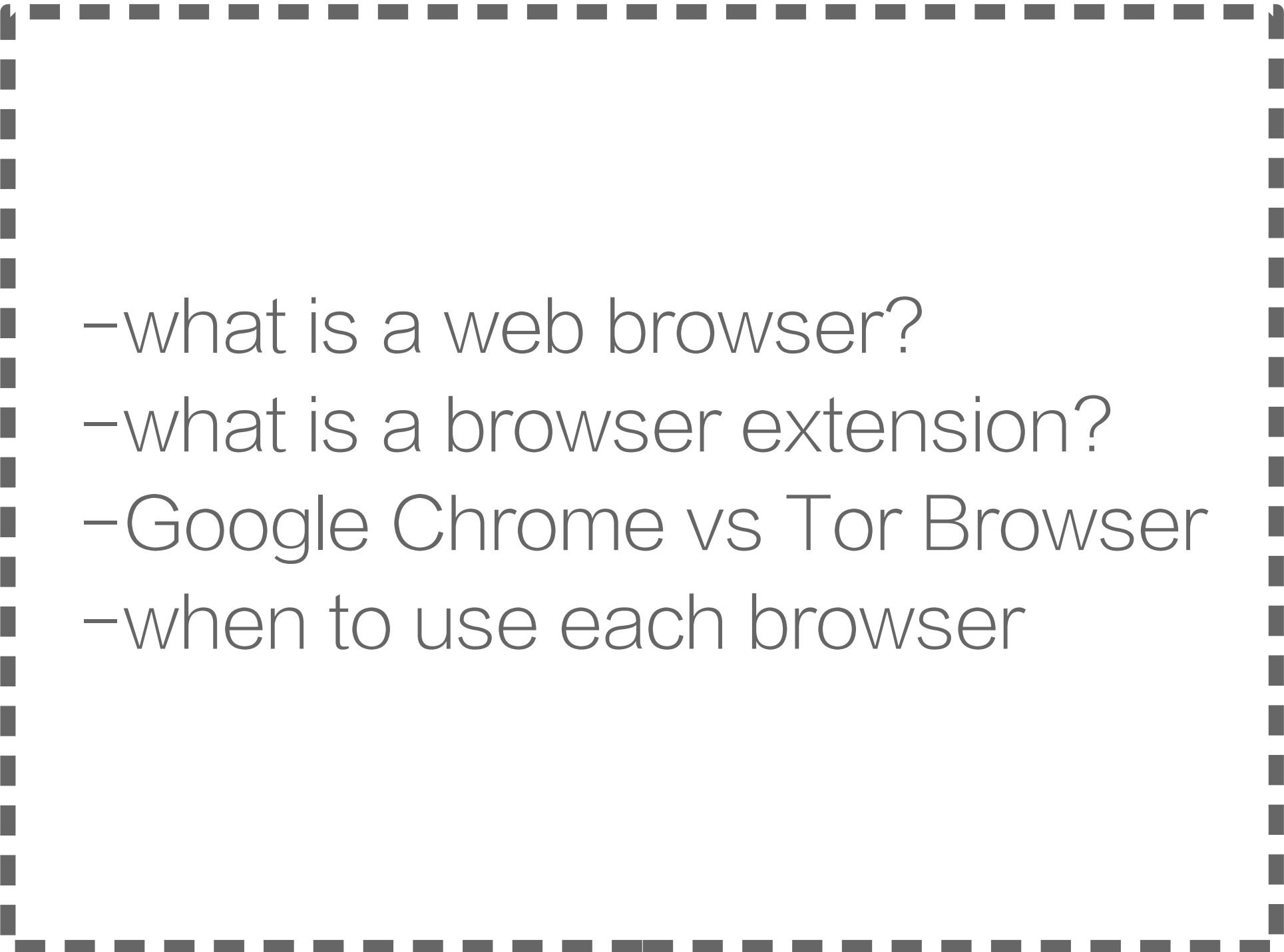


# SOFTWARE UPDATES





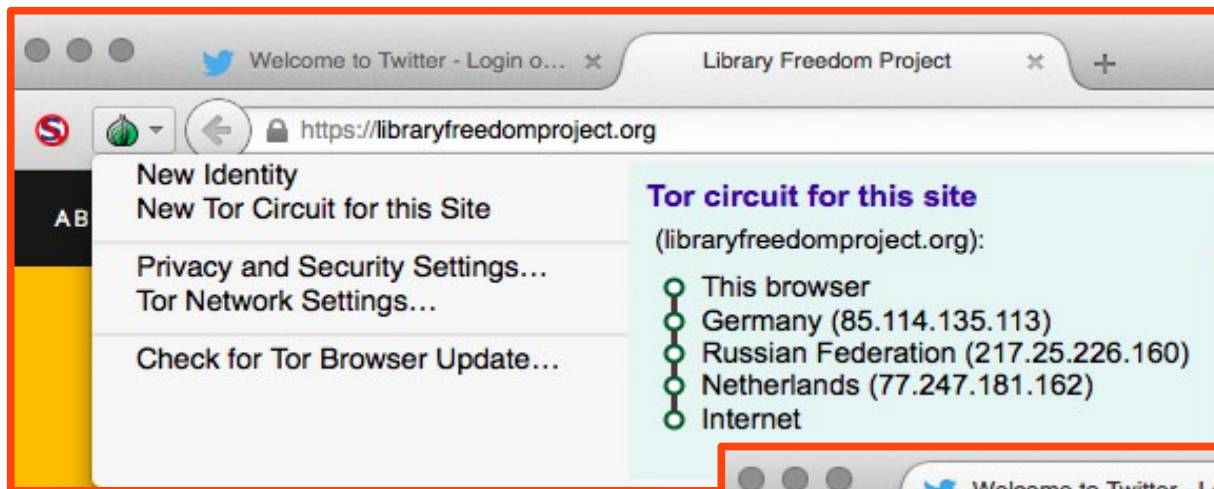
BROWSERS

- 
- what is a web browser?
  - what is a browser extension?
  - Google Chrome vs Tor Browser
  - when to use each browser





TOR BROWSER



- location privacy
- prevent sites from correlating your browsing
- hide from ISPs, network operators
- Tor extensions: HTTPS Everywhere and NoScript
- Tor best practices



CHROME + EXTENSIONS

# How is Chrome more secure?

- Safe Browsing
- sandboxing
- auto updates
- HSTS support

Why is Chrome not-so-private?

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

Oh my gosh!  
It's a sign!  
I must buy this!

HOW TO MAKE YOUR  
**CUSTOMERS**  
**THINK**  
BUYING YOUR  
**PRODUCT IS**  
**THEIR FATE!**  
SWEENEYMAE.COM




This is a real image from an online marketing company.



- what is encryption?
- http vs https
- how to tell the difference
- be mindful of security warnings!

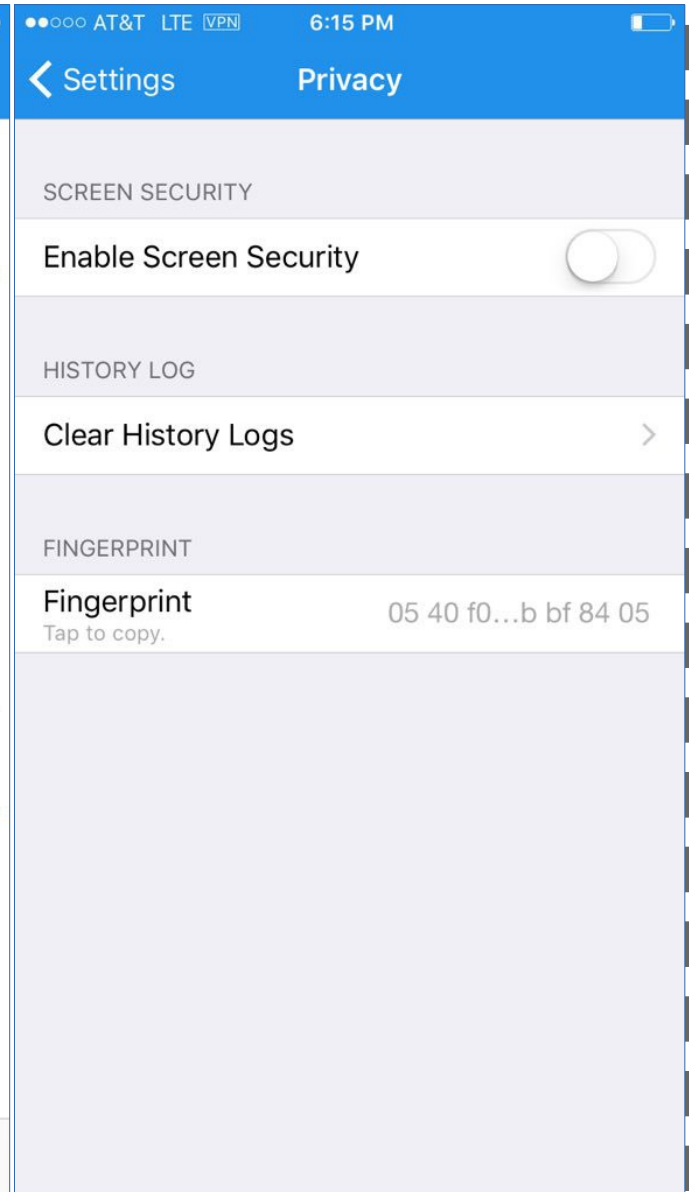
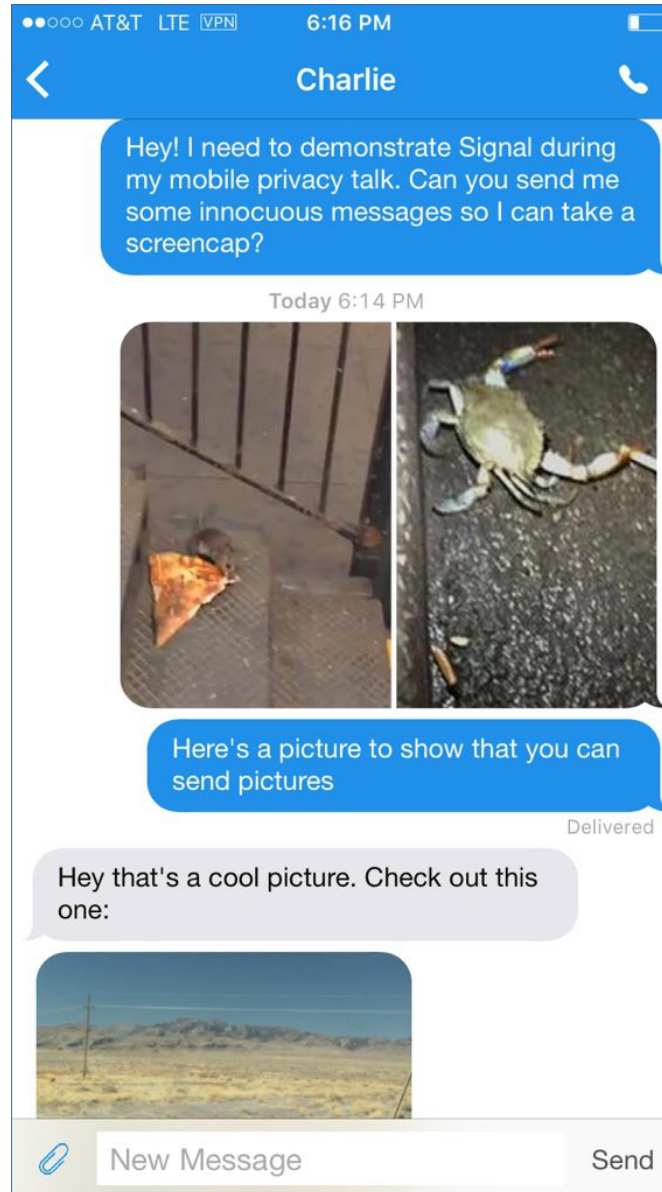


MOBILE DEVICES

- 
- Mobile devices: pretty hopeless!
  - The evil baseband
  - Android vs iOS
  - compartmentalization
  - mobile device passwords
  - mobile device encryption
  - The Guardian Project (Android)



Encrypted  
texts and calls  
with Signal (iOS  
and Android)





DISK ENCRYPTION



- What does disk encryption do?
- First: make backups (this can also help if you get malware)
- FDE OS X: Filevault
- FDE Windows: Bitlocker
- volumes, folders, and files: Veracrypt



MALWARE

- phishing and social engineering via malicious links, malicious attachments
- scary as heck ransomware
- how can I tell if I've been attacked?

antivirus: ClamAV

antimalware: MalwareBytes (Windows only, free vs pro)



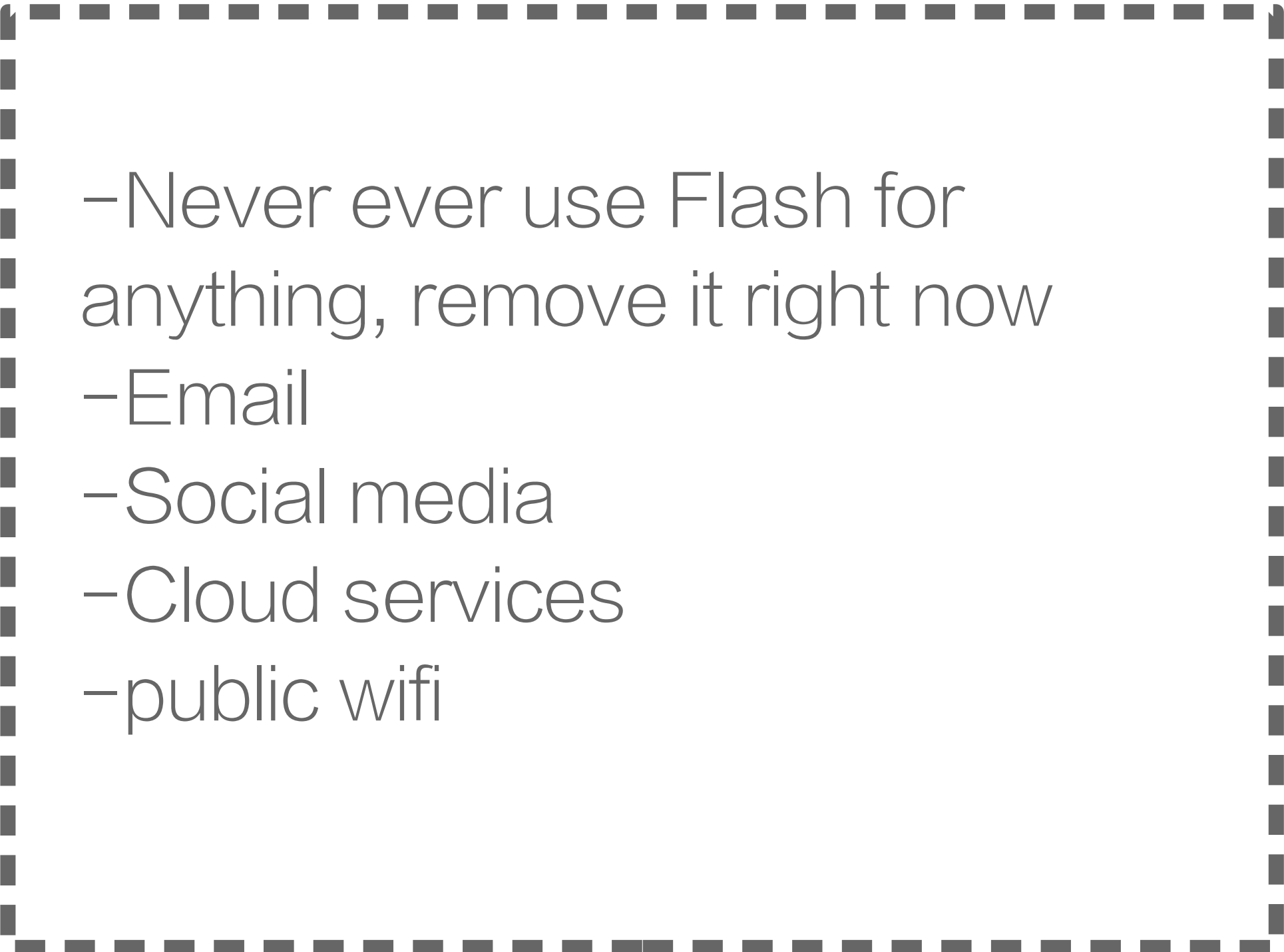
VPN

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



OTHER STUFF



- 
- Never ever use Flash for anything, remove it right now
  - Email
  - Social media
  - Cloud services
  - public wifi

# EXTRA CREDIT

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

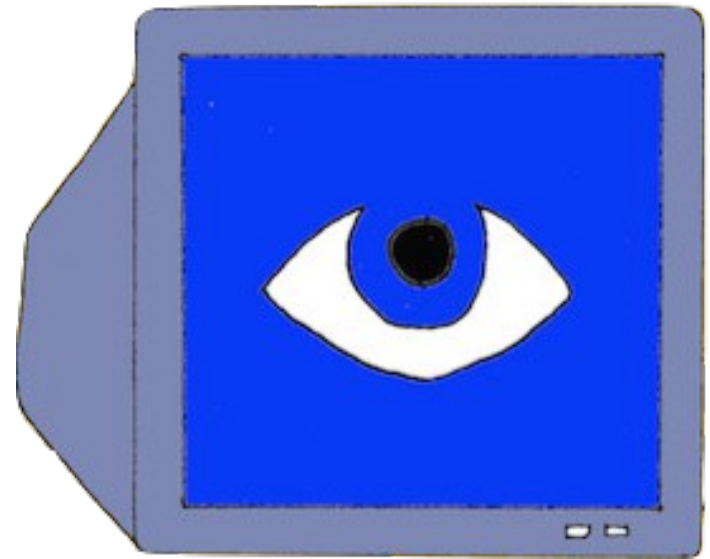


alison@libraryfreedomproject.org

@flexlibris

@libraryfreedom

libraryfreedomproject.org



Attribution-ShareAlike 4.0 International  
[www.creativecommons.org](http://www.creativecommons.org)