Surveillance Defense

Small Easy Steps for Security and Privacy

Pete Snyder
psnyde2@uic.edu - peteresnyder.com

Surveillance Defense

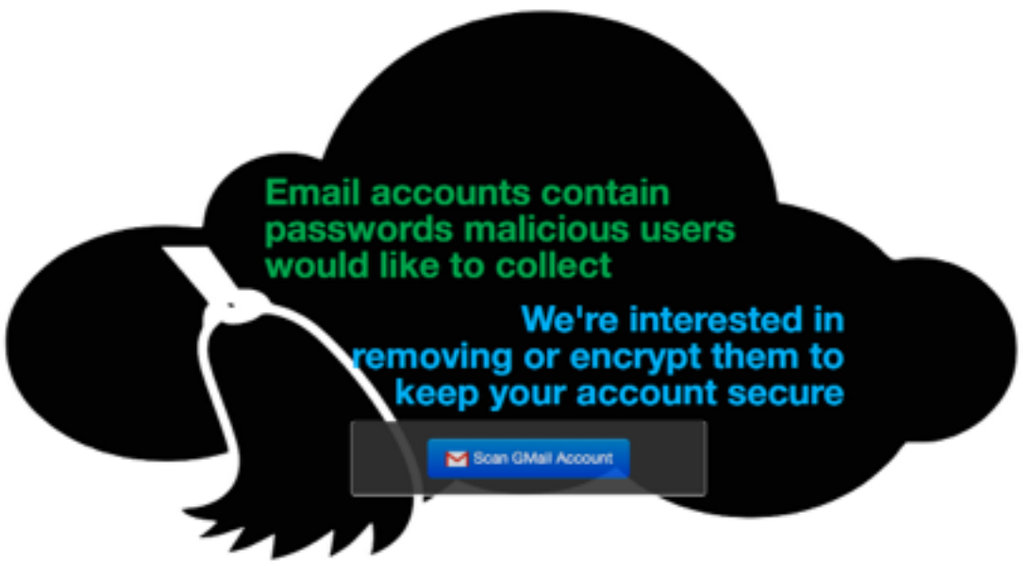
1. Good Practices
2. System / PC Security
3. Mobile Security
4. Browser Security
5. Secure Networking Tools

1. Good Practices

Choose A Good Password…

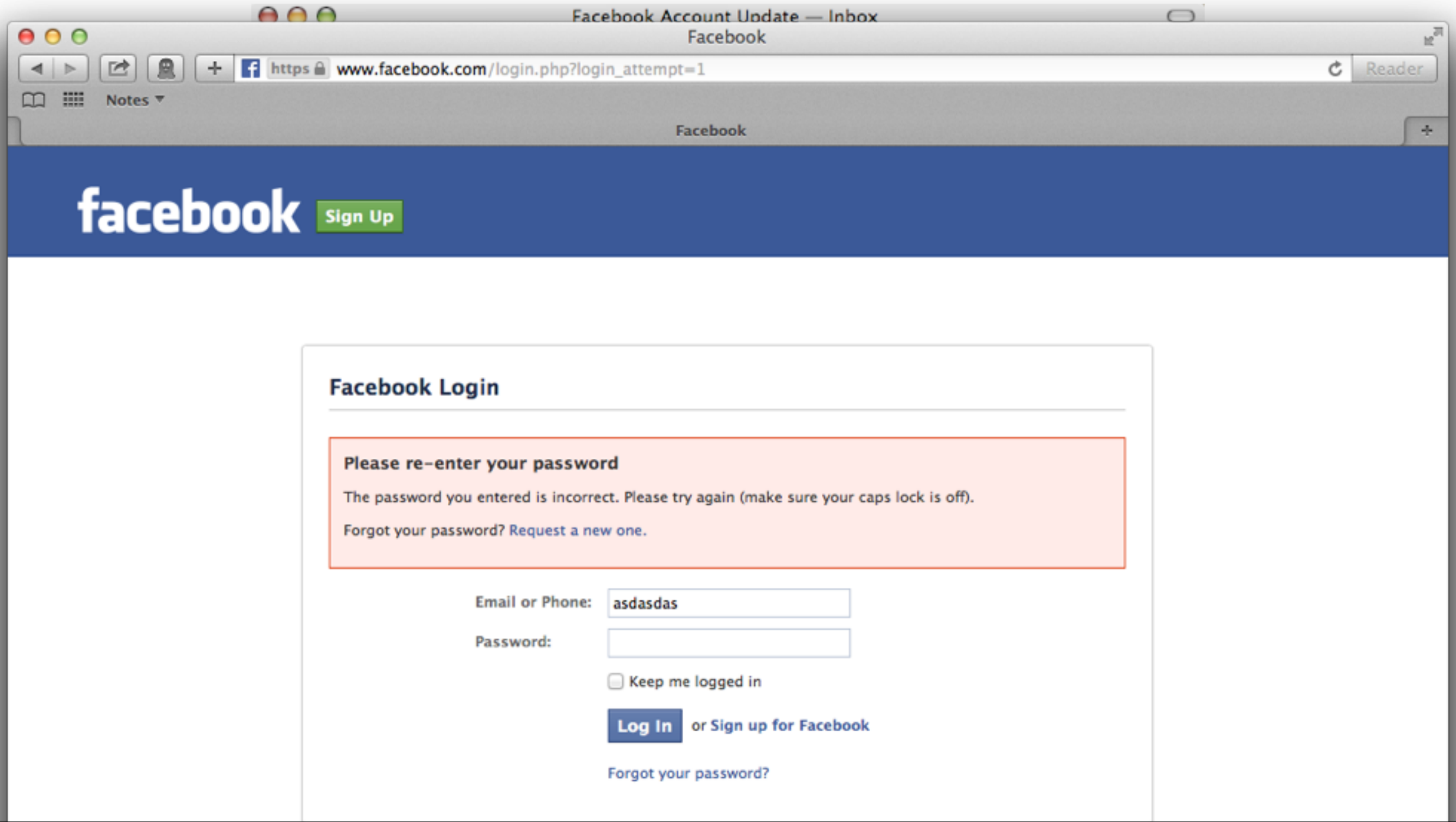
- 10+ characters (and pad)
- Mix of letters, numbers, characters
- Vary by site / use
- LastPass / iCloud Keychain / etc

…and Don’t Share It



- Cloudsweeper
- Use second channels
- Key-based auth

Phishing


Facebook Account Update — Inbox
Facebook
https www.facebook.com/login.php?login_attempt=1
Reader
Notes
Facebook
facebook
Sign Up
Facebook Login
Please re-enter your password
The password you entered is incorrect. Please try again (make sure your caps lock is off).
Forgot your password? Request a new one.
Email or Phone:
asdasdas
Password:
Keep me logged in
Log In
or Sign up for Facebook
Forgot your password?

Phishing Defenses

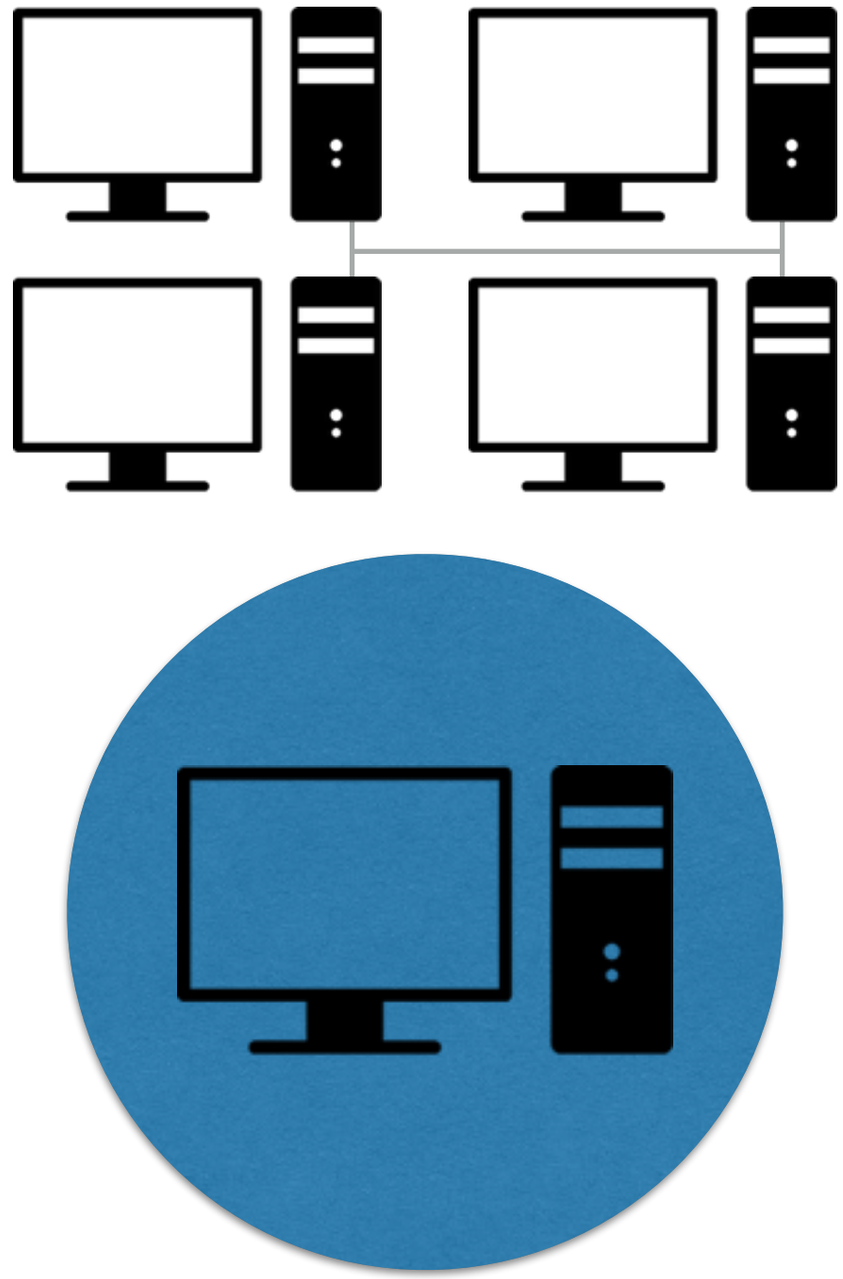
- Watch your URLs in your browser
- Don’t click on links in email
- "If you don't request it, ignore it"

Air Gapping

- Sensitive records

- No network / external connection

- Inconvenient / secure



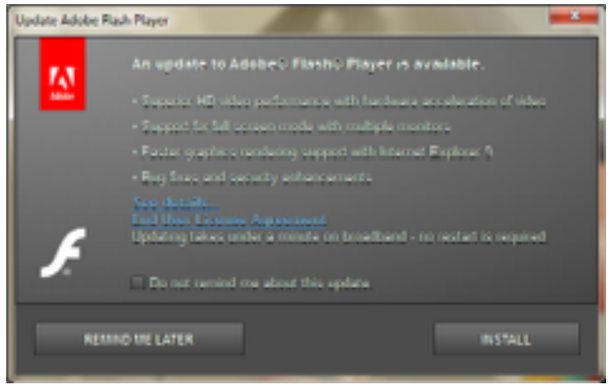
Crossing Borders

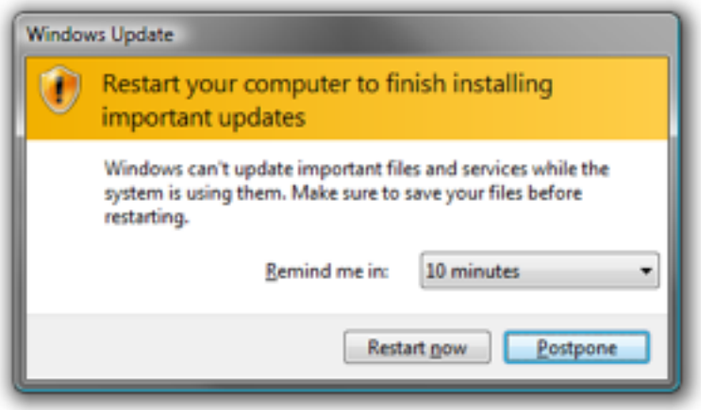
- Assume loss of control
- Travel with dumb devices (Tahoe-LAFS)
- Encrypt anything sensitive
- Power devices off

2. Securing Your System

Software Updates

- Automatically check for updates
- Apply immediately
- Unapplied updates are the worst case scenario





Firewalls

- Corse control over incoming and outgoing network data
- Built into your OS
- Don’t be afraid to click “no”

Virus / Malware Checker

- Mostly Windows
- 100s of options…
- Keep it updated
- Probably too late

Full Disk Encryption

- Transparently encrypts hard disk
- Protection when computer is off
- Lots of options
  - BitLocker (Windows > 7)
  - FileVault (OSX)
  - TrueCrypt (everywhere)

Virtual Machines

- Computer within a computer
- Perform risky operations in emulated computer
- Reset to safe state
- VirtualBox (free, everywhere)

3. Mobile Security

Mobile Security Bad News

- Easy to steal
- High value
- Networked to higher value
- Assume weak security

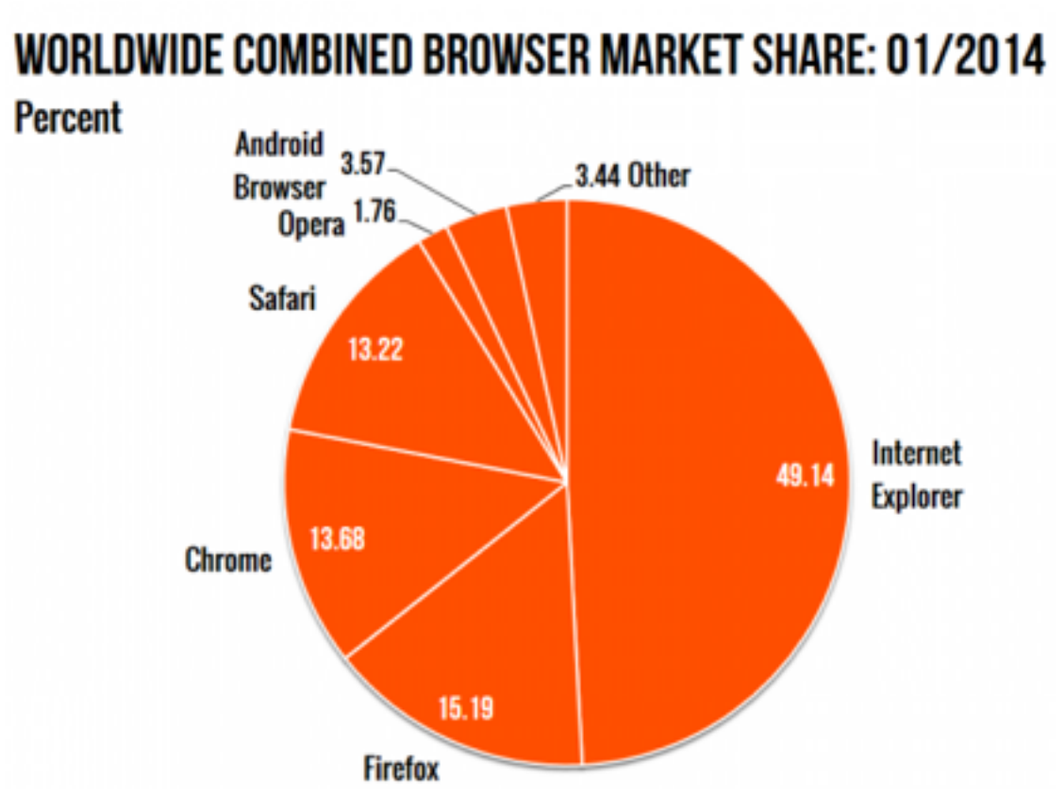
Mobile Security

- Use a password, not a PIN or swipe
    - Auto-wipe not so useful
- Full disk encryption
    - Automatic on iOS
    - Opt-In on Android
    - Doesn't protect most things…

4. Secure Browsing

Browser Choice

- Firefox / Chrome
- Regular updates
- Cross platform
- Independent security stacks
- Security extensions



Browser Plugins

- Popular infection vector
- Disable all unneeded plugins
- Enable click-to-play for needed plugins
- Remove Java!

Surveillance Browser Extensions

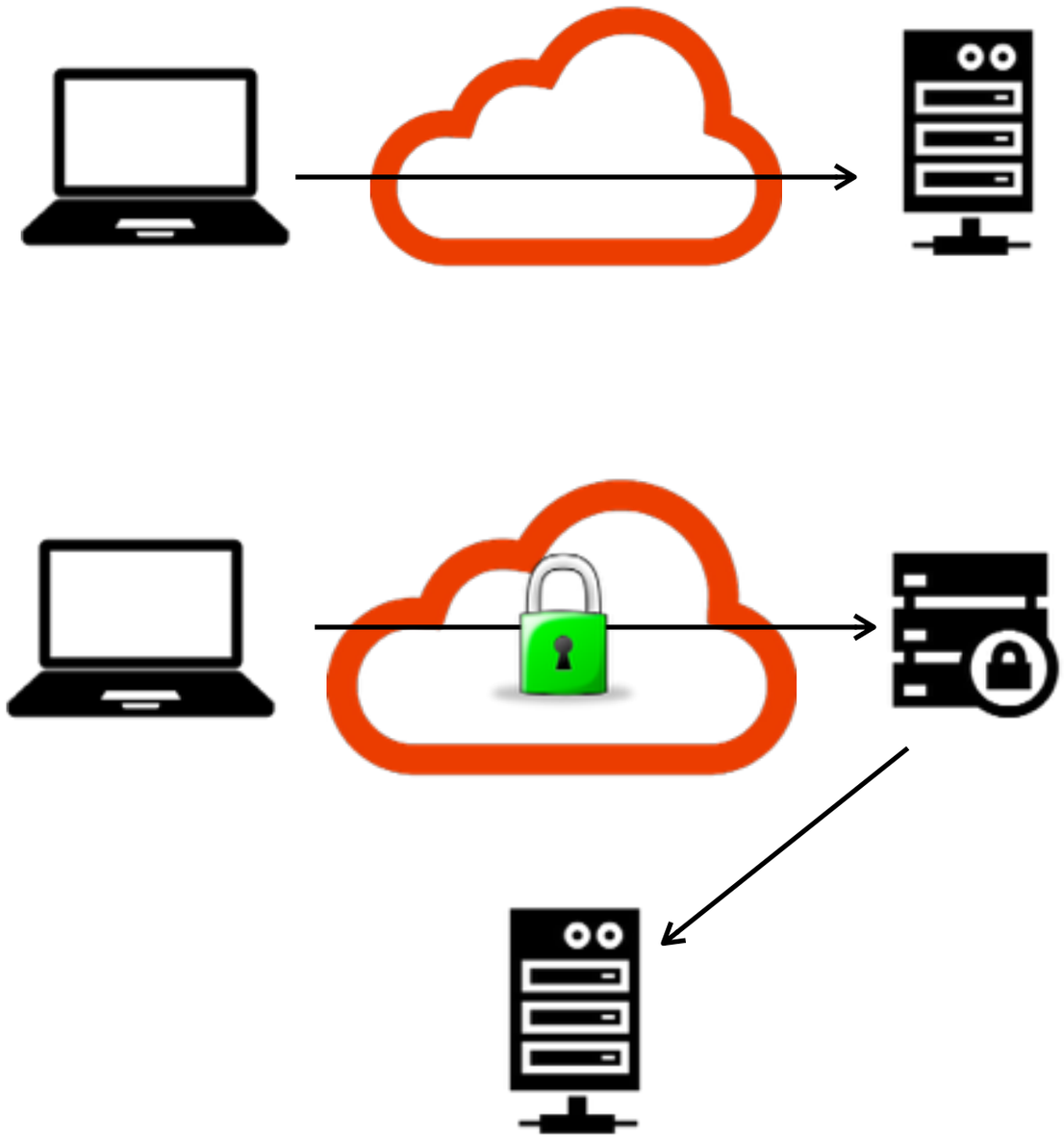
	Firefox	Chrome
Encryption	HTTPS Everywhere	HTTPS Everywhere
Control Javascript	NoScript	SafeScript
Cookie Management	Cookie Monster	Cookie Manager

5. Secure Networking Tools

2 Factor Authentication

- Authentication beyond passwords
- Popular
  - Gmail
  - Dropbox
  - Apple
  - Facebook
  - Microsoft

Virtual Private Networking



- Coffee shops, hotels, public WiFi, insecure networks
- Browse securely over insecure networks
- Support in Android, iOS, Windows, OSX, Linux

Other Tools

- Off-the-Record (OTR) Chat
    - Encrypted, end-to-end chat
    - Repudiation / plausible deniability
    - Cryptocat (cross-platform)
- File encryption
    - Before storing in cloud
    - TrueCrypt (cross-platform)
    - Tahoe-LAFS

Thanks!

Pete Snyder
psnyde2@uic.edu - peteresnyder.com