Personal Opsec

INFO 310 – CYBERSECURITY AND INFORMATION ASSURANCE

First a word

There is no way to be perfectly secure

Security is a balance of effort, expense, and security

Your level of risk should inform your choices

Risk is based on likelihood and impact

Risk reduction is about lowering your attack surface and the impact of an attack

Measures can be taken that range from common sense to truly paranoid

Defense in depth

Confidentiality, Integrity, Availability

Everyone has a different way of doing this and opinions are plentiful, these are just mine

Your data at rest

Confidentiality

- Lock your computers people
- Full disk encryption
- Encrypted containers
- Dropbox, Google Drive, iCloud, and ”the cloud” in general
- Encrypted backups – local, network, cloud
- Don’t plug your devices into unknown USB ports

Integrity

- Monitor your gear – little snitch, little flocker, oversight, knock knock, blockblock, sophos, etc.
- Verify signatures, verify fingerprints

Availability

- Only two types of people, those that back up and those that haven’t lost everything yet
- Redundant backups
- Offsite backups
- Turn off ”Find my Mac”
- Professional photography as an example

Data in transit

Confidentiality

- TLS for everything – HTTPSEverywhere
- Double check domains for sensitive things
  - How did you get there?
- VPN sensitive traffic, consider tethering
- Tor for the paranoid
- Don’t trust Wifi

Integrity

- Verify signatures of downloaded things
- Be careful of pirated software. Specialized tools are just as dangerous as mass market stuff

Your online presence

Confidentiality

- Ghostery, uBlock, Adblock Plus, Flash control
- Opt out of everything possible
- No track cookies
- Unsub from mailing lists
- Remove yourself from Spokeo, Whitepages, etc
- Lock down your Facebook profile, reddit profile, etc. - defense in depth
- Password creation and re-use

Integrity

- Make sure you have trusted means of out-of-band communication

Availability

- Don’t link all of your services to reduce impact

Payment

Confidentiality
- Really tough to do well
- Refillable debit cards
- Cash
- Bitcoin, Monero, Etherium, Zcash, Dogecoin, etc.
- Have people pay for you
- Square cash temporary card
- What I want – temp CC numbers

Integrity
- Double check your bank statements
- Set account alerts

Availability
- Mainly a concern while traveling
- Use several banks
- Have a couple cards, both debit and credit
- Venmo & Square cash

Movement

Confidentiality
- Your phone is a tracking device
- Some have literal tracking devices
- Bluetooth and Wifi beacons
- Car Bluetooth and Wifi
- Google maps searches
- Uber, Lyft, AirBnB, etc.
- Car OBD port dongles and GPS devices
- Payment
- For the love of all that is holy, don’t use checks or e-checks

Integrity
- Sometimes proving where you are is important
- Let people know where you’ll be, depending on the situation

Availability
- Always carry at least some cash

Communication

Confidentiality

- Signal, Whatsapp, Messanger, iMessages
- PGP encryption
- Don’t put things in writing if you can

Integrity

- Out of band communication
- Encryption provides integrity

Availability

- Out of band communcation

Law enforcement

Note – I am not a lawyer

4th Amendment Rights – Unreasonable search and seizure

5th Amendment Rights – Self incrimination

Boarder crossings

- Searches by boarder patrol
- TSA Pre, Global Entry, Nexus

https://www.youtube.com/watch?v=i8z7NC5sgik

https://www.youtube.com/watch?v=08fZQWjDVKE