Don’t Obey in Advance

And Other Advice for this Dark Timeline

Why Are We Here?

- Knowledge is Power.
- You have questions and I can help.
- Solidarity is necessary, especially now.
- This is an information/knowledge dump.
- More hands on stuff can be done later.

WARNING!

- Firstly you do not have as much privacy as you think.
- Secondly you will not be able to realistically avoid all potentially compromised services, applications, and activities.
- The goal is to minimize risk, not eliminate it.

Definitions

Privacy

- The state or condition of being free from being observed or disturbed by other people.

Security

- The state of being free from danger or threat.

Risk

- A situation involving exposure to danger.

Vulnerability

- The quality or state of being exposed to the possibility of being attacked or harmed, either physically or emotionally.

Encryption

- The process of converting information or data into a code, especially to prevent unauthorized access.

Authentication and Multifactor Authentication

- The process or processes of proving your identity to a system.

Your Data and Keeping It Safe

What Is Data?

- Facts and statistics collected together for reference or analysis.
- You are data.
- Anything you write, think, create, store, read, or access is all data.

Data At Rest

- Data that is stored on a medium, such as a hard drive or disk.
- Often **encrypted**.
- Generally you need to login to access data at rest.
- Build a process to encrypt and purge data.

Social Media

- Your posts, updates, photos, “check-ins” and other social media actions are DATA.
- Even what you don’t share is data used by the social media company.
- Limit what you post, when you post, and with whom.

Data Sharing Services

- Think Dropbox, Onedrive, and other file sharing services.
- Yes, the hosts have access.
- No, not a valid backup strategy.
- Restrict access and remove access regularly.

Backup Your Data

- Not everything needs to be backed up.
- Find a process that works for you.
- External USB drive + cloud + safe.
- Make this a regular process.

Authentication and MFA

Authentication

- Prove who you are.
- Username + Password (One Factor)
- Username + Password + MFA = Multifactor
- What you have, What you are, Where you are, What you are doing.

MFA

- SMS/Text: Good enough for you.
- OTP = One Time Passcode
- TOTP = Timed One Time Passcode
- Authenticator Apps: Microsoft Authenticator, Google Authenticator, Authy
    - Choose one app, use everywhere possible

MFA

- Yubikey / Hardware token == BEST
- Face ID: **Big Nope**
- Fingerprint: Yes but know how to disable on phone!!
- Turn on MFA everywhere. EVERYWHERE.

Managing Passwords

- Password <<< **Passphrase**
- Use a password manager (Bitwarden)
- Change only when needed.

Communication and Secure Comms

Encryption

- Most comms have encryption.
- Prevents a third party from snooping.
- Not encrypted on your device.
- Does not prevent a party from disclosing.

Insecure Comms

- Text/SMS is not secure.
- Email is not secure.
- Most social media “DMs” are not secure.
- Talking on a phone is not secure.

Secure Comms

- Options exist.
- Signal is end-to-end encrypted and encrypted on the device.
    - A party can still disclose!
- Text can be encrypted for use on insecure comms. High difficulty.

VPNs

- A tunnel between your device and the internet.
- Prevents local network and ISP from snooping.
- Easy to use!
- Opt for a paid VPN over a free one.
  - NordVPN

Social Media

- There is no secure social media.
- Consider everything to be publicly readable. Consider that the org can read anything you set to private.
- Admins always have full access by design.

Social Media

- If it is free then your data is what they want.
- You don’t control what they do with your data.
- No, posting a cryptic thing is not valid. Don’t do that. Stop it.

Social Media

- Stop taking quizzes! This is simply data collection.
- Restrict who you share with.
- Restrict *what* you share!
- Yes, social media is regularly monitored by law enforcement agencies.

Social Media

- Meta/Insta/Twitter/Etc… most have algorithms designed to manipulate you.
- You are easily manipulated through emotion.
- Social media + algorithms to engage == dopamine hits == addiction.
- Dead Internet Theory
    - https://en.wikipedia.org/wiki/Dead_Internet_theory

Social Media

- Not all social media is the same!
- Fediverse: The Fediverse is a collection of social networking services that can communicate with each other (formally known as federation) using a common protocol. Users of different websites can send and receive status updates, multimedia files and other data across the network. The term Fediverse is a portmanteau of federation and universe.

Social Media

- Fediverse -> Mastodon
- Mastodon == Twitter/Facebook
- Pixelfed == Insta
- PeerTube == YouTube
- Lemmy == Reddit
- Remember IRC? Early blogs? RSS Feeds?
- Individual Instances (servers/hosts/topics)

Is “XYZ” Secure?

Is Something Secure?

- It Depends!
- Is it a free product/service or paid?
- Who or what owns it? Domestic/foreign?
- Think outcome before looking for a tool/service/product. What is your end goal?

Is Something Secure?

- Ask someone in the know.
- Ask people like me.
- There must be some trust otherwise you’ll never move forward.
- Trust but verify.
  - “I trust everyone. I just don’t trust the devil inside them.”

Operating Environments

Microsoft vs Apple vs ??

- Microsoft Windows is the dominant operating environment on the planet.
- Apple is the close second.
- Everything else is a distant third.

Microsoft vs Apple vs ??

- Microsoft has a terrible track record for security and privacy rights.
- Apple can be more secure by default and often takes your privacy more seriously.

Microsoft vs Apple vs ??

- Microsoft CoPilot + Recall: Takes screenshots of your desktop and applications.
- Stores this data locally.
- Used to train local AI.
- Easy for threat actor to steal.

Microsoft vs Apple vs ??

- Apple AI is less intrusive and more secure by default.
- I recommend disabling all local AI whenever possible regardless of vendor.

Linux?!?!?!

- “Linux” is a generic term.
- The world runs on Linux. Your Android phone is Linux.
- Built by companies and volunteers.
- Open source and free.
- It’s a philosophy in some ways.

(Philosophy Lesson)

- It’s a philosophy in some ways.
- Hacker Manifesto: https://phrack.org/issues/7/3

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of **curiosity**. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

Linux?!?!?!

- Common Linux Distributions include:
  - Ubuntu (KUbuntu is very friendly)
  - Linux Mint
  - Fedora
- SteamOS from Valve is focused on PC gaming.

Linux?!?!?!

- Linux is more secure than Microsoft Windows by default.
- Linux bakes security in by default.
- Not highly targeted for malware, yet.

Apple vs Android vs ??

- It’s Apple or Android.
- Both work fine. User preference.
- Keep up to date!
- Use biometrics + PIN.
- Don’t use faceID.
- Know how to disable biometrics in an emergency!

OpSec and Physical Considerations

OpSec

- **Op**erational **Sec**urity.
- Precautions and actions taken to secure your daily lives and missions.
- Who, What, When, Where, Why, How.
- Exits and Cameras.

Physical Considerations

- Don’t stand out in a crowd. Mitigate calling attention to yourself.
- Avoid mobs.
- Protest carefully and understand when to leave.

Physical Considerations

- Make good use of facial covering if needed.
- Hats, scarves, and jackets make good disguises.
- Follow the laws as directed. You being gone doesn’t help anyone.

Know Your Rights

You Have Rights

- The Constitution
- State Law
- Never answer questions without an attorney. Make them follow the law.
- Be Respectful. It’s hard. Do it anyways.
- PRACTICE your rights.

Classic Resources for Living in a Fascist State

Anarchist Cookbook

- Full of interesting knowledge.
- Not illegal to read or have (yet).

Simple Sabotage Field Manual

- Written by America and distributed to civilian populations during WWI and WWII.
- Available at the CIA website.
- Tips/tricks for surviving and undermining.

All Files + Presentation

https://github.com/maloleyr/rebel

Focus

- You
- Yours
- Small Bubble
- Larger Bubble
- Actions you can take
- You cannot solve it all alone

QA