# Digital Security Workshop

- Introductions!

- A lot of information
- A lot of hands on training
- Do you have your electronic devices?
- Phone
- Laptop

**BIG BROTHER IS WATCHING...**

# Agenda

- What is encryption?
- Phone Encryption
- Secure Passwords
- Secure Messaging (Signal, Wire)
- Secure Email (GPG)
- Anti-surveillance browser tools
- Browsing the Internet anonymously (TOR)

BIG BROTHER IS WATCHING...

# What is Encryption?

- A way of making information unreadable for adversaries, but readable for allies

- Various uses

- File Encryption

- Message Encryption

- Password Encryption

BIG BROTHER IS WATCHING…

# Phone Encryption

- Will go over the following types of phones
  - Android Phones
  - IOS
- Windows Phones, non-Android Blackberry, etc. will not be covered
- Warning: If you forget your phone passcode your data will NOT be able to be recovered
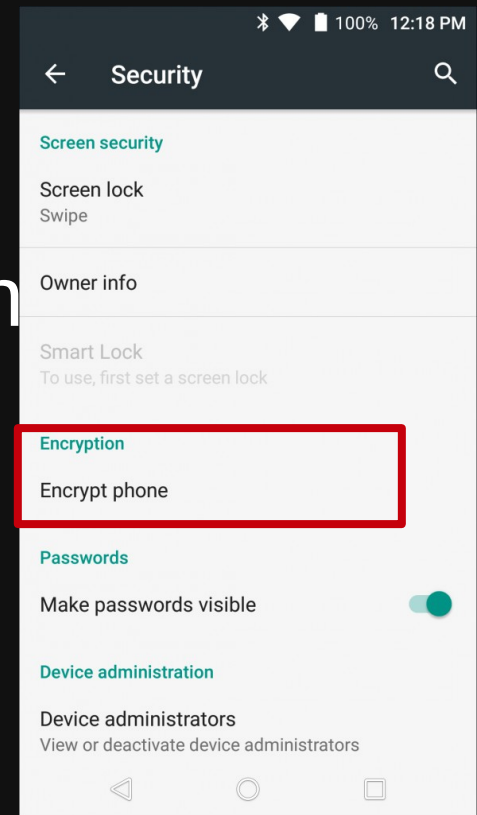
BIG BROTHER IS WATCHING...

# Android Encryption

- Will vary depending on the phone you have!
- Encryption process can take up to an hour!
- Make sure your phone is mostly charged or plugged in
- Feel free to ask for help at the end of the presentation
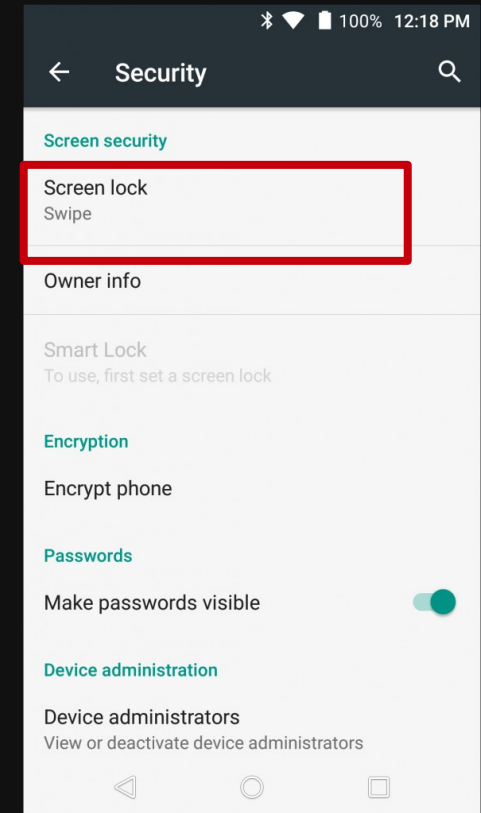
BIG BROTHER IS WATCHING...

# Android Encryption

- DO NOT DO THIS NOW!!!
- Open Phone Settings
- Navigate to the "Security" section
- Find the "Encryption" section
- Click on "Encrypt"



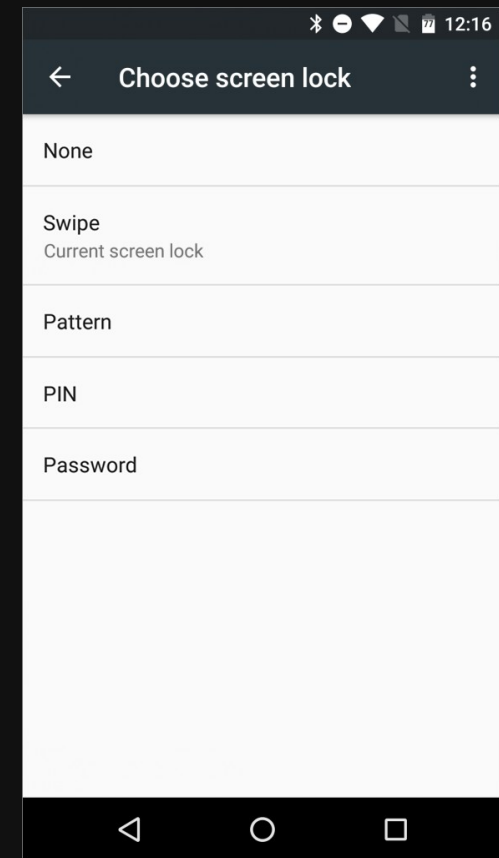BIG BROTHER IS WATCHING...

# Android Encryption

- Enable a passcode
  - Required for effective security
  - Also under the security section

# Android Encryption

- Do NOT simply have swipe
  - No security

- Recommended Passcodes
  - 6 digit or longer PIN
  - 8 character or longer password



BIG BROTHER IS WATCHING...

# Fingerprint Scanners

- Not Recommended

- Does not have the same legal protections as passwords/PINs
  - Law enforcement cannot (legally) force you to give up a password.
  - Law enforcement CAN legally force you to use your fingerprint
  - Same with FaceID and similar
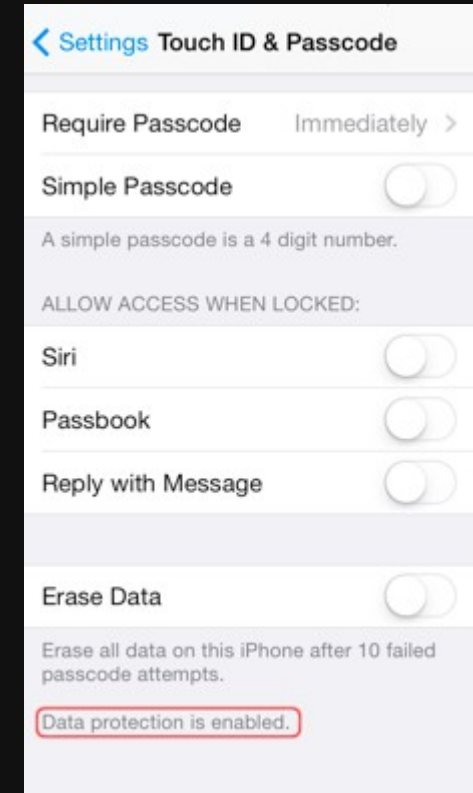
**BIG BROTHER IS WATCHING...**

# IOS Encryption

- IOS encrypts storage by default
- Nearly pointless unless also paired with a passcode

**BIG BROTHER IS WATCHING...**

# IOS Encryption

- Enable a passcode
  - Go to "Settings" app
  - Go to "Touch ID & Passcode"
  - Set Passcode
  - Set "Require Passcode" to "Immediately"



**BIG BROTHER IS WATCHING...**

# IOS Encryption

- Most iOS devices have fingerprint scanning (TouchID) or facial recognition (FaceID)
  - Same pitfalls as Android equivalents
  - Highly not recommended!
- ICloud data is seizable by law enforcement

BIG BROTHER IS WATCHING...

# Phone Encryption

- For extra precaution, turn your phone off when in doubt
  - Certain recently used data may be recoverable from memory if your phone is turned on
  - Not as big of a risk if phone is turned off

# Passwords

- Best practice to NOT reuse passwords for multiple accounts, especially important ones

- Use a password manager

  – KeepassXC recommended

    - https://keepassxc.org/

  – Generates passwords for you

  – Saves them securely on your computer/phone

BIG BROTHER IS WATCHING...

# Secure Messaging

- Signal and Wire

- Data is encrypted, only able to be seen by the sender and receiver(s)

- Open source

  – You can read the source code for yourself

- More secure apps, these are proven to be easy and secure

BIG BROTHER IS WATCHING...

# Signal

- Note: Signal is NOT an anonymous platform.
  - You must use a phone number for verification
  - To be messaged, participants must know your phone number
- ALL parties must have Signal installed for messages to be secure

BIG BROTHER IS WATCHING...

# Signal

- Signal can be used as a normal texting app

- Will automatically encrypt messages of all parties have Signal installed

- If someone does not have Signal, you can still text them via normal texting in the Signal app

BIG BROTHER IS WATCHING...

# Wire

- Is pseudonymous
  - This means you are known by your username
- Cannot be used as a normal texting app like Signal, but doesn't require you use your phone number
- Download "Wire" by Wire Swiss GmbH

BIG BROTHER IS WATCHING...

# Email Encryption

- Emails are not encrypted by default
  - Companies hosting your email server can read your emails

- Can encrypt emails using a technology called "PGP" (Pretty Good Privacy)
  - Works based on a paradigm known as "public key encryption"

BIG BROTHER IS WATCHING...

# Public Key Encryption

- Uses encryption "keys" for encryption and decryption
  - A "public key" that you give to anybody you want to talk to
  - A "private key" that ONLY YOU have and know

BIG BROTHER IS WATCHING…

# Public Key Encryption

- Think of the Public Key as the lock for your messages

- Think of the Private Key as the key for your messages

- Comrade encrypts their email with your public key (your "lock"). When you receive the email, you decrypt it with your private key (your "key")

BIG BROTHER IS WATCHING…

# Public Key Encryption

- Public Key Encryption Activity!

BIG BROTHER IS WATCHING...

# Installing GnuPG

- GnuPG (GPG) is a free, open source PGP key generator and manager

- Windows install GPG4Win

  – https://gpg4win.org/

- Linux GPG is typically installed by default

- GPG on Mac

  – Go to gnupg.org/download/

BIG BROTHER IS WATCHING...

# Email Encryption

- Thunderbird & Enigmail for Windows, Linux, and Mac

- K-9 Mail and OpenKeychain on Android

- IOS has no unpaid pgp options available
  - IPGMail is a paid option to be used with iOS Mail

BIG BROTHER IS WATCHING...

# Thunderbird Installation

- Download Thunderbird
  - Www.thunderbird.net
- After installation, setup your email account with Thunderbird
  - This can vary based on email provider
  - Can help set this up after presentation

BIG BROTHER IS WATCHING...

# Anti Browser Surveillance

- Nearly every website you go on is tracking you
  - Location, what you access, your computer specs, etc

- Google and Facebook are on nearly every large website
  - They track you across websites as well

BIG BROTHER IS WATCHING...

# Basic Surveillance Prevention

- Don't use Google Chrome
  - Firefox is a good alternative, but there are others
    - Firefox is open source and made by Mozilla, a non-profit
- Don't use Google or Bing
  - Use Startpage.com, searx.com, or duckduckgo.com

**BIG BROTHER IS WATCHING...**

# Basic Surveillance Prevention

- Most websites encrypt the data to and from you
  - This is the standard for modern websites

- If a website is unencrypted, an adversary can see ALL data you send to and from the website

`https://www.eff.org/https-everywhere`

- To see if a website is encrypting traffic, look and see if the website url starts with "https"

- Install "https everywhere" to force encrypted connections and get warnings for unencrypted

BIG BROTHER IS WATCHING...

# Website Surveillance Prevention

- Certain companies are tracking many different websites
  - Many different methods are used, such as "tracking cookies"
- Ads often are used for tracking
  - Download an ad blocker by searching for one
  - I recommend "uBlock Origin"

BIG BROTHER IS WATCHING...

# Website Surveillance Prevention

- Privacy Badger is a browser add-on tries to prevent tracking

  – Blocks tracking sources from loading in browser

  – "Fire and forget", once you install you generally don't have to do anything else

  – Download from www.eff.org/privacybadger

BIG BROTHER IS WATCHING...

# Advanced Surveillance Prevention

- Only use these add ons if you are fine with tinkering with settings

- "NoScript" add on

- "uMatrix" add on

- Both block certain scripts and resources from running, but must be manually configured

BIG BROTHER IS WATCHING...

# VPNs

- VPNs are a great way to increase online anonymity, making it much harder to track you
- Sends you internet traffic through another server
  - Requires that you trust the provider with your data
  - Make sure to choose a provider with a "No logs" policy
  - Riseup VPN recommended

BIG BROTHER IS WATCHING...

# Secure Email Providers

- Do NOT use gmail, yahoo, hotmail, etc.
- Protonmail is for-profit, and there is no guarantee they can't read your emails
- Riseup is the most recommended
  - Requires an invitation however
- Disroot.org is a free, secure service built for activists
  - Newer, not as well known as Riseup

BIG BROTHER IS WATCHING...

# Google Doc Alternatives

- Cryptpad
  - Secure, end to end encryption
  - Open source
  - Replaces docs, presentations, polls, and more
  - Can host a server yourself if desired

BIG BROTHER IS WATCHING...

# Accessing Internet Anonymously

- Anonymous means all personally identifying information is unknown
  - Name, identity
  - Location
  - Computer information

BIG BROTHER IS WATCHING…

# Accessing Internet Anonymously

- TOR – The Onion Router
  - A network for accessing the internet anonymously
  - Works by encrypting your traffic multiple times and sending your traffic through multiple different servers around the world
  - An important tool for remaining anonymous

BIG BROTHER IS WATCHING...
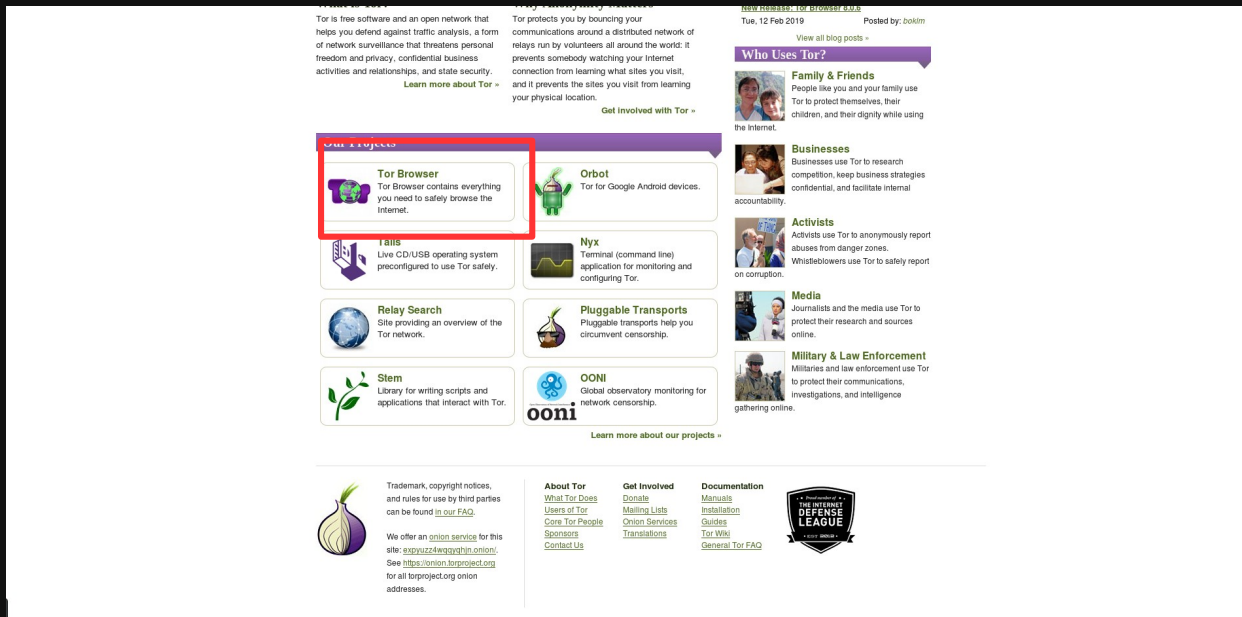
# Accessing Internet Anonymously

- TOR Browser
  - Allows you to access TOR network through a web browser
  - Can browse normal websites anonymously
  - Can also browser .onion websites
    - Secure, anonymous services that are specific to TOR

BIG BROTHER IS WATCHING…

# Downloading TOR Laptop

- Downloading TOR on a laptop
  - Www.torproject.org

# Downloading TOR Laptop

- Choose the 64-bit download according to your platform (Windows, Mac, or Linux)

# Downloading TOR Android

- Need to download two apps
  - Search for "Orbot" on the Google Play store
    - By "The Tor Project"
  - Then, search for "Orfox" on the Google Play store
    - Also by "The Tor Project"
  - Open the "Orfox" app after installing
    - May take a few minutes to start up to connect to TOR
    - You are now browsing on the TOR network!

BIG BROTHER IS WATCHING...

# TOR Tips

- Anonymity tips
  - TOR only protects your traffic from being traced back to you
    - If you sign in to any of your accounts, or otherwise post any information to breach your anonymity, TOR cannot help
  - Do not go to shady websites just because you are anonymous. You can still hacked
  - Follow any prompts the TOR browser gives you

BIG BROTHER IS WATCHING...

# Additional Anonymity Tips

- Keep your real full name and identity separate from your organizing

  - This is to protect yourself from potentially malicious groups or individuals that disagree with you

- Don't reveal any details that could be tied to your name (address, workplace, family, etc).

  - Think about what you'd do to try and find someone else's name

    - What information could you use?

BIG BROTHER IS WATCHING...

# Additional Anonymity Tips

- Using your real first name
  - try searching for your first name and city name to see what comes up
    - try multiple search engines
  - If you can find yourself then you should use an alias.
  - If you use your first name consider using a different spelling variation.

BIG BROTHER IS WATCHING...

# Additional Anonymity Tips

- Think through everywhere you might digitally interact with people you're organizing with and take precautions:

  – Email address -> Make a new account

  – Phone Number -> Use Google Voice or another service to get a different phone number. You can then use this number with Signal.

  – Google Docs -> Make a separate account with your organizing email address

**BIG BROTHER IS WATCHING...**

# Additional Anonymity Tips

Computer username -> Change so it doesn't use your full name

- Dropbox -> Use a different tool for organizing like share.riseup.net

- Facebook -> Make a separate account, or don't friend other organizers.

  - Be careful what you like because that is visible to others.

  - Change your privacy settings.

  - Ask friends to change settings so someone can't view all their friends.

- Use browser profiles to separate personal and activist

BIG BROTHER IS WATCHING...

# Questions and Help

- Topics covered
  - Phone encryption
  - Secure messaging (Signal, Wire)
  - GPG email encryption
  - Browser Surveillance Prevention
    - Ublock, HTTPS Everywhere, Privacy Badger, Decentraleyes
  - Anonymous browsing via TOR
  - https://neighborhoodanarchists.org/security-tools/

BIG BROTHER IS WATCHING...