# Ditial Security for Socialists

## Protecting Your Comrades & Mission

# Who is Sam

- A Founding Member of Humboldt DSA
- Senior SRE (Sysadmin, programer, security)
- Pentester
  - Trained to hack websites, and corporations.
- Has worked for Security and Fintech startups

# Risks of Security Failure

- Doxxing: Attack on the Individual
  - Personal safety or career.
- Account Takeover
  - Disinformation, information gathering, $$$.
- Infiltration
  - Sabotage, Setting us up publicly and legally
- State Surveillance
  - Building lists, Intimidation, Future

# Core Principles

- Encryption
  - Treat standard texts and emails like postcards. Anyone handling them can read them.
- The Mosaic Effect
  - Adversaries aggregate small, mundane mistakes to reveal your identity and penetrate accounts.
- Security is Solidarity
  - Your breach is everyone’s breach. An injury to one is an injury to all.

# Building Defense

- Identify Assets
  - Membership lists, strategy docs, meeting locations.
- Collective Security
  - We rely on each other.
- Layered Defense
  - MFA (Multi-Factor Authentication) alone makes you 99% less likely to be hacked.

# Passwords: Length is King

- The Rule: **Length beats complexity.**
  - Use unique words that are 13+ characters.
- Method: Random Words
  - Good: 'FrogYearPilesPhoneNail'
  - Better (Hardened): '5FROG!Year!Piles!Phone!Nail4'
- Management Strategy
  - Use a Password Manager (Proton Pass).
  - It acts as a 'phishing alarm'—it won't auto-fill on fake sites.

# MFA: Blocks 99% of Hacks

- Get an MFA/OTP app for your phone
    - Don’t put your MFA in a password manager.
- Phone and email codes are better than nothing, but not as good as an authenticator app on your phone.
- As a pentester when I see an MFA I look for another way in or resort to social engineering.

# Secure Communications

- Messaging: Signal
  - Use for ALL organizing voice/text, and enable expirating/disappearing messages.
- Email: Proton Mail
  - Proton-to-Proton emails are automatically secure.
- Collaboration
  - Use Proton Docs for co-editing strategy documents.

# Mobile Device Hardening

- Authentication
    - Minimum 6-digit passcode not (Face/Fingerprint)
- Physical Protection
    - Full-Disk Encryption (FDE) protects data if device is confiscated.
- App Hygiene
    - Delete apps unused for 60 days
    - Do not install random apps

# Defeating Phish: The Three Checks

- 1. Check the Sender
  - Verify the actual email address, not just the display name.
- 2. Check the Link
  - Hover (don't click). Look for misspellings (e.g., secure-login.co vs .com).
- 3. Check the Request
  - Does it create urgency or fear? Is it asking for a password/code?

# Phish Double Check

If some asks you to click a link, or give out information.  If suspicious, verify via a **SECOND** method.

- ○ Call them
- ○ Use a Signal message
- ○ **Do not** use an address or number provided by them.

# Why Proton? Security Meets Usability

- Uses End-to-End Encryption.
  - Proton ***cannot*** decrypt or hand over your data, even if served a warrant.
- Based in Switzerland.
  - Protected by strict privacy laws rather than US subpoenas.
- Not Google
  - They aren't dataminig you for Ads and AI.
- Open-source
  - The world's best Independent security experts audit it.

# Immediate Actions Checklist

| Action | Recommended Tool | Security Benefit |
|---|---|---|
| Encrypted Comms | Signal / Proton | Prevents surveillance & logging |
| MFA (2FA) | Proton Authenicator | Blocks 99% of account hacks |
| Device Lock | Passcode | Protects physical confiscation |
| Password Manager | Proton Pass | Prevents reuse & phishing |