# Digital Force Protection Checklist

## Do

**Use complex passwords**
-All account passwords should be password manager generated 22+ character passwords with UPPER, lower, numbers, and symbols

**Opt-out of all “personalized” ads**
-Disable “Advertising ID” on all devices

**Turn off WIFI, GPS, and Bluetooth when not directly in use**

**Always use Multi-Factor Authentication**
-Typically found under “privacy and security” account settings. SMS is the least secure method

**Google yourself and family**
-Request images or data to be taken down as needed
-Update account privacy settings as needed

## Don’t Do

**Don’t reuse ANY passwords**
-Breached passwords are sold and provided for free on the Dark Web. Even if you kept your password safe, companies can get hacked

**Don’t write down passwords openly**
-Use your password manager which is end-to-end encrypted to store passwords, pins, and combinations.
-Use auto-disappearing encrypted chat at a minimum to share combinations or pins

**Don’t set privacy to “All”, “Public”, or “Everyone”**
-Think of the Strava case study. Restrict posts and profile to “only with friends” or “only with myself”

**Don’t use SMS**
-Use Signal. Set your chats to auto-disappear by default

□ Use a Password Manager

□ Enable Automatic Updates

□ Disable Personalized Ads.
Use an AdBlocker.

□ Enable Multi-Factor Authentication
using Authenticator App or Physical Yubikey

□ Always Use A VPN, such as ProtonVPN

□ Turn Off WIFI “Auto-Connect”
Clear Unused WIFI & Bluetooth Devices

□ Make and Maintain Backups
Keep important files backed-up offline

□ Opt-Out of data collection:
https://simpleoptout.com/

□ Google Yourself.
Request Opt-Out and DMCA Takedowns

□ Uninstall Unused or Unrecognized Applications

□ Create and use NON-Admin Accounts

□ Lock Devices with 8 Digit Pin or Text Password
Don’t use Biometric options