# *The ABCDs of Security*

CLDC Digital Security Program

**cldc.org/security ★ security@cldc.org**

## A is for Accounts

### BASIC

- ☐ **Use a password manager** (lastpass.com or 1password.com[$])
- ☐ Lock down social media privacy settings as much as possible
- ☐ Avoid private or sensitive conversations on social media
- ☐ _____

### ELEVATED

- ☐ Use two-factor authentication (2FA) for important accounts
- ☐ Protect the password manager with a strong passphrase
- ☐ Use unique + random passwords for all important accounts
- ☐ Change the passphrase for the password manager every year
- ☐ Change passwords for important accounts every year
- ☐ _____

### ADVANCED

- ☐ Use an app for 2FA (instead of text messages)
- ☐ Use an offline password manager (KeePassXC.org)
- ☐ Backup the password manager database to an encrypted disk
- ☐ PIN-lock your phone SIM card
- ☐ _____

### MAXIMUM

- ☐ Use a hardware token (ex. Yubikey) for 2FA
- ☐ Change all important passwords quarterly
- ☐ Create and use pseudonymous accounts (*w/ Tor **exclusively***)

## B is for Browsing (+ Online Work + Research)

### BASIC

- ☐ Log out of accounts when convenient (webmail, social media)
- ☐ Lock down privacy settings + access to online documents
- ☐ Use HTTPS Everywhere + Privacy Badger (eff.org)
- ☐ _____

### ELEVATED

- ☐ Tor Browser (torproject.org) for sensitive research
- ☐ A reputable VPN[$] when Tor is blocked
- ☐ Log out of accounts (webmail, social media) to do research
- ☐ Try a privacy-focused web browser (brave.com)
- ☐ pad.riseup.net or share.mayfirst.org[$] for shared documents
- ☐ Avoid storing key documents on online corporate platforms
- ☐ Be aware that corporate platforms often hand over data
- ☐ _____

### ADVANCED

- ☐ cryptpad.fr for online collaboration + shared documents
- ☐ Share cryptpad addresses only using secure communications
- ☐ End-to-end encrypted cloud (sync.com or spideroak.com[$])
- ☐ Visit hidden (.onion) versions of websites using Tor Browser
- ☐ _____

### MAXIMUM

- ☐ onionshare.org to share documents anonymously
- ☐ Use Whonix (whonix.org) to access the Tor network

## C is for Communications

### BASIC

- ☐ Avoid social media for sensitive conversations
- ☐ Be aware that text/SMS/MMS messages are weakly private
- ☐ Avoid unencrypted wifi networks (those without passwords)
- ☐ _____

### ELEVATED

- ☐ **signal.org** or **wire.com for text messaging** (easy + secure)
- ☐ **signal.org** or **wire.com for voice/video calls** (easy + secure)
- ☐ Conference calls / videoconferencing with zoom.us is high quality but much less secure (requires trusting the company)
- ☐ riseup.net or protonmail.com or flowcrypt.com for email
- ☐ _____

### ADVANCED

- ☐ Wire for conference calls (10 parties maximum; videoconferencing under development)
- ☐ Verify safety numbers (Signal) or fingerprints (Wire)
- ☐ Publish your safety numbers/fingerprints (web/social media)
- ☐ Local PGP/GPG for email (thunderbird.net + enigmail.net)
- ☐ keybase.io for encrypted slack-style collaboration/messaging
- ☐ _____

### MAXIMUM

- ☐ XMPP + Tor + OTR/OMEMO for secure anonymous messaging
- ☐ Try riot.im for group voice/video/text
- ☐ Try tox.chat for decentralized voice/video/group messaging
- ☐ Watch for (and support) the launch of pursuanceproject.org !

## D is for Devices

### BASIC

- ☐ **Ensure devices get security updates** + apply them monthly
- ☐ **Lock devices** with a password / PIN / pattern / biometric
- ☐ Avoid leaving devices unattended in public/s spaces
- ☐ _____

### ELEVATED

- ☐ Lock devices with a password or (minimum) 8-digit PIN
- ☐ Disable biometrics whenever losing your device is a risk
- ☐ Encrypt your storage with a strong passphrase
- ☐ Make regular backups to an external encrypted disk
- ☐ Cover webcams with stickers or tape when not in use
- ☐ Keep devices under your physical control at all times
- ☐ Disable unneeded cloud backups/account syncing
- ☐ _____

### ADVANCED

- ☐ Power down devices whenever loss/confiscation is a risk
- ☐ Ensure laptops/desktops get updates to fix hardware flaws
- ☐ Secure devices in a separate room during sensitive meetings
- ☐ _____

### MAXIMUM

- ☐ Use tamper-proof phone (Pixel 3 > 2 > 1 iPhone XR/XS > X/8)
- ☐ Consider physically removing microphones (headset for calls)
- ☐ Use QubesOS (qubes-os.org) on a compatible laptop/desktop
- ☐ Secure devices at home/work during secret meetings