CYBER SAFETY GUIDE FOR LAW ENFORCEMENT OFFICIALS

Purpose: Provide law enforcement officials with practical guidance to identify areas of unauthorized entry, implement remedies, and maintain a safe online presence for professional and personal use.

QUICK WINS (FIRST 24–48 HOURS)

- Enable phishing-resistant MFA (FIDO2 security keys or platform passkeys) on email, case systems, cloud services, and social media.
- Move to a password manager and rotate any reused or weak passwords; activate breach alerts.
- Lock down social profiles: set profiles to private, remove work identifiers, and restrict friend lists.
- Opt out from major data brokers (people-search sites) and remove home address/phone exposure.
- Update devices and browsers; enable auto-updates and full-disk encryption on all endpoints (desktop, mobile, tablets).
- Turn on device-level protections: screen lock, biometric auth, and remote wipe for all devices.

COMMON AREAS OF UNAUTHORIZED ENTRY

Entry Vector	How It Happens	Indicators of Compromise	Immediate Actions
Phishing & Business Email Compromise	Fake login pages, urgent requests, spoofed colleagues/ domains	Unrecognized logins, rules auto-forwarding email, unusual OAuth consents	Change password, revoke OAuth tokens, enable FIDO2 MFA, run inbox rule audit
Password Reuse & Weak Credentials	Leaked credentials reused across systems	Breach alerts, login attempts from new locations	Rotate to unique passwords via manager; enable passkeys; enforce length (16+)

Entry Vector	How It Happens	Indicators of Compromise	Immediate Actions
MFA Fatigue & Prompt Bombing	Repeated push notifications leading to accidental approval	Multiple unsolicited MFA prompts	Switch to number-matching or FIDO2 keys; reset sessions; review devices
SIM Swap & Voice Phishing	Carrier social engineering to take over SMS-based MFA	Cell service drops; new device on account	Add carrier PIN/port-out lock; move off SMS to FIDO2/app-based MFA
Malware/RAT via Attachments	Malicious docs, USBs, or drive-by downloads	Unusual CPU/network, new processes, disabled AV	Isolate device, run EDR scan, reimage if needed, change credentials
Unsecured Home/ Field Wi-Fi	Open or weakly secured networks; rogue APs (Evil Twin)	Captive portal oddities, TLS warnings	Use WPA3 at home; use cellular hotspot/VPN; verify SSIDs
Exposed PII & Doxxing	Data brokers, court filings, social posts reveal identity/ location	Search results show home/work links	Opt-outs, PO boxes, remove metadata, request redactions where lawful
Shadow/Personal Accounts Tied to Work	Personal email/social used for work comms	Work info found on personal accounts	Separate identities; remove work links; enable strict privacy settings
Compromised Case/LE-Only Portals	Credential stuffing, legacy MFA, shared accounts	Access logs anomalies, alerts from admins	Force reset, add FIDO2, remove shared creds, audit access

REMEDIES AND HARDENING MEASURES

- **Identity & Access**
  - Adopt passkeys or FIDO2 security keys for primary MFA; avoid SMS.
  - Use a vetted password manager; enforce 16+ characters, unique per site.
  - Enable login alerts and session review for email, cloud suites, and case tools.
  - Create separate identities: *work*, *personal*, and (if applicable) *undercover* with strict separation.
- **Device Security**
  - Turn on full-disk encryption (BitLocker/FileVault/Android/iOS native).

    - Keep OS/firmware/browsers up to date; enable automatic updates.
    - Install reputable EDR/AV; enable real-time scanning and tamper protection.
    - Configure screen lock at 5 minutes or less; require biometric/PIN.
    - Enable remote find/lock/wipe; inventory all devices.
- **Network & Browser**
    - Use WPA3 at home; change default router credentials; disable WPS; update firmware.
    - Prefer cellular hotspot over unknown Wi-Fi; if Wi-Fi is required, use a trusted VPN.
    - Set DNS to a security-filtering resolver; enable DNS-over-HTTPS.
    - Harden browsers: disable third-party cookies, use privacy extensions, isolate work/personal profiles.
- **Data Minimization & PII Protection**
    - Replace home address with PO Box or department mail where policy permits.
    - Opt out from major data brokers; schedule quarterly re-checks.
    - Sanitize documents/photos: remove EXIF and document metadata before sharing.
- **Communications**
    - Use end-to-end encrypted messaging for sensitive comms where policy allows.
    - Verify out-of-band before sharing sensitive info or authorizing actions (call-back controls).
    - Avoid mixing undercover or operational details on personal channels.
- **Account Recovery & Backups**
    - Set recovery emails/phones that are not easily discoverable; use app-based codes/keys.
    - Store recovery codes in the password manager or secure physical storage.
    - Back up critical data using encrypted backups; test restorations.

MAINTAINING A SAFE ONLINE PRESENCE

- **Profile Hygiene**
    - Remove employer, rank, unit, badge numbers, and shift details from public profiles.
    - Limit audience for posts; disable public friend lists and birthday visibility.

    - Scrub old posts and photos that show home, vehicles, children's schools, or routines.
- **Search Yourself**
    - Quarterly self-audit: search engines, image search, and map listings for your name, aliases, and home address.
    - Create Google Alerts for your name, handle, and doxxing terms.
- **Family & Household**
    - Brief family on phishing, privacy settings, and not sharing your work affiliation.
    - Use separate guest Wi-Fi for visitors and IoT devices; change default passwords.
- **Marketplace & Forums**
    - Avoid buying/selling with traceable home addresses; use parcel lockers or PO Boxes.
    - Do not share badges/credentials in photos; cover unique identifiers.

OPERATIONAL SECURITY (OPSEC) CONSIDERATIONS

- Segment identities: separate browsers/profiles and devices when feasible.
- Avoid location-sharing in apps; disable geotagging and background location.
- Use burner/contact-only numbers for public interactions; enable carrier port locks.
- Delay posting until after leaving locations; use generic backgrounds.
- When conducting online research, use agency-approved investigation environments and policies.

INCIDENT RESPONSE: IF YOU SUSPECT COMPROMISE

1. **Contain**: Disconnect network, enable airplane mode (keep on if EDR needs connectivity per policy), isolate affected accounts.
2. **Preserve**: Do not wipe unless directed; capture timestamps, screenshots, and log IDs.
3. **Report**: Notify agency IT/security; follow chain of command and evidence handling procedures.
4. **Eradicate**: Password resets, revoke sessions/tokens, remove malicious apps/extensions.
5. **Recover**: Patch, reimage if needed, restore from clean backups, re-enroll MFA.

6. **Post-Incident**: Review root cause, update controls, brief team.

DATA BROKER OPT-OUTS (CORE LIST)

Schedule time (initial sweep then quarterly). Use a PO Box where allowed and a dedicated email for removals.

- Major brokers: Spokeo, Whitepages, Intelius, BeenVerified, PeopleFinders, Radaris, TruthFinder, MyLife, FastPeopleSearch, FamilyTreeNow.
- Process: Search your name → submit opt-out → verify email → track status in a spreadsheet → re-check quarterly.

TRAVEL & FIELD WORK

- Use a travel profile/device with limited data; assume border/device searches are possible.
- Disable auto-join Wi-Fi and Bluetooth discovery; prefer tethering.
- Carry a hardware security key; keep a spare separately.
- Use privacy screen filters; store devices in RF-shielded pouches when appropriate.

AGENCY-LEVEL RECOMMENDATIONS

- Mandate phishing-resistant MFA and password manager adoption.
- Provide data broker removal assistance and privacy training for staff.
- Deploy EDR, DNS filtering, mobile device management, and OS patch SLAs.
- Establish clear social media and doxxing response policies.
- Log and monitor: centralize logs, enable geo-velocity and impossible-travel alerts.
- Access governance: least privilege, quarterly access reviews, eliminate shared accounts.

30/60/90-DAY PERSONAL HARDENING PLAN

- **Day 0–30**: Enable FIDO2/passkeys; password manager migration; lock down social media; initial data broker opt-outs; encrypt all devices; update routers.
- **Day 31–60**: Network segmentation (guest/IoT); browser hardening; set up alerts; inventory all accounts/devices; implement secure backups.
- **Day 61–90**: Review recovery info; test incident response playbook; advanced privacy (credit freeze, PO Box, alias emails); quarterly re-audit.

CHECKLIST: WEEKLY/MONTHLY

- **Weekly**: Review login alerts; patch devices; scan with EDR; check social tagged photos.
- **Monthly**: Rotate critical passwords; audit browser extensions; verify backups; re-scan data brokers.
- **Quarterly**: Full digital footprint sweep; access reviews; emergency contact updates.

RESOURCES

- FIDO Alliance: Passkeys and security keys overview
- US-CERT/StopThinkConnect: Safe browsing and phishing guidance
- Agency IT/Security policies: Follow local directives for tooling and incident handling

Disclaimer: Follow your agency’s policies and legal requirements. This guide provides general practices and is not a substitute for official procedures.

David Keith Jr "mrdj" ✓