REVERE.ICU

Digital Security Quick Reference Guide

Safe and sensible digital hygiene can go a long way to protect individuals against physical and cyber security threats. Regardless of risk profile and exposure, many of these tips can add a layer of protection in the event of theft of a smartphone or similar device, in the event of compromise online data, or in the event that corporations can no longer be trusted to uphold the constitutional right to privacy as envisioned by the Fourth Amendment of the U.S. Constitution.

Online Security

Topic	Tip	What to do	Additional info
1. **Instant Messaging**	Switch to End-to-End Encrypted ('E2EE') messaging services, such as Signal.	• Install Signal app on mobile devices from an official app store. • Enable Registration Lock, Screen Lock, and Disappearing Messages (set a timer). • Disable message previews. • Create a username and prevent sharing of mobile number. • Use Signal's in-app camera to avoid saving sensitive photos to camera roll. • Avoid linking Signal to desktop, unless desktop is secure. • Keep Signal app and OS updated.	• E2EE prevents providers from reading contents. • Encryption doesn't protect if devices are compromised or physical access is obtained. • Encryption does not protect against devices infected with malware.

2. **Email**	Switch to end-to-end encrypted email service providers, preferably hosted in countries with strictly enforced privacy laws, such as Proton Mail (hosted in Switzerland).	• Create a Proton Mail account for sensitive email. • Enable two-factor authentication and use the Proton Mail app or secure web browser to access email. • Utilize Proton's suite of security resources, such as Proton Drive (for document storage), Proton Authenticator (for multi-factor authentication) and Proton VPN (for secure network activity).	• Proton mail provides E2EE security within the Proton server (Proton to Proton), and provides encryption at rest once mail is received at the Proton server from a non-encrypted sender. • Encryption doesn't protect if devices are compromised or physical access is obtained. • Encryption does not protect against devices infected with malware.
3. **Online Identity**	Use a pseudonym for public engagement online	• Create separate accounts for public/pseudonymous activity. • Keep personal identifying details (full name, DOB, contact details, location) out of profiles and posts. • Use a dedicated recovery email and password manager for social media accounts. • Moderate or disable comments on personal online profiles if harassment is a risk. • When buying domains, use private WHOIS/registration options. • Use pseudonymous email addresses when signing up for non-essential services.	• Reduces risk of doxing and linking online activity to your real identity. • Measures may be impractical for some professional uses and LinkedIn profiles. • Carefully consider the contents of online activity where identity cannot be appropriately protected.

4. **Secure browsing**	Use privacy focused search engines and web browsers, such as Tor and DuckDuckGo.	• For high anonymity, use Tor Browser for web browsing. • For everyday private searches, use privacy search engines (DuckDuckGo). • Avoid signing into mainstream accounts when using Tor.	• Hides search history and reduces tracking. • Tor can be slower and some sites block it.
5. **Secure IP and network traffic**	Protect IP and traffic with a trustworthy VPN, such as Proton VPN, NordVPN or SurfShark VPN.	• Choose a no-logs, reputable VPN and enable it on public Wi-Fi. • Avoid free VPNs with unclear policies.	• Masks IP and network traffic from local observers. • VPN provider can still see metadata. It is important to pick a vetted provider.

Physical Device Security

Topic	Tip	What to do	Additional info
1. **Use of Biometrics / FaceID**	Disable biometrics for unlocking sensitive access, including access to mobile device from the lock screen.	• Turn off Face ID / Touch ID for device unlock and for apps holding sensitive data. • Use a strong passcode/password instead.	• Biometrics can be compelled or bypassed. • A strong passphrase or passcode is legally and technically more robust.
2. **Multi-factor Authentication**	Enable two-factor authentication (2FA) on all sensitive apps.	• Turn on 2FA. Use an authenticator app or hardware key such as Proton Authenticator or DuoMobile). • Avoid SMS 2FA where possible. • Store recovery codes in a secure password manager or offline safe.	• Prevents account takeover even if passwords leak. • Hardware keys offer strongest protection.

3. **Location trackers**	Disable unnecessary location trackers.	• Turn off location permissions for apps that don't need them. • Disable location history and GPS for apps where privacy matters. • Disable Significant Locations & Routes tracking on iPhone, and clear location history. • For temporary needs, grant location access only while using the app.	• Limits real-time tracking and places you on less surveillance maps. • Location can still leak via photos or metadata. • Clear metadata from photos and electronic documents if they are to be distributed or shared publicly.
4. **Device encryption**	Require device encryption and strong lock screen.	• Ensure device encryption is enabled (modern iPhones and updated Androids do this by default). • Use a long alphanumeric passphrase if practical. • Enable auto-lock after short inactivity.	• Protects local data if device is lost or stolen. • Encryption is ineffective if passcode is weak or device is unlocked.
5. **Backups and Cloud syncing**	Limit sensitive backups and cloud syncing.	• Turn off automatic photo backups to cloud services for sensitive content. • Use in-app capture for photos (such as Signal) or encrypted cloud storage (such as Proton Drive). • Review what data (call logs, app data) syncs to cloud and disable if necessary.	• Backups can create copies accessible via cloud accounts. • Secure backups require strong account protection and encryption.
6. **Software security**	Keep software up to date and minimize risky apps from unsecured stores.	• Install OS and app updates promptly. • Remove apps you don't use; avoid sideloading untrusted apps. • Use official app stores and check app permissions.	• Updates patch vulnerabilities; malicious or outdated apps are common infection vectors.

7. **Cameras and microphones**	Cover or protect cameras and microphones when not in use.	• Use a physical camera cover or removable sticker. • Revoke microphone/camera permissions for apps that don't need them.	• Prevents remote activation or casual spying if a device or IoT camera is compromised.
8. **Prepare for loss**	Prepare for loss/theft of physical devices (remote wipe, contacts, account list).	• Enable Find My Device / remote erase features. • Keep an offline list (or secure password manager) of hosting, domain, and account recovery contacts. • Have a plan for changing passwords and notifying contacts if an account is compromised.	• Speeds recovery and containment after a physical loss or targeted attack.

Legal Liability Disclaimer

The information in this Digital Security Quick Reference Guide is provided for general informational purposes only and does not constitute professional, legal, or technical advice. While the guide aims to present accurate and practical steps for improving digital and device security, no guarantee is made regarding its completeness, suitability, or effectiveness for any particular situation.

You assume full responsibility for any actions you take based on the information in this document. Always exercise your own judgment and, when appropriate, consult a qualified professional for advice tailored to your specific circumstances. Neither the author nor any distributor of this checklist accepts liability for any loss, damage, injury, or other consequences that may result from following or attempting to implement the recommendations herein.