

Edno Chovak

PRACTICAL HANDBOOK OF COUNTERMEASURES

TACTICAL BRIEFING

I-BF-06-02

Digital Self-Defense on iPhone

The Complete Privacy Guide



Version 1.1



Imprint

Practical Handbook of Countermeasures –
Tactical Briefing BF-06-01: Digital Self-Defense on iPhone: The Complete Privacy Guide
Version 1.1 – First Edition in English Language 2026

Copyright © 2026 Edno-Chovak.com
c/o IP-Management #8444
Ludwig-Erhard-Straße 18
20459 Hamburg
E-Mail: contact@edno-chovak.com
Web: edno-chovak.com

Filename: TB-I-BF-06-02-v1_en_DigitalSelfDefenseonApple_IOS.pdf
Checksum Verification File: TB-I-BF-06-02-v1_en_CHKSUM.txt

All rights reserved.

I used AI assistance systems in researching and initially drafting this tactical briefing. I am responsible for all content, which has been checked for accuracy and edited.

This text may not be scanned, copied, translated, reproduced, distributed, or used in any other way without the author's consent, not even in excerpts: neither in printed nor electronic form. Any violation infringes copyright and may be prosecuted.

This Tactical Briefing is part of the Practical Handbook of Countermeasures and is available to readers of the book as a free download. The files obtained in this way or these download links may only be shared within a close circle of family and friends. Publication of the files or download links on the internet, in chat groups, forums, on social media, or in other publications is not permitted and may be prosecuted as a copyright infringement.

Table of Contents

Table of Contents	4
1 Situational Overview	8
1.1 Focus of this Tactical Briefing.....	8
2 Your Apple ID — Account, iCloud, and Security	9
2.1 Verify and Strengthen Two-Factor Authentication.....	9
2.2 Review Devices Signed In to Your Apple ID.....	9
2.3 Selectively Configure iCloud Sync	9
2.4 Enable Advanced Data Protection for iCloud (Strongly Recommended).....	10
2.5 Restrict Web Access to iCloud Data	11
2.6 Audit Third-Party Apps Using Sign In with Apple	11
3 iOS System Settings — Privacy & Security	12
3.1 Disable App Tracking Completely.....	12
3.2 Systematically Configure Location Services	12
3.3 Systematically Review App Permissions	13
3.4 Disable Analytics & Improvements	13
3.5 Turn Off Personalized Ads.....	13
3.6 Use the Safety Check Feature	14
3.7 Device Security: Passcode, Face ID, and SIM PIN.....	14
3.8 Enable the App Privacy Report.....	14
3.9 Lockdown Mode for High-Risk Individuals	14
4 Siri — Apple's Voice Assistant	16
4.1 Restrict Siri Activation	16
4.2 Restrict Siri's Access to Your Apps	16
4.3 Delete Your Siri History and Voice Data	16
4.4 Configure Apple Intelligence	16
5 Safari — Privacy in Apple's Default Browser	17
5.1 Configure Safari's Privacy Settings	17
5.2 Clear Safari History and Switch Your Search Engine	17
5.3 Private Browsing and Face ID Lock.....	17
6 iMessage, FaceTime, and Communication	19
6.1 iMessage Security	19
6.2 FaceTime Privacy.....	19
6.3 Mail Privacy Protection	19
7 Apps and the App Store	20
7.1 Check App Privacy Nutrition Labels Before Installing	20
7.2 Enable Automatic App Updates and Restrict Background Refresh.....	20
7.3 Require Authentication for Purchases	20
8 Network, VPN, and iCloud Private Relay	21
8.1 Wi-Fi Privacy: Private Wi-Fi Address	21
8.2 iCloud Private Relay (Requires iCloud+ Subscription).....	21
8.3 Encrypted DNS	21
9 Passwords, Keychain, and Passkeys	22
9.1 Apple Keychain vs. Independent Password Managers	22

9.2	Identify Weak and Compromised Passwords	22
9.3	Adopt Passkeys Where Available.....	22
10	Health, Fitness, and Sensors	23
10.1	Restrict Apple Health Data Sharing	23
10.2	Motion & Fitness Data	23
11	Complete Action List by Priority	24
11.1	Immediate Actions (approx. 30 minutes)	24
11.2	High-Priority Actions (approx. 45 minutes)	24
11.3	Medium-Priority Actions (approx. 45 minutes)	25
12	What This Guide Achieves — and What It Doesn't	27
13	Practical Handbook and Tactical Briefings	28
13.1	About the "Practical Handbook of Countermeasures"	28
13.2	About the "Tactical Briefings"	29
13.3	Disclaimer	29

Digital Self-Defense on iPhone: The Complete Privacy Guide

Audience: iPhone users running iOS 17 or iOS 18, with an Apple ID, iCloud enabled, and typical Apple services in use (Siri, Safari, iMessage, FaceTime, App Store).

Time required: Approximately 2–3 hours for all measures; the most critical immediate steps can be completed in under 30 minutes.

Structure: This guide works from the outside in, starting at the Apple ID account level, moving through the operating system, and then covering individual services and apps, closing with a complete prioritized action list.

A note on Apple and privacy. Apple actively markets itself as the most privacy-conscious of the major tech companies, and in many respects, that reputation is earned. App Tracking Transparency, Advanced Data Protection for iCloud, and on-device processing for many AI features represent genuine progress. At the same time, Apple collects substantial data by default: usage statistics, Siri requests, App Store activity, and location data all flow to Apple's servers unless you explicitly turn them off. Many of these settings ship enabled and must be manually disabled. This guide shows you exactly how.

1 Situational Overview

Digital threats don't start with an attack. They start with data collection. Search histories, location data, click patterns, and metadata are aggregated into behavioral profiles from which systems draw conclusions that you never disclosed-about your income, health, political beliefs. The real target is not your device. It's the predictive model of your behavior.

Surveillance is harmful, even if nothing happens. The chilling effect, learned helplessness, and chronic background stress are measurable psychological consequences, long before any concrete damage occurs. And: Digital traces outlive governments. What is legal today can be used against you tomorrow.

Your devices and services are not designed for data protection in their default configuration. The leakage of personal information is the norm, not the exception.

Consequence: You need to take action yourself. Every protective measure reduces your vulnerability, strengthens your digital self-determination, and has a proven positive effect on your mental well-being. Those who protect themselves also protect others-data protection is a social good.

This tactical briefing shows you exactly how to do this.

1.1 FOCUS OF THIS TACTICAL BRIEFING

PA-I-4	Privacy protection
TF-06	Mobile Usage
IMMEDIATELY	Minimizing the database for metadata analysis

Smartphones are the most personal and, at the same time, the most closely monitored devices in our digital everyday lives. They know your location, your contacts, your habits, your health data, and your communications. The default configuration of Android and iOS is optimized for data collection.

Operational guideline:

The smartphone is the most comprehensive surveillance device that has ever existed - and you carry it around with you voluntarily. Any restriction on data collection is a gain in personal sovereignty.

2 Your Apple ID — Account, iCloud, and Security



Your Apple ID is the central identity anchor of the entire Apple ecosystem. It ties together iCloud storage, App Store purchases, iMessage, FaceTime, Find My, Apple Pay, and, if you use Apple Intelligence, AI activity. Securing and cleaning up your Apple ID is therefore the logical first step.

2.1 VERIFY AND STRENGTHEN TWO-FACTOR AUTHENTICATION

Two-factor authentication (2FA) for your Apple ID should already be active — Apple has made it mandatory for new accounts. Even so, you should verify the status and review which trusted phone numbers and devices are on file.

What to do: Open **Settings** → **[Your Name]** → **Sign-In & Security**. Under "Two-Factor Authentication," review which phone numbers are listed as trusted. Remove any numbers you no longer use or that don't belong to you. Make sure at least one current number is on file — it's required for account recovery.

One important caveat: unlike Google, Apple does not support third-party authenticator apps (such as Authy or Google Authenticator) as a second factor for the Apple ID. Apple relies exclusively on device-generated verification codes and SMS. If you want maximum security, make sure the phone number on file is protected by a SIM PIN to guard against SIM-swapping attacks (see Section 3.7).

2.2 REVIEW DEVICES SIGNED IN TO YOUR APPLE ID

Open **Settings** → **[Your Name]** and scroll to the bottom. You'll see every device currently signed in with your Apple ID. Tap each one and confirm you recognize it. For any device you no longer own or don't recognize, tap "Remove from Account."

2.3 SELECTIVELY CONFIGURE ICLOUD SYNC

By default, iCloud syncs a wide range of data to Apple's servers: photos, contacts, calendars, notes, messages, passwords, health data, and more. Open **Settings** → **[Your Name]** → **iCloud** and review each toggle.

For most users, the following configuration makes sense. Leave enabled: iCloud Backup (for device recovery), Contacts, Calendars, and Passwords (Keychain), unless you're using alternative services. Carefully review or disable: Photos (if you don't need cross-device photo sync, or if you're using Proton Drive as an alternative), Messages (iMessage history in the cloud, more on this in Section 6.1), Notes (if you prefer local-only notes), Siri (Siri history and suggestions), Mail (if you don't use an iCloud email address), and Health (health data in the cloud).

Tap each enabled service to see exactly what data is being synced. Disabling a service keeps your data on the device, it simply stops syncing to Apple's servers.

2.4 ENABLE ADVANCED DATA PROTECTION FOR ICLOUD (STRONGLY RECOMMENDED)

This is the single most impactful step for iPhone users who want to continue using iCloud. Advanced Data Protection extends end-to-end encryption to nearly all iCloud data categories, including iCloud Backup, Photos, Notes, and iCloud Drive.

In the default configuration (without Advanced Data Protection), Apple holds the encryption keys for most iCloud data and can hand them over to law enforcement in response to a valid legal request, such as a court order or national security letter. With Advanced Data Protection enabled, the keys exist only on your trusted devices, Apple itself cannot decrypt your data.

Data Category	Without Advanced Data Protection	With Advanced Data Protection
iCloud Backup	Not end-to-end encrypted	End-to-end encrypted
iCloud Drive	Not end-to-end encrypted	End-to-end encrypted
Photos	Not end-to-end encrypted	End-to-end encrypted
Notes	Partially end-to-end encrypted	Fully end-to-end encrypted
Safari History	Not end-to-end encrypted	End-to-end encrypted
iCloud Mail	Not E2E (by design)	Not E2E (by design)
iMessage	End-to-end encrypted	End-to-end encrypted
Health Data	End-to-end encrypted	End-to-end encrypted
Passwords (Keychain)	End-to-end encrypted	End-to-end encrypted

What to do: Open **Settings** → **[Your Name]** → **iCloud** → **Advanced Data Protection**. Follow the setup wizard. All devices linked to your Apple ID must be running a recent OS version (iOS 16.2 or later, macOS 13.1 or later, watchOS 9.2 or later). You'll also need to set up a recovery contact or a recovery key, because Apple can no longer access your data once Advanced Data Protection is on, there is no Apple-assisted account recovery. Store your recovery key somewhere safe and offline.

Important: iCloud Mail, iCloud Calendar, and iCloud Contacts remain outside end-to-end encryption even with Advanced Data Protection enabled. This is because these services must interoperate with open protocols (IMAP, CalDAV, CardDAV). For full end-to-end encryption of email and calendar data, switching to Proton Mail, Proton Calendar, and Proton Contacts (as part of Proton Mail) is required.

2.5 RESTRICT WEB ACCESS TO ICLOUD DATA

By default, you and anyone with your credentials can access your iCloud data through a browser at iCloud.com. If you don't need this, turn it off.

What to do: Open **Settings** → **[Your Name]** → **iCloud** and disable "Access iCloud Data on the Web." Your iCloud data will then only be accessible from your trusted devices, not through any browser.

2.6 AUDIT THIRD-PARTY APPS USING SIGN IN WITH APPLE

Just as with a Google account, third-party apps can request access to your name, email address, and other data when you sign in using your Apple ID.

What to do: Open **Settings** → **[Your Name]** → **Sign-In & Security** → **Apps Using Apple ID**. You'll see every app where you've used "Sign in with Apple." Tap each entry to review what permissions were granted. For apps you no longer use, select "Stop Using Apple ID." Note that this only revokes the Apple ID connection, your account with the app itself remains active until you delete it directly within that service..



3 iOS System Settings — Privacy & Security

The **Settings** → **Privacy & Security** section is the control center of iOS privacy configuration. It contains all the key controls for app permissions, tracking, and system-wide privacy features.

3.1 DISABLE APP TRACKING COMPLETELY

Since iOS 14.5, apps must ask for permission before using your device's advertising identifier (IDFA) for cross-app and cross-website tracking. This is Apple's App Tracking Transparency (ATT) framework. By default, however, apps are still allowed to ask: you need to actively prevent them from doing so.

What to do: Open **Settings** → **Privacy & Security** → **Tracking** and turn off "Allow Apps to Request to Track." All future tracking requests will be automatically denied without any prompt appearing. Also review the list of apps that have already been granted tracking permission and revoke access for all of them.

3.2 SYSTEMATICALLY CONFIGURE LOCATION SERVICES

Location data is one of the most sensitive permission categories. iOS offers fine-grained control that should be used consistently.

What to do: Open **Settings** → **Privacy & Security** → **Location Services**. Work through every entry using the following framework:

Setting	Recommendation
Location Services (global toggle)	Leave on (needed for emergency calls and navigation)
Apps set to "Always"	Reduce to "While Using the App" or "Never"
Apps set to "While Using the App"	Verify that location is actually needed for core functionality
"Precise Location"	Enable only for mapping apps; disable for everything else
System Services → Significant Locations	Disable
System Services → Product Improvement (all)	Disable
System Services → Routing & Traffic	Optional (useful for Apple Maps)
System Services → Location Alerts	Only if actively used

Scroll to the bottom of System Services and disable all entries under "Product Improvement": "iPhone Analytics," "Routing & Traffic" (if not needed), and "Improve Maps." Also disable **Significant Locations**: this feature builds a detailed timeline of your movements on the device, similar to Google's Location History, and stores it locally but in a form accessible to Apple and law enforcement.

3.3 SYSTEMATICALLY REVIEW APP PERMISSIONS

Below the Location Services and Tracking sections, iOS displays a categorized list of all permissions. Work through each category:

Permission	Risk Level	Recommendation
Microphone	Very high	Phone, Voice Memos, trusted messengers only
Camera	High	Camera app and trusted messengers only
Contacts	High	Phone, messengers only; deny all others
Calendars	Medium	Calendar apps only
Reminders	Medium	Task management apps only
Photos	Medium	Use "Selected Photos" instead of "All Photos"
Bluetooth	Medium	Bluetooth-dependent apps only
Local Network	Medium	Smart home apps only
Health	High	Fitness apps only; review data sharing
Motion & Fitness	Medium	Fitness apps only
Speech Recognition	High	Trusted apps only
Face ID / Touch ID	High	Authentication apps only

For the Photos permission specifically: for every app that requests photo access, choose "Selected Photos" rather than "All Photos." This limits the app to only the photos you explicitly share, it cannot see your entire photo library with all its embedded metadata (location, date, device information).

3.4 DISABLE ANALYTICS & IMPROVEMENTS

Open **Settings** → **Privacy & Security** → **Analytics & Improvements**. Turn off every toggle: "Share iPhone & Watch Analytics," "Share iCloud Analytics," "Improve Siri & Dictation," "Improve Assistive Voice Features," and "Improve AR Location Accuracy." Apple describes this data as anonymous, but that characterization is Apple's own, and the volume of usage statistics transmitted is substantial.

3.5 TURN OFF PERSONALIZED ADS

Open **Settings** → **Privacy & Security** → **Apple Advertising** and disable "Personalized Ads." Tap "View Ad Targeting Information" to see what data Apple uses for advertising purposes, including your birth year, zip code, and the categories of apps you've downloaded. This data is used for ads in the App Store, Apple News, and Apple Stocks.

3.6 USE THE SAFETY CHECK FEATURE

The Safety Check tool at **Settings** → **Privacy & Security** → **Safety Check** was introduced in iOS 16 and provides a complete overview of all data access and an emergency reset option.

Tap "Manage Sharing & Access" to see which people and apps can access your information. Pay particular attention to: who can see your location, which apps have access to your Health data, and with whom you're sharing your location through Find My.

The **Emergency Reset** option immediately stops all data access by apps and people: useful in situations where you need to quickly revoke all sharing, for example if a device has been compromised or a relationship has ended.

3.7 DEVICE SECURITY: PASSCODE, FACE ID, AND SIM PIN

Passcode: Open **Settings** → **Face ID & Passcode** (or "Touch ID & Passcode" on older devices). Make sure a passcode is set. Under "Change Passcode," tap "Passcode Options" and select **Custom Alphanumeric Code** with at least eight characters. Six-digit numeric codes are significantly faster to crack with modern hardware. Enable "Erase Data" (which wipes the device after 10 failed attempts) only if you're confident you won't forget your passcode.

Restrict Face ID / Touch ID: Under **Settings** → **Face ID & Passcode**, review which features Face ID is enabled for. Consider disabling "Siri" if you don't want Siri accessible without unlocking the device. Enable **Stolen Device Protection** (iOS 17.3 and later) at **Settings** → **Privacy & Security** → **Stolen Device Protection**: this feature adds a one-hour security delay before critical settings (Apple ID password, Face ID) can be changed when the device is at an unfamiliar location: a direct countermeasure against the "shoulder surfing + theft" attack that became widespread in major US cities.

Activate a SIM PIN: Open **Settings** → **Cellular** → **SIM PIN** and enable the PIN. Change the default PIN (typically 0000 or 1234) to a unique PIN of at least six digits. This prevents a stolen SIM card from being used in another device, a critical defense against SIM-swapping, which is used to bypass SMS-based two-factor authentication.

Restrict USB Accessories: In **Settings** → **Privacy & Security**, find "USB Accessories" and make sure "Allow When Locked" is set to off (the toggle should be disabled). This prevents forensic tools like Cellebrite from accessing a locked device over USB, a real-world threat documented in law enforcement use cases across the US.

3.8 ENABLE THE APP PRIVACY REPORT

Open **Settings** → **Privacy & Security** → **App Privacy Report** and turn it on. After a few days of use, the report shows which apps accessed which permissions and when, along with the network domains each app contacted. This is a valuable tool for detecting unwanted background activity: if an app accessed your microphone or location while you weren't actively using it, revoke that permission immediately.

3.9 LOCKDOWN MODE FOR HIGH-RISK INDIVIDUALS

Lockdown Mode at **Settings** → **Privacy & Security** → **Lockdown Mode** is an extreme security measure designed for individuals at elevated risk: investigative journalists, activists, attorneys, or anyone who may be targeted by sophisticated state-sponsored surveillance tools such as Pegasus

spyware. In Lockdown Mode, message attachments are blocked, FaceTime calls from unknown contacts are rejected, complex web technologies are disabled in Safari, and wired connections to computers are blocked. For the average user, Lockdown Mode is too restrictive for daily use, but it is an important tool for high-risk situations and worth knowing about.



4 Siri — Apple's Voice Assistant

Siri has access to your microphone, contacts, calendars, messages, call logs, location, photos, and - with Apple Intelligence enabled - the contents of virtually every app on your device. According to Apple's privacy policy, voice recordings may be used to improve the speech model unless you opt out.

4.1 RESTRICT SIRI ACTIVATION

What to do: Open **Settings** → **Siri**. Disable "Listen for 'Hey Siri'": this feature keeps the microphone in a persistent low-power listening state waiting for the wake word. Also disable "Allow Siri When Locked" so Siri cannot be invoked without unlocking the device. If you don't use Siri at all, disable "Press Side Button for Siri" (or "Press Home Button for Siri" on older devices with a Home button) as well.

4.2 RESTRICT SIRI'S ACCESS TO YOUR APPS

What to do: Open **Settings** → **Siri** → **Siri & Search**. For each app listed, you can control whether Siri can learn from and suggest content from that app. Disable access for any app whose contents you don't want Siri to process, particularly messaging apps, Notes, and Health-related apps.

4.3 DELETE YOUR SIRI HISTORY AND VOICE DATA

What to do: Open **Settings** → **Siri** → **Siri History** and tap "Delete Siri & Dictation History." This removes all previously stored Siri requests and voice recordings from Apple's servers. Also go to **Settings** → **Privacy & Security** → **Analytics & Improvements** and disable "Improve Siri & Dictation", this prevents new voice recordings from being used to train Apple's speech model going forward.

4.4 CONFIGURE APPLE INTELLIGENCE

Apple Intelligence (available from iOS 18.1 onward) is Apple's generative AI integration. It has system-wide access to app content, messages, emails, and photos. Apple emphasizes that most processing happens on-device, with Private Cloud Compute handling more complex requests on Apple's servers.

What to do: Open **Settings** → **Apple Intelligence & Siri**. If you don't want to use Apple Intelligence, you can disable it entirely here. If you do use it, tap "App Access" to review which apps grant Apple Intelligence access to their content. Disable access for any app whose data you don't want the AI to process.



5 Safari — Privacy in Apple's Default Browser

Safari offers significantly better privacy protections than Chrome out of the box, provided the right settings are enabled. It is worth taking the time to configure it properly.

5.1 CONFIGURE SAFARI'S PRIVACY SETTINGS

What to do: Open **Settings** → **Apps** → **Safari** → **Privacy & Security** (on iOS 17 and earlier: **Settings** → **Safari** → **Privacy & Security**). Enable or verify the following:

"Prevent Cross-Site Tracking" should be on. Safari uses Intelligent Tracking Prevention (ITP), a machine learning-based system that automatically identifies and blocks tracking cookies and scripts used by advertisers to follow you across websites.

"Advanced Tracking and Fingerprint Protection" (new in iOS 18): Set this to "All Browsing." This feature defends against browser fingerprinting — a technique where websites identify your device based on a unique combination of characteristics such as screen resolution, installed fonts, time zone, and system settings, without needing cookies. With this setting on, Safari actively obscures those characteristics.

"Hide IP Address" (requires iCloud+ subscription): Set to "Trackers and Websites." This routes your IP address through Apple's relay infrastructure so that websites cannot use it to identify or track you.

"Block All Cookies" is available but **not recommended**: it breaks many legitimate websites. Safari already blocks third-party cookies by default, which addresses the primary tracking risk while keeping first-party cookies functional.

Do not disable "Fraudulent Website Warning": this feature protects against known phishing sites and is an important security tool.

5.2 CLEAR SAFARI HISTORY AND SWITCH YOUR SEARCH ENGINE

What to do: Open **Settings** → **Safari** → **Clear History and Website Data** and clear all stored data. Set up automatic clearing: **Settings** → **Safari** → **Close Tabs** and **Settings** → **Safari** → **Advanced** → **Website Data** can be used to manage retention. For automatic history deletion, go to **Settings** → **Safari** and set "Close Tabs" to "After One Week" or "After One Day" depending on your preference.

For your search engine: open **Settings** → **Safari** → **Search Engine** and switch from Google to DuckDuckGo or Brave Search. Even when used through Safari, Google functions as a tracking instrument: every search query is associated with your IP address and, if you're signed into a Google account, with your profile. DuckDuckGo does not store search histories or build user profiles.

5.3 PRIVATE BROWSING AND FACE ID LOCK

Safari's Private Browsing mode prevents local storage of history and cookies. In iOS 17 and 18, Private Browsing tabs are locked by Face ID or Touch ID by default. Verify this is enabled at **Settings** → **Safari** → **Require Face ID to Unlock Private Browsing**.

Keep in mind: Private Browsing does not prevent server-side tracking. Your IP address and other device identifiers remain visible to the websites you visit. For full anonymity, a No-Log-VPN is required.



6 iMessage, FaceTime, and Communication

6.1 IMESSAGE SECURITY

iMessage is end-to-end encrypted when both parties are using Apple devices. When a message appears as a green SMS bubble rather than a blue iMessage bubble, it is not encrypted, it is transmitted as a standard SMS over the cellular network, where it can be intercepted or accessed by your carrier.

What to do: Open **Settings** → **Messages** and make sure iMessage is enabled. Consider disabling "Send as SMS" if you want to ensure that messages are only sent as encrypted iMessages, and not automatically downgraded to unencrypted SMS when iMessage is unavailable.

Regarding iMessage history in iCloud: if you have Advanced Data Protection enabled (Section 2.4), your iMessages stored in iCloud are end-to-end encrypted. Without Advanced Data Protection, Apple can access your iMessage history stored in iCloud and may be required to provide it in response to a valid legal order.

For communicating with people who don't have an iPhone, Signal is the recommended alternative. Signal provides end-to-end encryption across all platforms (iOS, Android, desktop) and is widely regarded as the gold standard for private messaging. It is free, open source, and used by journalists, attorneys, and security professionals across the US.

6.2 FACETIME PRIVACY

FaceTime calls are end-to-end encrypted. Additionally, review the following settings: open **Settings** → **FaceTime** and disable "FaceTime Live Photos" if you don't want your conversation partners to be able to take screenshots during a call. Also disable **SharePlay** if you don't use it. This feature allows other people to interact with content on your device during a call.

6.3 MAIL PRIVACY PROTECTION

Open **Settings** → **Apps** → **Mail** → **Privacy Protection** and enable "Protect Mail Activity." This feature prevents senders from using tracking pixels to determine whether and when you opened their email. It loads email content through Apple's proxy servers, hiding your IP address from the sender.

Note that iCloud Mail is not end-to-end encrypted and can be handed over to law enforcement in response to a valid legal request. For fully encrypted email communication, switching to Proton Mail is required.

Note that iCloud Mail is not end-to-end encrypted and can be handed over to law enforcement in response to a valid legal request. For fully encrypted email communication, switching to Proton Mail is required.



7 Apps and the App Store

7.1 CHECK APP PRIVACY NUTRITION LABELS BEFORE INSTALLING

Apple requires all app developers to publish a "privacy nutrition label" in the App Store listing, disclosing what data the app collects and whether it is linked to your identity. Open the App Store, tap any app, and scroll to "App Privacy." Make it a habit to check this section before installing any new app. Pay particular attention to the "Data Used to Track You" category.

7.2 ENABLE AUTOMATIC APP UPDATES AND RESTRICT BACKGROUND REFRESH

What to do: Open **Settings** → **App Store** and enable "App Updates" under "Automatic Downloads." Keeping apps up to date is one of the most effective security measures available. Outdated apps are a common attack vector.

Also open **Settings** → **General** → **Background App Refresh** and disable background refresh for every app that doesn't genuinely require it. Background App Refresh allows apps to fetch data in the background even when you're not actively using them, a capability that can be used to collect location data, sync usage statistics, or update advertising profiles.

7.3 REQUIRE AUTHENTICATION FOR PURCHASES

Open **Settings** → **[Your Name]** → **Media & Purchases** and set "Require Password" to "Always." This prevents accidental or unauthorized in-app purchases.



8 Network, VPN, and iCloud Private Relay

8.1 WI-FI PRIVACY: PRIVATE WI-FI ADDRESS

iOS randomizes the MAC address it presents to each Wi-Fi network by default, a feature called "Private Wi-Fi Address." This prevents Wi-Fi networks from tracking your device across locations using a persistent hardware identifier. Verify that this feature is enabled for all saved networks.

What to do: Open **Settings** → **Wi-Fi**, tap the info icon (i) next to each saved network, and confirm that "Private Wi-Fi Address" is enabled. For networks you visit regularly (such as your home network), choose "Fixed Private Address" so your device maintains a consistent but still private identifier. For public networks (coffee shops, airports, hotels), choose "Rotating Private Address" for maximum privacy.

8.2 ICLOUD PRIVATE RELAY (REQUIRES ICLOUD+ SUBSCRIPTION)

iCloud Private Relay is Apple's privacy feature for Safari browsing traffic, available with any paid iCloud+ plan. It works similarly to a VPN but is limited to Safari: your connection is routed through two separate servers, so neither Apple nor the exit node provider can see both your identity and your browsing activity simultaneously.

What to do: Open **Settings** → **[Your Name]** → **iCloud** → **Private Relay** and enable it. Under "IP Address Location," choose "Use General Location" for maximum privacy (rather than "Maintain General Location," which preserves your approximate region for location-based content).

Note that iCloud Private Relay only protects Safari traffic, not traffic from other apps. For comprehensive network-level protection, a full VPN such as Proton VPN or Mullvad is required

8.3 ENCRYPTED DNS

iOS supports encrypted DNS through configuration profiles. While Android offers a native DNS-over-TLS option in the system settings, iOS requires a slightly different approach.

What to do: Download *AdGuard* or *NextDNS* from the App Store. These apps install a DNS configuration profile that encrypts all DNS queries from your device and routes them through a privacy-respecting DNS server. Activate the profile at **Settings** → **General** → **VPN & Device Management**. This prevents your internet service provider and any network operator from seeing which domain names your device is looking up, a significant privacy improvement on public Wi-Fi and cellular networks.



9 Passwords, Keychain, and Passkeys

9.1 APPLE KEYCHAIN VS. INDEPENDENT PASSWORD MANAGERS

Apple's Keychain is deeply integrated into iOS and provides seamless AutoFill for passwords and passkeys. It is end-to-end encrypted and significantly more secure than unencrypted browser-based password managers. Its limitation is that it is tied to the Apple ecosystem: if you also use Windows or Android devices, you'll need a cross-platform solution.

What to do: If you use exclusively Apple devices, Keychain is a solid choice. Verify it's active at **Settings → Passwords → Password Options → AutoFill Passwords and Passkeys → iCloud Keychain**. For cross-platform use, Bitwarden (open source, free tier available) or Proton Pass are strong alternatives that work across iOS, Android, Windows, and macOS.

9.2 IDENTIFY WEAK AND COMPROMISED PASSWORDS

What to do: Open **Settings → Passwords** and review the Security Recommendations section. iOS automatically flags weak passwords, reused passwords, and passwords that have appeared in known data breaches (checked against the Have I Been Pwned database). Change any password marked as "Compromised" immediately: these are credentials that attackers can purchase on the dark web and use in credential-stuffing attacks against your accounts.

9.3 ADOPT PASSKEYS WHERE AVAILABLE

Passkeys are a modern replacement for passwords based on cryptographic key pairs. They are phishing-resistant and cannot be compromised in a data breach because no shared secret is transmitted to the server. iOS 16 and later support passkeys natively through the Keychain.

What to do: When a website or app offers a passkey option during sign-in or account creation, choose it. iOS stores the passkey automatically in your Keychain and syncs it across your Apple devices via iCloud (end-to-end encrypted). For a directory of services that support passkeys: passkeys.directory.

10 Health, Fitness, and Sensors



10.1 RESTRICT APPLE HEALTH DATA SHARING

Apple Health stores highly sensitive biometric data: heart rate, sleep patterns, step counts, menstrual cycle data, medications, and - with an Apple Watch - ECG readings. This data is end-to-end encrypted when Advanced Data Protection is enabled (Section 2.4).

What to do: Open the **Health app** → **your profile picture** → **Privacy**. Under "Apps and Services," review which third-party apps have access to your health data and revoke access for any that don't need it. Also disable "Health Research" if you don't want to participate in Apple-sponsored research studies, which share your health data with academic and commercial research partners.

10.2 MOTION & FITNESS DATA

What to do: Open **Settings** → **Privacy & Security** → **Motion & Fitness** and review which apps have access to motion and fitness data. Revoke access for any app that doesn't require it for its core function. Motion data can be used to infer your location, activity patterns, and even emotional state: it is more sensitive than it may appear.



11 Complete Action List by Priority

11.1 IMMEDIATE ACTIONS (APPROX. 30 MINUTES)

Action	Path	Time
Disable app tracking	Settings → Privacy & Security → Tracking	2 min.
Disable analytics & improvements	Settings → Privacy & Security → Analytics & Improvements	3 min.
Turn off personalized ads	Settings → Privacy & Security → Apple Advertising	1 min.
Disable Significant Locations	Settings → Privacy & Security → Location Services → System Services	2 min.
Delete Siri history	Settings → Siri → Siri History	2 min.
Disable "Hey Siri"	Settings → Siri → Listen for "Hey Siri"	1 min.
Review signed-in devices	Settings → [Your Name] → device list	5 min.
Audit third-party Apple ID apps	Settings → [Your Name] → Sign-In & Security → Apps Using Apple ID	5 min.
Enable Stolen Device Protection	Settings → Privacy & Security → Stolen Device Protection	2 min.
Restrict USB accessories	Settings → Privacy & Security → USB Accessories	1 min.
Enable Mail Privacy Protection	Settings → Apps → Mail → Privacy Protection	1 min.
Configure Safari privacy settings	Settings → Apps → Safari → Privacy & Security	3 min.
Switch Safari search engine	Settings → Apps → Safari → Search Engine → DuckDuckGo	1 min.

11.2 HIGH-PRIORITY ACTIONS (APPROX. 45 MINUTES)

Action	Path	Time
Enable Advanced Data Protection	Settings → [Your Name] → iCloud → Advanced Data Protection	10 min.
Systematically review app permissions	Settings → Privacy & Security → [each category]	20 min.

Action	Path	Time
Configure Location Services	Settings → Privacy & Security → Location Services	10 min.
Selectively configure iCloud sync	Settings → [Your Name] → iCloud	5 min.
Activate SIM PIN	Settings → Cellular → SIM PIN	2 min.
Enable App Privacy Report	Settings → Privacy & Security → App Privacy Report	1 min.
Restrict Siri's app access	Settings → Siri → Siri & Search	5 min.
Verify Private Wi-Fi Address	Settings → Wi-Fi → [network] → Private Wi-Fi Address	5 min.
Restrict Background App Refresh	Settings → General → Background App Refresh	5 min.
Limit Photos permission to Selected Photos	Settings → Privacy & Security → Photos	5 min.

11.3 MEDIUM-PRIORITY ACTIONS (APPROX. 45 MINUTES)

Action	Path	Time
Enable iCloud Private Relay (iCloud+)	Settings → [Your Name] → iCloud → Private Relay	2 min.
Disable web access to iCloud data	Settings → [Your Name] → iCloud → Access iCloud Data on the Web	1 min.
Run Safety Check	Settings → Privacy & Security → Safety Check	10 min.
Set up automatic Safari history clearing	Settings → Apps → Safari → Close Tabs	2 min.
Lock Private Browsing with Face ID	Settings → Apps → Safari → Require Face ID to Unlock Private Browsing	1 min.
Configure Apple Intelligence	Settings → Apple Intelligence & Siri	5 min.
Restrict Health app data sharing	Health app → profile picture → Privacy → Apps and Services	5 min.
Review compromised passwords	Settings → Passwords → Security Recommendations	10 min.
Set up encrypted DNS	AdGuard or NextDNS from the App Store	5 min.

Action	Path	Time
Disable FaceTime Live Photos	Settings → FaceTime → FaceTime Live Photos	1 min.
Strengthen passcode	Settings → Face ID & Passcode → Change Passcode → Passcode Options	3 min.

12 What This Guide Achieves — and What It Doesn't



The measures in this guide substantially reduce data collection by Apple and third-party apps. They do not eliminate it entirely. Apple continues to collect data through the App Store, iCloud connections, and aggregated usage statistics — even with all the settings above configured — because certain system services operate with privileged access that user-facing settings do not fully control.

An important distinction from Android: Apple has introduced structural privacy improvements through App Tracking Transparency and Advanced Data Protection that go beyond what Google offers by default. At the same time, the Apple ecosystem is more closed — users have fewer options to inspect system services, install alternative operating systems, or audit what data leaves the device.

For deeper protection, structural changes are necessary. Switching to privacy-respecting services — Proton Mail instead of iCloud Mail, Proton Drive instead of iCloud Drive, Signal instead of iMessage for cross-platform communication — reduces the amount of data Apple can collect in the first place. Using a full VPN (Proton VPN, Mullvad) protects all network traffic from the device, not just Safari browsing as iCloud Private Relay does. Switching to a privacy-focused browser such as Brave or Firefox Focus is worth considering for research or browsing sessions where maximum anonymity is desired.

This guide should be understood as the **first and most important step**: it provides the maximum available protection within the existing Apple ecosystem, without requiring a complete platform migration.

Anyone who completes the Immediate Actions list has done more for their digital privacy in 30 minutes than the vast majority of iPhone users ever will.



13 Practical Handbook and Tactical Briefings

13.1 ABOUT THE "PRACTICAL HANDBOOK OF COUNTER-MEASURES"

The "Practical Handbook of Countermeasures" is a multi-volume, practice-oriented complete work. It is based on several years of research and exchange with experts from various disciplines.

The target group is people who want to secure their self-responsibility, ability to act, and autonomy in a complex, crisis-prone, and increasingly digitized environment.

The approach is operational, not theoretical.

The focus is on implementable strategies for everyday life, without ideological digressions.

The work will be published from 2026 in four independently usable volumes:

- Vol. 1: Digital Resistance (April 2026)
- Vol. 2: Resilience and Preparedness (October 2026)
- Vol. 3: Manipulation Defense (Spring 2027)
- Vol. 4: Contemporary Masculinity (Fall 2027)

Each volume deals with an independent area of action.

Common Guideline:

- Analysis of the situation.
- Definition of countermeasures.
- Implementation in everyday life.

This Tactical Briefing belongs to "Volume 1: Digital Resistance"

The book is not aimed at hackers or IT experts, but at ordinary users of smartphones and Windows computers.

In a digitally connected world of social media, cloud services, and artificial intelligence, data collection and analysis are growing rapidly, and with them the risks of data misuse, identity theft, data leaks, and targeted manipulation. Profiling and scoring automatically create a digital user profile from your internet, email, and social media usage, which is recorded and evaluated and used to predict and influence your behavior. For corporations such as Google or Meta, you are not a customer, but a source of data.

Your digital profile can determine what job, housing, or credit opportunities you have, what prices you are shown, or what you pay for flights and insurance. This makes it all the more important to minimize your digital footprint and maintain control over your own data.

In addition, the book advocates for responsible, respectful, and legally conscious use of social media. It shows how you can exercise your freedom of expression without taking unnecessary personal or criminal risks, and how you can remain calm during a search and seizure and protect your civil rights.

In addition, the book shows how current legislative proposals by the EU and the German government could jeopardize privacy, civil rights, and freedom of expression.

13.2 ABOUT THE "TACTICAL BRIEFINGS"

The "Tactical Briefings" series is a series of small eBooks, each of which condenses and prepares a single topic from the "Practical Handbook of Countermeasures" in a practical way in the style of professional operational documents.

The focus is on practical use and immediate implementability.

More information and books can be found on my website:

<https://edno-chovak.com>

13.3 DISCLAIMER

- All information in this Tactical Briefing has been carefully researched, and the instructions have been tested in practice. However, I make no warranty regarding the timeliness, accuracy, completeness, or quality of the information provided, nor its suitability for any particular purpose. This is especially true because I do not know how your specific device is configured or how you use it. This Tactical Briefing cannot replace individual consultation with a professional IT security specialist. Use of this book and the information contained herein is therefore at your own risk.