
SpyWiper Pro

SpyWiper Pro — The Complete Resource Guide

Version 1.0 | 2026 Edition

Your Comprehensive Companion to Smartphone Privacy, Spyware Detection, and Digital Surveillance Protection

Published by Moni Media West LLC
Support: support.prospy@mmwguides.com | (305) 600-0858
Website: https://spywiperpro.app

IMPORTANT — PLEASE READ FIRST

Thank you for purchasing SpyWiper Pro. This Resource Guide is your comprehensive companion document, designed to be used alongside the SpyWiper Pro Intelligence Hub — your members-only online resource center.

What You Received With Your Purchase:

1. **SpyWiper Pro Application** — Available for download from your Customer Dashboard
2. **Intelligence Hub Access** — Members-only online resource center at spywiperpro.app/hub
3. **This Resource Guide** — The document you are reading now (50+ pages of curated privacy resources)

Your Login Credentials:

Your login credentials were sent to the email address used during purchase. Use them to access your Customer Dashboard at https://spywiperpro.app/login

If you did not receive your credentials, please contact us immediately at support.prospy@mmwguides.com

100% Satisfaction Guarantee:

We stand behind SpyWiper Pro completely. If you are not satisfied with your purchase for any reason, contact our support team within 30 days for a full refund — no questions asked.

Table of Contents

Chapter 1: Introduction to SpyWiper Pro

SpyWiper Pro is a comprehensive smartphone security application designed specifically to detect, identify, and remove hidden spyware, stalkerware, and surveillance software from Android and iPhone devices. Unlike traditional antivirus applications that focus on malware and viruses, SpyWiper Pro is purpose-built for the unique threat of personal surveillance.

The Growing Threat of Personal Surveillance

In today's digital landscape, personal surveillance has become an epidemic. Commercial spyware — often marketed as "parental monitoring" or "employee tracking" tools — is routinely misused by abusive partners, stalkers, and bad actors to monitor victims without their knowledge or consent.

These applications can:

- Read all text messages, emails, and chat conversations
- Track GPS location in real-time
- Record phone calls and ambient audio
- Access photos and videos
- Monitor social media activity
- Capture keystrokes and passwords
- Activate the camera and microphone remotely

Who Needs SpyWiper Pro?

SpyWiper Pro is designed for anyone who:

- Suspects their phone may be monitored
- Has left an abusive relationship and wants to ensure their device is clean
- Values their digital privacy and wants proactive protection
- Has noticed unusual phone behavior (battery drain, data usage, overheating)
- Wants to audit their device permissions and security settings

How SpyWiper Pro Is Different

Unlike generic security apps, SpyWiper Pro:

- Specifically targets stalkerware and commercial spyware signatures
- Detects hidden apps that don't appear in the app drawer

- Identifies suspicious device administrator privileges
- Scans for rogue configuration profiles (iOS)
- Monitors for unauthorized accessibility service abuse
- Checks for signs of device rooting or jailbreaking

Chapter 2: Understanding Spyware and Surveillance

What Is Spyware?

Spyware is software that is installed on a device without the owner's informed consent, designed to secretly collect information and transmit it to a third party. While some forms of monitoring software have legitimate uses (parental controls for young children, corporate device management), the term "spyware" specifically refers to software used for unauthorized surveillance.

Types of Spyware

Commercial Stalkerware: Applications like mSpy, FlexiSpy, Cocospy, and Spyic that are marketed for monitoring partners or family members. These require physical access to install on Android but can sometimes be deployed on iPhone through iCloud credentials.

Government-Grade Spyware: Advanced tools like Pegasus (NSO Group) that can infect devices through zero-click exploits. While primarily used by nation-states, awareness of these tools is important for understanding the full threat landscape.

Keyloggers: Software that records every keystroke, capturing passwords, messages, and all text input. Some keyloggers are standalone apps while others are components of larger spyware packages.

Screen Recorders: Applications that periodically capture screenshots or record the screen, providing visual documentation of all device activity.

GPS Trackers: Software or hardware devices that report location data. Software trackers run silently on the phone, while hardware trackers (like misused AirTags or Tile devices) can be hidden in belongings.

How Spyware Gets Installed

Physical Access (Most Common): The vast majority of stalkerware requires brief physical access to the target device. An abuser may install the app during a moment when the victim's phone is unlocked and unattended.

Social Engineering: Victims may be tricked into installing spyware disguised as a legitimate app, or may be sent a malicious link that triggers an exploit.

iCloud Exploitation: On iPhone, if an abuser knows the victim's Apple ID credentials, they can access iCloud backups containing messages, photos, and location data without installing anything on the device itself.

MDM Profiles: Mobile Device Management profiles can be installed that grant extensive control over a device, including the ability to silently install apps, monitor communications, and track location.

Signs Your Device May Be Compromised

- Unusual battery drain (spyware runs continuously in the background)
- Increased data usage (captured data must be transmitted)
- Device running hot when idle
- Strange sounds during calls (older spyware)
- Apps you don't remember installing
- Device takes longer to shut down (flushing captured data)
- Unexpected text messages with codes or garbled characters
- Settings that change without your action

Chapter 3: How SpyWiper Pro Protects You

Multi-Layer Detection Engine

SpyWiper Pro employs a sophisticated multi-layer approach to detecting surveillance software:

Layer 1 — Signature Scanning: Compares installed applications against a continuously updated database of known spyware signatures, package names, and developer certificates.

Layer 2 — Behavioral Analysis: Monitors for suspicious behaviors common to spyware: excessive permission usage, background data transmission, hidden processes, and unauthorized accessibility service activation.

Layer 3 — Permission Auditing: Analyzes all installed apps' permissions to identify those with surveillance-capable access (camera, microphone, location, contacts, messages) that don't have a legitimate reason for such access.

Layer 4 — System Integrity Check: Verifies that the device hasn't been rooted (Android) or jailbroken (iOS), checks for unauthorized device administrator privileges, and scans for rogue

configuration profiles.

Layer 5 — Network Analysis: Monitors outbound connections for communication with known command-and-control servers associated with spyware families.

What SpyWiper Pro Scans For

- 200+ known stalkerware applications
- Hidden apps not visible in the app drawer
- Device administrator abuse
- Accessibility service exploitation
- Root/jailbreak indicators
- Suspicious configuration profiles
- Unauthorized MDM enrollment
- Rogue certificates
- Background process anomalies
- Unusual network connections

Chapter 4: Getting Started with SpyWiper Pro

Installation

1. Log in to your Customer Dashboard at https://spywiperpro.app/login
2. Navigate to the Downloads section
3. Download the SpyWiper Pro APK (Android) or follow the iOS setup guide
4. Install the application following the on-screen instructions
5. Run your first scan

Running Your First Scan

After installation, SpyWiper Pro will guide you through an initial comprehensive scan. This scan checks all installed applications, system settings, permissions, and device configuration for any signs of surveillance software.

The initial scan typically takes 2-5 minutes depending on the number of installed applications.

Understanding Scan Results

Green (Clear): No spyware or suspicious activity detected. Your device appears clean.

Yellow (Attention): Some items require your review. These may be legitimate apps with surveillance-capable permissions that you should verify.

Red (Threat Detected): Spyware or highly suspicious software has been identified. SpyWiper Pro will provide removal instructions.

Regular Scanning Schedule

We recommend:

- **Weekly:** Run a quick scan to check for new threats
- **After suspicious events:** If you suspect someone had access to your device
- **After relationship changes:** If you've recently separated from a partner
- **Monthly:** Run a full comprehensive scan

Chapter 5: Spyware Detection and Removal

Detection Tools and Resources

The following tools complement SpyWiper Pro for comprehensive device security:

Tool	Platform	Type	Description
SpyWiper Pro	Android/iOS	Commercial	Primary spyware detection and removal
Malwarebytes	Android/iOS	Freemium	General malware and adware detection
Lookout Security	Android/iOS	Freemium	Mobile threat protection
Certo AntiSpy	iOS	Commercial	iPhone spyware detection
Norton Mobile	Android/iOS	Commercial	Comprehensive mobile security
Kaspersky Mobile	Android	Freemium	Stalkerware detection alerts
AVG AntiVirus	Android/iOS	Freemium	Basic malware scanning
Bitdefender Mobile	Android/iOS	Commercial	Advanced threat detection

Manual Detection Steps (Android)

1. **Check Device Administrators:** Settings → Security → Device Administrators. Remove any you don't recognize.
2. **Review Accessibility Services:** Settings → Accessibility. Disable any services you didn't enable.
3. **Check App Permissions:** Settings → Apps → Permissions. Review which apps have camera, microphone, and location access.
4. **Look for Hidden Apps:** Settings → Apps → Show System Apps. Look for unfamiliar entries.
5. **Check Battery Usage:** Settings → Battery. Look for unknown apps consuming significant power.
6. **Review Data Usage:** Settings → Network → Data Usage. Identify apps transmitting unusual amounts of data.

Manual Detection Steps (iPhone)

1. **Check Configuration Profiles:** Settings → General → VPN & Device Management. Remove any profiles you didn't install.

2. **Review Location Services:** Settings → Privacy → Location Services. Check which apps have “Always” access.
3. **Check for Jailbreak:** Look for Cydia, Sileo, or other jailbreak-related apps.
4. **Review Apple ID Sessions:** Settings → [Your Name] → Devices. Remove any you don’t recognize.
5. **Check Screen Time:** Settings → Screen Time. Ensure no one else has set a passcode.
6. **Verify iCloud Access:** Check if anyone else has access to your Apple ID.

Removal Procedures

For Known Stalkerware:

1. Run SpyWiper Pro scan to identify the specific application
2. Follow the guided removal process
3. Revoke device administrator privileges if applicable
4. Uninstall the application
5. Change all passwords from a different device
6. Enable two-factor authentication on all accounts

For Persistent Threats: If spyware persists after removal attempts:

1. Back up essential data (photos, contacts) to a secure location
2. Perform a factory reset
3. Set up the device as new (do not restore from potentially compromised backup)
4. Install SpyWiper Pro immediately after setup
5. Run a verification scan

Chapter 6: Privacy Protection Toolkit

VPN Services

A Virtual Private Network encrypts your internet traffic and hides your IP address, preventing network-based surveillance.

Service	Jurisdiction	Servers	No-Log Policy	Price
NordVPN	Panama	5,500+	Audited	$3.99/mo
ExpressVPN	BVI	3,000+	Audited	$6.67/mo
ProtonVPN	Switzerland	1,700+	Audited	Free tier available
Mullvad VPN	Sweden	800+	Audited	€5/mo
Surfshark	Netherlands	3,200+	Audited	$2.49/mo

Secure Messaging

End-to-end encrypted messaging prevents anyone — including the service provider — from reading your messages.

App	E2EE	Open Source	Metadata Protection	Self-Destruct
Signal	Yes	Yes	Minimal metadata	Yes
WhatsApp	Yes	Partial	Some metadata	Yes
Telegram	Optional	Partial	Limited	Yes
Wickr Me	Yes	Partial	Strong	Yes
Briar	Yes	Yes	Tor-based	No

Privacy Browsers

Browser	Platform	Key Features
Brave	All	Built-in ad/tracker blocking, Tor mode
Firefox Focus	Mobile	Auto-delete history, tracker blocking
DuckDuckGo Browser	Mobile	Privacy-first, tracker blocking
Tor Browser	Desktop/Android	Anonymous browsing via Tor network
Librewolf	Desktop	Hardened Firefox fork

DNS Privacy

Your DNS queries reveal every website you visit. Private DNS services encrypt these queries.

Service	Encryption	Filtering	Free
NextDNS	DoH/DoT	Customizable	Yes (limited)
Quad9	DoH/DoT	Malware blocking	Yes
Cloudflare 1.1.1.1	DoH/DoT	Optional	Yes
AdGuard DNS	DoH/DoT	Ad blocking	Yes (limited)

Chapter 7: Monitoring and Surveillance Detection

GPS Tracking Detection

Software Trackers: SpyWiper Pro scans for apps with continuous location access that shouldn't need it. Check Settings → Location → App Permissions regularly.

Hardware Trackers: Physical Bluetooth trackers can be hidden in bags, cars, or clothing.

Detection App	Detects	Platform
Apple Find My (built-in)	Unknown AirTags	iOS
AirGuard	AirTags, SmartTags, Tile	Android
Tracker Detect	AirTags	Android
BLE Scanner	All BLE devices	Android/iOS

Vehicle Tracking: Check under the car (wheel wells, bumpers, OBD-II port), inside the dashboard, and in the trunk for magnetic GPS devices.

Hidden Camera Detection

Method	How It Works
RF Detector	Scans for wireless camera transmissions
Infrared Scanner	Detects IR LEDs used by night-vision cameras
Lens Finder	Uses light reflection to spot camera lenses
Network Scanner	Identifies cameras connected to local WiFi
Phone Camera	Some phone cameras can detect IR light

Network Monitoring

Monitor your home network for unauthorized devices and suspicious traffic:

Tool	Type	Use Case
Fing	Mobile App	Scan network for unknown devices
GlassWire	Mobile/Desktop	Monitor app network activity
Wireshark	Desktop	Deep packet inspection
Pi-hole	Hardware	Network-wide ad/tracker blocking
Little Snitch	macOS	Outbound connection monitoring

Chapter 8: Android Privacy Hardening Guide

Essential Settings

1. **Disable Unknown Sources:** Settings → Security → Install Unknown Apps → Disable all
2. **Enable Google Play Protect:** Play Store → Profile → Play Protect → Enable scanning
3. **Review App Permissions:** Settings → Privacy → Permission Manager → Audit each category
4. **Disable USB Debugging:** Settings → Developer Options → Disable USB Debugging
5. **Enable Screen Lock:** Use biometric + strong PIN (6+ digits)

6. **Encrypt Device:** Settings → Security → Encryption (usually enabled by default on modern devices)
7. **Disable Bluetooth When Not in Use:** Prevents Bluetooth-based tracking
8. **Use Private DNS:** Settings → Network → Private DNS → Set to dns.google or one.one.one.one

Permission Best Practices

Permission	Should Have Access	Suspicious If
Camera	Camera apps, video calls, QR scanners	Calculators, flashlights, games
Microphone	Voice recorders, calls, video apps	Weather apps, file managers
Location	Maps, ride-sharing, weather	Alarm clocks, note apps
Contacts	Messaging, email, phone	Games, utilities
SMS	Messaging apps, 2FA apps	Any other app type
Storage	File managers, media apps	Simple utility apps
Phone	Dialer, contacts	Games, calculators

Recommended Security Apps for Android

- SpyWiper Pro (spyware detection)
- Shelter (work profile isolation)
- NetGuard (firewall without root)
- Bouncer (temporary permissions)
- TrackerControl (tracker blocking)

Chapter 9: iPhone Privacy Hardening Guide

Essential Settings

1. **Enable Lockdown Mode** (if available): Settings → Privacy & Security → Lockdown Mode
2. **Review Configuration Profiles:** Settings → General → VPN & Device Management

3. **Disable Significant Locations:** Settings → Privacy → Location Services → System Services → Significant Locations → Off
4. **Limit Ad Tracking:** Settings → Privacy → Apple Advertising → Disable Personalized Ads
5. **Review App Tracking:** Settings → Privacy → Tracking → Disable "Allow Apps to Request to Track"
6. **Enable Advanced Data Protection:** Settings → [Your Name] → iCloud → Advanced Data Protection
7. **Use Face ID/Touch ID + Strong Passcode:** Minimum 6-digit numeric or alphanumeric
8. **Enable Find My iPhone:** For remote wipe capability if device is stolen

iCloud Security

- Enable two-factor authentication on Apple ID
- Review devices signed into your Apple ID
- Check shared albums and shared notes for unauthorized access
- Review Family Sharing members
- Check if anyone has access to your Find My location
- Disable iCloud backup if you suspect iCloud credential compromise

App Privacy Report

Settings → Privacy → App Privacy Report shows:

- Which apps accessed sensitive data (location, camera, microphone, contacts)
- Which domains apps contacted
- Which apps accessed your network

Review this weekly to identify suspicious behavior.

Chapter 10: Understanding App Permissions

The Permission Threat Model

Every permission granted to an app is a potential surveillance vector. Spyware requires specific permissions to function:

Spyware Capability	Required Permission(s)
Read messages	SMS, Notifications
Track location	Location (Always)
Record calls	Phone, Microphone
Take photos	Camera
Read contacts	Contacts
Monitor browsing	Accessibility, VPN
Keylogging	Accessibility
Screen capture	Screen Overlay, Media Projection

Permission Audit Checklist

Perform this audit monthly:

- [ ] Review all apps with “Always” location access
- [ ] Check which apps have camera permission
- [ ] Verify microphone access list
- [ ] Review accessibility services
- [ ] Check device administrators (Android)
- [ ] Review notification access
- [ ] Check apps with phone/call access
- [ ] Verify SMS access list
- [ ] Review storage/files access
- [ ] Check background data usage permissions

Chapter 11: Network Security and Monitoring

Home Network Security

Your home WiFi network can be a surveillance vector if compromised:

1. **Change default router password** — Use a strong, unique password
2. **Enable WPA3 encryption** (or WPA2 minimum)
3. **Disable WPS** — WiFi Protected Setup is vulnerable to brute force
4. **Update router firmware** regularly
5. **Use a guest network** for IoT devices
6. **Monitor connected devices** using Fing or router admin panel
7. **Consider a DNS sinkhole** (Pi-hole) to block trackers network-wide

Public WiFi Safety

- Always use a VPN on public WiFi
- Avoid accessing sensitive accounts on public networks
- Disable auto-connect to open networks
- Use cellular data for sensitive transactions
- Forget public networks after use

Detecting Network-Based Surveillance

Signs your network may be monitored:

- Unknown devices on your network
- Router settings changed without your knowledge
- DNS settings modified
- Unusual outbound traffic patterns
- New port forwarding rules you didn’t create

Chapter 12: Advanced Privacy Resources

Open Source Security Tools

Tool	Purpose	Platform
Tails OS	Anonymous operating system	USB bootable
Qubes OS	Security-focused desktop OS	Desktop
GrapheneOS	Hardened Android	Pixel phones
CalyxOS	Privacy-focused Android	Pixel phones
LineageOS	De-Googled Android	Various devices

Security Research Platforms

- VirusTotal (virustotal.com) — Scan files and URLs for malware
- Have I Been Pwned (haveibeenpwned.com) — Check if your email was in a data breach
- Shodan (shodan.io) — Search engine for internet-connected devices
- URLScan (urlscan.io) — Analyze suspicious URLs safely

OSINT (Open Source Intelligence) Awareness

Understanding OSINT helps you protect yourself from information gathering:

- **What stalkers can find:** Public records, social media, data brokers, voter registration, property records
- **How to reduce your footprint:** Opt out of data brokers, make social media private, use a PO Box, register domains privately
- **Data broker opt-out services:** DeleteMe, Privacy Duck, Kanary

---

Chapter 13: Emergency and Crisis Resources

If You Are in Immediate Danger

Call 911 or your local emergency number.

Domestic Violence Resources

Resource	Contact	Services
National DV Hotline	1-800-799-7233	24/7 crisis support
NNEDV Safety Net	techsafety.org	Technology safety planning
Stalking Resource Center	stalkingawareness.org	Stalking-specific resources
Cyber Civil Rights	cybercivilrights.org	Tech-facilitated abuse
WomensLaw	womenslaw.org	Legal information

Digital Safety Planning

If you are in an abusive situation and suspect monitoring:

1. **Use a safe device** — a friend's phone or library computer — to research and plan
2. **Do not remove spyware yet** if doing so could alert your abuser and put you in danger
3. **Contact a DV hotline** for safety planning assistance
4. **Document evidence** from a safe device (screenshots, dates, behaviors)
5. **Create a safety plan** before taking action

SpyWiper Pro Support

- Email: support.prospy@mmwguides.com
- Phone: (305) 600-0858
- Contact Form: https://spywiperpro.app/contact
- Business Hours: Monday – Friday, 9:00 AM – 5:00 PM ET

Chapter 14: Community and Educational Resources

Privacy-Focused Communities

Community	Platform	Focus
r/privacy	Reddit	General privacy discussion
r/PrivacyGuides	Reddit	Tool recommendations
r/degoogle	Reddit	Reducing Google dependence
Privacy Guides	privacyguides.org	Curated tool recommendations
EFF	eff.org	Digital rights advocacy
Access Now	accessnow.org	Digital security helpline

Educational Resources

- **Surveillance Self-Defense (EFF):** ssd.eff.org — Comprehensive guides for protecting yourself online
- **Security in a Box:** securityinabox.org — Digital security tools and tactics
- **Privacy Guides:** privacyguides.org — Recommendations for privacy tools and services
- **The New Oil:** thenewoil.org — Beginner-friendly privacy guides

Podcasts and Blogs

- Darknet Diaries — True stories from the dark side of the internet
- Privacy, Security, & OSINT Show — Michael Bazzell's privacy podcast
- Krebs on Security — Brian Krebs' cybersecurity blog
- The Hacker News — Daily cybersecurity news

Chapter 15: Frequently Asked Questions

Q: Will SpyWiper Pro detect ALL spyware? A: SpyWiper Pro detects 200+ known stalkerware applications and uses behavioral analysis to identify unknown threats. However, no security tool

can guarantee 100% detection of all possible threats, especially zero-day exploits. Regular updates improve detection capabilities.

Q: Can spyware be installed remotely? A: Most commercial stalkerware requires brief physical access to the device. However, some advanced threats can be deployed through phishing links, compromised iCloud credentials, or zero-click exploits. SpyWiper Pro helps detect all of these.

Q: Will the person monitoring me know I installed SpyWiper Pro? A: SpyWiper Pro is designed to be discreet. However, if someone has full access to your device through spyware, they may see app installations. If you're in a dangerous situation, consult with a DV hotline before taking action.

Q: Should I confront my partner about spyware? A: If you are in an abusive relationship, confrontation can be dangerous. Contact the National DV Hotline (1-800-799-7233) for safety planning before taking any action.

Q: How often should I scan my device? A: We recommend weekly quick scans and monthly comprehensive scans. Also scan after any suspicious event or if someone had physical access to your device.

Q: Does SpyWiper Pro work on both Android and iPhone? A: Yes. SpyWiper Pro is available for both platforms, though the detection methods differ due to the different security architectures of each operating system.

Q: What should I do after removing spyware? A: Change ALL passwords from a different device, enable two-factor authentication everywhere, review connected sessions/devices on all accounts, and consider a factory reset for maximum security.

Q: Is my purchase confidential? A: Yes. Your purchase will appear as "MMWGUIDES.COM" on your bank statement. We do not share customer information with any third parties.

Chapter 16: Social Media Privacy Protection

Platform-Specific Privacy Settings

Facebook/Meta:

- Set profile to Friends Only
- Disable face recognition
- Review tagged photos before they appear
- Limit who can look you up by email/phone
- Disable location history

- Review third-party app access quarterly

Instagram:

- Set account to Private
- Disable Activity Status
- Restrict story sharing
- Review Close Friends list
- Disable similar account suggestions
- Turn off login activity notifications to others

Twitter/X:

- Protect your tweets
- Disable location tagging
- Remove phone number from account
- Disable personalization and data settings
- Review connected apps

TikTok:

- Set account to Private
- Disable personalized ads
- Turn off “Suggest your account to others”
- Disable comments from strangers
- Review third-party access

General Social Media Safety

- Never share real-time location
- Disable geotagging on photos
- Use a separate email for social media accounts
- Enable 2FA on all social accounts
- Regularly review followers/friends lists
- Be cautious of new connection requests from unknown people

- Don’t share vacation plans publicly (indicates empty home)

Chapter 17: Digital Forensics for Personal Use

Preserving Evidence

If you discover spyware and need to preserve evidence for legal proceedings:

1. **Do not remove the spyware yet** — document first
2. **Take screenshots** from a second device showing the spyware
3. **Record the app’s package name** and installation date
4. **Note permissions** the app has been granted
5. **Check data usage** to document unauthorized transmissions
6. **Save network logs** if possible
7. **Contact law enforcement** — unauthorized surveillance is illegal in most jurisdictions

Legal Considerations

- Installing spyware on someone’s device without consent is illegal in most US states
- Federal laws (Computer Fraud and Abuse Act, Wiretap Act) may apply
- Evidence of spyware can be used in divorce proceedings, restraining orders, and criminal cases
- Consult with an attorney before taking legal action

Documentation Template

For each piece of evidence, record:

- Date and time of discovery
- Device make, model, and OS version
- Screenshot or photo of the evidence
- What the spyware was doing (permissions, data access)
- How you believe it was installed
- Any witnesses

Chapter 18: Workplace and Corporate Privacy

Understanding Employer Monitoring

Employers have broad rights to monitor company-owned devices. However:

- They must typically disclose monitoring in employee handbooks
- Personal devices (BYOD) have different rules
- Some states require explicit consent for monitoring
- Union contracts may limit surveillance

Protecting Personal Privacy at Work

- Use personal devices for personal communications
- Don't use work WiFi for personal browsing (use cellular + VPN)
- Assume all activity on work devices is monitored
- Keep personal accounts off work devices
- Use a separate browser profile if you must use a work computer for personal tasks

Corporate Spyware vs. Legitimate MDM

Feature	Legitimate MDM	Suspicious Activity
Disclosed to employee	Yes	No
Limited to work apps	Yes	Monitors personal apps
Respects off-hours	Yes	$^{24}/_{7}$ monitoring
Transparent policies	Yes	Hidden or vague
Proportionate access	Yes	Excessive permissions

Chapter 19: Future Threats and Emerging Technologies

AI-Powered Surveillance

Artificial intelligence is making surveillance more powerful and harder to detect:

- AI-generated deepfakes for social engineering
- Automated behavioral analysis from device sensors
- Natural language processing of captured communications
- Predictive location tracking based on patterns

IoT and Smart Home Surveillance

Smart home devices can be surveillance vectors:

- Smart speakers (always listening)
- Smart cameras (can be accessed remotely)
- Smart TVs (some have cameras and microphones)
- Smart locks (track entry/exit patterns)
- Robot vacuums (map your home layout)

Protecting Against Future Threats

- Keep all devices and software updated
- Follow security researchers and news
- Regularly audit connected devices
- Use hardware kill switches when available
- Consider privacy-focused alternatives to smart home devices
- Stay informed through the SpyWiper Pro Intelligence Hub

Chapter 20: Building Your Personal Security Plan

Risk Assessment

Rate your risk level in each category:

Category	Low	Medium	High
Abusive relationship history	No history	Past relationship	Current situation
Public profile	Private person	Some online presence	Public figure
Valuable data	Minimal	Some financial/personal	High-value targets
Device sharing	Never shared	Occasionally	Regularly shared
Technical sophistication of threat	None	Basic	Advanced

Your Security Action Plan

Immediate (Today):

- [ ] Run SpyWiper Pro scan
- [ ] Change passwords on critical accounts
- [ ] Enable 2FA on email and banking
- [ ] Review app permissions

This Week:

- [ ] Install a VPN
- [ ] Switch to a private DNS
- [ ] Review social media privacy settings
- [ ] Set up a password manager
- [ ] Check for unknown Bluetooth devices

This Month:

- [ ] Complete Android/iPhone hardening guide
- [ ] Opt out of major data brokers
- [ ] Set up encrypted messaging (Signal)

- [ ] Review home network security
- [ ] Create secure backups

Ongoing:

- [ ] Weekly SpyWiper Pro scans
- [ ] Monthly permission audits
- [ ] Quarterly social media review
- [ ] Stay updated via Intelligence Hub

Appendix A: Complete Tool Directory

Spyware Detection Tools

Tool	Platform	Price	Key Feature
SpyWiper Pro	Android/iOS	$29.99	Purpose-built stalkerware detection
Malwarebytes	Android/iOS	Free/Premium	General malware detection
Lookout	Android/iOS	Free/Premium	Mobile threat protection
Certo AntiSpy	iOS	$49.99/yr	iPhone-specific detection
Norton Mobile	Android/iOS	$29.99/yr	Comprehensive security
Kaspersky	Android	Free/Premium	Stalkerware alerts
Bitdefender	Android/iOS	$14.99/yr	Advanced scanning

VPN Services

Service	Price	Servers	Jurisdiction
NordVPN	$3.99/mo	5,500+	Panama
ExpressVPN	$6.67/mo	3,000+	BVI
ProtonVPN	Free-$9.99/mo	1,700+	Switzerland
Mullvad	€5/mo	800+	Sweden
Surfshark	$2.49/mo	3,200+	Netherlands
IVPN	$6/mo	80+	Gibraltar

Secure Communication

Tool	Type	E2EE	Open Source
Signal	Messaging	Yes	Yes
ProtonMail	Email	Yes	Yes
Tutanota	Email	Yes	Yes
Briar	Messaging	Yes	Yes
Session	Messaging	Yes	Yes
Wire	Messaging	Yes	Yes

Privacy Browsers

Browser	Platform	Key Feature
Brave	All	Built-in blocking
Firefox Focus	Mobile	Auto-delete
DuckDuckGo	Mobile	Privacy-first
Tor Browser	Desktop/Android	Anonymity
Librewolf	Desktop	Hardened Firefox
Vanadium	GrapheneOS	Hardened Chromium

Appendix B: Privacy Hardening Checklists

Android Hardening Checklist

- [ ] Set strong screen lock (6+ digit PIN or biometric)
- [ ] Disable USB debugging
- [ ] Disable Install from Unknown Sources
- [ ] Enable Google Play Protect
- [ ] Review all app permissions
- [ ] Remove unused apps
- [ ] Disable Bluetooth when not in use
- [ ] Use Private DNS
- [ ] Enable automatic updates
- [ ] Review device administrators
- [ ] Check accessibility services
- [ ] Disable NFC when not in use
- [ ] Review notification access
- [ ] Enable Find My Device
- [ ] Set up SIM lock PIN

- [ ] Disable Smart Lock
- [ ] Review connected devices
- [ ] Check background app refresh settings

iPhone Hardening Checklist

- [ ] Set strong passcode (6+ digit or alphanumeric)
- [ ] Enable Face ID/Touch ID
- [ ] Review configuration profiles
- [ ] Enable Advanced Data Protection for iCloud
- [ ] Disable Significant Locations
- [ ] Review Location Services for each app
- [ ] Enable Lockdown Mode (if high-risk)
- [ ] Disable personalized ads
- [ ] Review App Privacy Report
- [ ] Check for unknown devices on Apple ID
- [ ] Enable two-factor authentication
- [ ] Review Family Sharing settings
- [ ] Disable AirDrop for everyone
- [ ] Review Siri permissions
- [ ] Check Screen Time settings
- [ ] Enable automatic updates
- [ ] Review notification previews (show when unlocked only)
- [ ] Disable USB accessories when locked

Appendix C: Legal Considerations

United States Federal Law

Computer Fraud and Abuse Act (CFAA): Unauthorized access to a computer system is a federal crime. Installing spyware without consent may violate this law.

Wiretap Act (18 U.S.C. § 2511): Intercepting electronic communications without consent is illegal. Spyware that captures messages, calls, or emails may violate this law.

Stored Communications Act: Unauthorized access to stored electronic communications (emails, messages) is prohibited.

State Laws

Most states have their own laws regarding:

- Unauthorized computer access
- Wiretapping and eavesdropping
- Stalking and cyberstalking
- Invasion of privacy
- Domestic violence and protective orders

What to Do If You're a Victim

1. Document the spyware (screenshots, dates, evidence)
2. File a police report
3. Consult with an attorney
4. Consider a restraining order
5. Contact the National DV Hotline if in an abusive situation
6. Report the spyware app to Google Play / Apple App Store

Disclaimer

This guide provides general information and is not legal advice. Laws vary by jurisdiction. Consult with a qualified attorney for legal guidance specific to your situation.

Appendix D: Glossary of Privacy and Security Terms

ADB (Android Debug Bridge): A command-line tool for communicating with Android devices. Can be exploited to install spyware if USB debugging is enabled.

AirTag: Apple's Bluetooth tracker. Can be misused for stalking; detection apps like AirGuard help identify unknown trackers.

APK (Android Package Kit): Android app installation file. Spyware is often distributed as sideloaded APKs.

Backdoor: A hidden method of bypassing authentication. Spyware may install backdoors for persistent access.

BLE (Bluetooth Low Energy): Wireless technology used by tracking devices. BLE scanning apps detect nearby trackers.

Brute Force Attack: Cracking passwords by trying every combination. Strong passwords and lockout policies protect against this.

C2 Server (Command and Control): Remote server that controls malware/spyware. Network monitoring can detect C2 communications.

Configuration Profile (iOS): Files that configure iPhone settings. Malicious profiles can grant extensive device access.

Data Broker: Companies that collect and sell personal information. Opt-out services help reduce your digital footprint.

Device Administrator (Android): Elevated app permission that can prevent uninstallation. Stalkerware frequently abuses this.

DNS (Domain Name System): Translates website names to IP addresses. Private DNS prevents DNS-based surveillance.

E2EE (End-to-End Encryption): Only sender and recipient can read messages. Signal, WhatsApp use E2EE.

EXIF Data: Photo metadata including GPS coordinates. Strip EXIF before sharing photos.

Exploit: Code that takes advantage of software vulnerabilities for unauthorized access.

Geofencing: Virtual geographic boundaries that trigger alerts. Can be misused for monitoring movements.

IMEI: Unique device identifier. Can be used to track devices through cellular networks.

Jailbreak/Root: Removing device restrictions. Enables customization but removes security protections.

Keylogger: Records all keystrokes, capturing passwords and messages.

MDM (Mobile Device Management): Legitimate corporate tool that can be abused for surveillance.

Metadata: Data about data. Communication metadata reveals who, when, where — even if content is encrypted.

OSINT (Open Source Intelligence): Information from public sources. Stalkers use OSINT to gather victim information.

Pegasus: Advanced government-grade spyware by NSO Group. Uses zero-click exploits.

Phishing: Social engineering attack impersonating trusted entities to steal information.

RAT (Remote Access Trojan): Malware providing complete remote device control.

Sandbox: Isolated environment limiting app access. Spyware may exploit vulnerabilities to escape sandboxing.

Sideloading: Installing apps from outside official stores. Stalkerware is typically sideloaded.

Stalkerware: Commercial surveillance software designed to be hidden. Provides comprehensive monitoring.

TLS (Transport Layer Security): Encrypts data in transit. The padlock icon indicates TLS protection.

2FA (Two-Factor Authentication): Requires two verification forms. Prevents unauthorized access even with compromised passwords.

VPN (Virtual Private Network): Encrypts internet traffic and hides IP address.

Zero-Click Exploit: Attack requiring no victim interaction. Most dangerous and difficult to defend against.

Zero-Day Vulnerability: Unknown vulnerability with no available patch.

Appendix E: Quick Reference Cards

If You Suspect Spyware — Quick Action Guide

1. **Stay calm** — do not alert the potential monitor
2. **Use a different device** to research and plan
3. **Run SpyWiper Pro scan** on the suspected device
4. **Check for:** unknown apps, device administrators, accessibility services, configuration profiles
5. **Document everything** with screenshots from a second device
6. **Contact support** if you need help: support.prospy@mmwguides.com
7. **If in danger:** Call National DV Hotline 1-800-799-7233

Emergency Contacts

Resource	Contact
SpyWiper Pro Support	support.prospy@mmwguides.com
SpyWiper Pro Phone	(305) 600-0858
SpyWiper Pro Contact Form	spywiperpro.app/contact
National DV Hotline	1-800-799-7233
NNEDV Safety Net	techsafety.org
Stalking Resource Center	stalkingawareness.org
Access Now Helpline	accessnow.org/help
Cyber Civil Rights	cybercivilrights.org

Weekly Security Routine (5 Minutes)

Day	Action
Monday	Run SpyWiper Pro scan
Wednesday	Check app permissions for changes
Friday	Review battery and data usage
Weekend	Update OS and apps

Chapter 21: Advanced Android Security Techniques

Using Work Profiles for App Isolation

Android's Work Profile feature (available through apps like Shelter or Island) creates an isolated environment where apps cannot access data from your personal profile. This is invaluable for:

- Isolating social media apps that request excessive permissions
- Running apps you don't fully trust in a sandboxed environment

- Keeping work apps separate from personal data
- Testing suspicious apps without risking your main profile

Setting Up Shelter:

1. Install Shelter from F-Droid or Google Play
2. Follow the setup wizard to create a work profile
3. Clone apps into the work profile that you want isolated
4. Apps in the work profile cannot access personal contacts, files, or other apps

ADB Security

Android Debug Bridge (ADB) is a powerful tool that can be exploited:

- **Disable USB Debugging** when not actively developing
- **Revoke USB Debugging Authorizations** periodically: Settings → Developer Options → Revoke USB debugging authorizations
- **Disable Wireless Debugging** — this allows ADB over WiFi without a USB connection
- **Check for ADB over Network:** If enabled, anyone on your network can control your device

App Verification and Integrity

Before installing any app, verify its legitimacy:

Check	How	Red Flag
Developer name	Play Store listing	Generic or misspelled
Install count	Play Store listing	Very low for a “popular” app
Permissions	Before install	Excessive for app’s purpose
Reviews	Play Store	Fake-sounding or all 5-star
Last updated	Play Store listing	Not updated in years
Privacy policy	Developer website	Missing or generic

Firewall Configuration Without Root

NetGuard and similar apps provide firewall functionality without requiring root access:

- Block internet access for apps that shouldn't need it
- Monitor which apps are connecting to the internet
- Block background data for specific apps
- Create per-app rules for WiFi vs. cellular
- Log connection attempts for forensic purposes

Secure Boot and Verified Boot

Modern Android devices use Verified Boot to ensure system integrity:

- **What it does:** Verifies the boot chain hasn't been tampered with
- **Why it matters:** Prevents persistent rootkits that survive factory resets
- **How to check:** Settings → About Phone → look for "Verified Boot State: Green"
- **Warning signs:** Orange or red verified boot state indicates system modification

---

Chapter 22: Advanced iPhone Security Techniques

Lockdown Mode Deep Dive

Apple's Lockdown Mode provides extreme protection for high-risk individuals:

What it disables:

- Most message attachment types (except images)
- Link previews in Messages
- Incoming FaceTime calls from unknown contacts
- Shared albums in Photos
- Complex web technologies (JIT JavaScript compilation)
- Wired connections to computers when locked
- Configuration profile installation

Who should use it:

- Journalists covering sensitive topics
- Activists and human rights workers
- Domestic violence survivors with tech-savvy abusers

- Anyone who suspects state-level surveillance

Limitations:

- Some websites may not function properly
- Reduced functionality in Messages
- Cannot receive FaceTime from new contacts
- Some apps may behave differently

iCloud Security Audit

Perform this audit monthly:

1. **Settings → [Your Name] → Devices:** Remove any device you don't recognize
2. **Settings → [Your Name] → Password & Security → Apps Using Apple ID:** Review and revoke access
3. **Settings → [Your Name] → iCloud:** Review which apps sync to iCloud
4. **Settings → [Your Name] → Family Sharing:** Verify all members are legitimate
5. **Settings → [Your Name] → Find My:** Check who can see your location
6. **appleid.apple.com:** Log in and review account security, trusted devices, and recovery contacts

Safari Privacy Configuration

Setting	Location	Recommended
Prevent Cross-Site Tracking	Safari Settings	ON
Block All Cookies	Safari Settings	Consider ON
Fraudulent Website Warning	Safari Settings	ON
Privacy Preserving Ad Measurement	Safari Settings	OFF
Check for Apple Pay	Safari Settings	OFF if not used
Hide IP Address	Safari Settings	From Trackers (or All)

Shortcuts Automation Security

iOS Shortcuts can be exploited for surveillance:

- Review all automations: Shortcuts app → Automation tab
- Delete any automations you didn't create
- Be cautious of shared shortcuts from unknown sources
- Disable "Allow Running Without Asking" on sensitive automations

---

Chapter 23: Email Security and Phishing Protection

Email-Based Surveillance Vectors

Email is a primary attack vector for installing spyware:

Phishing Emails: Disguised as legitimate communications to trick you into:

- Clicking malicious links that install spyware
- Downloading infected attachments
- Entering credentials on fake login pages
- Granting OAuth access to malicious apps

Email Tracking: Invisible tracking pixels in emails reveal:

- When you opened the email
- Your IP address (approximate location)
- Your device type and email client
- How many times you opened it

Protecting Against Email Threats

Protection	Tool/Method	Purpose
Disable remote images	Email client settings	Blocks tracking pixels
Use email aliases	SimpleLogin, AnonAddy	Prevents email correlation
Encrypted email	ProtonMail, Tutanota	Prevents content interception
Phishing detection	Built-in filters + awareness	Prevents credential theft
2FA on email	TOTP or hardware key	Prevents account takeover

Recognizing Phishing Attempts

Red Flags:

- Urgent language (“Your account will be closed!”)
- Sender address doesn’t match the organization
- Generic greeting (“Dear Customer” instead of your name)
- Suspicious links (hover to check before clicking)
- Requests for passwords or personal information
- Unexpected attachments
- Poor grammar or formatting (though AI is making phishing more convincing)

Email Account Security Checklist

- Enable 2FA (preferably hardware key or TOTP, not SMS)
- Review connected apps and revoke unnecessary access
- Check forwarding rules (attackers add forwarding to intercept emails)
- Review recovery email and phone number
- Check recent login activity
- Use a strong, unique password
- Consider a dedicated email for sensitive accounts

Chapter 24: Password Security and Authentication

Password Manager Comparison

Manager	Platform	Open Source	Price	Key Feature
Bitwarden	All	Yes	Free/$10yr	Self-hostable
1Password	All	No	$2.99/mo	Travel mode
KeePassXC	Desktop	Yes	Free	Fully offline
ProtonPass	All	Yes	Free/$3.99/mo	Integrated with ProtonMail
Dashlane	All	No	$4.99/mo	Dark web monitoring

Two-Factor Authentication Methods

Method	Security Level	Convenience	Phishing Resistant
SMS codes	Low	High	No
TOTP apps (Authy, Google Auth)	Medium	Medium	No
Push notifications	Medium	High	Partially
Hardware keys (YubiKey)	Very High	Medium	Yes
Passkeys	Very High	High	Yes

Password Best Practices

- Use a unique password for every account (password manager handles this)
- Minimum 16 characters for important accounts
- Use passphrases for passwords you must remember: “correct-horse-battery-staple”
- Never reuse passwords across sites
- Change passwords immediately if a breach is reported
- Enable 2FA on every account that supports it
- Use a hardware security key for critical accounts (email, banking)

Account Recovery Security

Account recovery is often the weakest link:

- Use a strong, unique security question answer (or random string stored in password manager)
- Set recovery email to a secure, separate email account
- Don't use SMS recovery if possible (SIM swap attacks)
- Store recovery codes in your password manager
- Consider a recovery contact you trust (Apple, Google support this)

Chapter 25: Physical Security and Device Protection

Device Physical Security

Threat	Protection
Shoulder surfing	Privacy screen protector
Unattended device access	Always lock when leaving
USB attacks (juice jacking)	Use a data blocker or power-only cable
SIM swap	Set SIM PIN, use eSIM if possible
Theft	Enable Find My, set remote wipe
Forensic extraction	Use strong encryption + long passcode

Travel Security

When traveling, especially internationally:

1. **Before departure:**
    - Back up device to secure location
    - Remove sensitive apps and data
    - Enable travel mode (1Password) or log out of sensitive accounts
    - Consider a travel-only device

2. **During travel:**
    - Use VPN on all connections
    - Disable Bluetooth and WiFi when not needed
    - Don’t charge at public USB ports
    - Keep device in sight at all times
    - Be aware of surveillance cameras
3. **At borders:**
    - Know your rights (varies by country)
    - In the US, you can be asked to unlock devices at borders
    - Consider having a minimal device for border crossings
    - Power off device before approaching border control

Secure Device Disposal

Before selling, donating, or recycling a device:

1. Back up anything you need
2. Remove all accounts (Google, Apple, Samsung, etc.)
3. Disable Find My Device / Find My iPhone
4. Remove SIM and SD cards
5. Perform a factory reset
6. For maximum security: encrypt the device, then factory reset (overwrites encrypted data)
7. Verify the device boots to setup screen

Chapter 26: Children's Privacy and Parental Guidance

Age-Appropriate Privacy Education

Age Group	Key Lessons
5-8	Don't share personal info online, tell a trusted adult if something feels wrong
9-12	Password safety, recognizing phishing, social media awareness
13-15	Digital footprint, privacy settings, sexting dangers, online predators
16-18	Data broker awareness, secure communications, preparing for independence

Legitimate vs. Abusive Monitoring

Legitimate parental monitoring:

- Age-appropriate for the child
- Transparent (child knows about it)
- Decreases as child matures
- Focused on safety, not control
- Discussed openly as a family

Abusive monitoring (even of children):

- Used to control rather than protect
- Hidden from the child
- Doesn't decrease with age/maturity
- Used to punish rather than guide
- Violates reasonable privacy expectations

Recommended Parental Control Approaches

Age	Approach	Tools
Under 8	Full supervision, shared device	Built-in Screen Time/Family Link
8-12	Supervised with increasing freedom	Content filters, time limits
13-15	Trust with verification	Occasional check-ins, open dialogue
16+	Privacy with safety net	Emergency location sharing only

Chapter 27: Data Broker Opt-Out Guide

What Data Brokers Know About You

Data brokers compile extensive profiles including:

- Full name, aliases, maiden names
- Current and past addresses
- Phone numbers (current and historical)
- Email addresses
- Family members and associates
- Employment history
- Property ownership records
- Court records and criminal history
- Social media profiles
- Estimated income and net worth

Major Data Brokers and Opt-Out Links

Broker	Type	Opt-Out Difficulty
Spokeo	People search	Medium
WhitePages	People search	Easy
BeenVerified	Background check	Medium
Intelius	People search	Medium
MyLife	Reputation	Hard
Radaris	People search	Medium
TruePeopleSearch	People search	Easy
FastPeopleSearch	People search	Easy
Acxiom	Marketing data	Medium
LexisNexis	Background check	Hard

Automated Opt-Out Services

If manually opting out of dozens of brokers is overwhelming:

Service	Price	Brokers Covered	Frequency
DeleteMe	$129/yr	40+	Quarterly
Privacy Duck	$500/yr	90+	Continuous
Kanary	$89/yr	100+	Monthly
Optery	$39–249/yr	100+	Monthly

Chapter 28: Incident Response Playbook

If You Discover Active Spyware

Step 1: Assess the Situation (5 minutes)

- Are you in immediate physical danger?
- Who likely installed the spyware?
- How long might it have been active?
- What information has been compromised?

Step 2: Secure Yourself First

- If in danger: Call 911 or leave the situation
- If not in immediate danger: Proceed with documentation

Step 3: Document (15 minutes)

- Screenshot the spyware from a second device
- Note the app name, package name, and permissions
- Record the date/time of discovery
- Save any evidence of who installed it

Step 4: Secure Communications

- Switch to a known-clean device for sensitive communications
- Do not discuss your discovery on the compromised device
- Contact trusted support from the clean device

Step 5: Decide on Action

- Remove immediately (if safe to do so)
- Leave in place and seek legal/safety advice first (if in dangerous situation)
- Contact law enforcement if appropriate

Step 6: Remediation

- Remove the spyware (or factory reset)
- Change ALL passwords from a clean device
- Enable 2FA everywhere
- Review all account sessions and revoke unknown devices
- Monitor accounts for unauthorized access
- Consider credit freeze if financial data was exposed

Step 7: Prevention

- Install SpyWiper Pro for ongoing protection
- Implement the security hardening guides in this document
- Set up regular scanning schedule
- Review the Personal Security Plan chapter

After a Data Breach

If your information was exposed in a data breach:

1. **Determine what was exposed:** Check the breach notification or haveibeenpwned.com
2. **Change passwords:** For the breached service AND any service where you reused that password
3. **Enable 2FA:** On the breached account and all critical accounts
4. **Monitor financial accounts:** Watch for unauthorized transactions
5. **Consider credit freeze:** Contact all three bureaus (Equifax, Experian, TransUnion)
6. **Watch for phishing:** Breached data is often used for targeted phishing

---

Final Notes

Staying Updated

The threat landscape evolves constantly. Stay informed through:

- **SpyWiper Pro Intelligence Hub** — Updated regularly with new tools and resources
- **SpyWiper Pro Application Updates** — New spyware signatures added continuously
- **This Resource Guide** — Updated editions released periodically

Getting Help

If you need assistance at any point:

- **SpyWiper Pro Support:** support.prospy@mmwguides.com
- **Phone:** (305) 600-0858
- **Contact Form:** https://spywiperpro.app/contact
- **Business Hours:** Monday – Friday, 9:00 AM – 5:00 PM ET

Thank You

Thank you for choosing SpyWiper Pro. Your privacy and safety are our top priorities. We are committed to providing you with the tools, knowledge, and support you need to protect yourself from digital surveillance.

Stay safe. Stay private. Stay protected.

— The SpyWiper Pro Team
Moni Media West LLC

SpyWiper Pro — The Complete Resource Guide
Version 1.0 | 2026 Edition

Appendix F: Complete Privacy Audit Worksheet

Device Security Audit

Use this worksheet to perform a comprehensive security audit of your device. Complete each section and mark items as you verify them.

Android Device Audit

Item	Status	Notes
Screen lock enabled (PIN/Biometric)	☐	
Lock timeout set to 30 seconds or less	☐	
USB debugging disabled	☐	
Unknown sources disabled	☐	
Device encryption enabled	☐	
Find My Device enabled	☐	
Google Play Protect enabled	☐	
No unknown device administrators	☐	
No suspicious accessibility services	☐	
App permissions reviewed	☐	
Battery usage checked for anomalies	☐	
Data usage checked for anomalies	☐	
All apps up to date	☐	
OS up to date	☐	
No unknown apps installed	☐	
SIM PIN enabled	☐	
Bluetooth off when not in use	☐	
WiFi auto-connect disabled	☐	
Location sharing reviewed	☐	
Google account security reviewed	☐	

iPhone Device Audit

Item	Status	Notes
Passcode enabled (6+ digits)	☐	
Face ID / Touch ID configured	☐	
Auto-lock set to 30 seconds	☐	
Find My iPhone enabled	☐	
No unknown configuration profiles	☐	
No signs of jailbreak	☐	
Screen Time not set by someone else	☐	
iCloud devices reviewed	☐	
Location services reviewed	☐	
App permissions reviewed	☐	
Safari privacy settings configured	☐	
Mail privacy protection enabled	☐	
Significant locations cleared	☐	
Shared albums reviewed	☐	
AirDrop set to Contacts Only	☐	
Bluetooth off when not in use	☐	
All apps up to date	☐	
iOS up to date	☐	
Apple ID recovery contacts verified	☐	
Two-factor authentication enabled	☐	

Account Security Audit

Account	2FA Enabled	Password Unique	Recovery Info Verified	Last Activity Checked
Primary Email	☐	☐	☐	☐
Secondary Email	☐	☐	☐	☐
Apple ID	☐	☐	☐	☐
Google Account	☐	☐	☐	☐
Banking	☐	☐	☐	☐
Social Media 1	☐	☐	☐	☐
Social Media 2	☐	☐	☐	☐
Cloud Storage	☐	☐	☐	☐
Password Manager	☐	☐	☐	☐
Phone Carrier	☐	☐	☐	☐

Network Security Audit

Item	Status	Notes
Home WiFi password strong and unique	☐	
Router firmware up to date	☐	
WPA3 or WPA2 encryption enabled	☐	
Default router admin password changed	☐	
Guest network enabled for visitors	☐	
UPnP disabled on router	☐	
Remote management disabled	☐	
DNS set to privacy-respecting provider	☐	
VPN configured for public WiFi use	☐	
Connected devices list reviewed	☐	

Appendix G: Emergency Quick Reference Card

I Think My Phone Has Spyware — What Do I Do Right Now?

IMMEDIATE STEPS (Do these first):

1. **DO NOT** alert the person who may have installed it
2. **DO NOT** discuss your suspicion on the compromised device
3. **Use a different device** (friend's phone, library computer) for sensitive communications
4. **Run SpyWiper Pro** scan to confirm
5. **Document** what you find (screenshot from another device)

IF YOU ARE IN DANGER:

- National Domestic Violence Hotline: 1-800-799-7233
- Text "START" to 88788

- Chat: thehotline.org

NEXT STEPS:

- Change all passwords from a CLEAN device
- Enable 2FA on all accounts
- Contact SpyWiper Pro support for guided removal
- Consider contacting law enforcement
- Consult with a domestic violence advocate if applicable

Emergency Contacts

Resource	Contact
Emergency Services	911
National DV Hotline	1-800-799-7233
Stalking Resource Center	1-855-484-2846
Cyber Civil Rights Initiative	1-844-878-2274
Identity Theft (FTC)	1-877-438-4338
SpyWiper Pro Support	support.prospy@mmwguides.com
SpyWiper Pro Phone	(305) 600-0858

Quick Spyware Indicators

Your phone might be compromised if:

- Battery drains unusually fast
- Phone is hot when you’re not using it
- Data usage spikes unexpectedly
- You hear clicking or static during calls
- Apps appear that you didn’t install
- Settings change without your action
- Phone takes a long time to shut down

- Someone knows things they shouldn't know

Password Reset Priority Order

If you suspect compromise, change passwords in this order:

1. **Email** (most critical — controls password resets for everything else)
2. **Phone carrier** (prevents SIM swap)
3. **Banking and financial**
4. **Apple ID / Google Account**
5. **Social media**
6. **Cloud storage**
7. **All remaining accounts**

Remember: Change passwords from a CLEAN device only. Never change passwords on a device you suspect is compromised.

SpyWiper Pro — The Complete Resource Guide
Version 1.0 | 2026 Edition

For support: support.prospy@mmwguides.com | (305) 600-0858
Contact Form: https://spywiperpro.app/contact
Intelligence Hub: https://spywiperpro.app/hub
Customer Dashboard: https://spywiperpro.app/dashboard