Protecting Against Spyware

ACTIVIST CHECKLIST

Last updated on **October 15, 2026** Takes about **30 minutes**

This copy was made on November 14, 2026. We update our guides often as threats change and as better ways to protect yourself become available. For the latest version, visit **activistchecklist.org/spyware/**

Spyware is software that infects your device to spy on you and steal your data without your knowledge or consent. Phones are most often targeted because they record detailed location data, multi-factor authentication (2FA) codes, and a great deal of other personal information, but laptops and other devices can be targeted as well.

Spyware can extract your private messages (even on encrypted messenger apps like Signal), access your 2FA codes, monitor your conversations, track your location in real time, and even turn on your camera or microphone without your awareness. All this data gets sent back to whoever controls the spyware. It's like they are looking over your shoulder as you use your phone.

Spyware is made and sold by private companies to governments. It gets used not just against criminals but also against activists, journalists, and lawyers. Most recently, ICE has purchased access to spyware tools[1].

The two most well-known mobile spyware programs are Pegasus (from NSO Group) and Graphite (from Paragon Solutions). Both companies were founded by executives who used to work for Unit 8200, Israel's equivalent of the NSA in the US. But newer[2] spyware[3] is being discovered all the time, and spyware is one corner of the larger world of "malware" and "stalkerware," which are also used by oppressive governments and by abusive intimate partners to silence people. Spyware can even be delivered through ordinary online ads[4], with no click needed.

How likely am I to be the target of spyware?

While governments claim to use spyware only against criminals, there are many documented cases of it being deployed against political activists, journalists, and lawyers by governments:

- High-profile organizers and activists (In Catalonia[5])
- Human rights lawyers (In Mexico[6])
- Investigative journalists (See Forbidden Stories[7] and Amnesty International[8])
- We have also seen cases where families of targets have had devices infected with spyware. (See Citizen Lab[9])

Spyware like Pegasus and Graphite costs governments **tens or hundreds of thousands** of dollars to deploy. **Therefore, the vast majority of activists will NOT be targeted with spyware and would benefit more from protecting against other threats[10].**

We suggest folks start with our Security Essentials Checklist[10] and then come back to this guide. That guide will help you protect against cheaper-to-deploy surveillance technologies like location tracking or phone-cracking software police can use after they seize your device.

As repressive politicians continue to push the US towards authoritarianism, we should expect sophisticated spyware to be used more broadly against activists.

The good news: the steps you need to take to help protect yourself from spyware and stalkerware will also help you protect against other kinds of attacks that are more likely to affect you, so they are good to complete regardless.

Don't panic: It's easy to read about these advanced hacking tools and get very concerned. Most activists will not be targeted with spyware. The authoritarians want us to believe that they are all powerful and can see everything we do. With a few simple steps we can make it very costly, and politically risky, for them to surveil us.

Baseline protections

EVERYONE This section is for anyone doing activism or advocacy work.

Complete our Digital Security Essentials checklist

This guide covers other important doxxing protection steps like passwords, app location permissions, and software updates.

If you're concerned about doxxing, it's a good idea to complete the steps outlined in our Digital Security Essentials checklist → [10]

Many of these will protect you against someone trying to access your accounts or devices if you're the target of doxxing.

These items from the Essentials checklist are especially important:

- **Turn off location tracking** for most apps
- **Install the latest software updates** for your laptop, phone, and apps
- Use a **password manager**
- **Change your existing passwords** if they are weak or reused across multiple sites.
- Enable **two-factor authentication** on your important accounts
- Don't click on **suspicious links**

Keep your phone (and laptop) updated to the latest operating system version

Protects you from hackers, spyware, and the phone hacking tools the cops use.

DO: Install updates as soon as you're prompted

DO NOT: Keep pushing the "update later" button

Every time a new operating system update comes out, it is fixing security holes. Each update you haven't installed represents a longer list of ways the cops can hack into your device. Think of it as a big building with more and more doors left unlocked.

If your operating system is not up-to-date, many of the other recommendations in this guide will not protect your data.

Start with your phone. If you're doing something higher risk, make sure to update all your devices.

HOW TO RUN UPDATES

Because security updates are so important, **we designed a tool to walk you through the process**.

Check your phone and computer updates →

HOW TO RUN UPDATES MANUALLY

If you prefer to run updates manually, here is how to do it for each device:

Click to show the manual steps

iPhone

1. **Verify your device is still supported:** Check if your iPhone is still supported[11]
2. **Operating System:** Settings → **General** → **Software Update**
3. **Apps** are set to update automatically by default. To check, go to **Settings** → **Apps** → **App Store** and make sure **App Updates** is on.

Mac

1. **Verify your device is still supported:** Check if your Mac is still supported[11]
2. **Operating System:** Apple menu → **System Settings** → **General** → **Software Update**
3. **Apps installed via the Mac App Store:** These apps are set to update automatically by default. To check, open the **App Store**, go to **App Store** → **Settings**, and make sure **Automatic Updates** is on.
4. **Other apps:** Check for updates by going to top menu bar → Click on the app name → Click either **Check for updates** or **About [APP NAME]**, or look inside **Settings...**. If you don't see an option to update, it may be set to automatically update in the background.

Android

1. **Verify your device is still supported:** Check if your Android is still supported[11]
2. **Operating System:** Settings → **System** → **System Update** (may vary by manufacturer)
3. **Apps** from the Google Play Store are set to update automatically by default. To check, open the **Play Store**, tap your profile icon, then go to **Settings** → **Network preferences** → **Auto-update apps**.

Windows

1. **Update your system:** Start → **Settings** → **Update & Security** → **Windows Update**
2. **Verify your device is still supported:** Check if your Windows machine is still supported[11]
3. **Microsoft Store apps:** Make sure you enable automatic updates[12] (on by default).
4. **Other apps:** Look for updates in menu bar → **Help** → **Check for Updates**, or search for **Updates** or **About** in the app's settings.

☐ Enable Lockdown Mode (iPhone) or Advanced Protection (Google & Android)

Spyware is an advanced type of attack, exploiting sophisticated vulnerabilities on our devices. In response, Apple and Google have introduced an advanced security mode that offers enhanced protection against spyware.

On iPhones, it's called **Lockdown Mode**[13] and on Android, it's called **Advanced Protection Program**[14]. (You can also enable Advanced Protection Program on just your Google Account even if you don't have an Android phone.)

We have **no reports** of anyone getting infected with spyware who had Apple's Lockdown Mode enabled. Android's Advanced Protection is more recent and its effectiveness has yet to be tested.

> **Usability trade-offs:** Both features come with some functionality sacrifices. See the full list of trade-offs[15]. If you encounter issues that don't work for your needs, you can always disable the feature later.

HOW TO ENABLE LOCKDOWN MODE FOR IPHONES

IPHONE

Settings → **Privacy & Security** → **Lockdown Mode** → **Enable**

This feature is available for iOS version 16 and above.

HOW TO ENABLE ADVANCED PROTECTION ON ANDROID

ANDROID

Settings → **Security & Privacy** → under **Other Settings** tap **Advanced Protection**

Note: The location of this setting may vary between Android devices, so we recommend searching for 'Advanced Protection' in the Settings search bar.

This feature is available for Android 16 and above.

Block ads on your phone and computer

Spyware has been delivered through ordinary online ads, with no click needed.

Citizen Lab found[4] spyware being delivered through targeted ads shown inside everyday apps and websites. Just loading the ad was enough to infect a device, even if you never saw it or clicked on it.

Blocking ads closes off this path. It also makes it harder for cops and data brokers to track your location through ad networks[16].

HOW TO BLOCK ADS

- [ ] **Install a trusted VPN with ad-blocking[16] on your phone and keep it on.** This is the most important step because it blocks ads inside your apps, not just in your browser. In IVPN, turn on **AntiTracker**. In Proton VPN, turn on **NetShield** (paid plans only). See how to set up a VPN[16].
- [ ] **Install the same VPN on your computer** and turn on ad-blocking there too.
- [ ] **Use a privacy-focused browser[10] that blocks ads**, like Brave or Firefox with uBlock Origin[17]. This only protects what you do in that browser.

If you don't want to use a VPN, an ad-blocking DNS service like AdGuard[18] can block ads across your phone instead. See encrypted DNS[16].

Disable Advertising ID (which can let cops track your location)

Law enforcement uses tools that rely on your advertising ID to track you

We know that ICE and other law enforcement agencies are using location tracking tools[19] that partially rely on the "advertising ID" that your phone provides. These tools are often using these to repress social movements.

Advertising IDs have also been used to pick targets for spyware[20] that gets delivered through ads.

iPhones have this feature disabled by default. On Android, it is on by default and needs to be disabled.

HOW TO DISABLE ADVERTISING ID

IPHONE

Settings → **Privacy & Security** → **Tracking** → **Disable app tracking**

By default, iPhones already have this setting disabled. But you can double-check to make sure.

ANDROID

Settings → Click the search icon and search for "ads" or "advertising" → Tap **Delete advertising ID**

This setting is different on different phones, so searching is easiest.

Enable iCloud Advanced Data Protection (iPhone) or Google Advanced Protection Program

Apple, Google, and other services offer additional security features to protect against targeted attacks on your accounts and data. These protect your online accounts with each company, not your device itself.

Apple's Advanced Data Protection enables end-to-end encryption for most of your content.

HOW TO ENABLE ADVANCED PROTECTION ON YOUR EMAIL/CLOUD ACCOUNTS

Protect your data:

- iCloud Advanced Data Protection[21] - Enables end-to-end encryption for almost all data stored in iCloud, protecting your information against government court orders. Make sure you save the recovery key somewhere very safe (like a password manager[10]).

Protect your account:

- Google's Advanced Protection Program[22] - Helps protect your account from phishing and unauthorized access.
- Microsoft's Account Guard[23]
- Proton Sentinel[24]

Don't click suspicious links

You can protect yourself against spyware by being cautious about what you click on

Spyware[20] often arrives through a text or email with a link custom-designed to feel impossible to ignore, specifically for you. These aren't random spam - they're personalized attacks that exploit what matters most to you.

HOW TO CATCH AND RESPOND TO SUSPICIOUS LINKS

When in doubt: *Do not click the link!*

1. Instead, contact the sender (whether a business or a friend) through a different method (call them, use a different app) to verify they actually sent it. Taking 2 minutes to verify is always better than clicking and compromising your device.
2. If it is a shortened URL like bit.ly or tinyurl.com, you can use ExpandURL.net[25] to view the destination page, but this provides no guarantee that the page isn't spyware. It just helps you view the true URL so you can make a better assessment of whether you trust it.
3. To check whether a link has already been flagged as malicious, you can paste it into a phishing and malware database like VirusTotal[26] (owned by Google/Alphabet). Only submit links that are public and non-personal, because VirusTotal is a public repository that anyone can search.

Red flags to watch for:

- **Messages from numbers you don't recognize:** We all get messages from services that aren't in our contact book often, so it can take work to discern whether this is a legitimate message or not. If it's someone not in your contact book, approach it with more caution.
- **Urgency or fear**: "Your account will be locked," "Urgent security alert," "Family emergency"
- **Unfamiliar domain name:** Spyware texts often come from weird domains like `adsmetrics[.]co`
- **Too personal**: References your activism, recent events you attended, or people you know - designed to bypass your critical thinking
- **Unexpected messages**: A contact sends a link with no context, unusual phrasing, or at a strange time (their account may be compromised)
- **Shortened URLs**: `bit.ly`, `tinyurl.com`, or other link shorteners that hide the real destination
- **Slight misspellings in the URL**: `goog1e.com` instead of `google.com`

Spyware messages can be highly targeted. Here are some real-world examples of how Pegasus Spyware has been deployed:

> "Dear Carmen my brother died in an accident, I'm devastated, I send you the information about the funeral, I hope you can come: [spyware link]" (source[27])

> USEMBASSY.GOV/ WE DETECTED A PROBLEM WITH YOUR VISA PLEASE GO PROMPTLY TO THE EMBASSY. SEE DETAILS [spyware link] (source[27])

> LX 1955 BCN-ZRH 26Jun2020 - Click on the link to receive your mobile boarding pass [spyware link] (source[28])

Be aware: Some spyware is deployed using exploits that don't require you clicking a link at all ("zero click exploits"). These might show up as missed calls on WhatsApp, for example.

Enhanced protections

MEDIUM-THREAT This section is for you if you are in a leadership role or you are doing activism that is more likely to be

targeted by the state or your opposition.

Remove as many apps as you can from your phone/device

If you want to make it tougher for a thief to get into your home, one easy step is to cut down on the number of doors. On your device, each app acts as a "door" to the outside world, exposing you to increased risk of attack. If the app has a bug or vulnerability, it can make your whole device vulnerable.

HOW TO REMOVE APPS

1. **Scan through all the apps on your phone** and computer.
2. **Decide if you truly need it.** Many apps can just as easily be accessed via their website instead. It is usually a little more inconvenient, but you get more privacy and security as a result.
3. **Uninstall it if at all possible.** If you're not sure, try uninstalling it for a week and see if you can manage without it. You can always reinstall later.

Examples of apps that have been used by spyware in the past:

- Apple HomeKit + FindMy + iMessage[29]
- Apple Calendar[30]

Turn off link previews on Signal and WhatsApp

When you include a link in a message, it often generates a "link preview." Even though you can't see it, your device is visiting that webpage to extract the correct preview image. If the webpage is malicious, a sophisticated attacker can identify your location or in extreme cases, implant spyware on your phone.

HOW TO DISABLE LINK PREVIEWS

- **Signal:** Open Signal → Tap your profile picture → **Settings** → **Chats** → **Disable Generate Link Previews**
- **WhatsApp:** **Settings** → **Privacy** → **Advanced** → **Disable link previews**

Cover the front camera

If you were infected by spyware already, it can perform live surveillance on your device, accessing the camera and microphone. To limit what spies can see, it's a good idea to cover at least your front camera.

HOW TO COVER YOUR FRONT CAMERA

1. Get a sticker that has enough stickiness to be reusable. Or consider this sticker pack from SLNT[31].
2. Put it on your phone and your laptop
3. Move it off temporarily when you need the front camera, then remember to move it back.

Consider getting a secondary or burner phone for activist work

If it fits your workflow, consider setting up a second phone or computer just for your higher-risk work.

Check our Secondary Phone Checklist[32] for more on this.

If you do this, make sure you still take security precautions on all devices. Even though only one device has sensitive communications/data on it, both devices could be a target for spyware since they reveal your location and other personal information an attacker might want. You might consider getting a phone that supports **GrapheneOS**[33]. It is security-focused and privacy-focused version of Android that runs on Google Pixel phones.

☐ Reboot your device regularly

Most spyware attempts to hide its tracks by not writing any files to your device. Because of that, rebooting your device will likely cause the spyware to be removed for the moment. That said, if you are still a target, they will likely try to reinfect your phone immediately. Some of the infections require you to click on a link (or take some other kind of action), but some occur without any user interaction. So while rebooting your phone frequently can help make things more difficult for your attackers, it isn't a guarantee that you're free from spyware.

Testing Devices

If you use an iPhone, you can run a spyware analysis using iMazing[34]. It is free (don't click any of the "buy" buttons). Technical users can also run the Mobile Verification Toolkit (MVT)[35] for detailed consensual device forensics.

However, detecting spyware on a device is not a trivial task and you shouldn't rely on just anyone to test your phone. Civil society members globally have turned to these institutions to help test their phones and run detailed analysis with the support of experts:

- Citizen Lab[36] - the leading experts on spyware analysis
- Access Now[37]
- Amnesty Security Lab[38]
- Constitutional Communications[39] - helping get spyware analysis to more people in activist communities
- Electronic Frontier Foundation[40] - for people in the US

Each organization will have its own vetting process, and it might take some time for them to respond to your request while they verify everything on their end.

How to notice if you might be infected

Spyware generally presents no noticeable symptoms and infects *silently*. However, some common complaints from spyware targets over the years have included:

- Rapid drainage of the phone battery
- Suspicious behavior from certain apps
- Abnormal data usage
- Receipt of suspicious links or attachments

If you notice any of these symptoms, it does not necessarily mean that your device has been hacked with spyware. We recommend contacting one of the organizations linked above to get your device tested.

Spyware is highly advanced malware that a regular antivirus **will not detect**. We recommend contacting expert, trusted organizations for support with determining whether your device exhibits signs of (past or present) compromise.

Apple and **WhatsApp** now regularly notify users they suspect their devices have been targeted with mercenary spyware. Here's more on Apple's threat notifications[41] and WhatsApp's threat notification[42].

Learn more

- Citizen Lab has traced Pegasus operations to 45 countries[43]
- Forensic Architecture has mapped the human cost of those operations on their site, Digital Violence[44]

Related: History of how the US government has compromised internet security:

- Microsoft handed the NSA access to encrypted messages[45] - The Guardian, 2013
- Revealed: how US and UK spy agencies defeat internet privacy and security[46] - The Guardian, 2013
- N.S.A. Able to Foil Basic Safeguards of Privacy on Web[47] - The New York Times, 2013
- NSA infected 50,000 computer networks with malicious software[48] - NRC, 2013
- Secret contract tied NSA and security industry pioneer[49] - Reuters, 2013
- N.S.A. Devises Radio Pathway Into Computers[50] - The New York Times, 2014
- How the NSA Plans to Infect 'Millions' of Computers with Malware[51] - The Intercept, 2014
- Prying Eyes: Inside the NSA's War on Internet Security[52] - Der Spiegel, 2014
- New Discovery Around Juniper Backdoor Raises More Questions About the Company[53] - Wired, 2016
- The NSA Leak Is Real, Snowden Documents Confirm[54] - The Intercept, 2016

Keep learning with these related guides

Doxxing defense

Make your home address, workplace, etc. much harder for harassers to compile and publish.

Emergency planning

Make a plan for if you're detained or there may be threats from the opposition at your home.

"Police at the door" poster [55]

Links

1. 404media.co/were-suing-ice-for-its-2-million-spyware-contract/
2. unwall.app/www.wired.com/story/coruna-iphone-hacking-toolkit-us-government/
3. unwall.app/www.wired.com/story/hundreds-of-millions-of-iphones-can-be-hacked-with-a-new-tool-found-in-the-wild/
4. citizenlab.ca/research/how-discover-tech-turned-targeted-ads-into-a-pipeline-for-spyware/
5. citizenlab.ca/research/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/
6. citizenlab.ca/research/lawyers-murdered-women-nso-group/
7. forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/
8. securitylab.amnesty.org/case-study-the-pegasus-project
9. citizenlab.ca/research/reckless-exploit-mexico-nso/
10. activistchecklist.org/essentials/
11. activistchecklist.org/updates/
12. support.microsoft.com/en-us/windows/turn-on-automatic-app-updates-70634d32-4657-dc76-632b-66048978e51b
13. support.apple.com/en-us/105120
14. landing.google.com/intl/en_us/advancedprotection/
15. activistchecklist.org/lockdown/
16. activistchecklist.org/vpn/
17. ublockorigin.com
18. adguard.com/en/welcome.html
19. 404media.co/inside-ices-tool-to-monitor-phones-in-entire-neighborhoods/
20. activistchecklist.org/spyware/
21. support.apple.com/en-us/108756
22. landing.google.com/advancedprotection/
23. accountguard.microsoft.com
24. proton.me/support/proton-sentinel
25. expandurl.net
26. virustotal.com/gui/home/url
27. citizenlab.ca/2017/06/reckless-exploit-mexico-nso/

28. citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/
29. citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/
30. citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/
31. slnt.com/products/webcam-cover
32. activistchecklist.org/secondary/
33. grapheneos.org
34. imazing.com/spyware-analyzer
35. github.com/mvt-project/mvt
36. citizenlab.ca/spyware-outreach/
37. accessnow.org/help/
38. securitylab.amnesty.org/get-help/
39. constitutionalcommunications.org
40. eff.org/about/contact
41. support.apple.com/en-us/102174
42. faq.whatsapp.com/641700318302674
43. citizenlab.ca/research/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/
44. digitalviolence.org
45. theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data
46. theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
47. unwall.app/archive.nytimes.com/www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html
48. nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software-a1429487
49. reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131220
50. unwall.app/www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html
51. theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/
52. spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html
53. unwall.app/www.wired.com/2016/01/new-discovery-around-juniper-backdoor-raises-more-questions-about-the-company/
54. theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/
55. activistchecklist.org/police/