



## Phone Stalkerware and Safety Guide

### A Note on Language



In this toolkit, we will sometimes use the word woman/women and feminine pronouns for simplicity and to recognize the significant impact technology-facilitated violence has on women and girls. We recognize that TFGBV also impacts trans, non-binary, and Two-Spirit people. We hope that all people impacted by TFGBV will find these documents useful.

## What Is Stalkerware?

Stalkerware refers to tools – apps, software programs, and devices – that enable another person to secretly monitor your phone activity.

Stalkerware can monitor almost everything you do on your phone, including photos and videos you take, websites you visit, messages you send and receive, your call history, and your location. Stalkerware can allow someone to turn on the webcam or microphone, take screenshots, see activity on third-party apps (such as Snapchat or WhatsApp), and intercept, forward, or record phone calls.

Almost all phone stalkerware requires physical access to the device to install. Once installed, it runs in stealth mode without any notification or identifying activity and is difficult to detect or remove. To access your phone activity, the person monitoring you signs in to a website or app on a different device. They may also receive notifications of certain activities, such as copies of text messages or an alert that you are on a call so they can secretly join and listen in.

## How Do I Find Out if Stalkerware Is on My Phone?

Detecting stalkerware can be difficult. Some signs could include your battery draining rapidly, your device turning off and on, or spikes in your data usage. The most common sign that your activity is being monitored will be the other person's suspicious behaviour. They may know too much about your phone activities, for example. Trust your instincts and look for patterns. A trained professional may have to check the device to know for sure.

## Responding to Stalkerware

Safety first. Before looking for or trying to remove stalkerware, think about your safety. Some people may escalate their abusive behaviour when stalkerware is removed. You can speak with an [anti-violence worker](#) about safety planning.

***If you suspect stalkerware, what you do on your phone could be seen by the other person. For calls or online activity where you want more privacy, use a phone or other device that isn't being monitored. This could be a friend's phone or a computer at a library, school, or work.***

## Documenting the Stalkerware

You can make notes about what you're experiencing. Our [Documenting Digital Abuse](#) info sheet and sample [Technology-Facilitated Violence Log](#) will provide you with some helpful information.

Alternatively, when you're ready, some police or forensics experts can look for evidence on your device. It may also be worth reading WSC's Preserving Digital Evidence Toolkit on a device that is not being monitored for more helpful documentation tips.

## Removing Stalkerware

In most cases, a full factory reset can remove the stalkerware. However, reinstalling apps or files from a backup can re-load it onto the device. In addition to doing the factory reset, you could also create a new iCloud or Google account for your device so you're starting the device with a blank slate without any option for the stalkerware to be reinstalled.

## Preventing Stalkerware

- **Consider access.** Be cautious if someone wants to update or use your phone. Stalkerware is easy and quick to install. Trust your instincts. Beware of gifts of a new phone or tablet from the perpetrator to you or your children.
- **Update accounts.** Change passwords and set up two-factor authentication. Read more about [Password Safety](#).
- **Lock your phone.** Because most stalkerware requires physical access to the phone to install, place a passcode lock on your phone (and don't share it) to minimize risk. Many devices allow you to choose between a number, pattern, thumbprint, or other security features. Read more [Phone Security Tips](#).
- **Use anti-virus and anti-stalkerware protection.** Download security apps to your phone; these apps can help prevent stalkerware from being installed and can scan your phone for malware or stalkerware apps.
- **Use security features.** Review the security features under your settings to learn what is available on your devices. Android phones allow installations from "unknown sources"; make sure this is turned off. Always install the latest updates for your phone and apps. Not doing so can make them more vulnerable to security and privacy issues.
- **Do not "root" (Android) or "jailbreak" (iPhones) your phone.** "Rooting" or "jailbreaking" a device means removing the operating system limitations to allow for third-party installations (ones not in the app stores). Doing this impacts the built-in security features designed to protect the device and makes the device vulnerable. Many of the more invasive stalkerware features don't work unless the protections put in place by the manufacturer are bypassed. On iPhones, most stalkerware cannot be installed unless the device is jailbroken. A rooted or jailbroken phone will be more vulnerable to viruses and malware, making it easier for stalkerware to be installed.

[KG]Link to 1.24

link 1.08 [\[RW2\]](#)

## When It's Not Stalkerware

There are many other methods someone can use to access information on your phone or know your activities without installing stalkerware. If the perpetrator has physical access to the phone or your cloud accounts, they may not need to install stalkerware to monitor you. Sometimes, the perpetrator uses friends and family members to gather information. Look for patterns in what the person knows and where that information might have come from to help you to narrow down the possibilities. An anti-violence worker can help you figure out what may be happening and plan next steps.

*Technology-Facilitated Gender-Based Violence (TFGBV) is part of a continuum of violence that can be both online and in-person. If you or someone you know is experiencing TFGBV, you are not alone. You can use [sheltersafe.ca](#) to find a shelter/transition house near you to discuss options and create a [safety plan](#). You don't need to stay in a shelter to access free, confidential services and support.*

*Adapted for Canada with permission from NNEDV's Safety Net project, based on their resource [Stalkerware: Phone Surveillance & Safety for Survivors](#).*

---

© Copyright 2024 Women's Shelters Canada | All Rights Reserved

This project is made possible through funding from the department of Women and Gender Equality (WAGE) Canada.

