STALKERWARE

UNDERSTANDING AND STOPPING TECHNOLOGY-FACILITATED DOMESTIC VIOLENCE

NATIONAL CYBERSECURITY ALLIANCE

IN COLLABORATION WITH

ESET

NNEDV

53,870 mobile users were survivors of stalkerware in 2020. Stalkerware is a form of monitoring software which enables a remote user to track activities on another user's device, such as location data, call logs and messages. It is most often used to monitor a spouse or partner without their permission.

The term stalkerware, also known as spyware, refers to a type of app designed to be hidden from the survivor. Survivors are often unaware when this software has been installed on their device. The National Cyber Security Alliance has partnered with ESET and the National Network to End Domestic Violence to bring awareness to the dangers of stalkerware, how to detect it, and what to do if you are a target.

NEED HELP?

The most common users of stalkerware are abusive partners or spouses. If you or someone you know needs help, contact the **National Domestic Violence Hotline at 1-800-799-7233**.

WHAT IS STALKERWARE?

Stalkerware apps can allow someone to track virtually anything you do on your device: following your location, listening to phone calls, viewing text messages and emails, etc. These apps must be manually installed onto a device, so they are most often used by someone close to the survivor, such as a partner, ex-partner, spouse, boss or parent. Many stalkerware apps will market themselves as “parental-monitoring” tools, for parents to track their underaged children.

IT'S MORE COMMON THAN YOU MAY THINK

According to a study from NPR, 85% of domestic violence shelters surveyed said they're working directly with survivors whose abusers tracked them using GPS. 75% said they're working with survivors whose abusers eavesdropped on their conversation remotely — using hidden mobile apps.

STALKERWARE

UNDERSTANDING AND STOPPING TECHNOLOGY-FACILITATED DOMESTIC VIOLENCE

PREVENTING STALKERWARE

The following tips may help minimize the risk of stalkerware being downloaded to your device and help you stay cyber secure overall:

DON'T LEAVE YOUR DEVICE UNATTENDED

Whether you are at home or out in public, ensure your devices are with you at all times.

LOCK YOUR DEVICE

Make sure you lock your device with the use of a passcode or extra security features (like facial recognition).

ONLY DOWNLOAD APPS FROM VERIFIED DEVELOPERS AND OFFICIAL APP STORES

Before downloading any app from the App Store, Google Play or any other app service, check the reviews and ratings of the app, and look it up online to ensure the developer is credible.

CREATE STRONG PASSPHRASES ONLY YOU WOULD KNOW

A strong passphrase is a sentence that is at least 12 characters long. Focus on sentences or phrases that you like to think about and are easy to remember, including special characters and numbers. On many sites, you can even use spaces. Be mindful not to use birth dates, repeating digits, a year of birth, your social security number, phone numbers or anything the abuser can easily guess.

REVIEW YOUR DOWNLOADED APPS

Do a periodic review of the apps downloaded onto your phone. Check the settings of used apps to make sure the privacy and security settings are configured to protect you and your information. Delete any apps you no longer use or do not recognize. Don't forget to check your phone settings for a list of all the apps downloaded to the phone, not just the ones that appear on your home screen.

USE ANITVIRUS SOFTWARE

Cybersecurity antivirus software will scan your device for stalkerware and any other malicious apps, and warn you if they find known stalkerware apps. Learn more about the different antivirus softwares available.

STALKERWARE

UNDERSTANDING AND STOPPING TECHNOLOGY-FACILITATED DOMESTIC VIOLENCE

DETECTING STALKERWARE

Once installed, it can be very difficult to detect stalkerware, as these apps are designed to be hidden from the device user. However, there are ways to find this software within your phone's settings:

CHECK YOUR DEVICE'S SETTINGS OR APP STORE

Even when an app is hidden, it may still appear in your device's settings or app store. To find a list of downloaded apps, follow the below steps:

- For iOS users:
  - Go to your settings app
  - Scroll to the bottom to see a list of all downloaded apps
  - *To check which apps have access to your camera, microphone and location, go to **Settings -> Privacy** for complete lists of apps that have access to your camera, microphone, location and other features.*
- For Android users:
  - Go to your settings app
  - Select Apps & Notifications -> See All Apps
  - *To check which apps have access to your camera, microphone and location, go to **Settings -> Privacy -> Permission Manager** for complete lists of apps that have access to your camera, microphone, location and other features.*

NOTE: STALKERWARE APPS MAY NOT BE IMMEDIATELY OBVIOUS

They may have a different label to disguise themselves, or a label that looks similar to a legitimate app. Look for any apps in your device settings that you don't recognize. Discuss a safety plan with an advocate before you delete the app. Keep in mind that the abuser will know that the app has been removed from the device and this may escalate the abuse.

OTHER INDICATORS OF STALKERWARE

While one of these indicators alone may not be a sign of stalkerware, multiple signs may mean something has been installed on your device:

- The stalker has had access to your device. This can mean your device goes missing and reappears or if you've loaned your device to someone for an extended period of time.
- Unknown applications have access to your camera.
- Your screen starts glitching, lagging or your phone's battery starts draining faster, unexpectedly.

STALKERWARE

UNDERSTANDING AND STOPPING TECHNOLOGY-FACILITATED DOMESTIC VIOLENCE

IF YOU FIND STALKERWARE ON YOUR DEVICE

If someone is tracking your device, they will know when the stalkerware app is deleted. If you decide not to delete the app, consider the following steps on page one to seek help first. If you decide to delete the app first, consider the following steps:

DO A FACTORY RESET

A factory reset restores your phone to its original state by deleting all information from the device, including apps and accounts. This can help ensure that all possible stalkerware has been removed from your device. Be sure to backup any necessary files and information before doing so. *Note: After a reset, do not restore your device's data from the cloud or from a back up source. This may reinstall the stalkerware.*

GET A NEW DEVICE

To be absolutely sure there is no stalkerware on your device, consider purchasing a new one.

CHANGE LOGIN CREDENTIALS

If someone has been viewing your online activities, they will know the credentials for any account you've logged into while stalkerware was installed. Change all your passwords, security questions, etc. for your online accounts.

SEEK HELP

Contact the National Domestic Violence Hotline at 1-800-799-7233 or local law enforcement.

ADDITIONAL RESOURCES

- ☑ THE COALITION AGAINST STALKERWARE
- ☑ TECHSAFETY.ORG SPYWARE/STALKERWARE OVERVIEW
- ☑ TECHSAFETY.ORG NATIONAL HOTLINES
- ☑ TECHSAFETY.ORG RESOURCES FOR SURVIVORS

NATIONAL CYBERSECURITY ALLIANCE

The National Cyber Security Alliance (NCSA) builds strong public/private partnerships to create and implement broad-reaching education and awareness efforts to empower users at home, work and school with the information they need to keep themselves, their organizations, their systems and their sensitive information safe and secure online and encourage a culture of cybersecurity. www.staysafeonline.org