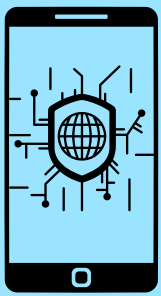
Recommendations for STALKERWARE VICTIMS

1 How can I prevent stalkerware apps from being installed on my phone?

Keep your phone up close and under observation to prevent any unwanted person from accessing it and potentially installing malicious apps. Stay aware whenever someone else could have potentially used your phone, even with your consent. Use strong passwords or PIN codes and avoid sharing them with other people to prevent unwanted use.

2 How can I know if a stalkerware has been installed on my phone?

Watch out for potential indicators of compromise, including: abnormal (increased) battery consumption, unexpected pop-ups, performance drops, suspicious app duplicates or apps with seemingly important name ("Sync manager", a second "Settings" apps), green dot icon at the top of the screen (indicating that the phone is recording), and any other strange behaviour from the phone. Regularly check that the Protect feature of Google Play is active. If disabled, this would indicate that someone have tampered with the phone. This feature can also be used to easily detect apps that were not downloaded from the Play Store. Keep the phone updated to its latest version, as many stalkerware apps could lose compatibility with newer system versions.



3 I think my phone is being monitored by a stalkerware, what should I do?

If you observe any of the previously cited behaviors, or observe other proofs of a stalkerware being installed on your mobile device, seek help from a qualified organization or professional. Using a non-monitored device, you can find help materials related to your country on stopstalkerware.org, or on this Canadian government website for Canadian resources. Canadian crisis lines for intimate partner violence victims can be found on www.dawncanada.net -- they are anonymous and reachable for free 24 hours a day.

Concordia University

For more information, scan this QR code