Recommendations for SERVICE PROVIDERS

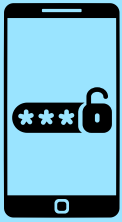
1 How can we reduce the amount of stalkerware apps in circulation

It is crucial to keep potential victims educated about the existence of stalkerware apps, and how to protect themselves against such tools. Awareness campaigns can be conducted through social media, school programs or community events to teach users how to prevent, avoid or detect early signs of stalking.

Fighting against stalkerware websites (e.g., blocking) can also lower the amount of monitoring apps available online.

2 How can operating system providers improve the situation for IPV victims?

Operating systems, such as Android OS can also play a role to reduce affects for victims. For example, enforcing PIN/unlock requirement for sensitive configuration updates (e.g., disabling Play Protect), warning users periodically that such changes have been made (e.g., once a day), and disabling blatant and constant information collecting apps such as stalkerware (almost no legitimate apps would behave the same way).



3 How can payment/ad providers improve the situation for IPV victims?

Advertisement platforms such as Google Ads should establish clear policies or blacklists to detect and block advertisements on stalkerware websites, as well as content promoting such applications. Similarly, domain providers, and web hosting platforms have to effectively prevent access to malicious websites when reported.

Payment and ad service providers should check the apps and websites before offering their services, to avoid aiding the stalkerware ecosystem.

For more information, scan this QR code

Concordia University

This project was funded by

Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada