

Mijn toestel wordt afgeluisterd

1. Wat te doen bij stalkerware?

Heb je de indruk dat je wordt afgeluisterd via je mobile telefoon? Dat is mogelijk. Er bestaat software die in staat is om je locatie door te geven, telefoongesprekken af te luisteren, je toetsenaanslagen te volgen of je gegevens te bekijken. Dit heet stalkerware. Er bestaat ook een hoog technologische variant, nl. spyware. Daarover hebben we het hier verder niet.

Hoe kan je stalkerware detecteren?

Heeft iemand fysieke toegang (gehad) tot jouw toestel?

Het is enkel mogelijk om stalkerware te installeren wanneer iemand fysiek toegang heeft tot jouw toestel. Als niemand toegang heeft (gehad) tot je toestel, kan je ervan uitgaan dat je geen stalkerware hebt.

Reageert jouw toestel ongewoon?

Enkele voorbeelden: de batterij loopt snel leeg zonder dat je het toestel gebruikt, er is hoog datagebruik, je krijgt notificaties die je niet verwacht, het toestel voelt heet aan, het herstart op onverwachte momenten, enz.

Staan er onbekende apps of programma's op je toestel?

Bekijk de lijst van apps op je telefoon. Staan er onbekende apps tussen? Sommige stalkerware apps zijn vermomd als kalender of rekenmachine. Bij je privacy instellingen kun je nakijken welke apps toegang hebben tot bijvoorbeeld je locatie, microfoon en foto's.

Op je PC kan je in de *task manager* (Windows via ctrl+alt+del) of *activity monitor* (MacOS) op zoek gaan naar ongekende programma's. Kijk vooral naar programma's die veel CPU, memory en disk space gebruiken.

Voer een antivirusscan uit

Sommige antivirus software kan stalkerware opmerken. Het is dus nuttig om [een virusscan uit te voeren op je toestel.](#)

2. Hoe kan je stalkerware verwijderen?

Denk na voordat je stalkerware verwijderd

Sommige stalkerware sturen een notificatie naar de stalker. De stalker weet dus dat jij de stalkerware verwijderd hebt. Als je een hevige reactie vreest van de stalker, zorg er dan voor dat je op een veilige plaats bent.

Door de stalkerware te verwijderen, verwijder je ook alle bewijzen die nuttig kunnen zijn voor de politie. Doe dus eerst een aangifte bij de politie, alvorens de stalkerware te verwijderen. Zo kan de politie de bewijzen op je toestel verzamelen en onderzoeken.

Het verwijderen van stalkerware is complex

Laat je helpen door een expert, als je de minste twijfel hebt over bepaalde acties.

- Verwijder de gevonden stalkerware app of programma via 'delete' en controleer met je antivirussoftware of de stalkerware volledig verwijderd is. Soms kan ook je antivirussoftware de stalkerware verwijderen.
- Om zeker te zijn, moet je je toestel opnieuw instellen naar fabrieksinstellingen (resetten). Voor dat dit doet, raden wij aan om een back-up te maken van je persoonlijke data. Dit zorgt ervoor dat je je gegevens niet verliest.
- Na het resetten kan je je back-up terugplaatsen. Wees voorzichtig met het terugplaatsen van je persoonlijke data van je back-up. Je wil namelijk vermijden dat je de stalkerware zich opnieuw installeert. Gebruik de cloud backup van je Google of Apple account en selecteer manueel de applicaties die je terug wil installeren.
- Verander je wachtwoorden. Zodra de stalkerware verwijderd is, moet je onmiddellijk al je wachtwoorden veranderen. De stalker heeft misschien lange tijd kunnen meekijken en kent al je wachtwoorden. Misschien heeft de stalker ook een 'rule' ingesteld die jouw berichten doorstuurt. Verander in de eerste plaats de wachtwoorden van je mailbox en social media en vervolgens alle andere wachtwoorden.