**De 10 meest voorkomende tekenen dat je digitaal wordt gestalkt & wat je moet doen als je denkt dat je slachtoffer bent**

Een ongelukkig element aan daten in het digitale tijdperk is de mogelijk om gestalkt te worden. Volgens recent onderzoek van Kaspersky blijkt dat bijna een kwart (23%) van de Nederlandse respondenten wel eens is gestalkt door iemand met wie ze net aan het daten waren. Maar als we het daten achterwege laten, blijkt dat meer dan een derde (37%) van de Nederlanders online is gestalkt.

Ondanks onschuldige 'due diligence' of het doen van een ‘back ground check’ waarbij een potentiële aanbidder stiekem iemands sociale netwerk bekijkt, is cyberstalking veel onheilspellender. Dat komt vooral omdat we gewend zijn geraakt aan het overmatig delen van persoonlijke informatie zoals foto's en wachtwoorden.

Hieronder vind je een top 10 van de meest voorkomende manieren om erachter te komen of je het risico loopt om gestalkt te worden. Dit lijstje is gerangschikt op basis van de onderzoekscijfers in volgorde van waarschijnlijkheid:

1. Er verschijnen ongewenste e-mails of berichten op je apparaten.
2. Je locatie-instellingen kunnen willekeurig worden geactiveerd.
3. Je apparaat sluit onverwachts af, start opnieuw op of apps worden afgesloten.
4. De online status verandert zonder dat je het door hebt.
5. Iemand anders wordt zich te veel bewust van je dagelijkse activiteiten.
6. Privacy-instellingen op je sociale media-accounts worden gewijzigd.
7. Ongebruikelijke app-suggesties verschijnen op je apparaat.
8. Je batterij loopt sneller leeg dan normaal, wat suggereert dat er in stilte monitoringsoftware (vaak stalkerware genoemd) op je telefoon is geïnstalleerd zonder je toestemming.
9. Berichten zijn gemarkeerd als "gelezen" voordat je ze hebt gezien.
10. Netwerkstoringen/slecht bereik.

Als je vermoedt dat je digitaal wordt gestalkt, is dat nooit jouw schuld. Toch is het handig om deze stappen/voorzorgsmaatregelen overwegen:

1. Documenteer alle verdachte of intimiderende communicatie, inclusief data, tijden en details.
2. Verbeter de beveiliging van je apparaten door sterke, unieke wachtwoorden in te stellen en twee-staps-verificatie in te schakelen.
3. Neem de controle over je online aanwezigheid terug door je privacy-instellingen aan te passen en na te denken voordat je gevoelige informatie deelt.
4. Zoek emotionele steun bij vertrouwde personen of hulporganisaties en overweeg juridische of wethandhavingsdeskundigen te raadplegen om gevallen van intimidatie te melden.
5. Als je vermoedt dat er stalkerware-apps op je apparaat zijn geïnstalleerd zonder je toestemming, verwijder deze dan niet omdat dit je misbruiker kan waarschuwen. Zoek in plaats daarvan hulp bij de [Coalition Against Stalkerware](https://stopstalkerware.org/), met een nieuw apparaat of de telefoon van een vriend.