

4.

WIS JE SPOREN

De browser op je telefoon slaat veel informatie over jou op – waar je bent, wat je zoekt, welke websites je gebruikt – en kan die informatie weggeven. Je kunt de controle over een deel van die informatie terugkrijgen als je een aantal veranderingen doorvoert.

Telefoons, tablets en computers zijn vaak voorzien van een vooraf geïnstalleerde browser die minder privacyvriendelijk is. In plaats daarvan kan je **een browser downloaden en gebruiken** die **standaard meer privacy biedt** en die je beschermt tegen trackers.

En om je privacy nog beter te beschermen kun je add-ons en extensies installeren (dat zijn makkelijk te installeren mini-programmaatjes voor je browser die je **online activiteit nog beter afschermen**).



Om spiedende advertenties en onzichtbare trackers te blokkeren, installeer je uBlock Origin (voor Chrome, Safari en Firefox) of **Privacy Badger** (voor Chrome, Firefox en Opera).

Om je verbinding met websites zo goed mogelijk te beveiligen, installeer je HTTPS Everywhere: een browserextensie die ervoor zorgt dat de communicatie tussen je browser en veel belangrijke websites wordt versleuteld en beschermd. Als je dit een nuttige functie vindt en Safari gebruikt, kies dan als standaard zoekmachine eentje die niet van Google is, zoals DuckDuckGo, die je automatisch omleidt naar een versleutelde verbinding.



D A T A
D E T O X
K I T

HOUD CONTROLE OVER JE SMARTPHONEGEGEVENS

om je online privacy te vergroten

5.

ONT-TAG JEZELF EN ANDEREN

Heb je geholpen bij het opbouwen van de gegevensberg van je vrienden doordat je ze wel eens hebt getagd in foto's en berichten? Je kunt hun gegevensberg afgraven (en je geweten sussen) door die **tags te verwijderen** in zoveel mogelijk foto's en berichten.

Geef het door! Betrek je vrienden, familie en collega's ook bij het beheersen van die losgeslagen data. Als we allemaal samenwerken om onze dataspooren onder controle te houden kunnen we elkaar beter helpen bij het detoxen.

Als je nadenkt over wat je gegevens prijsgeven over jou lijkt dat op het eerste gezicht niet belangrijk: wat boeit het iemand anders dat je groot fan bent van Nederlandse hits, dat je meer schoenen koopt dan je nodig hebt of dat je je vakantie een jaar van tevoren boekt?

Het probleem is wat er met die gegevens gebeurt. Als ze in de loop der tijd worden samengevoegd, **ontstaan er persoonlijke digitale patronen:** je gewoontes, locaties, relaties, voorkeuren, overtuigingen en geheimen worden tot in detail blootgelegd aan degenen die de gegevens **verzamelen en eraan verdienen**, zoals bedrijven en datahandelaars.

Met het volgen van deze afkickcursus word je ervan bewust hoe en waarom dit allemaal gebeurt en leer je praktische stappen te zetten om de **dataspooren die je op het internet achterlaat te beheersen**.

Aan de slag!

Een product van

TACTICAL
TECH

Ondersteund door



datadetoxkit.org
#datadetox

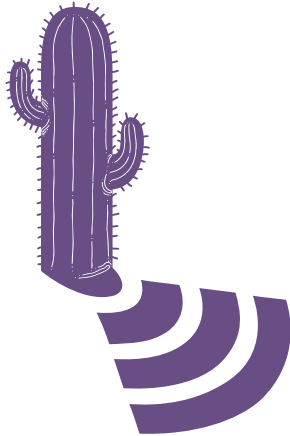
1.

VERANDER DE NAAM VAN JE TELEFOON

Het kan zijn dat je in het verleden je telefoon een naam hebt gegeven voor **wifi, bluetooth** of beide – of dat er automatisch een naam is aangemaakt tijdens de installatie. Dat betekent dat 'telefoon van Janneke Jonkman' zichtbaar is voor de eigenaar van het wifi-netwerk en, als je bluetooth hebt ingeschakeld, voor iedereen in de buurt die zijn bluetooth ook aan heeft staan.

Als je een café, gym of winkel inloopt vertel je niet aan iedereen hoe je heet en dat zou je telefoon ook niet moeten doen.

Je kunt de naam van je telefoon wijzigen naar iets wat minder identificerend is, maar nog steeds uniek voor jou. Zo doe je dat:



iPhone:
Telefoonnaam veranderen:
Instellingen → Algemeen → Info → Verander de naam

Android:
Wifi-naam veranderen:
Instellingen → Wi-Fi → Menu → Geavanceerd / Meer eigenschappen → Wi-Fi Direct → Apparaatnaam veranderen
Bluetooth-naam veranderen:
Instellingen → Bluetooth → Zet Bluetooth aan als die uitstaat → Menu → Apparaatnaam veranderen → Zet Bluetooth uit



2.

WIS JE LOCATIESPOREN

De locatiedata lijken misschien willekeurige stukjes informatie, maar al die stukjes samen onthullen **belangrijke gegevens over jou** en je gewoontes, zoals je woonplaats, waar je werkt en waar je naartoe gaat met je vrienden. Daarom zijn die gegevens zeer gewild bij veel bedrijven en datahandelaars.

Je kunt **per app de instellingen beheren** en de **locatievoorzieningen uitschakelen**. Bekijk welke apps de locatievoorziening eigenlijk niet nodig hebben om goed te kunnen werken (moet een game echt weten waar je bent?) en voor welke apps je de locatievoorziening liever uitschakelt:



Android:
Instellingen → Apps → Locatietoegang per app beheren

iPhone:
Instellingen → Privacy → Locatievoorzieningen → Locatietoegang per app beheren

Android:
Instellingen → Apps → Selecteer de app die je wilt verwijderen → Verwijderen

iPhone:
Hou het app-icoontje ingedrukt totdat er een menu verschijnt.

Selecteer de optie app verwijderen.

Bevestig verwijderen van de app.

3.

APPS OPRUIMEN

De apps die je gebruikt voor social media, games en het weerbericht hebben interesse in je gegevens... en de kans is groot dat ze veel van die gegevens verzamelen.

De apps die je nooit gebruikt kun je beter van je telefoon verwijderen, want het is een perfecte manier om je digitale ik te detoxen.

Bovendien krijg je met zo'n schoonmaakactie weer meer ruimte op je telefoon, je verbruikt minder data en je batterij gaat langer mee.