4.

REDUCER DINE DIGITALE FODSPOR

Den browser du har på din smartphone gemmer en masse information om dig - din lokation, din søgehistorik, hvad du søger efter og hvilke hjemmesider du bruger og udbyderen kan videreformidle den information. Du kan beholde lidt mere af kontrollen med dine informationer via et par enkelte ændringer.

Smartphones, tablets og computere har typisk en pre-installeret browser, som ikke nødvendigvis sætter dit privatliv først. Du kan istedet vælge at **downloade and bruge en browser**, der som standard beskytter din internetaktivitet bedre, så du skærmes fra unødvendig sporing.

Og ønsker du at beskytte dit privatliv i endnu højere grad, kan du installere ekstra funktioner kendt som "add-ons eller extensions" (det er små programmer, som er nemme at installere i din browser og som på flere måder kan **øge privatlivet i dine internetaktiviteter**).

5.

FJERN UØNSKEDE TAGS AF DIG SELV OG ANDRE

Har du tidligere tagget dine venner i fotos og opslag? Så har du bidraget til at øge mængden af tilgængelige data om dem på internettet! Hjælp dem med at reducere mængden af tilgængelige data (og dine egen samvittighed i processen) ved at **fjerne tags** på så mange fotos og opslag du kan.

Giv budskabet videre! Opforder dine venner, familie og kollegaer til at gøre det samme. Hvis vi samarbejder om at minimere de spor vi efterlader på internettet om hinanden, så kan vi hjælpe hinanden med detox.

A product of

TACTICAL TECH

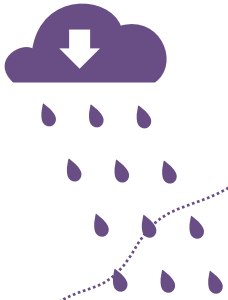
Supported by

Firefox

datadetoxkit.org
#datadetox

For at blokere spyware og usynlig sporing af din internetaktivitet, installer **uBlock Origin**(til Chrome, Safari og Firefox) eller **Privacy Badger** (til Chrome, Firefox og Opera).

For at sikre dine internetaktivteter bedst muligt, installer HTTPS Everywhere: en browser extension der sikrer at din kommunikation med mange store hjemmesider bliver krypteret og beskyttet undervejs. Hvis du er en dedikteret bruger af Safari, så kan de sætte din standard søgemaskine til at være et ikke-Google produkt, som f.eks. DuckDuckGo, der automatisk omdirigerer dig til sikre, krypterede forbindelser.



DATA DETOX KIT

TAG KONTROL OVER DIN SMARTPHONES DATA

og øg din sikkerhed online

Du tænker måske ikke umiddelbart, det er problematisk, at andre har adgang til dine data: Hvem kan gå op i om jeg er countryfan, køber flere sko end jeg har brug for eller planlægger min næste ferie et år i forvejen?

Problemet ligger i hvad der gøres med dine data. Over tid opstår der intime digitale spor: Dine vaner, bevægelser, forhold, præferencer, overbevisninger og hemmeligheder afsløres til dem, der analyserer og profiterer af dine data, såsom virksomheder og datamæglere.

Gennem denne Data Detox får du indblik i hvordan og hvorfor alt dette sker, og du bliver i stand til at tage praktiske forbehold, så du kan kontrollere dine dataspor på internettet.

Lad os komme i gang!

1.

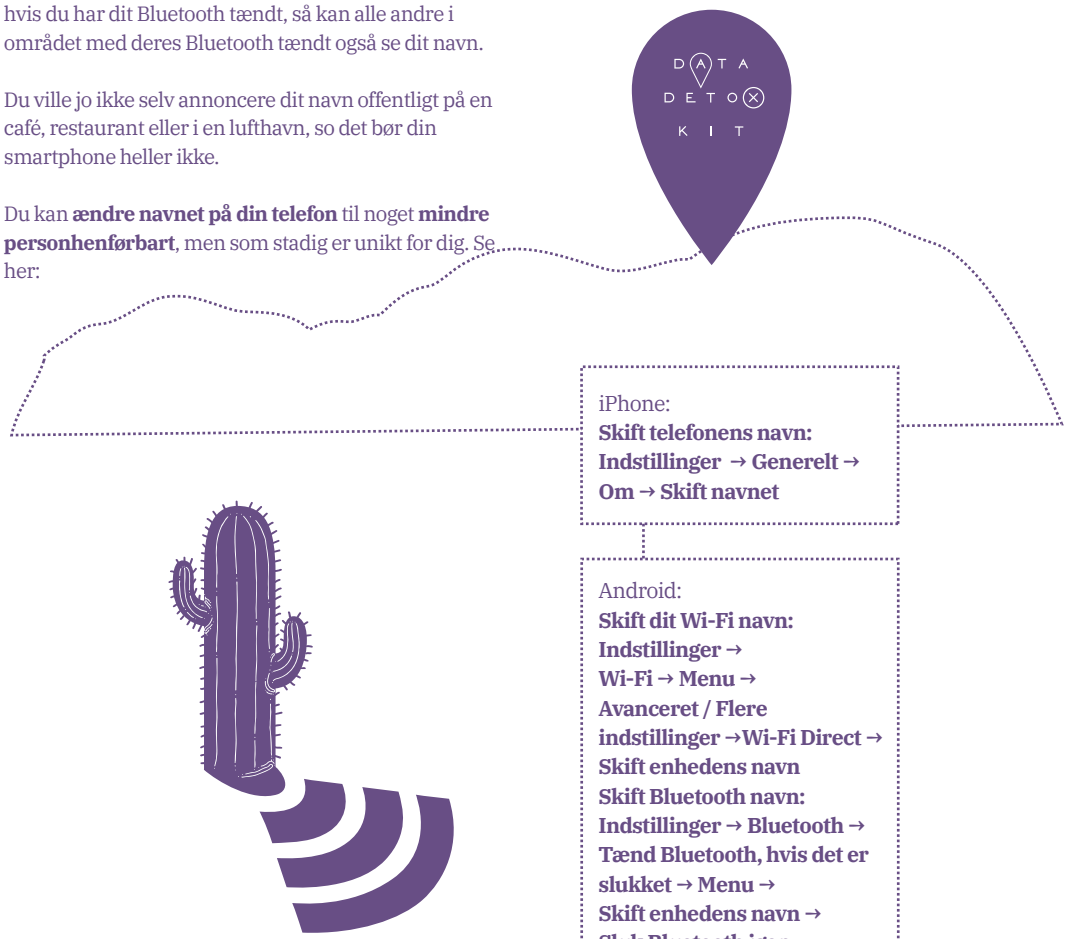
GIV DIN SMARTPHONE ET NYT NAVN

På et eller andet tidspunkt har du givet din smartphone et navn til **Wi-Fi, Bluetooth** eller begge dele - måske navnet er blevet autogenreret da du satte telefonen op.

Det betyder at dét navn, f.eks. "Alex Chung's Phone" er synligt for netværksejerne af det Wi-Fi, du bruger eller hvis du har dit Bluetooth tændt, så kan alle andre i området med deres Bluetooth tændt også se dit navn.

Du ville jo ikke selv annoncere dit navn offentligt på en café, restaurant eller i en lufthavn, so det bør din smartphone heller ikke.

Du kan **ændre navnet på din telefon** til noget **mindre personhenførbart**, men som stadig er unikt for dig. Se her:



iPhone:
Skift telefonens navn:
Indstillinger → Generelt → Om → Skift navnet

Android:
Skift dit Wi-Fi navn:
Indstillinger → Wi-Fi → Menu → Avanceret / Flere indstillinger → Wi-Fi Direct → Skift enhedens navn
Skift Bluetooth navn:
Indstillinger → Bluetooth → Tænd Bluetooth, hvis det er slukket → Menu → Skift enhedens navn → Sluk Bluetooth igen

2.

RYD DINE PLACERINGSAFTRYK

Det virker måske som om dine lokaltionsdata bare er **tilfældige brokker** af data, men når de ses som et hele, kan de afsløre **vigtige detaljer om dit liv** og dine vaner, som hvor du bor, arbejder eller hænger ud med venner. Derfor er disse data også meget eftertragtede af firmaer og datamæglere.

Du kan **gå igennem de tilladelser, du har givet hver enkelt app** og **fravælge lokationsservices**. Kig efter apps, som i virkeligheden slet ikke har brug for dine lokationsdata for at fungere (Har det her spil virkelig brug for at vide, hvor du er?) og for de apps, som du ikke ønsker at give adgang, kan du:

Android:
Indstillinger → Apps → Tilladelser → Placering

iPhone:
Indstillinger → Privatliv → Placering → Adminsitrer adgang til dine lokationsdata for hver enkelt app

3.

RYD OP I DINE APPS

Alle dine apps, uanset om det er til sociale medier, spil eller vejret er interesserede i dint data... og potentielt kan de indsamle en hel del.

At rydde op i de apps på din smartphone, som du aldrig bruger, er en rigtig god måde at få renset ud i dit digitale liv.

Derudover, kan en god oprydning også skaffe dig **mere ledig hukommelse** på din smartphone, sænke dit dataforbrug og **forlænge levetiden af dit batteri**. Alt i alt vil du måske opleve en bedre performance på din smartphone, alt efter hvilke apps, du får ryddet ud i.

Android:
Indstillinger → Apps → Programmer → Udvælg de apps, du ønsker at afinstallere → Afinstaller

iPhone:
Tryk på en app og hold fingeren inde indtil alle apps begynder at ryste og et lille kryds kommer til syn i øverste venstre hjørne på dem.

For at slette en app, tryk let på det lille kryds i hjørnet af app'en.

For at få iPhone tilbage i normaltilstand tryk på hjem-knappen.