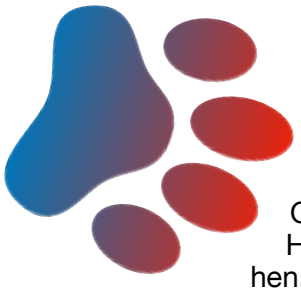


Dæk dine spor - undgå sporing - check din browser

Det sneede i nat.
Der lå et fint uberørt lag sne, og dog, jeg kunne se at en kat havde passeret gennem min have i nattens løb.
Kat eller ?
OK, et dyr - jeg er ikke ekspert i dyrespor.
Hvis man er ihærdig kan man finde ud af hvorfra den kom og hvor den skulle hen.

Internettet er ligeledes dækket med sne, og hver gang du besøger et websted, sender din browser små informationer om sig selv - og derefter om dig.

I den enkleste verder er der 3 aktører, dig, hjemmesiden du besøger og annoncenetværket.
Da det er det tredje hjul i samspillet kaldes det ofte tredjepartsannoncenetværk.

I vores enkle verden leverer et enkelt tredjepartsannoncenetværk annoncer på et antal websteder*, som alle skal indeholde noget usynlig kode, der indlæses, når du besøger siden.
Det sker - f.eks. når du tjekker nyhederne uden en trackerblokker installeret.

**/Nu udvidede vi den enkle verden med et antal andre websteder;-)*

Annoncenetværket får en anmodning fra din computer og har pludselig adgang til en mængde meget individualiserede oplysninger. (hvis du ikke tror det, så kig i en af mine tidligere episoder: Hvorfor sendes dine data til Polen? https://brugdintablet.dk/tracking-sporing/)

Noget af det sendes som standard (f.eks. din enhed og browserversion), og meget af det opsamles af tredjeparter - annoncenetværk, der har integreret sporingsmekanismer på tværs af store områder af internettet.

Fordi trackere (ikke at forveksle med hackere) er så almindelige, kaster de et bredt net, og ved første øjekast virker de data, de indsamler, relativt ufarlige. Men når de sammensættes, danner de en usædvanligt afslørende adfærdsprofil, der fungerer som en live oversigt over din online aktivitet og kan afsløre alt fra politisk tilknytning til uddannelsesniveau til indkomstgruppe. Så længe denne række data om dig er knyttet tilbage til dig, bliver din online aktivitet logget.

Annoncenetværk er primært afhængige af to metoder: cookies og browserens fingeraftryk.

Hvad er cookies?

Cookies er små klumper af oplysninger, som websteder gemmer i din browser. De bruges primært til automatisk at huske ting som dine loginoplysninger for kontoen, eller hvilke varer der var i din online indkøbskurv - med andre ord, de gemmer dine informationer. De kan dog også bruges til at linke alle dine besøg, søgninger og andre aktiviteter på et websted sammen. Mange mennesker føler, at dette er en krænkelse af deres privatliv, og browsere giver dig generelt mulighed for at blokere, begrænse eller slette cookies.

Hvad er et digitalt fingeraftryk?

Et digitalt fingeraftryk er i det væsentlige en liste over egenskaber, der er unikke for den enkelte bruger, deres browser og deres specifikke hardwareopsætning. Dette inkluderer oplysninger, som browseren sender automatisk, samt en række tilsyneladende ubetydelige data (som skærmopløsning og installerede skrifttyper), der indsamlet af sporingsscript. Annoncenetværk/ Sporingssteder kan sy alle de små stykker sammen for at danne et unikt billede eller "fingeraftryk" af brugerens enhed.

Hvad er forskellen?

Tænk på de små sporingsenheder, som forskere bruger til at følge dyremigrationsmønstre, eller en GPS-sender, der er knyttet til en bil. Så længe de er knyttet til "måldyret" eller køretøjet, er de nøjagtige og effektive - men de mister al værdi, hvis de bliver slået af eller kasseret. Dette er

omtrent, hvordan cookies opfører sig: de sporer brugere op til det punkt, som en bruger sletter dem. Fingeraftryk følger en lignende driftsform, men bruger mere permanente identifikatorer, såsom hardwarespecifikationer og browserindstillinger. Dette svarer til at spore en fugl ved hjælp af sang- eller fjermarkeringer eller en bil med nummerplade, mærke, model og farve - med andre ord målinger, der ikke ændres så let.

Første feber handling

Du sletter dine cookies, div. annoncenetværket mister forbindelse til dig.
Men næste gang du kommer på webstedet identificeres dit fingeraftryk, og nu ved annoncenetværket at det er dig.

Anden kølige overvejelse

Kan jeg i min opsætning af browser gøre noget?
Ja, du kan teste din browser her: **https://coveryourtracks.eff.org**, hvorfra jeg også har kopieret/ hentet inspiration til ovennævnte tekst

Jeg har kørt nogle test på min iPad og på min Mac, med forskellige browsere (Safari og Chrome).

Her er resultaterne:

Chrome (på en Mac men mit gæt er at det er det samme på en PC)

Trackers use a variety of methods to identify and track users. Most often, this includes tracking cookies, but it can also include browser fingerprinting, which is a sneakier way to track users and makes it harder for users to regain control of their browsers.

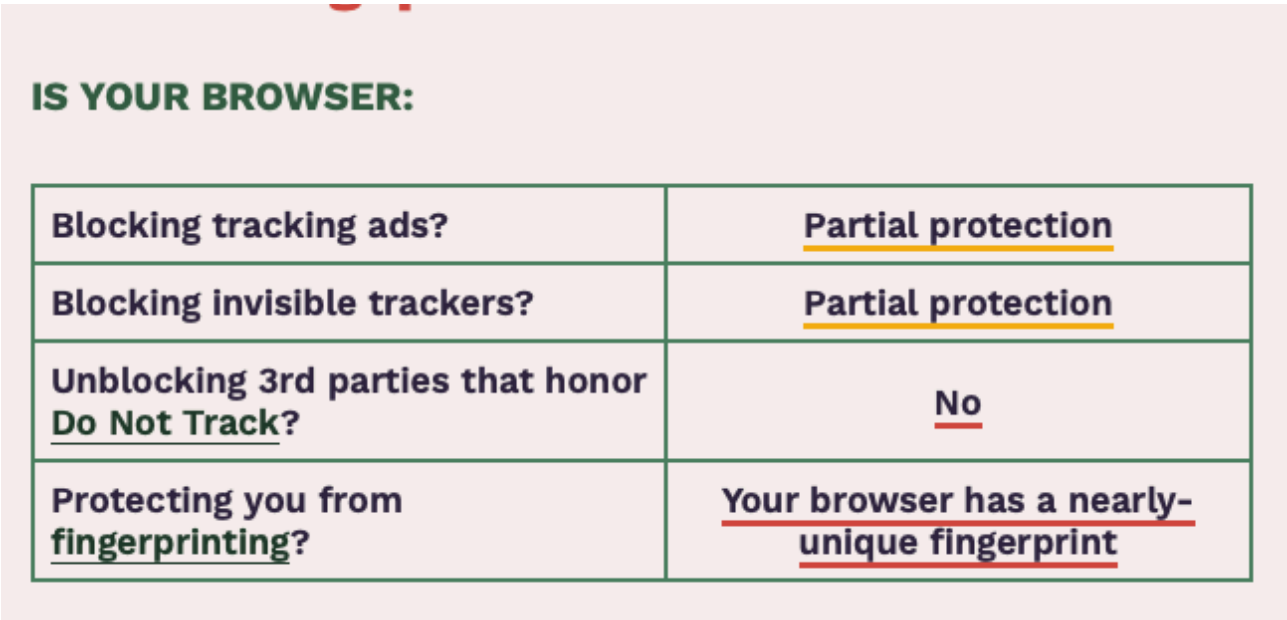
Our tests indicate that you are not protected against tracking on the Web.

IS YOUR BROWSER:

Blocking tracking ads?	**No**
Blocking invisible trackers?	**No**
Unblocking 3rd parties that honor Do Not Track?	**No**
Protecting you from fingerprinting?	**Your browser has a unique fingerprint**

Ingen, overhovedet ingen beskyttelse!!!!

iPad Safari (standard)

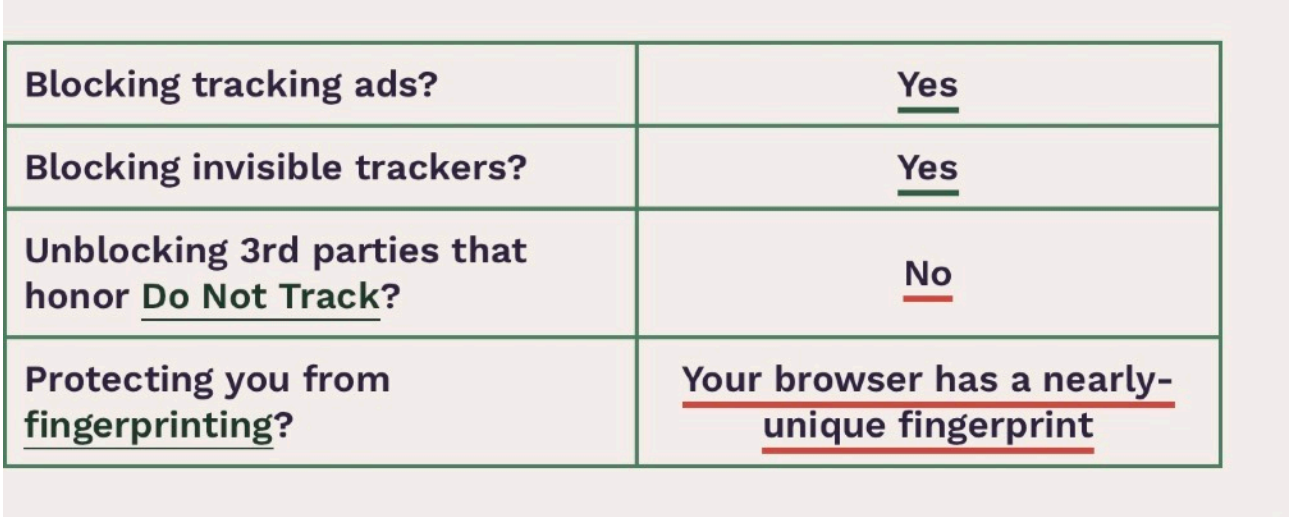


IS YOUR BROWSER:

Blocking tracking ads?	Partial protection
Blocking invisible trackers?	Partial protection
Unblocking 3rd parties that honor Do Not Track?	No
Protecting you from fingerprinting?	Your browser has a nearly-unique fingerprint

Delvis beskyttet

Safari i PRIVAT mode (se nedenfor hvordan du vælger mellem standard og privat)



Blocking tracking ads?	Yes
Blocking invisible trackers?	Yes
Unblocking 3rd parties that honor Do Not Track?	No
Protecting you from fingerprinting?	Your browser has a nearly-unique fingerprint

Temmelig godt beskyttet

Nogle vil måske sige hvorfor jeg ikke også har testet Tor Browseren og DuckDuckGo, det har jeg men syntes ikke de gav noget særligt i forhold til Safari Privat.

Blockere

Der findes naturligvis værktøjer der kan blokere for fracking. Et af dem hedder 1Blocking.
Det installerede jeg på min iPad

Safari m. 1Blocker - Privat

Our tests indicate that you have strong protection against Web tracking.

IS YOUR BROWSER:

Blocking tracking ads?	Yes
Blocking invisible trackers?	Yes
Protecting you from fingerprinting?	Partial protection

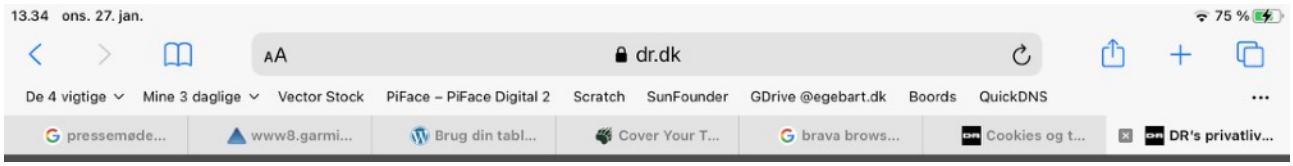
Lidt bedre end Safari Privat

Du får denne beskrivelse ved Safari

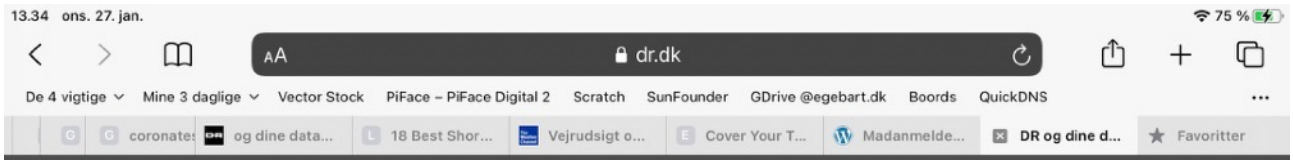
Our tests indicate that you have strong protection against Web tracking, though your software isn't checking for Do Not Track policies.

Safari - Standard - hvordan ser man det?

Det er lettest at se om dagen (hvis du har valgt at skifte dag og net ud med lys og mørk)



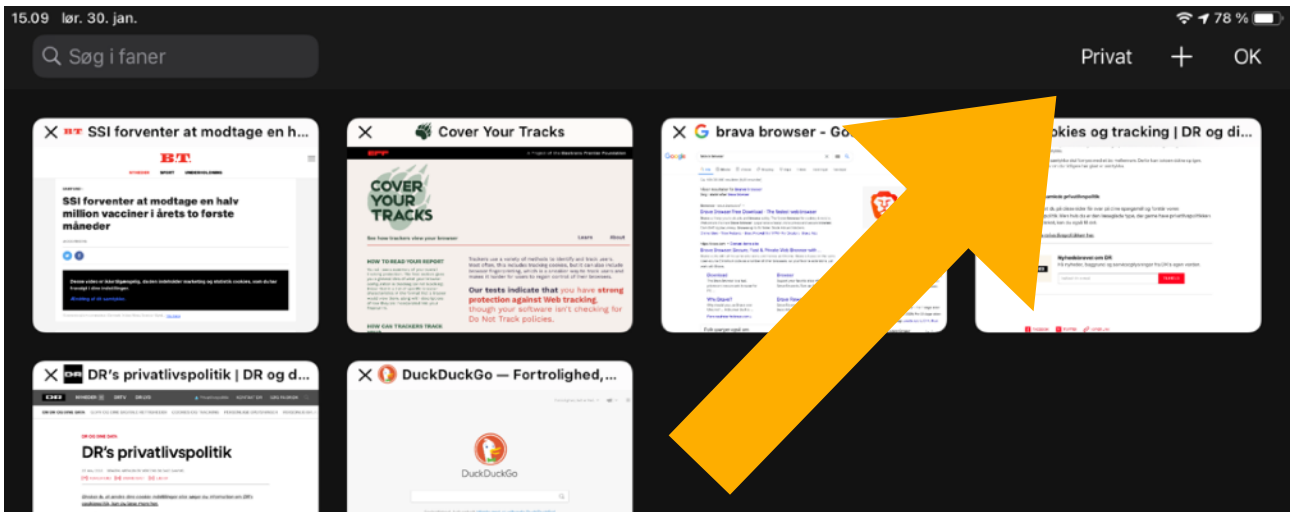
Safari - Privat - hvordan ser man det



PRIVAT - vises som sort baggrund med hvide bogstaver

Hvor vælger man mellem Standard og Privat?

Du bestemmer Standard/Privat her, klik på de 2 overlappende firkanter øverst til højre og du får dette billede:



Pilen viser at PRIVAT **ikke** er valgt

På det efterfølgende billede er PRIVAT valgt og trykker du på +'et så åbnes en privat session

Når du tester og ændre på indstillingerne i Safari, så husk at Safari skal lukkes og startes igen for at være sikker på at indstillingerne er taget med.

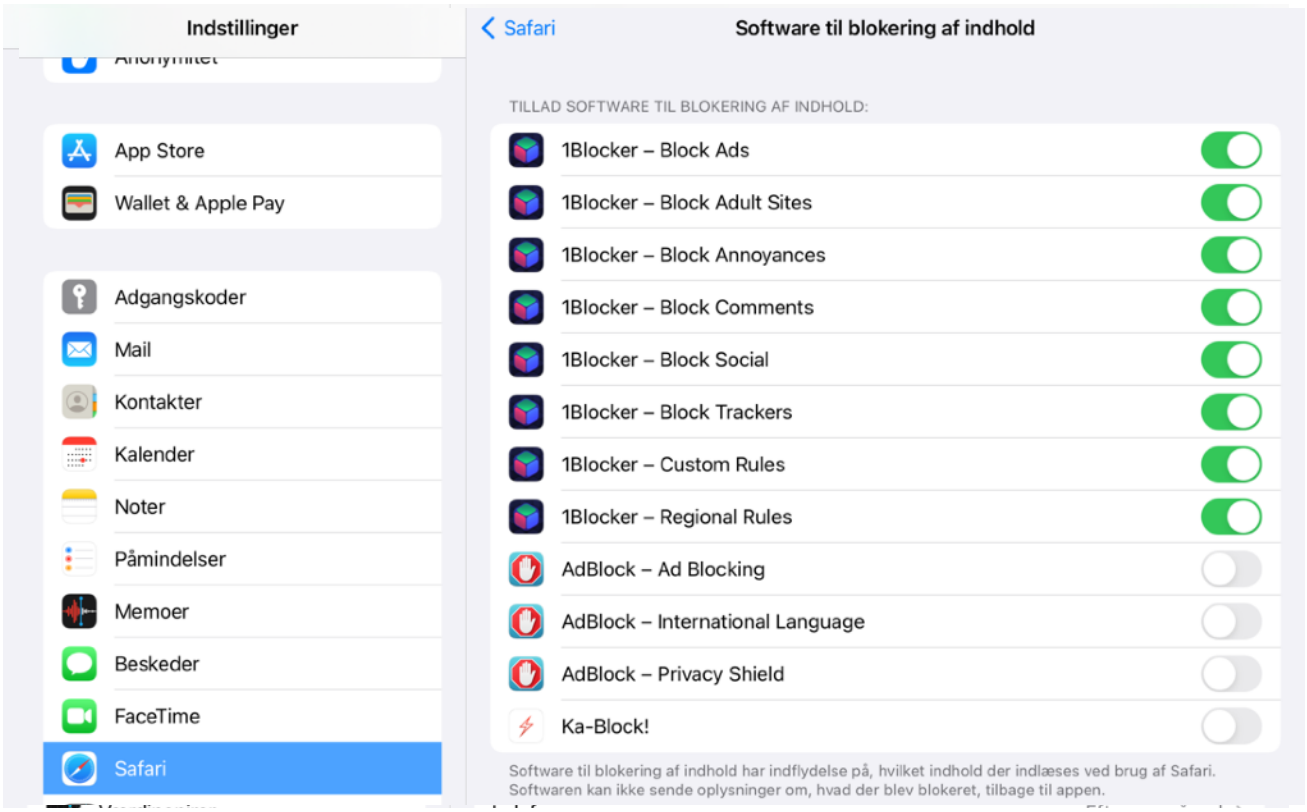
Jeg er og har været meget glad for Chrome, der kan nogle spændende ting, men efter disse test må jeg tænke mig om, det er dog helt klart at spørger du mig om hvad du skal vælge så er svaret Safari i Privat indstilling (Jeg har fjernet 1Blocker, da Safari klarer det lige så godt uden. Safari har taget nogle store skridt i 2020 for at hindre sporing, Google og annoncenetværkene er sure.

Du kan let køre nogle websteder i standard og andre i privat, men så må du lægge en strategi du følger - altid! De 2 billeder overfor vises Standard og Privat, i hvert tilfælde kan du se hvilke webster, der optræder under Standard og Privat.

Konklusion: Brug Safari PRIVAT, det er let og kræver ikke app m.m. installeret.

Kræver du mere kan 1Blocker være en mulighed

Vælg indstillinger -> Safari ->Software til blockering af indhold ->vælg indstillinger
1Blocker skal naturligvis være installeret før du kan se dette



AdBlock og Ka-Block! er blokkere jeg tidligere har afprøvet