DIGITALT SELVFORSVAR

Tag kontrol over dine data og dit digitale liv

GUIDE TIL TEENAGERE, FORÆLDRE & LÆRERE

DIGITALT SELVFORSVAR - Guide til teenagere, forældre og lærere: Tag kontrol over dine data og dit digitale liv
4. udgave 2018

Forfatter: Pernille Tranberg
Grafisk opsætning: PubliShare ApS / Spintype.com
Redaktion: Pernille Tranberg
Cover: Paws Fabrik

Indholdsfortegnelse

Kapitel 1

Hvad er privacy – og hvorfor

Hvad kan kommende arbejdsgivere se om dig, når de søger på dit navn? Eller (eks)kærester, forældre, uddannelsesinstitutioner og alle andre? Det at have nogenlunde kontrol over egne data er definitionen på digitalt privatliv eller privacy:

Retten til selv at bestemme, hvem der ved hvad om dig hvornår.

Der er mange gode grunde til at have kontrol over sine data. Den vigtigste er dit 'digitale CV' – altså det man finder om dig, når man søger på dit navn. Det skal du sørge for så vidt muligt selv at sammensætte. En anden god grund er at slippe for målrettede priser, reklamer og politiske budskaber. Og en trejde er at undgå kun at få serveret indhold, som er målrettet dig og dine digitale fodspor, så du ender i din egen lille filter-boble uden at blive udfordret med ny og overraskende viden.

Her er en guide til de bedste værktøjer til at tage kontrol over egne data. Guiden fremstiller det ideelle, så tag den som en inspiration og et skridt ad gangen. Brugervenlighed er et væsentligt kriterium, da det er den, som får mange til at droppe sikre tjenester. Så en kombi af sikkerhed/privacy og brugervenlighed er det bedste. Listen af værktøjer er ikke en blåstempling fra hverken forfatter eller sponsor, men tips til nogle værktøjer, der forsøger at beskytte vores privatliv. Teknologien

går så hurtigt, at de kan stå for noget andet i morgen, hvorfor denne guide findes opdateret digitalt på **DataEthics.eu/selvforsvar** og bliver opdateret før tryk af nye udgaver.

Hvis du vil nørde videre, er der endnu flere her;

Privacytools.io

Kapitel 2

Søgning

Alt, hvad du søger på, når du bruger værktøjer som Google og Bing trackes og gemmes om dig til senere brug. Ofte søger vi på emner, som ikke rager andre. Private søgemaskiner:

- **Startpage.com** (hollandsk)
- **Qwant.com** (fransk/tysk)
- **Findx.com** (dansk)
- **Hulbee.com** (schweizisk)
- **Duckduckgo.com** (amerikansk)

Browseren **Firefox** har også en række udvidelser, som kan bruges, hvis man vil søge på Google: fx Blur og Adnauseam, som drukner dine søgninger i en hel masse spøgelsessøgninger. Hvis du bruger Google til søgning, så log ud af Gmail først (så er trackingen ikke nødvendigvis koblet direkte op på dit navn).

Kapitel 3

Blokeringsværktøjer

Du kan forhindre andre i at følge dig fra webside til webside og indsamle viden om, hvad du interesserer dig for og evt har af problemer ved at installere nogle værktøjer – plug-ins eller udvidelser – i din browser. De *kan* give dig problemer med visse tjenester som fx din bank eller nyhedssider, men så må du have en ren browser til det. Det er godt at bruge flere browsere, da det spreder dine spor. Blokeringsværktøjerne blokerer typisk ikke for *førsteparts-cookies*, der husker passwords eller indhold i indkøbskurven, og de deler *ikke* data om dig med andre. De blokerer for *tredjepart-cookies* eller *marketing-cookies*, der deler dine data med alt og alle.

Her er nogle gode værktøjer:

- **Disconnect.me/disconnect** er rigtig god til din computer. Med den ser du stadig reklamerne (og støtter dermed fx nyhedssider, der lever af det) men den blokerer for marketing-cookies.
- **uBlock.org** til Chrome, Safari og Firefox er en god cookie-blocker, der også blokerer for reklamer.
- Appen **Adblockfast** er den bedste til dine mobile enheder. Den blokerer både for reklamer og marketing-cookies. Slås til og fra med et enkelt touch på skærmen.

- **Ghostery.com** blokerer cookies og malware og kan bruges både som plugin til browser på computere eller som browser på dine mobile enheder. Den er blevet købt af den tyske browser, **Cliqz.com**, som kan anbefales, da den beskytter dine data som standardindstilling – altså pr default.

Kapitel 4

Sikre chat og 'skype' apps

Facebook Messenger, WhatsApp og ligende er ikke sikre. Facebook Messenger anklages for at lytte med på det, der sker i rummet omkring dig, via mikrofonen, som du sandsynligvis har givet appen adgang til (tjek under indstillinger og anonymitet på iphone). Det gør nogle apps for at vide så meget som muligt om dig for bedre at sælge adgang til dig via deres reklamesystemer. Du kan finde rigtig gode alternativer, når det gælder chat- og video-apps. De bedste er;

- **Wire**.com (tysk/schweizisk) som er finansieret af bl.a. Janus Friis, der med-grundlagde Skype.
- **Signal** (US) er også fremragende – omend ikke så brugervenlig og lækker som Wire.
- **Jitsi Meet** (australsk) er baseret på open source og er et godt bud, når du skal mødes med flere på en gang i en video-konference.

Kapitel 5

VPN

Med en VPN-tjeneste har du først og fremmest sikkerhed: Den krypterer trafikken mellem din gadget og det gratis og åbne wifi, der ofte er på hoteller og cafeer, så ingen kan dermed med lethed hacke din gadget. Samtidig kan du med en VPN-tjeneste kontrollere din lokation. Det er både en fordel i forhold til din privacy; lokationsdata fortæller rigtig meget om dig, men også en fordel, hvis du vil opnå bedre priser eller fx se DR, når du er i udlandet.

Med **Opera-browseren** kan du begynde at lege med VPN. Den norske browser giver dig gratis adgang til at hoppe på servere fra tre forskellige kontinenter. Download browseren på opera.com, og gå derefter ind i indstillingerne under 'beskyttelse af personlige...' og scroll lidt ned. Her kan du aktivere VPN, så kan du lade som om, du er i et andet land. Du kan desværre ikke længere vælge land selv (det skal du købe en VPN for), men du kan altid se, hvor din ip-adresse er, på Whatismyipaddress.com.

Når du søger efter og køber en VPN-tjeneste, så vælg en, der har hovedsæde i Europa (med bedre privacy-lovgivning end Kina og USA) og efter hvilke lande, de har servere i. Rejser du meget i Italien og vil se DR, så skal tjenesten have en server i Danmark.

Der er masser af gode VPN-tjenester at vælge imellem. De

koster alle sammen penge (du er ikke produktet her - du betaler ikke med dine data) – her blot nogle bud;

- **IBVPN.com** (rumænsk) mange servere
- **Earthvpn.com** (cypriotisk) - mange servere
- **F-secure.com** (finsk)
- **Ipredator.se** (svensk)

Kapitel 6

Sikker cloud

Brug sikre cloud-tjenester fremfor fx Dropbox. Her nogle af dem:

- **Tresorit** (schweizisk)
- **Seafile** (tysk)
- **Nextcloud** (open source, oprindeligt tysk – gratis, ubegrænset, minder om Dropbox)
- **Cozy** (fransk)
- **Icloud** fra Apple (amerikansk)

Kapitel 7

Self-tracking

De fleste fitness trackere har ikke en god datapolitik og er ikke sikre, men disse to har en god datapolitik:

- **TomTom.com** (hollandsk)
- **Apple Smartwatch** (amerikansk)

De største apps, der lader dig tracke din fertilitet, er amerikanske og reguleret efter forbrugerlovgivningen dvs ikke så stramt som sundhedsdata i hænderne på læger og forsikringsselskaber. Derfor anbefales denne;

- **Clue** på helloclue.com (tysk)

Kapitel 8

FakeNameGenerator

Hvis du ønsker at bruge Facebook, Instagram, SnapChat, Musically etc til alle mulige opdateringer, der ikke har noget med dit arbejde eller din faglighed at gøre, så overvej at bruge et andet navn end dit eget og hold dit rigtige navn 'rent', indtil du skal opbygge en professionel identitet. Brug kun Facebook og Instagram i eget navn, hvis det er til dit professionelle virke. Brug dog aldrig Facebook til det, du opfatter som privat – heller ikke i et andet navn, da det kun giver en lav grad af sikkerhed. Med et andet navn, er det sværere for arbejdsgivere, uddannelsesinstitutioner, eks-kærester, identitetstyve og andre at finde dig. Brug også et alias, når du downloader rapporter, apps, spil osv., hvor de beder om dit navn, adresse, email o.lign. medmindre du har fuld tillid til servicen, eller skal betale med kreditkort og derfor skal bruge dit eget navn (der findes faktisk 'kreditkort' uden ens navn på, såkaldte gift cards, som bl.a. MasterCard udsteder). Brug kun dit eget navn på services, du har tillid til - herunder din skoles og andre offentlige tjenester - og når du optræder seriøst og professionelt. Du kan finde aliaser på **fakenamegenerator.**com.

Husk ikke at stjæle andres navne eller lade som om, du er en anden (det er de kriminelle, der gør det). Dem, du chatter med i et andet navn, skal vide, hvem du er. Det handler ikke om at

snyde andre mennesker men om at forvirre algoritmerne/maskinerne.

Når du bruger et alias, skal du huske at tilknytte en alias-email til det. Det kan du bare bruge nogle af de gratis emailtjenester til, fx Gmail og Hotmail.

Kapitel 9

Beskyt din email

Der er masser af gratis email-services, men de er ikke private. Det er en betalings-email som regel. Det kan være enten via din families teleselskab, dit webhotel eller fx en betalingsservice som;

- **Protonmail** (schweizisk)
- **Mailbox** (tysk)
- **Startmail** (hollandsk)
- **Countermail** (svensk)

De går alle op i at beskytte dine data og tracker dig ikke på samme måde, som de fleste gratis email-services gør.

Kapitel 10

Brug flere browsere

Det er godt at bruge flere browsere for at sprede dine digitale fordspor. Blandt de gængse browsere er de bedste Firefox og Safari. Firefox, fordi der er så mange gode plug-ins (udvidelser), som kan beskytte dine data. Safari, som er Apples browser, er også god, fordi den helt automatisk blokerer for tredjepart-cookies. Udover de gængse browsere har følgende tre fokus på privacy:

- **TOR browseren, torproject.org** er den absolut mest private, fordi den også skjuler din ip-adresse, men den kan godt være lidt langsom. Bedst til computer. Ikke særlig god på mobile enheder (hvor den hedder Onion).
- **Cliqz.com** (tysk) anonymiserer alle de data, trackere opsamler, og sikrer dermed, at du er anonym, når du bruger den. Den har egen søgemaskine men leder over til Google Search ved svar, som den ikke selv har.
- **Brave.com** (amerikansk) blokerer automatisk for tracking og er hurtig.

Kapitel 11

Sociale medier

De kendte sociale medier er offentlige platforme. Dvs alt hvad du laver der, kan andre end dig selv få adgang til. Nogle påstår, at du kan være privat derinde ved at sætte 'privatlivsindstillinger,' eller at billeder forsvinder. Det betyder, at du måske kan kontrollere dit sociale liv – altså hvem der umiddelbart kan se dine opdateringer, men det sociale medie selv har typisk fuld adgang til alt. Og hvis en af dine venner deler en opdatering, tager et screendump eller tagger dig på sin offentlige væg, så er din kontrol væk. Derfor; tænk altid før du poster; *ville jeg sige det i TV-Avisen?* så er du godt hjulpet på vej.

Overvej at operere med flere identiteter på sociale medier. Du behøver ikke bruge dit eget navn. Gem dit rigtige navn til du er klar til dit første job og kan begynde at opbygge en professionel identitet. Læs mere om det under 'FakeNameGenerator' og 'Professionel identitet'.

Grunden til, at du skal være påpasselig med at dele oplysninger, er, at sociale medier bruges af data-købmænd (*data brokers*) og andre til at høste data, kategorisere mennesker og sælge data videre i form af fx lister over dem, der har været ramt af kræft eller fædre til børn, der er døde i bilulykker.

De færreste forstår 'privatlivs-instillingerne' på fx Facebook, Instagram eller Musically. Prøv for eksempel selv at tjekke på

Stalkscan.com, hvor meget du kan se om folk, du ikke er venner med på Facebook. Log ind med en profil, som ikke er din egen, en vens eller en vens ven. Man kan ikke se noget, hvis man ikke er logget ind, og ens venner kan se mere end fremmede kan.

Facebook-indstillinger:

Som minimum bør du slå den funktion til på Facebook, der gør, at du skal godkende, hvis nogen tagger dig, før det ryger ud på din væg. Det finder du under indstillinger/settings og Timeline/Tagging - nederst under Review.

Under Privatliv/Privacy kan du sige nej til, at søgemaskiner kan finde din Facebook-profil samt sikre, at det kun er dig, der kan se din vennekreds (da den er offentlig som udgangspunkt og siger mere om dig, end du tror).

Stalk evt dig selv med Stalkscan og brug den til at fjerne dine mange likes på en relativ hurtig måde.

Hvis du vil slette dig fra Facebook er her et link: https://www.facebook.com/help/delete_account.

Overvej ikke at dele:

- **Helbredsoplysninger** (heller ikke, at du, din bror eller din ven er blevet helbredt for kræft) og selvfølgelig ikke dit **cpr-nummer**. Ja, helst ikke din fødselsdato, da det er guf for identitets-tyve verden over.
- **Rejseplaner** før og under rejsen. Hvis du vil dele feriefotos, så gør det efter ferien. De smarte tyve er derude, og det samme er forsikringsselskaberne, så skriv ikke på din hoveddør, at du ikke er hjemme.

- **Løbe- og cykelruter** (så man kan se, hvor du bor).
- **Billeder af børn** (de skal selv have lov til at kontrollere deres data, når de bliver store nok) - herunder dine mindre søskende.
- **Negative tanker** om andre – herunder også din (tidligere) arbejdsgiver. Brok, sladder, mobning om andre er noget, de færreste arbejdsgivere ønsker.
- **Nøgenbilleder, drukbilleder** eller andre kompromitterende billeder af dig selv og andre (det skader *dit* omdømme). Det er ulovligt at dele nøgenbilleder af folk uden deres samtykke.
- **Religiøse, politiske og seksuelle holdninger** (husk det, når du deltager i debatter med politikere på Facebook).
- **Risikoadfærd**, der kan skade dit omdømme i forhold til bl.a. banker og forsikringsselskaber.
- **Din lokation**. Hvor du er. Også på Snapchat, hvor du i dag kan se, hvor alle dine venner er, hvis de har sagt ja til at dele deres lokation med Snapchat.

Alternative sociale medier

Prøv at få dine venner med over på sociale medier, som giver dig kontrol over dine data;

- **Diaspora**
- **Mastodon**
- **Minds**
- **Ello**

Kapitel 12

Apps & indstillinger

Vær varsom når du downloader apps til din smartphone (og undgå så vidt muligt Facebook apps), hvad enten det er spil, quizzer, karriere-apps eller programmer. Tjek først hvilke data, de vil have af dig. Og spørg dig selv, om tjenesten er dine data værd.

Det ér svært at vurdere prisen på dine data, men nogle apps beder om adgang til din kalender, dine kontakter, din indbakke og din mikrofon, uden at det er nødvendigt. Måske er der et alternativ, der ikke beder om så meget? En vækkeur-app behøver vel ikke kende din lokation? Det gør din løbe-app, så det måske er ok, så længe du stoler på virksomheden, der står bag appen.

Du bør gennemgå dine indstillinger på din smartphone (på iphone; 'anonymitet'). Hvilke apps har adgang til hvilke data. Ofte har mange apps fx adgang til din mikrofon og din lokation og kan dermed optage det, du taler med andre om, eller følge din fysiske færden. Måske skulle du slå apps' adgang til mikrofon, lokation, fotos, kamera mv fra, når du ikke bruger dem? Du bør slå lokalitetstjenester fra dit kamera, for på den måde forsvinder de 'meta-data' - tid og sted - som ligger gemt i alle billeder som udgangspunkt. På en iphone kan du også overveje at slukke 'hyppige lokaliteter', som du finder under 'systemtjenester' under 'lokalitetstjenester'.

Et godt værktøj til at styre, hvem der forsøger og du vil give adgang til dit webcam og mikrofon på din Mac er Oversight, som du kan finde på objective-see.com.

Kapitel 13

Slet dine spor

Det er aldrig for sent at gå i gang med at få kontrol over sine data og slette de spor, du ikke er glad for. Noget er måske videredelt, og det kan du ikke få kontrol over, men meget ofte kan du få slettet det, du vil af med.

Første trin er at spørge sig selv, hvem har **oprindeligt** postet det? En ven, dig selv på en andens site eller en helt tredje. Du går så til originalkilden og beder om at få det fjernet. Hvis det fx er noget, du har skrevet på Instagram, så fjern det selv. Hvis du er tagget, bed vedkommende om at untagge dig, og hvis du har deltaget hidsigt i en debat på et nyhedssite, som ofte kommer højt op i søgeresultaterne, kan du bede dem om at fjerne dit navn eller i det mindste pseudonymisere det – altså bruge et andet navn end dit eget (men det rigtige så er redaktionen bekendt). Dermed forsvinder det efter kort tid, når man søger på dit navn, for Googles og andre søgemaskiners algoritmer bliver overskrevet igen og igen.

Hvis du ikke kan overtale dem (brug argumenter som *Det ødelægger mit omdømme* eller *Jeg har ret til selv at kontrollere mine data* eller *Jeg går til Datatilsynet*). **Datatilsynet** skriver faktisk, at de bør pseudonomisere dig. Det samme kan du gøre over for venner, som har delt billeder o.lign af dig uden dit samtykke (accept). Det

er ulovligt, hvis der fx er delt nøgenbilleder af dig uden dit samtykke.

På norske **slettmeg**.no eller amerikanske **justdelete**.me kan du få hjælp til at slette dig selv på forskellige hjemmesider. På **deseat**.me kan du få hjælp til at finde alle de tjenester, du har signet op med vha af Google og så slette dem.

Hos **Google** kan du få slettet søgeresultater på dit navn, hvis det er løgn eller uddateret. Find linket ved at søge på 'Delete me Google'. Det er en rettighed, vi kun har i Europa. Se også kapitel 14 om dine rettigheder.

Dit mobiltelefonnummer er offentligt pr default – så du skal selv sige det til dit teleselskab, hvis du ønsker hemmeligt nummer.

Hvis du ønsker hemmelig adresse, så gør du det på **cpr.dk,** hvor der er forskellige former for beskyttelse – herunder den såkaldte **robinsonlisten.dk** som sikrer, at ingen må ringe til dig for at sælge dig et eller andet.

Kapitel 14

Dine rettigheder

Som europæer har du en række rettigheder i forhold til dine data, som ikke findes i hverken USA eller Kina. Retten til et privatliv en menneskeret, og med den nye europæiske datalovgivning GDPR (virker fra maj 2018) har du ret til følgende;

- Få besked når dine persondata behandles.
- Få adgang til de informationer, der behandles.
- Få rettet ukorrektheder.
- Blive glemt - altså få slettet de af dine data, som tjenesten ikke skal opbevare pga en anden lov.
- Retten til portabilitet - at tage dine data med dig over til en konkurrent i et brugbart format.
- Gøre indsigelser mod dataanalyse med dine data.

Kapitel 15

Hvem kan jeg stole på?

For at finde ud af, hvem du kan stole på, så tjek følgende:

- Hvad **lever** virksomheden af? Andres data eller sælger den – for penge – et produkt eller en ydelse, som ikke er baseret på dine data? Med andre ord: Tager virksomheden ikke penge for sit produkt, er det ikke gratis, som de lover, for du er produktet – du betaler med dine eller dine venners data (såsom lokation, kontakter, beskeder mv).
- Hvor har virksomheden **hovedsæde?** Hvis den bor i Europa, skal den efterleve en strengere lovgivning end i USA og Kina.
- Kan du tydeligt se, **hvem der står bag** sitet, og hvordan man kan komme i kontakt med dem?
- Kan brugerne af sitet **interagere** med dem, der står bag sitet og med hinanden, og hvad siger de om produktet?
- Har virksomheden en **privatlivspolitik**, en datapolitik eller nogle handelsbetingelser, der er til at forstå for helt almindelige mennesker, så har den sandsynligvis tænkt godt og grundigt over, hvordan den passer på dine data.
- **Videresælger** eller -deler virksomheden data med andre, og hvem er det? Husk 'gratis' betyder betaling med dine data – ofte også til tredjeparter.

- Er virksomheden **ærlig omkring de data**, den indsamler og henter? Sammenlign det, de siger, de samler ind, med de data, som du kan regne ud, at de har brug for for at give dig den service, du efterspørger.
- Hvordan optræder virksomheden på forskellige tjenester, der **rangerer dem på privacy**, fx Ranking Digital Rights, TOSDR, TermsOfConditions, Electronic Frontier Foundation og TrustPilot. Og hvad kommer der frem om den, hvis du søger på dens navn og så persondata/privacy?
- Husk; mange virksomheder markedsfører sig som om, de er på din side. Vær varsom overfor den slags markedsføring.

Kapitel 16

Ekstra

- **Sluk wifi og bluetooth** og slå din **mikrofon og lokation fra** så ofte som muligt. Giv kun de apps, du har tillid til, adgang til din mikrofon (mange apps 'lytter med' for at indsamle viden om dig) og lokation (som kan sige lige så meget om dig som dine fingeraftryk). Sæt tape over dit webcam, da din gadget kan blive hacket, og andre kan kigge på dig fra den anden side af dit webcam.
- Brug ikke det samme kodeord på alle dine tjenester. Det er bedre at have forskellige kodeord på en lille seddel i din pung. Der skal altid være store og små bogstaver samt tal i dine kodeord. Download evt. en **password manager** (som du kan have som app på både computer og mobil), hvor du kun skal huske ét svært kodeord, og så ligger resten bag lås og slå. Vælg **1password** (canadisk) eller **Keepass** (fransk - *open source*, som er godt, fordi så kan andre se, hvordan det er udviklet).
- Vælg så vidt muligt hjemmesider, der begynder med **HTTPS** - s'et er et tegn på, at siden krypteret og dermed beskytter dine oplysninger.

- Brug **tofaktor-identifikation** hos de tjenester, du bruger, som tilbyder det, eller gør det selv med; FreeOPT eller Yubikee.

Kapitel 17

Professionel identitet

Det er vigtigt, at du er synlig digitalt. Sociale medier er gode til at dele din professionelle identitet med, dvs dit job og jobrelaterede ting, eller hvis du har en faglighed (er du fx supergod til at programmere spil?), en sportsgren etc, som du kan vise frem. Når du skal til at søge dit første job overvej derfor følgende;

Opret dig med dit rigtige navn på **LinkedIn, about.me og Twitter.**com. Sørg for et godt foto, et kort og klart resumé/bio (det er det, de fleste orker at læse) og en klar kontakt-mulighed til dig – gerne en email, som de fleste chefer bruger.

Lav din **egen hjemmeside** og find nogle faste tagord, som du bruger igen og igen, når du skriver blogs og indhold på dit site (så bliver du lettere fundet i søgninger). Det handler om at producere søgbart indhold.

Hvis du liker meget på Facebook eller tweeter meget på Twitter, så prøv at logge ind med en af de to på **applymagicsauce**.com Her kan du få en analyse af din psykologiske profil og få en ide om, hvad andre også kan finde ud af om dig. Hjemmesiden er udviklet af forskere fra Cambridge Universitet og bliver brugt af arbejdsgivere og politikere til at målrette budskaber til dig. Man kan også analysere tekster på sitet.

Husk at det er meget nemt for andre at tolke ting om dig, som du er uenig i, og har du ikke nogenlunde kontrol over dine

digitale fodspor, kan det nemmere ske. Hvis du ikke kom til den og den jobsamtale eller fik det og det studenterjob, så får du sjældent at vide, hvis det skyldes dine digitale fodspor. Så få styr på dem. Tænk bare selv, hvad du gør, når du skal undersøge noget nyt eller et menneske, du vil vide mere om.