Digitalt självförsvar

– Ta kontroll över din data och ditt digitala liv

En guide till ungdomar, föräldrar och lärare

Innehåll

Vad är integritet – och varför?

Vad kan kommande arbetsgivare läsa om dig när de gör en sökning på ditt namn på nätet? Eller föräldrar, utbildningsinstitutioner och alla andra? Att ha kontroll över den egna informationen och egna uppgifter kan ses som en definition av digitalt privatliv eller integritet.

Rätten till att själv bestämma vem som ser vad om dig och när.

Det finns många olika orsaker till varför du ska ha kontroll över dina uppgifter och din information. Den viktigaste orsaken är ditt digitala CV – alltså det man hittar om dig på nätet när man söker på ditt namn. Du ska sträva till att så långt som möjligt själv vara upphovsman till det som kan läsas om dig. En annan orsak är att slippa riktade priser, riktad reklam och politiska budskap. En tredje är att undvika att endast få innehåll som riktar sig till dig och dina digitala fotavtryck så att du hamnar i din egen lilla filterbubbla utan att bli utmanad med ny och överraskande kunskap och information. Det här är en guide för att ta kontroll över din egen information. Använd materialet som inspiration och ta ett steg i gången. Användarvänligheten är viktig när vi väljer tjänster och kan också vara anledningen till att vi lämnar en säker tjänst framför en tjänst som känns smidigare att använda. En kombination av säkerhet/integritet och användarvänlighet kan vara en bra väg att gå.

Listan på verktyg i guiden har inte någon säkerhetsstämpel från författaren men kan ses som tips på några verktyg som försöker skydda privatlivet. Teknikutvecklingen är så snabb att en webbtjänst kan stå för något helt annat i morgon och därför kommer uppdateringar av guiden att i första hand finnas digitalt på **utbildning.ax/digitalt-sjalvforsvar**

Du kan läsa mer kring integritet på **privacytools.io**

Sökning

Allt du söker på när du använder sökmotorer som Google och Bing samlas in och sparas hos respektive tjänst för att användas senare.

Exempel på privata sökmaskiner som värnar om din integritet:

- **Metager.org**
- **Startpage.com**
- **Qwant.com**
- **Hulbee.com**
- **Duckduckgo.com**
- **Searx.me**
- **Mojeek.com**

Sökmotorn Firefox har också en del tillägg som kan användas om du vill söka på Google. Ett exempel är Blur och Adnauseam som också finns som tillägg till Google Chrome. Dessa gömmer dina sökningar i en mängd spegelsökningar. Om du använder dig av Google till sökning så är ett tips att först logga ut från din Gmail (då blir sökningen inte nödvändigtvis kopplat direkt till ditt namn).

Apple Maps och Open Street Map är bättre än Google Maps när det gäller integritet.
Om du inte vill använda dig av Googles program finns det en hel del alternativ. En guide till dessa alternativ hittar du på **restoreprivacy.com/google-alternatives.**

Blockeringsverktyg

Du kan förhindra andra från att följa dig från webbsida till webbsida för att samla in information om vad du intresserar dig för och vad du har för problem, genom att installera några verktyg – plug-ins eller tillägg – i din webbläsare. De kan skapa problem när du ska använda vissa tjänster såsom bank- eller nyhetssidor, eftersom du då behöver en ren webbläsare utan tillägg. Det är bra att använda sig av flera webbläsare då det sprider dina spår. Blockeringsverktygen blockerar inte förstaparts – cookies, dvs. de som kräver lösenord och de delar inte data om dig med andra. De blockerar däremot tredjeparts-cookies eller marknadsförings-cookies som däremot delar din data med allt och alla.

Några tips på verktyg:

- **Disconnect.me** - är lämplig för din dator. Du kan se reklamen (och därmed stödja t.ex. nyhetssidor som lever på dem) men den blockerar marknadsförings-cookies.
- **uBlock.org** - för Chrome, Safari och Firefox är en bra cookie-blockerare som också blockerar reklam.
- Appen **Adblockfast** - fungerar bra till dina mobila enheter. Den blockerar både reklam och marknadsförings-cookies. Appen slås enkelt på och av med ett tryck på skärmen.
- **Ghostery.com** - blockerar cookies och skadliga program och kan användas både som plugin till browsers på din dator eller som browser på dina mobila enheter.
- **Cliqz.com** - kan rekommenderas eftersom den som standardinställning skyddar din information.

Säkra chat- och videoappar

Facebook Messenger, WhatsApp och liknande program är inte säkra. Facebook Messenger anklagas för att lyssna på det som sker i rummet omkring dig, via den mikrofon du ger appen tillgång till (kolla under Inställningar och anonymitet på Iphone). Vissa appar gör detta för att få veta så mycket som möjligt om dig så att de lättare kan skicka reklam till dig via sina reklamsystem. Det finns bra alternativ när det gäller chat- och videoappar. Några bra är:

- **Wire.com** - finansieras av bl.a. Janus Friis, medgrundare till Skype. Programmet är tyskt och Tyskland är känt för att ha en väldigt stark dataskyddslagstiftning.
- **Signal** - appen hittar du i App Store.
- **Jitsi Mee**t - jitsi.org/jitsi-meet – är baserad på öppen källkod och är ett bra val när du ska möta fler på en gång i en video-konferens.

VPN

En VPN-tjänst ger dig först och främst en säkerhet då den krypterar trafiken mellan din digitala enhet och de gratis och öppna nätverk som t.ex. finns på hotell och caféer. Det blir då svårare att hacka din enhet. Du kan också kontrollera din position med en VPN-tjänst. Det kan både vara en fördel i förhållande till ditt privatliv då positionsdata informerar en hel del om dig, men också vara en fördel när du t.ex. vill titta på program över de geografiska gränserna. Du kan alltid kontrollera var din IP-adress finns på Whatismyipaddress.com.

Om du önskar välja ett specifikt land måste du köpa en VPN-tjänst. När du söker efter och köper en sådan tjänst välj då en som finns i Europa (som har bättre integritetslagstiftning än **t.ex**. Kina och USA) och kolla vilket land de har sina servrar i.

Det finns många bra VPN-tjänster att välja mellan och de är alla betaltjänster (du är inte själva produkten – du betalar inte med din egen information):

- **IBVPN.com** - rumänsk med många servrar
- **Earthvpn.com** – cypriotisk med många servrar
- **F-secure.com** – finsk
- **Ipredator.se** – svensk

Säkra molntjänster

Använd säkra molntjänster framom t.ex. Dropbox.

EXEMPEL ÄR:

- **Tresorit.com**
- **Seafile.com**
- **Nextcloud.com**
- **Cozy.com**
- **Icloud.com**
- **Sync.com**

Samarbetsverktyg

- **CryptPad.fr** - ett franskt alternativ till Google Docs
- **Screen.io** - ett bra finskt verktyg för frågor, avstämning osv. utan inloggning
- **Meet.jit.si** - ett australiensiskt alternativ till Skype, ett video-konferensprogram som bygger på öppen källkod där du endaste behöver skapa ett namn och mötas via en internet-länk

Self-tracking – Smartklockor

De flesta smartklockor som samlar in information om dig och hur du rör dig är inte helt säkra och har oftast inte en god datapolicy. Några smartklockor är dock lite säkrare.

- **Tom Tom.com**
- **Apple Smartwatch**

Smartklockor används också till att mäta din fertilitet och de är oftast amerikanska. De är därför reglerade enligt användarlagstiftningen i landet. Det betyder att den data som samlas in inte är lika säker som den data som forskare och läkare samlar in. En app som kan rekommenderas är den tyska Clue på **helloclue.com.**

FakeNameGenerator

Om du vill använda dig av Facebook, Instagram, SnapChat osv. till olika inlägg och som inte har med ditt arbete eller din kompetens att göra så kan du fundera på om det skulle vara bättre att använda ett annat namn än ditt eget och hålla ditt riktiga namn 'rent' tills du bygger upp en yrkesidentitet. Använd Facebook och Instagram i ditt eget namn om det hör till ditt yrke. Se då till att inte posta något på Facebook som du uppfattar som privat – inte ens i ett annat namn då det skapar en lägre grad av säkerhet. Genom att använda ett fingerat namn är det svårare för arbetsgivare, utbildningsinstitutioner, identitetstjuvar och andra att hitta dig.

Använd också ett alias när du laddar ner rapporter, appar, spel osv. där namn, adress, e-post och liknande krävs ifall du inte fullständigt litar på utgivaren eller om du ska betala med kreditkort och därför måste använda ditt eget namn. Använd ditt eget namn när du använder service som du litar på – t.ex. din skolas eller offentliga tjänster -och när du ska synas seriöst och professionellt. Du hittar alias på **fakenamegenerator.com.**

Du ska inte ta någon annans namn eller bygga en identitet som om du vore en annan eftersom det är en kriminell handling. De du chattar med i annat namn bör veta vem du är. Det handlar inte om att lura andra människor utan att förvirra algoritmerna/datorerna.

När du använder ett alias ska du komma ihåg att knyta ett alias-mejl till det. Det kan du använda någon av gratistjänsterna Gmail och Hotmail till.

Skydda din epost

Det finns en mängd gratis epost-program med de är inte privata. Det är däremot i regel de som man måste betala för. Dessa kan antingen gå via ett telebolag, ett webbhotell eller exempelvis en betalservice som:

- **Protonmail.com**
- **Mailbox.org**
- **Startmail.com**
- **Countermail.com**

De har alla som mål att skydda din data och samlar inte in information om dig på samma sätt som gratis epost-program gör.

Använd flera webbläsare

Det kan vara bra att använda dig av flera webbläsare för att sprida dina digitala fotspår. Firefox och Safari är två webbläsare som fungerar bra. Firefox för att den har så många insticksprogram (plug-ins) som kan skydda din data och Safari, som är Apples webbläsare, för att den helt automatiskt blockerar tredjeparts-cookies. Utöver dessa två finns även andra webbläsare som har fokus på integritet:

- **Torproject.org** - är den mest privata då den också skyddar din IP-adress men den kan också vara lite långsam. Den fungerar bäst för datorer och inte så bra till mobila enheter (då heter den Onion)
- **Cliqz.com** - anonymiserar all den data som samlas in om dig och därför är du anonym när du använder den. Den har en egen sökmotor som leder över till Google Sök för svar som den själv inte kan ge
- **Brave.com** - blockerar automatiskt spårning och är dessutom snabb

Sociala medier

De mest kända sociala medierna är offentliga plattformar. Det vill säga allt som du lägger upp kan även andra få åtgång till. Några påstår att du kan vara privat även på dessa genom att ändra i inställningarna eller genom att inte göra bilderna synliga. Det betyder att du kanske kan kontrollera ditt sociala liv – alltså vem som omedelbart kan se dina inlägg – men plattformarna i sig har full tillgång till all din data. Om en av dina vänner delar ett inlägg, tar en skärmdump eller taggar dig på en offentlig sida är din kontroll borta.

Överväg ifall du ska agera med flera identiteter på sociala medier. Du behöver inte använda ditt eget namn. Ge ditt riktiga namn när du har fått ditt första jobb och kan bygga upp en yrkesidentitet. Kolla närmare i kapitlet FakeNameGenerator och Professionell identitet.

Anledningen till att du ska vara försiktig med att dela upplysningar om dig själv är att sociala medier används av marknadsföringsföretag (data brokers) för att lagra data, kategorisera människor och sälja data vidare till andra. Det kan t.o.m. handla om listor på personer som fått cancer eller föräldrar till barn som dött i bilolyckor.

”Integritets-inställningarna” på t.ex. Facebook, Instagram och Tik Tok är inte helt enkla att förstå sig på. Försök t.ex. själv att kolla på Stalkscan.com hur mycket du kan se om folk du inte är vän med på Facebook. Logga in med en profil som inte är din egen, din väns eller väns vän. Du kan inte se något om du inte är inloggad men dina vänner kan se mer än vad en främmande profil kan se.

Facebook-inställningar

Som ett minimum ska du slå på den funktion på Facebook som gör att du måste godkänna om någon ska kunna tagga dig eftersom det i annat fall automatiskt dyker upp på din vägg. Du hittar funktionen under inställningar/settings och Timeline/Tagging längst ner under Review.

Under Integritet/Privacy kan du tacka nej till att sökmaskiner kan hitta din Facebook profil och samtidigt försäkra dig om att det är endast du som kan se din vänkrets (den är offentlig som standardinställning och säger mer om dig än du tror).
Följ dig själv med Stalkscan och använd den till att ta bort dina många ”gilla/likes” på ett ganska snabbt sätt. Om du vill avsluta ditt Facebook-konto kan du göra det via den här länken **facebook.com/help/delete_account**

FUNDERA PÅ OM DU FAKTISKT SKA DELA FÖLJANDE

- **Hälsoinformation** (inte heller att du, din bror eller din vän blivit botad från cancer) och naturligtvis inte ditt personsignum och inte heller din födelsetid då det är av stort värde för identitetstjuvar.
- **Resplaner** före och under resan. Om du delar semesterbilder gör det då efter semestern. Det finns smarta tjuvar liksom försäkringsbolag så skriv inte på din ytterdörr att du inte är hemma.
- **Löpnings- och cykelturer** – så att man se var du bor
- **Bilder på barn** – de ska själv ha möjlighet att kontrollera sin data när de blir tillräckligt stora. Det gäller även minderåriga syskon
- **Naken- och fylleribilder** eller andra kompromettерande bilder på dig och andra (det skadar ditt omdöme). Det är olagligt att dela nakenbilder på folk utan deras samtycket

- **Religiösa, politiska och sexuella åsikter** (kom ihåg det när du deltar i debatter med politiker på Facebook)
- **Riskbeteende** som kan skada ditt omdöme i förhållande till bland annat banker och försäkringsbolag
- **Din position** – där du är, också på Snapchat där du idag kan se var alla dina vänner befinner sig ifall de sagt ja till att dela position med Snapchat

Alternativa sociala medier

Testa att få med dina vänner till sociala medier som ger dig kontrollen över din data:

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

Appar och inställningar

Var försiktig när du laddar ner appar till din telefon (och undvik så långt som möjligt Facebook-appar), oavsett om det är spel, quizz, karriär-appar eller program. Kolla först vilken data de vill ha av dig och fråga dig själv om tjänsten är värd din data.

Det är svårt att värdera priset på sina egna uppgifter men vissa appar begär åtkomst till din kalender, dina kontakter och din mikrofon utan att det är nödvändigt. En väckarklocks-app behöver väl inte känna till din geografiska position? Men det behöver en motions-app, vilket kanske är ok så länge du litar på den leverantör som står bakom appen.

Du behöver gå igenom inställningarna på din telefon (i Iphone: anonymitet). Vilka appar har tillgång till vilken data. Ofta har appar tillgång till din mikrofon och din position och kan då spela in det du pratar om med andra eller följa hur du rör dig. Kolla om du kan stänga av apparnas tillgång till mikrofon, position, foton, kamera osv. när du inte använder dem. Du behöver också stänga av positionstjänsterna från din kamera om du vill att den meta-data (tid och plats) som ligger gömd i bilderna ska tas bort. I Iphone kan du också överväga att stänga ”signifikanta platser” som finns under platstjänster/systemtjänster.

Ett verktyg som är bra för att se vem som försöker använda din webkamera och mic utan ditt tillstånd på din Mac är Oversight som du hittar på **objective-see.com/products/oversight.html**

Sopa igen dina spår

Det är aldrig försent att försöka få kontroll över din data och sopa igen de spår du vill bli av med. Vissa data kan ha spridits vidare och det kan du inte få kontroll över men väldigt ofta kan du radera det du vill bli av med.

Ett första steg är att fråga sig själv vem som ursprungligen lagt upp informationen om dig. En vän, du själv på någon annans site eller kanske någon helt annan. Du kan då gå till originalkällan och be dem ta bort informationen. Om det t.ex. är något du har skrivit på Instagram så kan du ta bort det själv. Om du blivit taggad i ett inlägg kan du begära att den som gjort det tar bort taggningen. Och om du hetsigt deltagit i en debatt på en nyhetssida som ofta hamnar högt upp i sökningsresultaten kan du be dem att ta bort ditt namn eller åtminstone pseudonymisera det – alltså använda annat namn än ditt eget (men ditt riktiga namn är känt inom redaktionen). På så sätt försvinner det efter en kort tid när man söker på ditt namn eftersom Googles och andra sökmaskiners algoritmer kommer att skrivas över gång på gång.

På Datainspektionen på Åland **di.ax**, hittar du information om vilken typ av uppgifter som inte får lämnas ut. Och när du vänder dig till någon och begär att de ska radera dina uppgifter så kan du använda dem som argument. Det samma kan du göra med dina vänner som har lagt upp bilder och liknande utan din tillåtelse. Det är olagligt att t.ex. lägga upp nakenbilder på dig utan ditt samtycke.

På norska slettmeg.no eller amerikanska justdelete.me kan du få hjälp med att radera dina uppgifter från en mängd olika webbsidor. På deseat.me kan du hitta alla de tjänster som du har loggat in på med hjälp av Google och hur du kan radera dem.

På Google kan du radera sökresultat med ditt namn om det är sammankopplat med en direkt lögn eller om uppgiften är föråldrad. Du hittar webbplatser genom att söka på ”Delete me Google”. Det är en rättighet som endast vi i Europa har. Du kan läsa mer i avsnittet om dina rättigheter. Ditt telefonnummer är automatiskt offentligt och du måste själv meddela ditt telefonbolag om du önskar hålla det hemligt.

Dina rättigheter

- Som europeisk medborgare har du en mängd rättigheter när det gäller din data och som varken finns t.ex. i USA eller i Kina. Rätten till privatliv är en mänsklig rättighet och med det nya dataskyddsdirektivet GDPR har du rätt till följande:

- få information om när din persondata behandlas
- få tillgång till den information som behandlas
- få felaktig information rättad
- bli glömd – alltså få de delar av din information raderad som ifrågavarande tjänst inte har rätt att lagra med stöd av lagstiftning
- portabilitet – att ta med din information till konkurrerande data-tjänster i ett användbart format
- göra invändningar mot dataanalys som baseras på din information

Vem kan jag lita på

Punkterna nedan kan vara till hjälp när du vill veta vem du kan lita på:

- Vad lever webbtjänsten av? Andras data eller försäljning av dem för pengar eller en produkt eller en tjänst som inte är baserat på din data? Med andra ord – om tjänsten inte tar betalt för sin produkt är den inte gratis så som den lovar. Då är det du som är produkten – du betalar med dina eller dina vänners data (såsom position, kontakter, inlägg osv).
- Var finns tjänstens huvudkontor? Om den är i Europa ska den följa en strängare lagstiftning än t.ex. i USA och Kina.
- Kan du tydligt se vem som är ansvarig för webbtjänsten och hur du kan komma i kontakt med dem?
- Kan webbtjänstens användare interagera med dem som är ansvariga och med varandra och vad säger de om produkten?
- Har verksamheten en integritetspolicy, en datapolicy eller några affärsvillkor, som vanliga människor kan förstå, har de förmodligen grundligt övervägt lagringen av din data.
- Säljer eller delar webbtjänsten data med andra och vilka är dessa i så fall? Kom ihåg att ”gratis” innebär betalning med din egen information – till och med till tredje part.
- Är webbtjänsten ärlig gällande den data de samlar in om dig? Jämför vad de säger att de samlar in med de data som du tror att de behöver för att ge dig den service du frågar efter.

- Hur syns webbtjänsten på olika tjänster som rankar dem enligt policy och regler, ex Ranking Digital Rights, TermsOfConditions, Electronic Frontier Foundation och TrustPilot. Och vad kommer fram om webbtjänsten när du söker på dess namn och person-data/integritet?
- Kom ihåg att många webbtjänster marknadsför sig som om de är på din sida. Var på din vakt för sådan typ av marknadsföring

Yrkesidentitet

Det är viktigt att du också är synlig digitalt. Sociala medier är bra för att visa din yrkesidentitet med, dvs. ditt arbete och arbetsrelaterade saker eller om du har en kompetens (du är t.ex. jättebra på att programmera) eller en sport osv som du vill visa upp. När du söker ditt första jobb bör du därför överväga följande:

Uppträd med ditt riktiga namn på LinkedIn, about.me och Twitter.com. Se till att du lagt upp ett bra foto på dig och en kort biografi samt tydlig information om hur du kan kontaktas – gärna en epost-adress.

Skapa din egen webbsida och hitta några återkommande ord som du använder om och om igen när du skriver bloggposter och innehåll på webbplatsen (då hittas du lättare genom en sökning). Det handlar om att skapa ett sökbart innehåll som du vill visa utåt.

Om du ofta gillar saker på Facebook och Twitter, testa då att logga in med en av dem på **applymagicsauce.com**. Här kan du få en analys av din psykologiska profil och få en idé om vad andra också kan hitta om dig. Webbsidan är utvecklad av forskare vid Cambridge University och används av arbetsgivare och politiker för att rikta meddelanden till dig. Man kan också analysera texter på webbsidan.

Kom ihåg att det är väldigt lätt för andra att tolka saker om dig som du är oenig med och om du inte har någorlunda kontroll över dina digitala fotspår kan du lätt bli feltolkad. Om du inte fick komma till den och den arbetsintervjun eller inte fick det och det studentjobbet så får du sällan veta om det beror på dina digitala fotspår. Tänk bara själv hur du gör när du ska undersöka något nytt eller försöka få reda på mer om en person.

Övrigt

- Stäng wifi, bluetooth, mikrofon och position så ofta som möjligt. Ge endast de appar du litar på tillgång till din mikrofon (många appar ”lyssnar på dig” för att samla in information om dig) och din position/plats (som kan säga lika mycket om dig som dina fingeravtryck). Tejpa för din webbkamera eftersom den kan bli hackad och andra kan titta på dig.
- Använd inte samma lösenord på alla dina tjänster. Det är t.o.m. bättre att ha olika lösenord på en liten lapp i din väska. Lösenordet ska alltid innehålla både stora och små bokstäver och tal/specialtecken. Ladda eventuellt ner en password manager (som du kan ha som app både på din dator och i din telefon) med vilken du kan samla dina olika lösenord. Om du använder en sådan app behöver du endast komma ihåg ett svårt lösenord och de övriga finns oåtkomliga för andra personer. Välj iPpassword eller Keepass (open sorce, vilket är bra då andra kan se hur tjänsten är utvecklad).
- Välj så långt som möjligt webbsidor som börjar med https – s:et berättar att sidan är krypterad och skyddar därför din information
- Använd tvåfaktor-identifiering på de tjänster du använder och som erbjuder detta eller gör det själv. Sådana tjänster är t.ex. FreeOpt, Yubiko och LastPass

Om du har tips om bra och säkra tjänster eller om förbättrings-
förslag till guiden är du välkommen att rikta dem till

carola.eklund@regeringen.ax


Ålands
landskapsregering