

12-stepsprogram för digital frihet

1. Byt webbläsare - **enkel**
2. Byt sökmotor - **enkel**
3. Säkra kalender och kontakter - **enkel**
4. Installera F-Droid (Android) - **enkel**
5. Byt ut YouTube mot NewPipe - **enkel via andriod**
6. Flytta dina anteckningar - **enkel**
7. Skaffa en integritetssäker lösenordshanterare - **medelsvår/kritisk**
8. Avveckla Meta-plattformarna - **medelsvår (social utmaning)**
9. Lämna Microsofts ekosystem - **medelsvår**
10. Byt till en säker e-postleverantör och öppen källkodsklient - **medelsvår**
11. Skydda din nätverkstrafik - **Avancerat**
12. Ta steget till Linux - **Avancerat**

Gör dig fri från stängda tjänster!

Det här 12-stepsprogrammet är för dig som vill återta kontrollen över ditt digitala liv och bli fri från beroendet av proprietära tjänster. Genom att genomföra hela – eller bara valda delar av – programmet gör du en stor insats för din personliga integritet, din datasuveränitet och den öppna, demokratiska utvecklingen på internet.

Varje steg bort från övervakningskapitalismen är en vinst för din digitala frihet.

Det första steget är att erkänna att du har ett problem; det andra är att tro på att det går att lösa.

1. Byt webbläsare

Nivå: **Mycket enkelt**

Webbläsaren är din dörr ut mot internet. De flesta standardval som Google Chrome och Microsoft Edge är utformade för att samla in data om ditt beteende, dina sökningar och dina besökta webbplatser. Att byta webbläsare är det enklaste och mest effektiva första steget mot en mer privat digital vardag.

Generella tips & rekommendationer

- **Byt till ett integritetsfokuserat alternativ:**
 - **Firefox:** Det mest etablerade alternativet med öppen källkod. Drivs av en icke-vinstdrivande stiftelse, har stor anpassningsförmåga och sätter användarens integritet i första rummet. Med ett Firefox-konto kan du dessutom enkelt synkronisera och interagera mellan dina olika enheter (dator, mobil och surfplatta) för att komma åt flikar, bokmärken och historik överallt.
 - **Brave:** Ett smidigt och snabbt alternativ som blockerar spårare, skript och reklam automatiskt direkt vid installation utan att kräva några krångliga inställningar.
 - **(Ladybird:** Ett lovande framtidshopp. Det är en helt ny, oberoende webbläsarmotor byggd helt från grunden. Den är ännu inte släppt som färdig webbläsare för dagligt bruk, men är ett projekt att hålla ögonen på framöver.)
- **Gör det gradvis:** Du behöver inte ta bort din gamla webbläsare direkt. Installera det nya alternativet, importera dina bokmärken automatiskt vid första starten och använd den parallellt under några dagar.
- **Sätt som standard:** När du känner dig bekväm ställer du in den nya webbläsaren som standard på både datorn och telefonen.
- **Aktivera spårningsskydd:** Gå in i inställningarna på din nya webbläsare och se till att skyddet mot spårare och kakor (cookies) från tredje part är aktiverat.

2. Byt sökmotor

Nivå: **Mycket enkelt**

När du söker på nätet kartlägger traditionella sökmotorer dina intressen, din position och ditt sökbeteende för att skapa en profil av dig i kommersiellt syfte. Att byta sökmotor är ett snabbt steg för att söka information utan att övervakas.

Generella tips & rekommendationer

- **Välj ett privat alternativ:**

- **[Björknets SearXNG](#):** En metasökmotor baserad på öppen källkod. Den samlar resultat från flera olika sökmotorer helt utan att spåra dig, lagra din IP-adress eller skapa en profileringsbild.
- **[DuckDuckGo](#):** Ett av de mest kända alternativen för privat sökning. Det levererar bra resultat direkt utan att spara din sökhistorik eller spåra dig mellan webbplatser.

- **Gör den till din standard:** Ställ in den valda sökmotorn som standard i adressfältet i din webbläsare, så söker du privat varje gång du skriver in en sökfråga.

- **Instruktioner och hjälp:**

- För information om hur du ställer in och använder SearXNG som din standardsökmotor, se [Björknets dokumentation om SearXNG](#).

3. Säkra kalender och kontakter

Nivå: Enkelt

Dina kontakter och din kalender innehåller känslig information om ditt privatliv, dina relationer och dina dagliga rutiner. När dessa lagras hos stora molntjänster som Google eller Apple utnyttjas datan för profilering och kartläggning. Genom att flytta dessa till en öppen plattform behåller du den smidiga synkroniseringen mellan dina enheter, men utan övervakningen.

Synkronisering kräver DAVx5 i mobilen, vilket kan köpas för en låg engångssumma.

Generella tips & rekommendationer

- **Välj ett öppet molnalternativ:**

- **Nextcloud:** Kör en egen molninstans eller anslut till [Björknets Nextcloud-instans](#) för att hantera kalendrar (CalDAV) och kontakter (CardDAV) säkert.

- **Instruktioner och hjälp:** Se [Björknets dokumentation om Nextcloud](#) för guider kring inställningar och synkronisering.

4. Installera F-Droid (Android)

Nivå: **Enkelt**

Google Play Butik kräver ett Google-konto och är fylld med appar som innehåller dolda spårare, reklam och stängd källkod. [F-Droid](#) är en alternativ appbutik för Android som enbart innehåller appar med fri och öppen källkod (FOSS). Apparna granskas noggrant för att säkerställa att de inte spårar dig eller kränker din integritet.

Generella tips & rekommendationer

- **Ladda ner från officiella källan:** Gå till f-droid.org i din mobilwebbläsare och ladda ner installationfilen (.apk).
- **Tillåt installation från okända källor:** Moderna Android-telefoner blockerar automatiskt installationer utanför Google Play av säkerhetsskäl. När du öppnar den nedladdade filen kommer systemet att be dig om tillåtelse:
 - Tryck på **Inställningar** i rutan som kommer upp.
 - Aktivera valet **Tillåt från denna källa** (för den webbläsare eller filhanterare du använde).
 - Gå tillbaka och genomför installationen.
- **Använd F-Droid som din primära appbutik:** Sök efter öppna alternativ i F-Droid innan du vänder dig till vanliga appbutiker. Många populära verktyg för integritet finns enbart här eller fungerar bäst via denna version.

5. Byt ut YouTube mot NewPipe

Nivå: **Enkelt (via F-Droid)**

När du använder den vanliga YouTube-appen loggas din tittarhistorik, dina pausningar och dina sökningar för att bygga en detaljerad profil av dina intressen och vanor. Dessutom avbryts uppspelningen regelbundet av riktad reklam. Med en öppen tredjepartsapp kan du ta del av innehållet på YouTube helt utan konto, spårning eller avbrott.

Generella tips & rekommendationer

- **Välj en öppen app för Android:**
 - **NewPipe:** Den mest etablerade lösningen med öppen källkod. Den spelar upp alla videor från YouTube utan reklam, tillåter bakgrundsuppspelning (så att du kan lyssna med släckt skärm) och stöder nedladdning av både video och ljud lokalt på telefonen.
 - **LibreTube:** Ett modernt alternativ baserat på Piped-nätverket. Det fungerar ungefär som NewPipe men har ett annat gränssnitt och låter dig synkronisera dina prenumerationer över flera

enheter utan ett Google-konto.

- **Flytta med dina prenumerationer:** Du behöver inte börja om från början. Exportera enkelt dina kanalprenumerationer från YouTube (via Google Takeout) och importera filen direkt i NewPipe eller LibreTube.
- **Fungerar helt utan Google-konto:** Apparna kräver ingen inloggning. Dina prenumerationer och bokmärken sparas enbart lokalt på din egen enhet.
- **Hämta via F-Droid:** Du hittar båda apparna enkelt genom att söka i F-Droid-butiken.

6. Flytta dina anteckningar

Nivå: Enkelt

Innehållet i dina anteckningar är ofta mycket personligt och kan innehålla allt från idéer och dagböcker till känsliga listor. Kommersiella anteckningsappar som Google Keep eller Apple Notes lagrar dina textfiler på servrar där operatören eller tredjepart har full insyn. Genom att byta till verktyg i öppen källkod skyddar du dina tankar med kryptering och behåller kontrollen över din data.

Generella tips & rekommendationer

- **Välj ett öppet alternativ:**
 - **Nextcloud Notes:** Ett enkelt och smidigt verktyg för dig som vill ha synkroniserade anteckningar direkt i ditt Nextcloud-konto. Du kommer åt tjänsten genom att logga in på [Björknets Nextcloud-instans](#). Det har dedikerade mobilappar och stödjer standardiserad textformatering (Markdown).
 - **Joplin:** Ett mer avancerat, fristående alternativ i öppen källkod med total totalsträckskryptering (end-to-end encryption). Du hittar appen och mer information på [Joplin](#). Joplin stödjer allt från enkla kom-ihåg-listor till strukturerade anteckningsböcker och kan synkas tryggt via [Björknets](#) eller din egen Nextcloud-instans eller andra lagringstjänster.
- **Exportera din gamla data:** De flesta tjänster låter dig ta ut dina befintliga anteckningar som textfiler eller Markdown-filer så att du enkelt kan importera dem i ditt nya verktyg.
- **Format i ren text:** Genom att använda öppna format som Markdown riskerar du aldrig att bli fastlåst i en leverantörs egna, stängda format framöver.

7. Skaffa en integritetssäker lösenordshanterare

Nivå: **Medelsvår / Kritiskt**

Att återanvända samma lösenord på flera ställen eller spara dem oskyddade i webbläsaren utgör en stor säkerhetsrisk. Om en tjänst läcker dina uppgifter kommer alla dina konton i farozonen. En dedikerad lösenordshanterare sparar dina inloggningar i ett krypterat valv som bara du kommer åt med ett enda huvudlösenord.

Generella tips & rekommendationer

- **Välj ett öppet och säkert alternativ:**
 - **[Björknets Vaultwarden-instans](#):** Ett lättviktigt alternativ byggt i öppen källkod och helt kompatibelt med alla Bitwarden-appar. Om du har ett befintligt konto loggar du in direkt via [Björknets Vaultwarden-instans](#). Vill du skapa ett nytt konto skickar du först en [ansökan om kontoregistrering](#) för att öppna tjänsten för registrering.
 - **[Bitwarden](#):** Ett av de mest uppskattade verktygen med öppen källkod för konsumenter. Det fungerar sömlöst på alla plattformar och har en välbeprövad säkerhetsarkitektur.
- **Skapa ett starkt huvudlösenord:** Välj en unik lösenordsfras bestående av flera slumpmässiga ord som du kan komma ihåg. Det är det enda lösenordet du behöver lägga på minnet framöver.
- **Separat två faktorsauktoriseringsapp:** Det är kritiskt att använda separat app för tvåfaktorsautentisering för inlogging på lösenordshanterare. Så du inte riskerar intrång eller bli utelåst.
- **Använd webbläsartillägg och mobilappar:** Installera appen på din telefon och tillägget i din webbläsare så fylls dina lösenord i automatiskt när du loggar in på webbplatser.
- **Nollställ och generera nytt:** Sluta hitta på egna lösenord. Låt lösenordshanteraren generera långa, unika och slumpmässiga lösenord för varje ny eller befintlig tjänst.
- **Hjälp med välja och hantera lösenord:** [Björknets Lösenordsguide](#).

8. Avveckla Meta-plattformarna

Nivå: **Medelsvår (social utmaning)**

Metas affärsmodell bygger helt på storskalig övervakning och profilering. Genom Facebook, Instagram och Messenger samlar de in data om dina kontakter, dina intressen, din position och dina kommunikationsmönster. Den största tröskeln för att lämna dessa plattformar är sällan teknisk, utan handlar om att flytta dina sociala kontakter till bättre alternativ.

Generella tips & rekommendationer

- **Ersätt med säkra och öppna alternativ:**
 - **Signal:** Den mest användarvänliga och säkra appen för direktmeddelanden och samtal. Den har inbyggd totalsträckskryptering (end-to-end) som standard och samlar minimalt med metadata.
 - **Matrix (t.ex. via Element):** Ett öppet och decentraliserat nätverk för meddelanden, gruppchattar och samtal. Det fungerar på liknande sätt som Discord eller Slack, men utan att en enskild aktör äger din data.
 - **Mastodon:** Ett decentraliserat och öppet alternativ till plattformar som X (Twitter) och Facebook. Det är en del av det så kallade *Fediversum*, där ingen enskild kommersiell aktör styr nätverket, och där du slipper algoritmdrivna flöden och reklam.
- **Flytta över dina kontakter i steg:**
 - Sätt upp din nya profil på Signal, Matrix eller Mastodon.
 - Uppdatera din status eller skicka ett sista meddelande på Meta-plattformarna där du förklarar hur man når dig framöver.
 - Ladda ner en kopia av din historik och dina bildarkiv via inställningarna på Facebook/Instagram innan du stänger kontona.
- **Börja med att inaktivera:** Om det känns för definitivt att radera kontona direkt kan du börja med att avinstallera apparna från telefonen eller inaktivera kontona under en period.

9. Lämna Microsofts ekosystem

Nivå: **Medelsvår**

Microsoft 365, OneDrive och Teams samlar in stora mängder telemetri och användardata. Dessutom kan plattformslåsningen göra det svårt att flytta dina dokument. Genom att ersätta dessa med lokala program och integritetsfokuserade molntjänster behåller du full kontroll över dina filer och din kommunikation.

Öppna alternativ och var de finns

Helhetssviter & Samarbetsplattformar (Ersättare för Microsoft 365 / Teams)

- **Twake Workplace:** En europeisk, öppen molnsvit utvecklad av Linagora som samlar chatt (Matrix-baserad), dokument, e-post, kalender och lagring i ett och samma ekosystem.
 - *Tillgänglighet:* Körs direkt via webbläsaren, som skrivbordsapp för Linux, Windows, macOS samt via mobilappar i App Store och Google Play / F-Droid. Kan även köras på egen server.
- **CryptPad:** En webbaserad, totalsträckskrypterad (end-to-end) kontorssvit för samarbete i realtid i webbläsaren. Den täcker allt från dokument och kalkylark till Kanban-tavlor.
 - *Tillgänglighet:* Körs direkt i valfri webbläsare via öppna instanser (t.ex. cryptpad.fr) eller egen drift.

Kontorsprogram (Ersättare för Word, Excel, PowerPoint)

- **LibreOffice:** Den mest etablerade och kompletta öppna kontorssviten för lokal användning.
 - *Tillgänglighet:* Finns för Linux, Windows och macOS. På Linux installeras det smidigast via **Flathub** eller distributörens pakethanterare.
- **ONLYOFFICE Desktop Editors:** Ett öppet alternativ med ett gränssnitt som påminner om Microsoft Office och som har hög kompatibilitet med `.docx`, `.xlsx` och `.pptx`.
 - *Tillgänglighet:* Finns för Linux, Windows och macOS. Installeras på Linux direkt via **Flathub** eller tillverkarens webbplats.

Kommunikationsverktyg (Ersättare för Microsoft Teams)

- **Mattermost:** En öppen plattform för lagchatt, fildelning och projektkommunikation som fungerar utmärkt som ersättare för Teams eller Slack.
 - *Tillgänglighet:* Serverdelen körs på egen hårdvara/cloud, och skrivbordsklienten finns för Linux, Windows och macOS (på Linux via **Flathub** eller direkt nedladdning).
- **Element / Matrix:** Ett öppet och federerat nätverk för krypterad text-, röst- och videokommunikation.
 - *Tillgänglighet:* Klienten Element finns för Android, iOS, Windows, macOS och Linux (via **Flathub**).

Generella tips för övergången

- **Byt filformat:** Börja spara och exportera dokument i öppna standardformat som `.odt` och `.ods` i stället för Microsofts proprietära format.
- **Separera lagringen:** Ersätt OneDrive med t.ex. Nextcloud eller Twake Drive för att synkronisera dina filer säkert mellan dina enheter.

10. Byt till en säker e-postleverantör och öppenkällkodsklient

Nivå: **Medelsvår**

Flytta din primära kommunikation från Gmail eller Outlook till en leverantör med fokus på integritet och öppen källkod, till exempel **Strato**, **ProtonMail** eller **Tuta**. Du kan också välja en öppenkällkods e-postklient för att visa dina e-post i så som Thunderbird eller Nextcloud.

Eposthantering finns i [Björknets Nextcloud-instans](#).

Säkra e-postleverantörer

- **Proton Mail:** En av de mest populära integritetstjänsterna i öppen källkod. Inkluderar automatisk totalsträckskryptering (end-to-end), kalender och molnlagring.
- **Tuta (tidigare Tutanota):** En tysk e-posttjänst helt i öppen källkod som krypterar alla data, inklusive ämnesrader och kontakter. Finns tillgänglig direkt via F-Droid utan Google-beroenden.
- **Strato / Egen domän:** Ett bra alternativ för dig som vill ha traditionell IMAP/SMTP via europeisk värdtjänst och driva e-post under din egen domän.

Öppna e-postklienter

Att använda en lokal klient ger dig full kontroll över dina meddelanden och minskar beroendet av stängda webbgränssnitt.

- **Mozilla Thunderbird:** Den mest etablerade e-postklienten i öppen källkod.
 - *Tillgänglighet:* Finns för Linux, Windows och macOS. På Linux installeras den smidigast via [Flathub](#).
- **Nextcloud Mail:** En e-postapp direkt i webbläsaren för dig som kör Nextcloud.
 - *Tillgänglighet:* Finns inbyggd i [Björknets Nextcloud-instans](#). Gör det enkelt att samla e-post, filer och kalendrar i samma gränssnitt.
- **FairEmail / K-9 Mail (Android):** Öppna och kraftfulla e-postappar för Android.
 - *Tillgänglighet:* Installeras enkelt via [F-Droid](#).

Tips för övergången

- **Vidarebefordra gammal post:** Sätt upp en automatisk vidarebefordran från din gamla Gmail/Outlook till din nya adress under en övergångsperiod.
- **Uppdatera dina inloggningar:** Byt kontaktadress i dina viktigaste tjänster (som bank, myndigheter och lösenordshanterare) i första hand.

11. Skydda din nätverkstrafik

Nivå: **Avancerat**

När du surfar utan skydd kan din internetleverantör (ISP), lokala nätverksägare (som öppna Wi-Fi-nät) och tredjeparter se vilka domäner du ansluter till och kartlägga din trafik. Genom att skicka din trafik genom en krypterad tunnel med det moderna protokollet WireGuard döljer du din IP-adress, skyddar dina data från avlyssning och säkrar dina interna anslutningar.

Alternativ för VPN-skydd

1. Anonymisera internettrafik (Kommersiella VPN-tjänster)

Det här alternativet är bäst för maximal anonymitet, men gör uppkopplingen långsam. Det är ett enkelt sätt att ha VPN för det är bara betala och använda. Om målet är att dölja din IP-adress och kryptera all utående internettrafik:

- **Mullvad VPN:** Svensk tjänst med starkt fokus på integritet. Kräver ingen e-postadress för att skapa konto, sparar inga loggar och applikationen är helt i öppen källkod.
- **IVPN / Proton VPN:** Andra oberoende leverantörer med öppen källkod i sina appar, stöd för WireGuard och granskade no-log-policys.

2. Egen slutnod

Detta alternativet kräver lite terminalhantering. Men är det snabbaste och stabilaste sättet att köra VPN. Då kan du också ha statisk IP som fungerar som en postbox. Varje gång du går in på en sida syns samma IP, vilket för att t.ex. inloggningar fungerar stabilare. Du kan använda egen slutnod:

- **VPS (Virtuell Server):** Att hyra en VPS (gärna i Sverige) är betydligt enklare och stabilare än att köra på egen hårdvara hemma, då du slipper hantera dynamisk IP, portöppningar i hemroutern och strömavbrott.
- **Egen hårdvara hemma:** Vill du nå dina lokala filer och enheter direkt i hemmanätverket kan du köra en server lokalt.
- **Verktyg:** Mjukvaror som [PiVPN](#) eller [Wg-Easy](#) förenklar installationen av en egen WireGuard-instans på t.ex. en Raspberry Pi.

Klienter och verktyg

- **WireGuard Officiella App:** Finns för Linux, Windows, macOS, Android och iOS. Konfigureras enkelt med en `.conf`-fil eller QR-kod.
- **F-Droid:** Både WireGuard, Tailscale och NetBird finns tillgängliga som öppna appar via F-Droid för Android

Koppla ihop dina egna enheter (Mesh-VPN)

Detta Om du vill nå dina egna enheter (t.ex. telefonen och hemmaservern/Nextcloud) säkert utan att öppna portar i routern eller exponera dem mot internet:

- **Tailscale / Headscale:**
 - **Tailscale:** Det enklaste sättet att skapa ett privat nätverk (ett så kallat *tailnet*). Det bygger på WireGuard och kräver ingen krånglig nätverkskonfiguration.

- **Headscale:** En helt öppen, självvärdad kontrollserver för dig som vill använda Tailscale-klienterna men köra hela infrastrukturen på egen server.
- **NetBird:** Ett helt öppet (FOSS) Mesh-VPN baserat på WireGuard. Det erbjuder samma smidiga hopkoppling av enheter som Tailscale, men där både klient och central servermjukvara är öppen källkod från start.

Tips för bästa skydd

- **Aktivera Kill Switch:** Se till att din VPN-klient stoppar all internettrafik automatiskt om anslutningen kopplas bort.
- **Kolla efter DNS-läckor:** Kontrollera att din enhet inte skickar DNS-frågor utanför den krypterade tunneln via sidor som dnsleaktest.com.

12. Ta steget till Linux

Nivå: **Avancerat**

Genom att ersätta Windows eller macOS med Linux tar du det sista steget för att helt lämna telemetri, övervakning och plattformslåsningar bakom dig. Du får ett operativsystem där du har full kontroll över din egen enhet, dina data och dina uppdateringar. Linux är faktiskt ganska lätt att installera. Du laddar ner en isofil, brännner den på t.ex. en usbsticka, startar datorn från usbstickan och följer installationsguiden. Som är enkel om du väljer t.ex. Linux Mint eller PopOS.

Fördelar i korthet

- **Integritet & Kontroll:** Ingen spårning, ingen inbyggd reklam och inga påtvingade uppdateringar.
- **Säkerhet:** Byggt på en säker grundarkitektur med minskad risk för skadlig kod.
- **Prestanda & Livslängd:** Drar mindre resurser och gör att äldre datorer fungerar som nya igen.
- **Enkelhet i vardagen:** När systemet väl är installerat fungerar det i praktiken som vilket operativsystem som helst. Uppdateringar av både system och appar sker smidigt med ett enda klick.

Kom i gång med Björknets guide

För en grundläggande förståelse för operativsystemet rekommenderas guiden [Introduktion till Linux](#). Som handlar om bland annat:

- **Vad Linux är:** Hur Linux-kärnan (kernel) fungerar och utgör grunden i systemet.
- **Öppen källkod och fri mjukvara:** Hur filosofin kring öppen källkod (Open Source) ger hög säkerhet, stabilitet och modularitet jämfört med proprietära system.
- **Användningsområden:** Hur Linux används i allt från servrar och inbäddade system till vanliga skrivbordsdatorer och mobiler.

“ *Integritet handlar inte om att gömma saker; det handlar om att skydda de saker som gör oss mänskliga.* ”

Moxie Marlinspike (Grundare av den öppna och krypterade meddelandeappen Signal)

Björknet - Infrastruktur på mänskliga villkor



Revision #25

Created 2026-07-12 21:24:10 UTC by Samuel

Updated 2026-07-22 11:54:49 UTC by Samuel