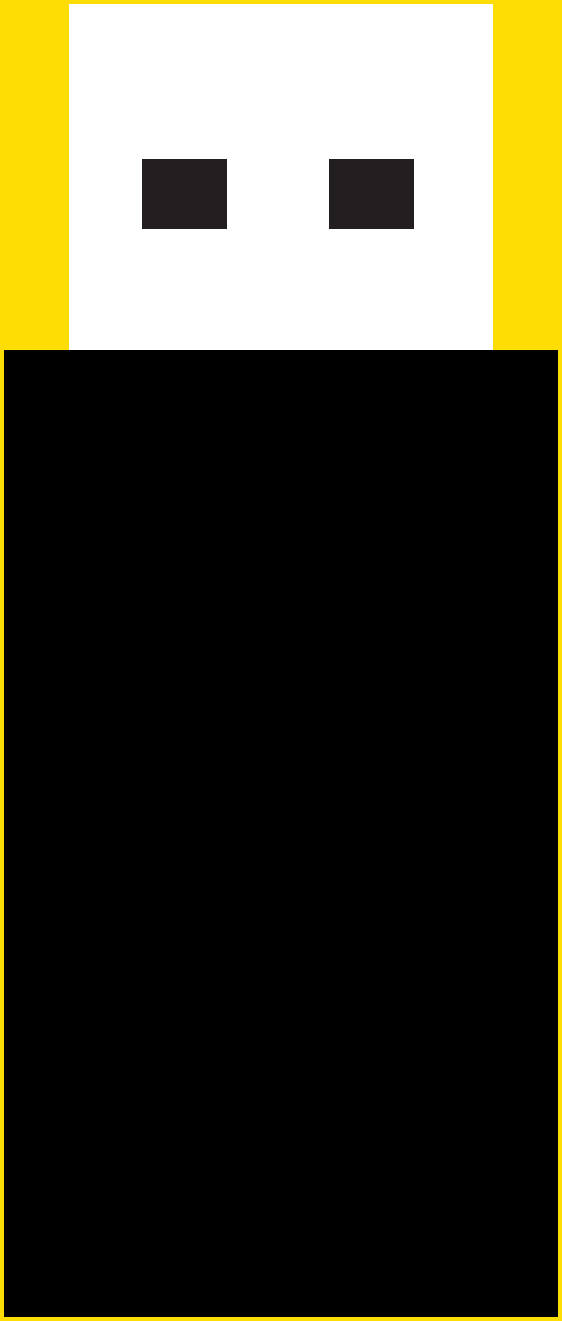
Internetguide #41

Kom igång med Tails!

Ett säkrare operativsystem



Anders Thoresson

I den här guiden lär du dig...

- ☑ Vad operativsystemet Tails är
- ☑ Hur Tails hänger ihop med anonymiseringsverktyget Tor
- ☑ Hur du installerar Tails
- ☑ Att använda Tails

Innehåll

1. Därför behöver du Tails

Att vara anonym på internet är svårt. Vi lämnar hela tiden massor av små digitala fotspår efter oss. De kommer i form av ip-adresser, cookies, webbläsaravtryck[1] och annat som vi normalt sett inte tänker på. Eller ens känner till.

I Internetguiden *Kom igång med Tor*! visar vi hur anonymiseringsverktyget Tor kan användas för att minska en del av de här riskerna, bland annat genom att på ett säkert sätt tillfälligt ”låna” en ip-adress som inte går att spåra. Tor kan också användas för att kringgå eventuell nätcensur, där vissa webbplatser eller visst innehåll på webbplatser är blockerat.

Tor är inte svårt att komma igång med. Men det finns också några egenheter som gör det lätt att tro att Tor ger anonymitet i situationer när så inte är fallet. I grundutförande krävs att den speciella webbläsaren Tor Browser används. Använder du din vanliga webbläsare utan att ändra i inställningarna kommer du att avslöja din faktiska ip-adress även efter det att du har installerat Tor. Inte heller är *annan* internettrafik än webben skyddad med Tor om du inte ändrar i din dators inställningar så att den skickar *all* internettrafik via Tor.

Vid sidan av de tekniska aspekterna finns också de rent mänskliga. Med två webbläsare i datorn, din vanliga i kombination med Tor Browser, är det lätt att välja fel. Du tänker kanske att du ska vara anonym men är inte uppmärksam på att det är Firefox och inte Tor Browser som du för tillfället använder.

Tails är ett operativsystem som bland annat adresserar båda de här problemen. Om du använder Tails skickas all internettrafik till och från din dator via Tor. Och eftersom Tails är ett operativsystem som är helt skilt från ditt vanliga operativsystem behöver du starta om din dator när du ska vara anonym och då använda ett gränssnitt som rent visuellt skiljer sig från hur datorn normalt ser ut. Konsekvensen av detta är att du måste fatta tydligare beslut om när du ska vara anonym och när du inte behöver vara det, du får visuella ledtrådar om att du använder datorn i anonymt läge och du minskar riskerna för att begå misstag som röjer vem du är.

Tails – med säkerhet och anonymitet i fokus

Att Tails är ett operativsystem som är helt skilt från din vanliga dator kräver en utförligare förklaring.

Ett operativsystem är den mest grundläggande programvaran i en dator. Den utgör länken mellan hårdvaran, de fysiska delar som datorn är konstruerad av, och alla de program användaren installerar. Vanliga operativsystem är Windows, OS X och Linux. Tails är en Linux-variant.

Tips! Tor och Tails och personliga nätkonton

Varje gång du loggar in på ett konto på en av nätets alla tjänster riskerar du att röja din identitet. Även om Tor och Tails ger dig en lånad ip-adress går den ändå att koppla till dig om du till exempel använder den för att logga in på ditt eget Gmail-konto.

Ett sätt att hantera den situationen är att skapa ett separat Gmail-konto, med ett konto-namn som inte avslöjar vem du är, när du använder Tails. Det kontot loggar du sedan aldrig in på igen om du inte använder Tails.

Det normala är att operativsystemet installeras på datorns inbyggda hårddisk och startar när strömmen slås på. Men det går också att koppla in en extern hårddisk eller ett usb-minne med ett annat operativsystem och tala om för datorn att den ska starta det operativsystemet i stället.

Det är den här möjligheten som Tails utnyttjar. Tails installeras inte på datorns inbyggda hårddisk, utan på ett usb-minne[2].

Det här är en lösning som ger fler fördelar än dem vi redan gått igenom ovan. Tack vare den här konstruktionen lämnar Tails inga spår efter sig på den dator där operativsystemet används. Du stänger av strömmen, stoppar i ditt usb-minne, startar datorn, gör det du ska i anonymt läge, stänger av datorn, plockar ut usb-minnet, startar den igen, nu med datorns vanliga operativsystem som finns på hårddisken. Och när datorn återigen är igång finns inga spår efter Tails på den.

Det här innebär bland annat att Tails ger ett extra skydd i situationer där det räcker att ha programvara för kryptering installerad i sin dator för att bli misstänkliggjord. Datorn kan användas som vanligt, medan usb-minnet med Tails hålls gömt. Det innebär också att det tillfälligt går att låna en dator, använda Tails en stund och sedan lämna tillbaka datorn till ägaren i ursprungsskick.

Tips! Installera inga egna program!

Det går att installera egna program i Tails. Men undvik att göra det. Du vet inte vilka säkerhetshål programmen har. Inte heller är det sannolikt att de skickar sin trafik via Tor om du inte ställer in dem att göra det.

Program som du installerar själv riskerar alltså att orsaka precis den typ av risker som du vill undvika genom att använda Tails.

Men det är inte bara datorn som lämnas utan spår efter att du använt Tails. Tails i sig återställs också i ursprungsskick varje gång du stänger av datorn. Därmed finns inga loggar sparade som visar vilka webbplatser du besökt, vilka nätverk du varit ansluten till, vilka chattmeddelanden eller vilken e-post du skickat.

Detta är en grundinställning som gör att den som eventuellt kommer över ditt usb-minne inte kan se vad du har använt Tails till. Å andra sidan innebär det också att Tails blir lite bökigare att använda än ditt vanliga operativsystem. Du måste exempelvis ansluta till ditt trådlösa nätverk på nytt, varje gång du startar Tails.

Det går därför att aktivera funktioner som sparar olika typer av inställningar och användardata. Om det är en bra idé för dig att göra det beror helt och hållet på i vilka sammanhang du använder Tails. Ibland är det kanske bäst att låta inställningarna vara som de är, att knappa in det trådlösa nätverkets lösenord varje gång och använda ett nätbaserat verktyg för e-post och ordbehandling. Andra gånger är det kanske tillräckligt säkert att låta Tails spara dina inställningar och dokument på usb-stickan och därmed göra ”Tails-datorn” lite mer lättanvänd.

Det här kan du göra med Tails

Eftersom ett operativsystem bara ger en dator de allra mest basala funktionerna krävs ett antal program för att kunna använda den till något nyttigt. Förinstallerat i Tails finns:

- Webbläsaren Tor Browser för att surfa på nätet.
- E-postprogrammet Icedove, i kombination med OpenPGP för kryptering.
- Program för krypterad chatt, för att skapa och hantera säkra lösenord, för att kryptera filer och för att använda Bitcoin.
- Ordbehandlare, kalkylblad och presentationer i kontorspaketet LibreOffice.
- Program för att jobba med bilder, ljud och video.

Kort sagt finns program för normal datoranvändning. Det är tekniskt möjligt att installera egna program om de som finns inte täcker behoven. Men det är en stark rekommendation att inte göra det. Programmen som följer med Tails är kontrollerade ur ett säkerhetsperspektiv, medan du inte känner till vilka eventuella luckor som finns i de program du själv skulle installera. Programmen som följer med Tails är dessutom inställda att skicka all sin trafik via Tor, medan program som du installerar själv sannolikt inte kommunicerar via Tor och därmed heller inte ger dig den anonymitet som Tor erbjuder.

2. Några säkerhets-aspekter att vara uppmärksam på

Det finns ytterligare några säkerhetsaspekter som påverkar Tails och som är viktiga att känna till.

Osäker hårdvara

Tails ger inget skydd mot eventuella manipulationer av den fysiska dator som du använder. Det innebär till exempel att om någon installerat en så kallad keylogger, en hårdvara som spelar in alla tangentbordstryckningar som görs, så kommer allt du skriver att samlas in.

I situationer där du använder en dator som du inte riktigt vågar lita på har Tails en lösning på åtminstone keylogger-problemet. Ett av programmen som finns i Tails är ett så kallat virtuellt tangentbord. Det dyker upp på skärmen och används genom att peka och klicka med musen. Så länge du inte använder tangentbordet spelar det ingen roll att någon spelar in det som skrivs på det.

Tors konstruktion

Anonymiseringsverktyget Tor ger inte hundraprocentig anonymitet. Många av de risker som är förknippade med Tor spiller över på Tails. Det handlar bland annat om risken att en så kallad exitnod i Tor, den dator som du lånar ip-adressen av, avlyssnar din internettrafik. Av den anledningen är det viktigt att se till att de tjänster du använder när du vill vara anonym krypterar trafiken. Logga till exempel inte in på en webbaserad e-posttjänst om den inte stödjer HTTPS. HTTPS krypterar till skillnad från HTTP de data som din webbläsare skickar och tar emot.

Tips! Lär dig mer om Tor

I Internetguiden *Kom igång med Tor!* kan du lära dig mer om hur Tor fungerar och vilka fallgropar som är förknippade med anonymiseringsverktyget.

Ta certifikatvarningar på allvar

Kopplat till HTTPS och krypterad webbtrafik finns ett behov av att ta så kallade certifikatvarningar på allvar. Du har säkert sett rutorna som ibland dyker upp när du besöker en webbplats och som i mer eller mindre svårbegripliga formuleringar varnar för att det finns tecken på att allt inte står rätt till hos webbplatsen i fråga. Det handlar ibland om att de certifikat som används för att kryptera trafiken är manipulerade av någon i syfte att avlyssna trafiken.

Om en sådan certifikatvarning dyker upp, ta den på allvar och fortsätt inte ändå! På Tails webbplats konstateras att den anonymitet som Tor ger gör det svårt att rikta den här typen av attacker mot utvalda individer. Å andra sidan finns det möjligheter att försöka angripa Tor- och Tailsanvändare på bred front med den här metoden.

Tails har ett eget ”fingeravtryck”

Den som är duktig på att analysera nätverkstrafik kan sannolikt se *att* du använder Tails. Det innebär att exempelvis en it-tekniker hos den internetleverantör du använder eller hos det företag du tillfälligt lånar en internetuppkoppling av kan se att du använder Tails. Det innebär däremot *inte* att de kan se vilken information du skickar och tar emot. Detta eftersom Tor ser till att trafiken är krypterad.

Tekniker hos de webbplatser du besöker har också möjlighet att se att du använder Tails. Däremot har de ingen möjlighet att veta vem du är, så länge du inte gör saker på webbplatsen – som att logga in på ett eget konto – som avslöjar dig.

Din e-post och dina dokument är inte krypterade

De data du skapar när du använder Tails, exempelvis den e-post du skickar och tar emot eller de dokument du skriver, är inte krypterade i utgångsläget. Däremot finns det program i Tails för att aktivera kryptering. Om du vill lära dig mer om krypterad e-post kan du läsa Internetguiden *Kom igång med PGP!*.

Metadata finns kvar i dina dokument

De filer du skapar, texter, bilder, ljud och så vidare, innehåller vad som kallas för metadata. Det här är information *om* dina dokument. I bildfiler kan det till exempel vara koordinater som visar var i världen bilden är tagen. I textdokument kan det finnas information om vem som skapat och vilka som redigerat dokumentet.

Tips! Fler varningar

Besök gärna varningssidan på Tails webbplats för att läsa en uppdaterad och mer utförlig lista med varningar: https://tails.boum.org/doc/about/warning

Det här är information som riskerar att avslöja känsliga uppgifter. Det gäller dokument som du arbetar med i Tails precis som i vilket annat operativsystem som helst.

Det finns dock sätt att ta bort sådana metadata. Med Tails kommer ett program som heter MAT, *Metadata anonymisation toolkit*[3].

Användarschabbel

Som vi redan konstaterat ger Tails och Tor ett bra tekniskt skydd. Men det kan raseras om du använder tekniken på ett oförsiktigt sätt, som att logga in på ditt personliga Facebook-konto. När du använder Tails och Tor för att vara anonym, gör då inte saker som avslöjar vem du är!

Uppdatera!

Precis som all annan mjukvara innehåller Tails buggar. Och i det här fallet är det extra viktigt att se till att de åtgärdas. Tails kommer därför i nya versioner ungefär var sjätte vecka. När du får ett meddelande om att en ny version finns tillgänglig, se till att installera den så fort som möjligt!

3. Så installerar du Tails

Tips! Mer detaljerade installationsinstruktioner

I den här guiden håller vi instruktionerna för hur du skapar ett usb-minne med Tails översiktliga. En mer detaljerad instruktion finns på Tails webbplats: https://tails.boum.org/install. Här finns instruktioner för båda installationsalternativen – från befintlig Tails-sticka eller från nedladdad fil – och hur processen ser ut beroende på om du har en Windows-, Mac- eller Linux-dator.

Om du bestämt dig för att börja använda Tails finns det två olika sätt att skaffa operativsystemet. Antingen hittar du en vän eller kollega som du litar på och som redan använder Tails. Då kan du göra en kopia av hens usb-minne. Annars surfar du till Tails webbplats och laddar ner operativsystemet därifrån.

Oavsett vilket alternativ du väljer blir slutresultatet detsamma: Ett usb-minne med Tails som du kan använda när du startar din dator.

Från en annan sticka

Att skapa ett usb-minne med Tails genom att skapa en kopia av ett annat är den enklaste metoden. Starta Tails genom att stoppa i usb-minnet i din dator och starta om den. Hur du får datorn att välja Tails i stället för operativsystemet som finns på hårddisken beror på vem som tillverkat datorn.

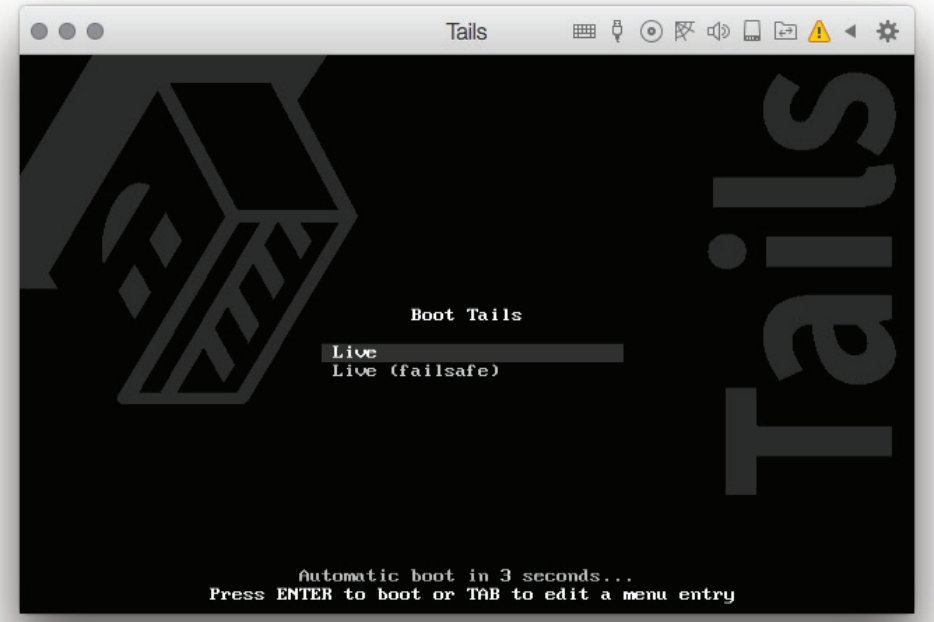
Är det en dator med Windows eller Linux som operativsystem är det ofta bara en tangenttryckning som krävs under datorns uppstart. De vanligaste alternativen är Esc, F10, F11 eller F12.

Fungerar inte någon av de knapparna får du leta upp datorns handbok och se om du kan hitta instruktioner där för hur datorn ska startas från ett usb-minne. Leta efter begrepp som ”boot menu”, ”boot from external drive” eller ”boot from removable device” [4].

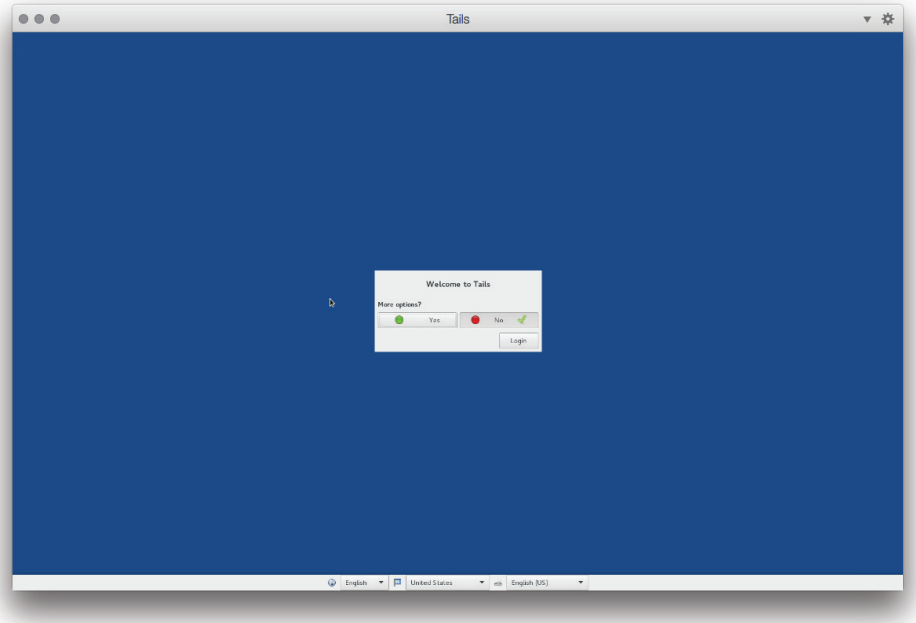
Har du en Mac är det enklare: Där ska du trycka ner den knapp som heter *Option* eller *Alt* medan datorn startar. Då kommer det upp en meny på skärmen där du får välja om datorn ska använda operativsystemet på hårddisken eller operativsystemet på usb-minnet.

Härifrån ser processen ut på samma sätt, oavsett vilken dator du har.

Efter en liten stund ska den första av två Tails-menyer dyka upp. Den heter *Boot Tails* och ger dig två alternativ: *Live* eller *Live (failsafe)*. Det senare tar man till om det första inte fungerar, så välj *Live*.



Efter en kort stund dyker nästa Tails-meny upp. Den heter *Tails Greeter* och är grafisk, till skillnad från *Boot Tails*, med ikoner, knappar och en muspekare som du kan röra.



Tips! Tails i en annan dator

Om du läser installationsinstruktionerna på Tails webbplats upptäcker du kanske att det är möjligt att köra Tails inifrån ditt vanliga operativsystem. Det innebär att Tails startar som ett vanligt program i din Windows- eller Mac. Som en dator i en dator. Om du inte är helt säker på hur en sådan installation fungerar är det bäst att undvika den, då det finns en del fallgropar du riskerar att trilla ned i.

I dialogrutan mitt på skärmen står det *Welcome to Tails*. Under den rubriken finns frågorna *Use persistence?* och *More options? No* är förvalt. Vi kommer senare att gå igenom de alternativ som finns, men nu är *No* rätt.

Längst ned på skärmen finns menyer för att ändra språk, tangentbordslayout och tidszon. Dem kan du lämna som de är den här gången. I den fortsatta texten refererar vi till vad de olika menyalternativen heter på engelska.

Efter att ha klickat på *Login* dyker snart Tails skrivbord upp. Tails är nu igång på din dator.

Om du har möjlighet att ansluta din dator till internet är det en bra idé att göra det nu. Tails kommer då att kontrollera om det finns en nyare version av operativsystemet. Om så är fallet kommer du att få en fråga om du vill installera den. Svara då ja på frågan, så att den kopia du skapar verkligen är den senaste versionen av Tails.

Om du har tillgång till en nätverkssladd kan du koppla in den. Annars hittar du en pilformad ikon i skärmens övre högra hörn. Klickar du på den öppnas en meny där du bland annat hittar en genväg till inställningarna för trådlösa nätverk.

När du är säker på att du har den senaste versionen av Tails på usb-minnet är det dags att skapa en kopia av det. Stoppa in usb-minnet som ska bli din Tails-sticka. Observera att allt som finns lagrat på den kommer att raderas, så välj ett usb-minne som *inte* innehåller saker som du vill spara! Klicka sedan på *Applications* i övre vänstra hörnet för att öppna programmenyn. Välj sedan *Tails* och starta *Tails Installer*.

Upp kommer då en ruta med tre alternativ. Du ska välja det översta, *Install by cloning*. Efter att ha klickat på den stora knappen väljer du ditt usb-minne som *Target Device* i dialogrutan som dyker upp. Därefter klickar du på *Install Tails*.

När processen är klar stänger du av datorn och tar ut det ursprungliga usb-minnet men låter din egen kopia sitta kvar i datorn. Därefter startar du datorn igen och trycker även denna gång på knappen som låter dig välja att datorn ska starta från usb-minnet i stället för från hårddisken.

Gör sedan om valen i de två menyerna *Boot Tails* och *Tails Greeter*. Om allt har gått som det ska startar nu Tails, men från din egen Tails-sticka!

Från nedladdad fil

Har du inte någon bekant som använder Tails får du i stället ladda ner Tails från webbplatsen och göra installationsprocessen helt på egen hand. Du kan också testa den här metoden om du inte lyckas skapa en fungerande kopia av en annan sticka. Det blir då en två-stegsraket: Först kommer du att skapa en tillfällig sticka, och sedan den färdiga.

Om du använder en dator med Windows surfar du till https://tails.boum.org/install/win/usb för att få de detaljerade instruktionerna. Använder du Mac väljer du i stället https://tails.boum.org/install/mac/usb.

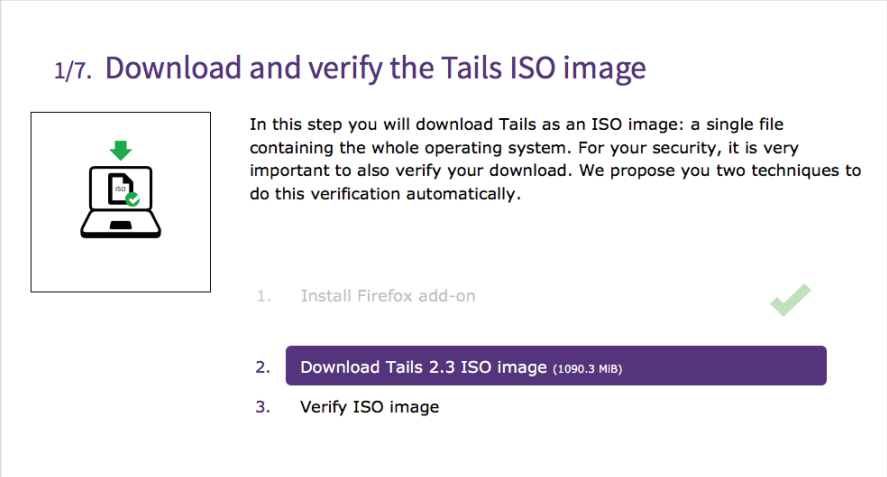
Tips! Därför behöver du verifiera den nedladdade filen

När du installerar genom att först hämta hem operativsystemet från Tails webbplats är det viktigt att du använder webbläsartillägget till Firefox. Det hittar du också på Tails webbplats. Tillägget verifierar att filen som du laddar hem är korrekt.

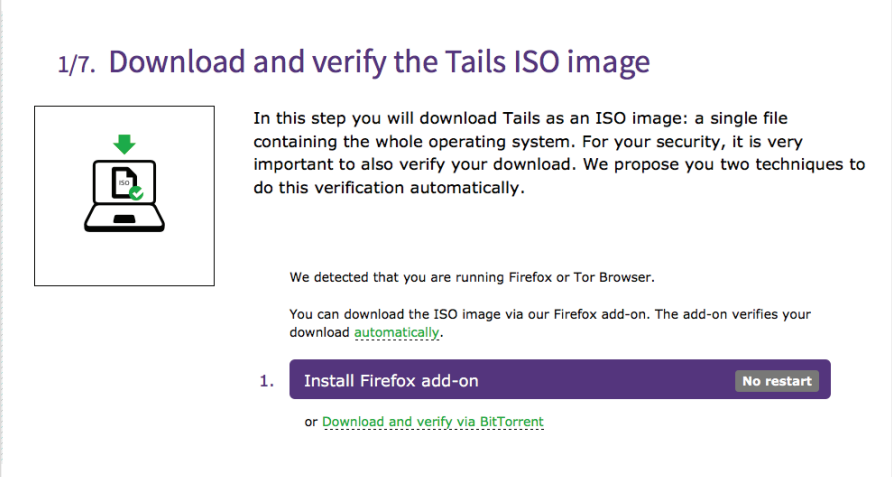
Detta görs för att säkerställa att någon inte lagt upp en manipulerad version av Tails på projektets webbplats. Det finns exempel där andra program drabbats av detta och bland annat ”extrautrustats” med funktioner som tjuvlyssnar på allt som skrivs på tangentbordet och skickar insamlade data till en server på nätet.

Om du inte redan har webbläsaren Firefox installerad på din dator ska du börja med att skaffa den. Har du Firefox behöver du se till att du har en uppdaterad version. Anledningen är att du ska installera ett speciellt webbläsartillägg i Firefox och att det bara fungerar med version 38 eller senare av webbläsaren. Det här tillägget kommer att kontrollera att filen du laddar hem från Tails webbplats inte är manipulerad på något sätt.

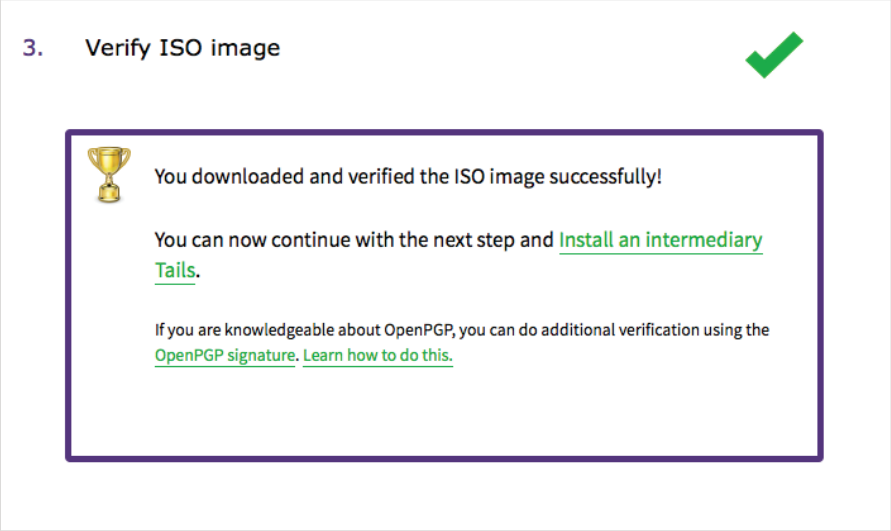
När du besöker https://tails.boum.org/install/win/usb/ eller https://tails.boum.org/install/mac/usb/ med en Firefox-version senare än 38 kommer du att få frågan om du vill installera Tails webbläsartillägg



Klicka på *Install Firefox add-on*. Upp dyker då eventuellt en ruta där du med ett klick bekräftar att du verkligen vill installera tillägget. När du slutfört installationen laddas webbsidan om och ser nu i stället ut så här:



Klicka på *Download Tails ISO image* och spara filen till din dators hårddisk. När nedladdningen är slutförd kommer webbläsartillägget att verifiera att filen inte är manipulerad och därmed är okej att använda för att skapa en Tails-sticka:



När du har fått hem Tails-filen till din dator är nästa steg att installera den på det tillfälliga usb-minnet. Använder du Windows behöver du programmet *Universal usb Installer* som finns länkat på installationssidan på Tails webbplats. Om du använder en Mac kommer du i stället använda *Terminalen*, ett program som följer med alla Macar. I Terminalen skriver du in kommandon i stället för att klicka på knappar och ikoner.

När du skapat det tillfälliga usb-minnet startar du om datorn med hjälp av det och sedan är installationsprocessen identisk med den ovan, för att skapa en kopia av en befintlig usb-installation.

Viktigt! Det här behöver du för att kunna använda Tails

För att kunna använda Tails behöver du en dator som har två usb-kontakter och kan starta från ett usb-minne i stället för den inbyggda hårddisken. De flesta moderna datorer kan det. Dessutom behöver du ett usb-minne som rymmer minst 4 GB. Observera att allt som finns på usb-minnet kommer att raderas under installationen, så välj *inte* ett usb-minne som innehåller saker du vill behålla!

Ska du installera Tails från en nedladdad fil behöver du dessutom en extra usb-sticka. Då är processen att *först* skapa en tillfällig Tails-installation och sedan följa stegen för att skapa en kopia av den. Anledningen är att den första stickan som skapas från en nedladdad fil inte kan förses med alla säkerhets- och användarmässiga finesser. De måste skapas från en annan Tails-sticka.

Tips! Kan man lita på Tails?

Vad talar för att du kan lita på Tails? Dels handlar det om vilka tekniska lösningar operativsystemet bygger på, dels på vilka personer och organisationer som rekommenderar Tails.

Tails utvecklas med det som kallas *fri och öppen mjukvara*. Det innebär bland annat att källkoden, alla de instruktioner som används för att konstruera Tails, är tillgänglig för vem som helst att titta på. Det hjälper inte användare som inte kan programmera, men det är ändå till indirekt nytta eftersom *andra* som kan programmera kan granska källkoden. Tails bygger dessutom på andra välrenommerade öppen källkodsprojekt. Grunden i själva Tails utgörs av en Linux-variant som heter Debian och Tor utnyttjas för att åstadkomma anonymitet. Svenska Sida är en av organisationerna som bidragit till utvecklingen av Tor. Den svenska biståndsmyndigheten ser Tor som ett viktigt verktyg i biståndsarbetet i länder där yttrandefrihet och nätfrihet saknas.

Bland dem som rekommenderar Tails finns bland andra amerikanska Freedom of The Press Foundation där några av världens mest erkända säkerhetsexperter är involverade.

Tips! Installera från nedladdad fil på Mac

Att installera Tails från filen du hämtar från webbplatsen är enkelt om du använder en Windowsdator. Då använder du programmet *Universal USB Installer* som finns länkat på installationssidan på Tails hemsida.

Om du använder en Mac är processen lite mer komplicerad. Instruktioner finns på Tails webbplats, men några saker kan behöva förtydligas i det andra steget, ”Installera an intermediary Tails”. Följande blir enklast att begripa om du läser texten parallellt med instruktionerna från Tails hemsida:

- Kommandon i *Terminalen* utförs genom att skriva in dem på tangentbordet och sedan avsluta med att trycka på *Return/Ny rad.*
- I steg 2–5 ska du ta reda på vilket namn din dator ger usb-stickan när du stoppar i den. Namnet inleds med */dev/disk, följt av* en siffra.
- Det är viktigt att du dubbelkollar namnet. Använder du fel namn i kommande steg finns en risk att du raderar innehållet på din hårddisk.
- I steg 6 ska du skriva in ett kommando som ”kopplar bort” usb-stickan från datorns inbyggda operativsystem. Du ska däremot *inte* koppla ur stickan rent fysiskt.
- I steg 7 ska du skriva in ett ganska långt kommando för att kopiera Tails till din usb-sticka: *dd if=/tails.iso of=/device/ bs=16m && sync.*

/tails.iso/ ska ersättas med namnet på den mapp där den nedladdade filen hamnade samt namnet på själva filen. *Och /device/* ska ersättas med namnet på din usb-sticka, från steg 2–5.

För att hitta namnet på mappen och den nedladdade filen kan du använda *Utforskaren/Finder.* Öppna *Utforskaren* och titta efter den nedladdade filen där du brukar spara filer som du hämtar med webbläsaren. Därifrån kan du sedan klicka och dra filen in i *Terminalen*.

Eventuellt får du upp ett felmeddelande som säger *Permission denied*. Du kan då lägga till *sudo* i början av kommandot från steg 6. I stället för att skriva in hela kommandot en gång till kan du prova att först trycka uppåtpil för att bläddra tillbaka till det och sedan använda vänsterpil för att ställa markören först. Därefter skriver du in *sudo* och avslutar med ett mellanslag. När du trycker på ny rad för att utföra kommandot får du skriva in ditt lösenord.

4. Så startar du Tails

Eftersom Tails inte installeras på din dators hårddisk måste du ha en dator med antingen dvd-läsare (om du har Tails på en dvd-skiva), minneskortsläsare (om du har Tails på ett minneskort) eller en usb-port (vilket alla datorer har och därför är vad den här instruktionen utgår från).

Stäng av datorn, stoppa i usb-minnet med Tails och starta den igen. För att Tails ska starta måste du instruera datorn att välja Tails i stället för operativsystemet som finns på hårddisken.

Hur du gör det beror på vilken dator du har. Är det en Windows- eller Linux-dator är det ofta en tangenttryckning som krävs under uppstarten. De vanligaste alternativen är Esc, F10, F11 eller F12. Trycker du på rätt knapp ska det dyka upp en meny där du får välja hur datorn ska starta.

Fungerar inte någon av de knapparna får du leta upp datorns handbok och se om du där kan hitta instruktioner för hur datorn ska startas från ett usb-minne. Leta efter begrepp som ”boot menu”, ”boot from external drive” eller ”boot from removable device”.

Har du en Mac ska du trycka ner den knapp som heter *Option* eller *Alt* medan datorn startar. Då visas det en meny på skärmen där du får välja om datorn ska använda operativsystemet på hårddisken eller operativsystemet på usb-minnet.

Vägen till skrivbordet

Oavsett hur du startar Tails kommer du först till *Bootmenyn* och därefter till *Tails Greeter*.

I **Bootmenyn** finns två alternativ, *Tails* och *Tails Failsafe*. Normalt ska du välja *Tails*. Det senare ska du använda om din dator har problem med att starta Tails. Operativsystemet startar då bland annat med vissa funktioner som kan ställa till problem avaktiverade.

Tails Greeter dyker upp efter en liten stund och är till skillnad från *Bootmenyn* grafisk, och du kan använda muspekaren för att göra dina val.

I rutan som dyker upp i *Tails Greeter* ställs frågan: *More options?*. Svarar du *Yes* på frågan hamnar du i en dialogruta där du kan göra ett antal olika inställningar:

Administration password: Startar du Tails på vanligt sätt finns det vissa grundläggande funktioner i operativsystemet som är blockerade. Det är funktioner som normalt inte behövs, men om du mot förmodan vill installera egna program eller komma åt filer som finns på datorns inbyggda hårddisk behöver du aktivera ett så kallat administratörskonto. Det gör du genom att välja ett tillfälligt lösenord här. Var dock medveten om att ett administratörskonto innebär säkerhetsrisker, så aktivera det bara om du vet vad du gör!

MAC adress spoofing: Varje nätverkskort i en dator (eller mobiltelefon och pekplatta) har ett unikt id-nummer. Personer med tillgång till de nätverk du ansluter din dator till kan se MAC-adressen. Det kan i vissa fall bland annat avslöja dig som Tails-användare. Om du ansluter till samma nät med både Tails och ditt vanliga operativsystem finns en möjlighet att lägga pussel där det går att se vilken MAC-adress som Tails-datorn har och sedan knyta den till dig när du använder ditt vanliga operativsystem. Genom att använda det som kallas för *MAC address spoofing* skapar Tails därför påhittade MAC-adresser varje gång du startar operativsystemet.

Ibland kan dock den här påhittade MAC-adressen orsaka problem. Den kan till exempel göra det omöjligt att ansluta till ett nätverk. Om du använder en lånad dator i exempelvis ett bibliotek kan det dessutom se misstänkt ut om administratörerna plötsligt upptäcker okända MAC-adresser i nätverket. För sådana här tillfällen finns därför möjligheten att avaktivera *MAC address spoofing*.

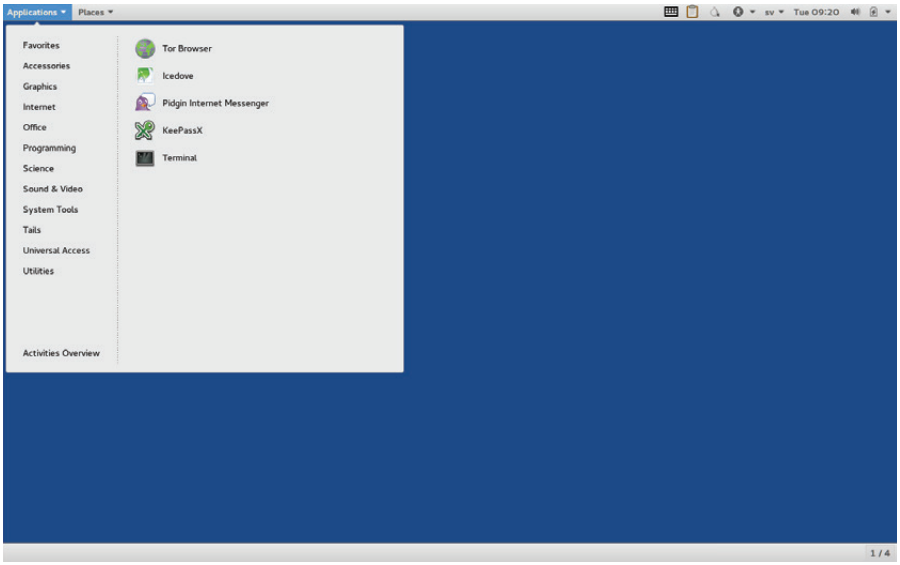
Network configuration: Från vissa nätverk kan det vara omöjligt att ansluta till Tor och därmed också omöjligt att använda Tails för att komma åt internet. Genom att aktivera *This computer's Internet connection is censored, filtered, om proxied*. *You need to configure bridge, firewall, or proxy settings.* hjälper Tails dig att ändå ansluta till nätet. När operativsystemet har startat dyker en ny dialogruta upp där du följer instruktionerna. Du kommer bland annat behöva adressen till en så kallad *bridge*, vilket du kan få om du besöker https://bridges.torproject.org eller skickar ett mail till bridges@torproject.org med ärenderaden *get bridges*. Ett sådant mail måste skickas från ett e-postkonto på www.riseup.net, mail.google.com eller mail.yahoo.com. Som sista utväg går det att skicka ett mail till help@rt.torproject.org.

Disable all networking: Om du över huvud taget inte tänkt använda internet kan du stänga av alla nätanslutningar här.

Om du klickar på *Documentation* bredvid varje alternativ i dialogrutan med *More options* får du mer detaljerade instruktioner om hur de fungerar och när de bör användas.

5. Så använder du Tails

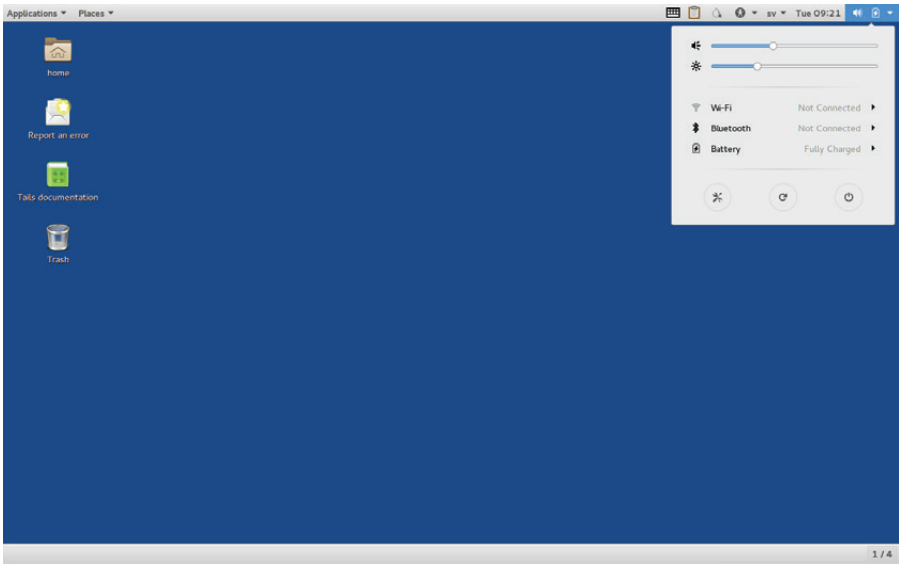
Eftersom Tails är ett eget operativsystem kommer datorn inte riktigt att se ut som du är van vid, oavsett om du har en Windows-dator eller en Mac. Däremot är skillnaderna inte större än att du direkt kommer att förstå hur själva gränssnittet fungerar. Längst upp till vänster på skärmen hittar du till exempel en knapp som fäller ut menyn med alla de program som finns installerade i Tails. Säkerhetsaspekten av operativsystemet för dock med sig vissa speciallösningar.



Ansluta till internet

Beroende på hur datorn du använder är utrustad kan du ansluta Tails till internet via ett trådlöst nätverk eller genom att koppla in en nätverkssladd.

Väljer du sladd behöver du bara plugga i den. För att koppla upp till ett trådlöst nätverk klickar du på systemmenyn i verktygsfältet längst upp till höger på skärmen och väljer *Wi-fi*.



Efter att du anslutit datorn till ett nätverk försöker Tails starta Tor. Lyckas det får du efter en liten stund ett meddelande om att datorn är redo att användas. Om du är för snabb kommer du att få en varning om att Tor inte är redo att användas. Ignorera inte den varningen eftersom den innebär att du ännu inte blivit anonym.

Om du däremot kopplat upp datorn till ett trådlöst nätverk som kräver inloggning via en webbsida måste du först starta den webbläsare som heter *Unsafe Browser*. Anledningen är att det inte går att använda den anonyma *Tor Browser* för att logga in på sådana sidor.

Efter att ha använt *Unsafe Browser* för att logga in på nätverket, stäng ner den webbläsaren och starta sedan *Tor Browser*. Undvik att ha båda webbläsarna igång samtidigt för att eliminera risken för att råka använda *Unsafe Browser* av misstag!

- *Unsafe Browser* för att kunna logga in på internet via så kallade *captive portals*.
- Kör inte *Unsafe browser* och *Tor Browser* samtidigt – det ökar risken för mänskliga misstag. Logga in med US först, stäng den sedan och byt till TB.
- Vänta på synkroniserad klocka.

Viktigt! Tor och kryptering

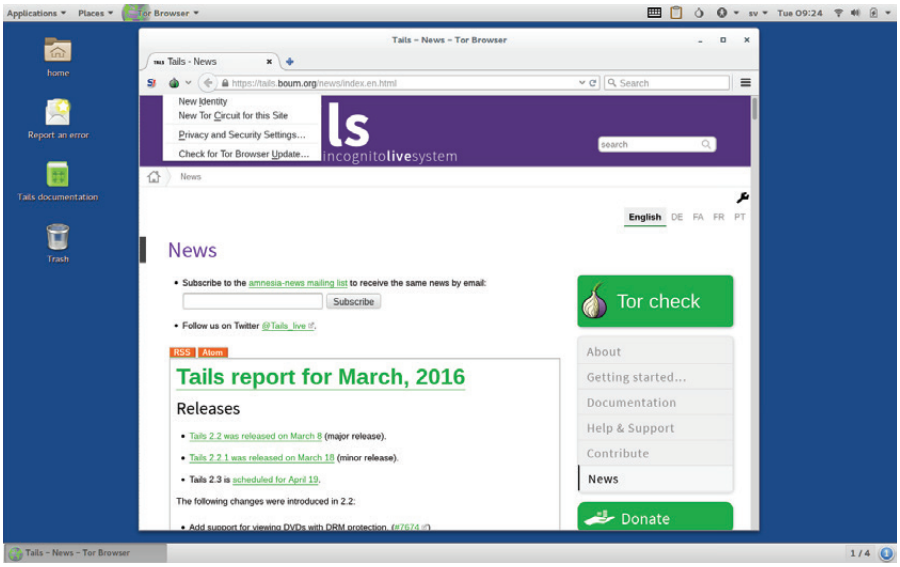
En viktig aspekt av hur Tor fungerar gäller kryptering. När internettrafik lämnar din dator krypteras den tre gånger, en gång för varje hopp inne i Tornätverket. Den första datorn tar bort det yttersta krypteringslagret, skickar vidare till den andra datorn som tar bort nästa krypteringslager och skickar vidare till den sista datorn. Den tar bort det tredje krypteringslagret och skickar din internettrafik vidare till slutmålet. Men om din internettrafik inte är krypterad innebär det att den från och med sista datorn i Tor-kedjan nu är möjlig att avlyssna. Antingen av den person eller av den organisation som sköter den sista datorn eller av någon på vägen mellan den och slutmålet. För att öka ditt skydd bör du därmed se till att du använder krypterade förbindelser, det vill säga https i stället för http i webbläsaren, en krypterad förbindelse till din e-postserver om du använder Icedove för mejl och så vidare.

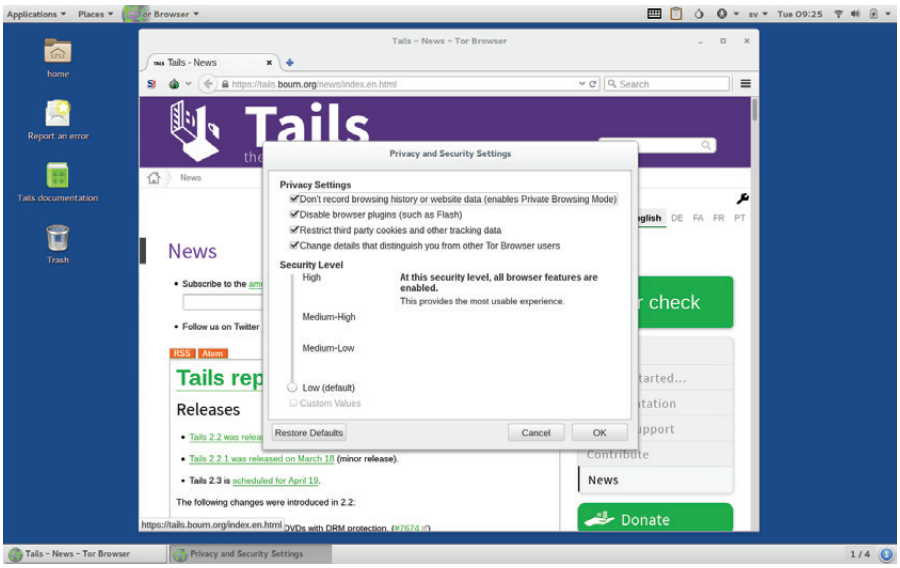
Tor Browser

Tor Browser är den webbläsare som du ska använda när du vill vara anonym. Jämfört med din vanliga webbläsare i ditt vanliga operativsystem kommer du att upptäcka vissa begränsningar i *Tor Browser*. Bland annat spärras vissa webb-funktioner som är utvecklade med en teknik som heter JavaScript. Anledningen är att det i en del JavaScript-program finns brister som riskerar att avslöja vem du är. Av samma anledning saknas också stöd för *Flash*, en populär teknik för att göra rörlig grafik på webben. Som en konsekvens av dessa begränsningar kommer inte alla webbplatser att fungera eller se ut som du är van vid.

En annan skillnad jämfört med hur du normalt upplever webben är att allt kommer gå långsammare när du använder *Tor Browser*. Det beror på att all trafik till och från din dator tar en omväg via Tor-nätverket för att göra den anonym.

I *Tor Browser* finns möjligheten att justera hur strikta säkerhetsinställningar du vill ha. Klicka på den lilla knappen med en lök precis till vänster om webbläsarens adressfält och välj sedan *Privacy and Security Settings*.





I dialogrutan som du då hamnar i finns två rubriker, *Privacy Settings* och *Security level.* Alla fyra kryssrutorna under integritetsinställningarna bör vara aktiverade. Under *Security level* kan din säkerhet genom att i fyra steg välja vilka funktioner i din webbläsare som ska stängas av.

För att skydda din anonymitet ytterligare finns en knapp i menyn som dyker upp när du klickar på lök-ikonen: *New Identity*. Klickar du på den kommer trafiken till och från *Tor Browser* att ta en ny väg via Tor-nätet. Dessutom stängs alla öppna flikar ned samtidigt som webbläsaren slänger alla cookies och andra filer som du hittills samlat på dig under ditt surfande.

Den här funktionen skyddar dig ändå inte helt från någon som lägger ihop två och två: Om du först använder Tails för att läsa din e-post och sedan publicera ett blogginlägg som är tänkt att vara anonymt finns det en möjlighet att lägga pussel och förstå att det är du som gjort publiceringen. Lösningen är att starta om Tails när du läst din e-post och därmed också få en helt ny, tillfällig internet-identitet.

En annan egenskap hos *Tor Browser* behöver också nämnas. Om du vill använda webbläsaren för att ladda upp filer från din usb-sticka, till exempel för att lägga till som bilaga i ett mail, måste filerna ligga i den mapp som heter just *Tor Browser* på usb-stickan. Anledningen är att *Tor Browser* av säkerhetsskäl inte får komma åt vilka mappar som helst.

Kontorsprogram

Officepaketet *Libre Office* finns i Tails. Där hittar du program för ordbehandling, kalkylblad, presentationer och enklare illustrationer. I menyn *Applications* finns också program som *Gimp* för bildbehandling och *Audacity* för redigering av ljudfiler.

Tips! Mer om krypterad e-post

För att lära dig mer om e-post, PGP och kryptering, läs guiden *Kom igång med PGP*! Läs om hur du bör hantera dina nycklar och varför du absolut inte får råka skicka iväg din privata nyckel till någon annan.

Krypterad e-post med Icedove och Enigmail

För att kunna skicka och ta emot krypterad e-post finns programmen *Icedove* och *Enigmail* installerade i Tails. *Icedove* är ett e-postprogram medan *Enigmail* ett verktyg för krypteringstekniken PGP.

Om du inte redan har de krypteringsnycklar som krävs för att kunna hantera krypterad e-post kan du skapa dem med programmet *Passwords and Keys* i *Applications*-menyn, under *Utilities*. Har du redan nycklar importerar du dem i stället till *Passwords and Keys*.

OpenPGP Applet

Att skriva saker som ska vara hemliga i ett webbläsarfönster är förenat med risker. Det finns olika sätt för en angripare att komma över texten som skrivs in. Vid sidan av kombinationen *Icedove* och *Enigmail* finns därför även PGP-programmet *OpenPGP Applet* i Tails.

OpenPGP Applet är ett litet anteckningsblock där känslig text skrivs i ett program i den egna datorn, krypteras med PGP för att slutligen kopieras in i webbläsaren.

Beständiga volymer

För att kunna skicka och ta emot krypterad e-post behöver du en PGP-nyckel. Mer om det kan du läsa i Internetguiden *Kom igång med PGP!*

Ett problem med PGP i kombination med Tails är att din Tails-dator återställs vid varje omstart, vilket gör att dina PGP-nycklar också försvinner.

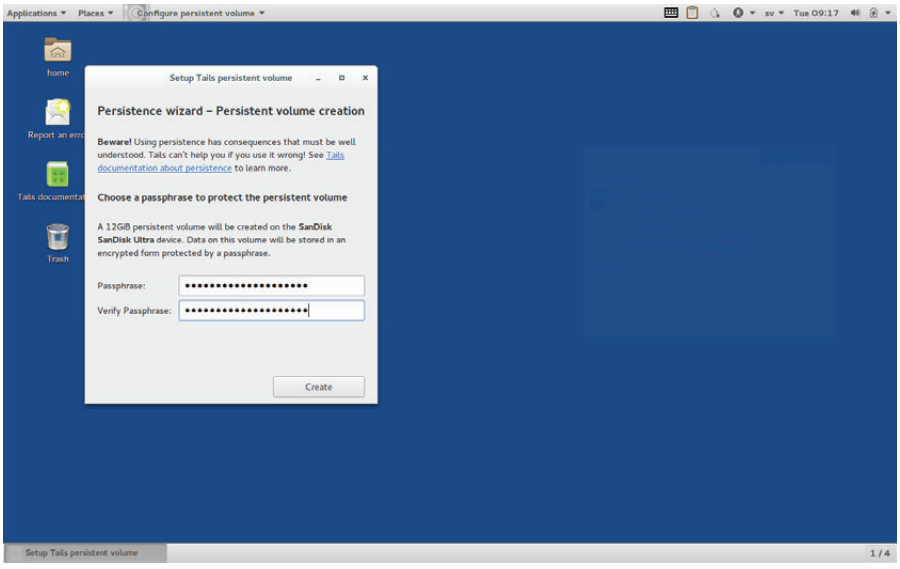
För att kunna lagra PGP-nycklar – och annan information som lösenord till trådlösa nätverk, bilder, dokument och så vidare – mellan olika Tails-sessioner finns därför en funktion i Tails som heter *Persistent volume*.

Persistent volume är ett sätt att skapa ett krypterat utrymme på ditt usb-minne. Här kan du lagra inställningar, dokument, PGP-nycklar och annat utan att det raderas varje gång du stänger av din Tails-dator.

Du behöver vara medveten om att en *persistent volume* inte är dold. Den som kommer över din usb-sticka ser att det krypterade utrymmet finns, men behöver ditt lösenord för att kunna öppna det.

Skapa en persistent volume

Du skapar en *persistent volume* genom att öppna *Applications*-menyn längst upp till vänster på skärmen. Under *System Tools* hittar du alternativet *Configure persistent volume*. I rutan som dyker upp matar du in ett lösenord och klickar sedan på *Create*.



När utrymmet är skapat på din sticka får du välja vilka saker du vill spara i det. Några användbara alternativ är:

- Dina egna dokument
- PGP-nycklar
- Inställningar för chattprogrammet Pidgin
- Inställningar för e-postprogrammet Icedove
- Nätverksinställningar
- Bokmärken
- Skrivarinställningar
- Bitcoin-plånbok

Ytterligare några valmöjligheter finns, men förstår du inte vad de innebär är det bäst att inte aktivera dem.

Öppna din ”beständiga volym”
När du skapat en beständig volym kommer ett nytt alternativ dyka upp i *Tails Greeter* när du startar din Tails-sticka: *Use persistence*? Den ska du svara *Yes* på om du vill komma åt dina egna dokument och inställningar som du sparat på usb-stickan.

Radera din PV
Vill du radera din beständiga volym och allt som finns i den väljer du *Delete persistent volume* från *System Tools*-alternativet i *Applications*-menyn.

Krypterad chatt med Pidgin

Pidgin är ett chattprogram som bygger på en teknik som heter *Off-the-record, OTR*. OTR krypterar bland annat de meddelanden som skickas, men ger också möjlighet att verifiera vem det faktiskt är du chattar med[5].

Om du vill använda Pidgin för att skicka och ta emot krypterade chattmeddelanden måste du först aktivera OTR i programmet. Du behöver också vara medveten om att filer som skickas via Pidgin inte är krypterade.

Virtuellt tangentbord

Om du använder en lånad dator, till exempel på ett internetkafé, kan du inte vara säker på att det inte finns en så kallad *keyboard logger* inkopplad. En *keyboard logger* spelar in alla tryckningar som görs på tangentbordet. För situationer där det inte är ett alternativ för dig att chansa, även om risken är aldrig så liten, har Tails ett så kallat virtuellt tangentbord. Aktiverar du funktionen dyker ett tangentbord upp på skärmen. På det kan du sedan skriva genom att peka och klicka med musen.

Tips! Kryptering och anonymitet

Det är viktigt att vara medveten om att kryptering och anonymitet är två olika saker. Ibland är du intresserad av båda egenskaperna, ibland räcker det med den ena.

Kryptering gör det omöjligt för en utomstående att ta del av den information som skickas via internet. PGP krypterar e-post, men döljer inte vem som skickar och vem som tar emot.

Anonymisering gör det omöjligt för en utomstående att veta vilka parter det är som kommunicerar med varandra. Tor ger anonymitet, så att exempelvis ett företag eller en organisation inte kan se vem som besöker webbplatsen.

Hantera lösenord

KeyPassX är ett program för att spara dina lösenord till webbplatser och andra nättjänster på ett säkert sätt. Aktiverar du den funktionen när du skapar en *persistent volume* erbjuder Tails på så sätt möjligheten att leva upp till säkerhetsexperternas råd om hur ett bra lösenord ska vara.

Rör inte datorns hårddisk

När en dator startas om efter en Tails-session finns det inga spår som avslöjar att Tails har använts på den. Tails rör nämligen inte informationen som finns på datorns hårddisk. Det innebär också att eventuella virus och andra skadliga program som finns på datorns hårddisk inte påverkar Tails.

Det går dock att komma åt data som finns på datorns hårddisk från Tails. Men eftersom det finns potentiella problem med att göra det är det bäst att låta bli. Dels finns en risk att Tails råkar förstöra information på hårddisken, dels finns en risk att Tails lämnar spår efter sig eller att information på hårddisken röjer din anonymitet.

Tips! Krypterad chatt via mobilen

Ett alternativ till Pidgin är att använda de senaste versionerna av antingen mobilapparna WhatsApp eller Signal. De skickar också alla meddelanden krypterat.

Tor är långsamt

Du kommer sannolikt upptäcka att det går långsammare att surfa när du använder Tor Browser.

Radera säkert

Information som raderas från en hårddisk går ofta att återskapa på olika sätt. Det finns många olika verktyg för att radera data på ett mer säkert sätt, och ett sånt finns inbyggt i Tails. Var dock uppmärksam på att det inte fungerar på en usb-sticka. Du kan alltså inte använda kommandot *Wipe* som dyker upp när du högerklickar på en fil för att radera den för alltid.

Detta gäller alltså bara de data som du lagrar i en beständig volym, om du väljer att skapa en sådan. Alla andra inställningar i Tails återställs automatiskt vid varje omstart. Det gäller även dokument och andra filer som du sparar på skrivbordet eller i andra mappar i din Tails-installation.

Egna program och plugin

Det går att installera egna program på din Tails-sticka. Men låt bli att göra det. Säkerhet har högsta prioritet i Tails och de program som finns förinstallerade i operativsystemet är också granskade ur säkerhetsperspektiv. Det innebär inte att de är helt säkra, men att riskerna är minimerade så långt det är möjligt. Vilka problem som finns i program du själv vill installera vet du däremot inte.

Uppdatera

Att uppdatera operativsystemet i en dator är alltid viktigt för att minimera riskerna med säkerhetsluckor. Men i ett operativsystem vars hela syfte är att ge dig en så säker internetförbindelse som möjligt är det extra viktigt.

Ungefär var sjätte vecka kommer nya versioner av Tails. Se till att installera dem så snart en ruta om att en ny version finns tillgänglig dyker upp i operativsystemet!

Lär dig mer

Läs också de andra guiderna om digitalt självförsvar och digitalt källskydd:

- *Digitalt källskydd – en introduktion*
- *Digitalt självförsvar – en introduktion*
- *Kom igång med säkrare mobiltelefon!*
- *Kom igång med PGP!*
- *Kom igång med Tor!*

Fotnot

1. Ip-adresser är nätets motsvarighet till telefonnummer, en sifferkombination som varje uppkopplad pryl behöver för att kunna kommunicera på internet. Cookies är små textfiler som sparas i webbläsaren när vi surfar runt på nätet. De används bland annat för att visa annonser baserade på våra surfvanor. Webbläsaravtryck är det ”digitala utseende” som vår webbläsare visar upp för en webbserver när vi besöker en webbplats.
2. Det går även att installera Tails på en dvd-skiva eller ett minneskort. I den här guiden utgår vi från ett usb-minne eftersom inte alla datorer har dvd-läsare eller plats för minneskort.
3. *MAT: Metadata Anonymisation Toolkit* https://mat.boum.org/
4. Boot är det engelska begrepp som används för att beskriva startproceduren för en dator.
5. Läs mer om OTR på: https://otr.cypherpunks.ca/.

Anders Thoresson

Anders Thoresson är journalist och föreläsare. Han har bevakat teknikutvecklingen sedan 1999. Först på tidningen Ny Teknik och sedan 2006 som frilans. Under åren 2011–2014 skrev han Teknikbloggen på dn.se. Han föreläser bland annat om digitalt källskydd för journalister och programmering i skolan för lärare och skolledare. Anders Thoresson har författat flera Internetguider för IIS, exempelvis om programmering för barn, it-säkerhet, webbpublicering och omvärldsbevakning.

Foto: Sebastian LaMotte CC-BY ND

Kom igång med Tails!
Ett säkrare operativsystem
IIS Internetguide, nr 41. 2016
Anders Thoresson

IIS klimatkompenserar för sina koldioxidutsläpp och stödjer klimatinitiativet ZeroMission.

Författare: Anders Thoresson
Redaktör: Hasse Nilsson
Projektledare: Jessica Bäck
Formgivning: AGoodId
Första upplagan
ISBN: 978-91-7611-694-4N

Vi driver internet framåt! IIS arbetar aktivt för positiv tillväxt av internet i Sverige. Det gör vi bland annat via projekt som samtliga driver utvecklingen framåt och gynnar internetanvändandet för alla. Exempel på pågående projekt är:

Bredbandskollen
Sveriges enda oberoende konsumenttjänst för kontroll av bredbandsuppkoppling. Med den kan du på ett enkelt sätt testa din bredbandshastighet. www.bredbandskollen.se

Internetdagarna
Varje höst anordnar vi Internetdagarna som är Sveriges ledande evenemang inom sitt område. Vad som för tio år sedan var ett forum för tekniker har med åren utvecklats till att omfatta samhällsfrågor och utvecklingen av innehållet på internet. www.internetdagarna.se

Internetfonden
Hos Internetfonden kan du ansöka om finansiering för fristående projekt som främjar internetutvecklingen i Sverige. Varje år genomförs två allmänna utlysningar, en i januari och en i augusti. www.internetfonden.se

Internetguider
IIS publicerar kostnadsfria guider inom en rad internetrelaterade ämnesområden, som webb, pdf eller i tryckt format och ibland med extramaterial.

Internetstatistik
Vi tar fram den årliga, stora rapporten ”Svenskarna och internet” om svenskarnas användning av internet och dessemellan ett antal mindre studier.

Webbstjärnan
Webbstjärnan är en skoltävling som ger pedagoger och elever i den svenska grund- och gymnasieskolan möjlighet att publicera sitt skolarbete på webben. www.webbstjarnan.se

Internetmuseum
I december 2014 lanserade IIS Sveriges första digitala internetmuseum. Internetmuseums besökare får följa med på en resa genom den svenska internethistorien. www.internetmuseum.se

Federationer
En identitetsfederation är en lösning på konto- och lösenordshanteringen till exempel inom skolans värld eller i vården. IIS är federationsoperatör för Skolfederation för skolan och Sambi för vård och omsorg. www.iis.se/federation

Internets infrastruktur
IIS verkar på olika sätt för att internets infrastruktur ska vara säker, stabil och skalbar för att på bästa sätt gynna användarna, bland annat genom att driva på införandet av IPv6. www.iis.se

Sajtkollen
Sajtkollen är ett verktyg som enkelt låter dig testa prestandan på en webbsida. Resultatet sammanställs i en lättbegriplig rapport. www.sajtkollen.se

Läs mer på nätet redan idag! På Internetguidernas webbplats hittar du mängder av kostnadsfria publikationer. Du kan läsa dem direkt på webben eller ladda ner pdf-versioner. Det finns guider för dig som vill lära dig mer om webbpublicering, omvärldsbevakning, it-säkerhet, nätets infrastruktur, källkritik, användaravtal, barn och unga på internet, digitalt källskydd och mycket mer.

Nya Internetguider!

Kom igång med säkrare mobiltelefon!
Av: Anders Thoresson

Guiden tar upp grunderna för säkrare användning av din mobil i praktiken och du får lära dig:

- Om säkerhetsproblem och annat som påverkar din integritet när du använder en mobiltelefon.
- Generella beskrivningar av de problem som finns.
- Tips om inställningar för Iphone, Android och Windows Phone.

Innehållet är ett komplement till Internetguiden ”Digitalt självförsvar – en introduktion”. Reportrar Utan Gränsers Martin Edström och Carl Fridh Kleberg från Expressen ger dig hjälp att med enkla verktyg skydda dig mot de hot som finns mot allas vår kommunikation och information på nätet. Författarna tar även upp sådant som massövervakning och de spår du lämnar efter dig på internet.

Digitalt självförsvar – en introduktion
Av: Martin Edström och Carl Fridh Kleberg

Reportrar Utan Gränsers Martin Edström och Carl Fridh Kleberg från Expressen ger dig hjälp att med enkla verktyg skydda dig mot de hot som finns mot allas vår kommunikation och information på nätet. Guiden vänder sig i första hand till människor som har information de vill ska komma ut till allmänheten, tipsare och uppgiftslämnare. Här finns också mycket att hämta om du vill börja kommunicera på säkrare sätt eller helt enkelt vill veta lite mer om hur internet fungerar. Författarna tar även upp sådant som massövervakning och de spår du lämnar efter dig på internet.