Sus Andersson

Så surfar du säkrare

Digitalt Källskydd - en introduktion

Det här dokumentet om att surfa säkrare på nätet är extramaterial som hör ihop med Internetguiden ”Digitalt källskydd – en introduktion” av Sus Anderson, Fredrik Laurin och Petra Jankov. Hela boken, och mer extramaterial, finns att ladda ned kostnadsfritt här: www.iis.se/guider

Så surfar du säkrare

Det finns en rad olika sätt att följa dina spår på Internet, och du behöver tänka igenom vad det är du vill skydda dig emot.

- Vill du skydda dina surfvanor emot den som kommer åt din dator? Någon som stjäl din dator, eller den som har koll på den offentliga dator du lånar? Ifall en källa ska tipsa redaktionen behöver denna sannolikt också tänka på att IT-personalen hos källans arbetsgivare kan se vilka webbsidor hon besöker på arbetstid.
- Vill du skydda dig mot den som äger den webbplats du besöker? Ifall du gör research om ett företag, och inte vill att personalen där ska ha koll på vilka av deras webbsidor du besöker behöver du tänka på detta.
- Vill du skydda dig mot någon angripare ute på nätet, som antingen vill se vart du surfar, eller snappa upp dina hemliga lösenord?

Skydda surfvanor på din dator

De här tipsen hjälper för att skydda dina surfvanor mot den som kommer åt den dator du använt. Det här kan vara bra tips för en källa som vill lämna anonym information till en redaktion. Även om tipssajter som Radioleaks och liknande skyddar innehållet i det meddelande som skickas kan källans webbhistorik ändå avslöja henne .

Ställ in läget privat surfning i din webbläsare.

”Privat surfning” ser till att din webbhistorik och tillfälliga Internetfiler inte sparas. Inte heller sparas så kallade kakor, filer som webbsajter du besöker sparar på din dator för att exempelvis lagra olika inställningar, och för att kunna analysera ditt beteende.

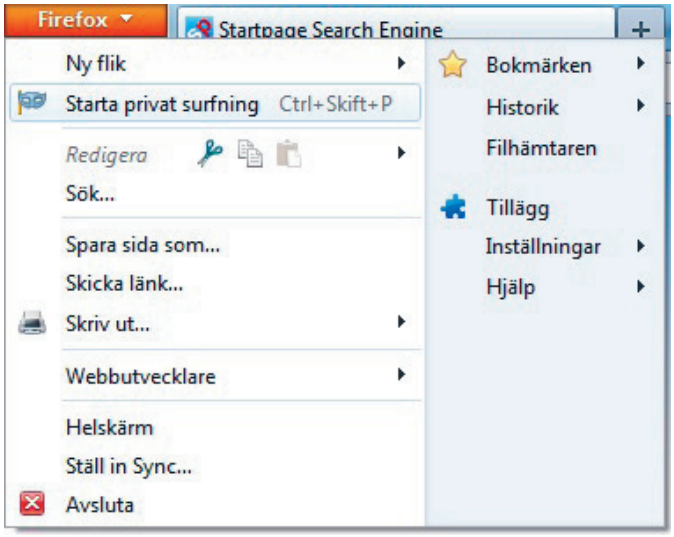
Genom att välja privat surfning går det inte att få fram vilka sidor du besökt genom att titta i historiken, eller på dina cookie-filer. Om du sparar bokmärken kommer de dock att finnas kvar.

Din dators IP-adress döljs dock INTE på det här viset. Ägaren till den webbsida du besöker kan se att du varit där.

En nackdel för din egen del är att webbläsaren inte kommer att hjälpa dig att skriva in webbadresser när du börjar skriva dem. En del webbsajter blir ganska konstiga när de inte får sätta kakor, eftersom de bygger på att du väljer att göra ett antal inställningar, som sparas i kakor.

I Firefox går du in i huvudfliken och väljer ”Starta privat surfning”. Om du alltid vill ha detta som utgångsläge går du in under ”Inställningar”, väljer ”Inställningar” och fliken ”Sekretess”. Under ”Historik” väljer du ”Inte spara någon historik”.

I Explorer går du in under ”Säkerhet” i övre högra hörnet av webbläsaren. Välj ”InPrivate-surfning”. Liknande inställningar finns även i andra webbläsare.



Stoppa flashkakor

Det finns också en typ av kakor som inte spärras av Privat surf-läget. Det är så kallade flash-kakor.

De är kopplade till Adobes flash-spelare, och sparar bland annat förval för ljud och liknande. Men det är också extra stora kakor, som kan spara mycket information om dig. Dessutom kan de ”återuppliva” vanliga kakor, ifall du försökt ta bort dem. Därför brukar de också kallas för ”zombiekakor”.

För att ta bort de flashkakor du redan har går du in på http://www.macromedia.com/support/documentation/se/flashplayer/help/settings_manager07.html och välj ”Ta bort alla”.

För att blockera flashkakorna i framtiden går du in på fliken Globala lagringsinställningar http://www.macromedia.com/support/documentation/se/flashplayer/help/settings_manager03.html

Ställ reglaget på noll och klicka i rutan ”Fråga inte igen”. Klicka bort rutan ”Tillåt att Flash-innehåll från tredje part lagrar data på din dator.

Du kan också rensa oönskat innehåll med hjälp av exempelvis programmet Ccleaner på PC och Flush 3.1 på Mac.

Skydda det du skickar

För att skydda innehållet i det du skickar behöver du någon form av kryptering.

Många webbsajter som vet att de hanterar känsligt innehåll – som lösenord eller banktjänster – krypterar överföringen, och det görs utan att du behöver göra någonting. Att det görs ser du genom att webbadressen börjar med ”https” istället för ”http”.

Alldeles för många sajter som borde kryptera överföringen gör det inte. Kontrollera därför alltid adressen innan du lämnar ifrån dig känslig information. Det finns också webbplatser som bara krypterar ingångssidan, men sedan kör okrypterat.

Många använder också en gammal version av krypteringsmetoden SSL, version 2.0. Du kan försäkra dig om att det är en stark kryptering som används genom att använda testet på https://www.ssllabs.com/ssltest.

Du kan också se till att överföringen sker krypterat att använda en så kallad VPN-tunnel, ett privat virtuellt nätverk. Det kräver dock litet mer att göra en sådan installation själv, och vi kommer inte att gå igenom det i den här guiden. Många företag har VPN-tunnlar. Det finns också kommersiella tjänster som erbjuder dem.

Ifall du behöver ansluta till Internet via ett trådlöst nätverk bör du absolut använda VPN. Även om den webbsida du tänker besöka har en krypterad överföring (adressen börjar på https), så kan det finnas luckor i överföringen i det trådlösa nätverket. Dina lösenord går då att avlyssna i alla fall, om du inte använder VPN.

Viktigt att komma ihåg är att ingen av de här metoderna döljer vem som kommunicerar med vem.

Skydda din identitet

De flesta som driver en webbsajt gör också någon form av uppföljning av sina besökare. Det finns ofta färdiga verktyg som håller koll på besökarnas datoradresser – IP-adresserna – hur länge de varit inne och på vilka sidor. Det finns också enklare funktioner för att logga besökarna.

Webbägaren kan också spåra besökarna genom så kallade kakor, små filer som sparas på besökarens dator. De spärrade vi nyss genom att ställa in privat surfning.

För att verkligen skydda din identitet bör du i vissa lägen använda dig av anonymiseringstjänster, som döljer din IP-adress. Det är dock betydligt mer än bara besökarens IP-adressen som ägaren till en webbsajt kan se. Insticksprogram, vilka typsnitt som är installerade och vilken skärmupplösning du har är några. En som verkligen vill spåra det du gör kan utnyttja denna din profil, även om du döljer IP-adressen.

Det finns flera kommersiella tjänster som döljer din IP-adress, och många kombinerar en VPN-tunnel med anonymiseringstjänsten.

Problemet med de flesta av dessa tjänster är att de bara har ett dolt steg mellan dig och Internet. Det innebär dels att den som driver tjänsten har full koll på vilka sajter du besöker, och du måste kunna lita på att informationen inte lämnas ut därifrån. Läs användarvillkoren innan du bestämmer dig.

Dessutom kan utomstående övervaka trafiken på anonymiseringstjänsten, matcha in- och utgående

och luska ut vilka Internetanrop som är dina.

I de flesta använder du också din vanliga webbläsare, och då kan du spåras genom din profil.

I vissa sammanhang duger dessa tjänster bra, i andra fall behövs mer avancerade metoder.

Det finns ett par tjänster som anonymiserar genom att vidarebefordra webbtrafiken i flera steg, som I2P, JonDoNym och Tor. Alla är fortfarande under utveckling, och har sina förtjänster och tillkortakommanden. De använder dock öppen källokod, vilket är en fördel, eftersom tekniken bakom kan granskas. Om det finns ”bakdörrar” där systemen kan avlyssnas brukar det upptäckas snabbt. Såväl JonDoNym som Tor har kopplingar till universitetsforskning.

Vi kommer här att gå igenom hur du installerar TorBrowserBundle – som vi i fortsättningen bara kallar Tor. I paketet ingår en webbläsare, som ”skalar av” mer av din personliga information för att du ska vara så anonym som möjligt.

I Tor-nätverket gör ditt Internetanrop tre hopp innan det går ut till den adress du vill besöka. De första stegen skickas krypterat, och varje dator på vägen kan bara se var trafiken kom ifrån och nästa steg – men inte hela vägen. Det är därmed extremt svårt att matcha ingående och utgående trafik på samma sätt som vid envägsanonymisering.

En nackdel med Tor är att det sista steget är okrypterat. Om du bara är ute efter att den sajt du besöker inte ska veta att just du varit där är det inget problem. Men om du vill skydda dig mot annan övervakning kan du behöva tänka till. Du vet inte vem som driver utgången, men den personen eller organisationen kan komma att fånga upp innehållet i trafiken. Vem som vill kan sätta upp en Tor-nod, och du måste ha med i kalkylen att det kan vara någon som är ute efter att övervaka trafik som andra vill dölja. Däremot kan utgångsnoden inte se vem du är – om du inte berättar det genom att skicka dina personuppgifter okrypterade. Även andra som kommer åt trafiken i det sista steget kan läsa den. Du måste alltså själv se till att innehållet är krypterat, om du exempelvis ska logga in någonstans.

En annan nackdel med Tor är att det blir väldigt långsamt att surfa.

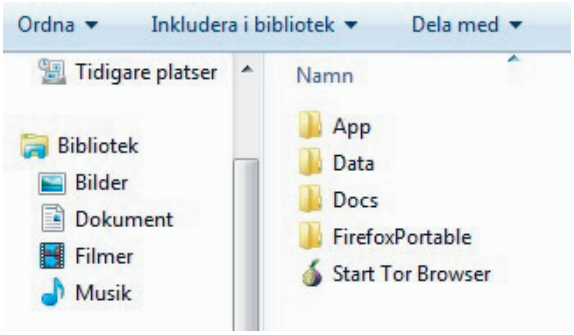
Du kan installera Tor på din dator, eller på en USB-sticka. Fördelen med det är att du kan ha med Tor när du reser bort, och du kan surfa anonymt utan att lämna spår. USB-minnet måste rymma minst 80 MB.

1. Börja med att göra en säkerhetskopia av ditt system. Gör det till en vana alltid när du installerar något nytt eller gör större uppdateringar av din dator. Om det visar sig att det du installerar inte fungerar som du tänkt kan du gå tillbaka dit där du var innan.
2. Ladda hem Tor Browser Bundle. Det är ett paket som innehåller både en anpas-

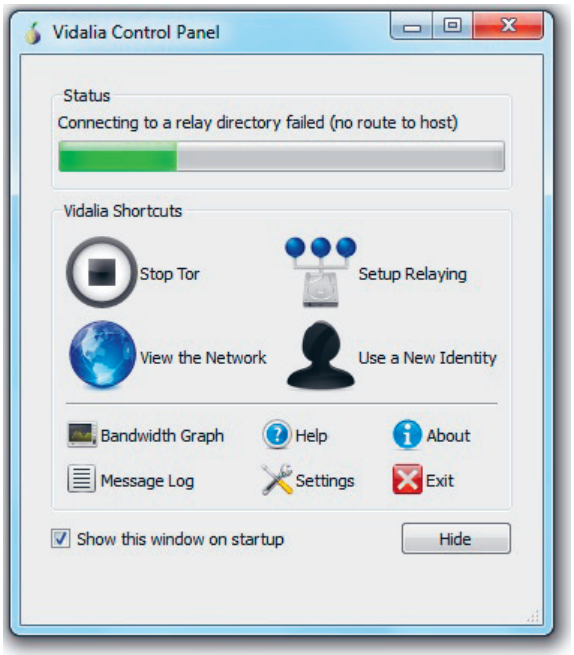
sad webbläsare och program som sköter hoppen över Internet i Tornätverket. https://www.torproject.org.

Ladda hem programmet genom att välja ”Download” för det språk du gillar bäst. Spara exempelvis på skrivbordet.

3. När du laddat hem programmet ska du inte köra det på en gång. Först bör du kontrollera att det är en korrekt version. Det gör du genom att verifiera den signatur som hör till programmet. Om du har programmet gnuPG – som du laddar hem för att kunna kryptera – ingår även funktioner för att kontrollera signaturer. Läs mer om hur du gör i XL-guiden ”Lär dig kryptering”
4. Dubbelklicka på programikonen och välj vad du vill spara själva programmet – på din hårddisk eller ett USB-minne. Lägg den INTE i programmapparna Program eller Program (x86) – det är ett känt fel att programmet inte funkar då. Torprojektet rekommenderar skrivbordet. Klicka på ”Extract”
5. Gå in i mappen du just skapade. Dubbelklicka på Start Tor Browser.



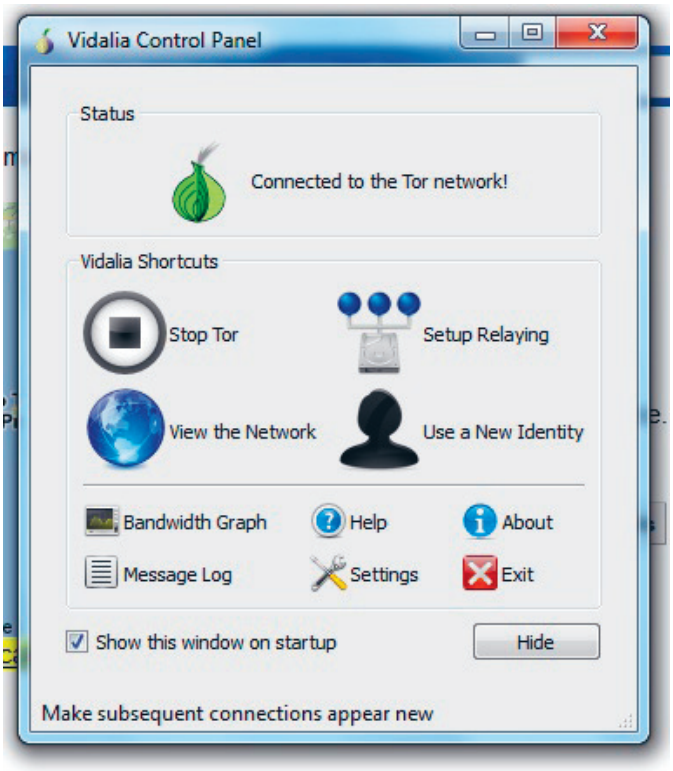
Nu startas bland annat programmet Vidalia, som sköter uppkopplingen. Beroende på hur du ställt in din brandvägg och ditt antivirus kan du få upp varningar nu. Godkänn att programmen ansluter till internet.



6. Om programmet hänger sig kan du testa att trycka på knappen ”Stop Tor” och sedan ”Start Tor”.
7. När uppkopplingen via Tornätverket har etablerats startas Tor-webbläsaren automatiskt. Nu är det bara att sätta igång att surfa. Tänk på att webbtrafik genom Tornätverket kommer att kännas extremt långsam, jämfört med när du använder din vanliga webbläsare. Det tar tid att hoppa mellan olika datorer på Internet.
8. Om du vill kolla att din verkliga IP-adress är dold kan du surfa in på någon sida som visar din adress, exempelvis http://whatismyipaddress.com.

9. Tänk på att det bara är webbsidor som du tittar på via Tor-läsaren där din anonymitet kan skyddas. Du är inte anonym om du kör någon annan webbläsare, även om Tor är igång.
10. Om du använder ett e-postprogram kommer inte Tor att skydda din identitet. Det finns ett insticksprogram för Thunderbird, TorBirdy, som är under utveckling. I skrivande stund fungerar det inte tillsammans med krypteringsprogrammet GnuPG.
11. Om du skickar e-post måste det gå via en webbtjänst, som du surfar till via Tor-läsaren. Då kommer inte IP-adressen på avsändaren att vara din egen. Om du vill uppnå hög säkerhet när du e-postar, genom att samtidigt kryptera innehållet och skicka mejlet med dold ip-adress kan du göra så här:
    a. använd en webbaserad e-posttjänst
    b. surfa in med hjälp av Tor
    c. skriv ditt meddelande, kopiera det och kryptera innehållet i klippbordet med hjälp av GnuPG (se XL-guiden om kryptering).
12. Stäng Tor-webbläsaren när du är färdig. Webbhistorik och kakor rensas då ut automatiskt.

Ibland kan du få problem att komma åt vissa webbsidor när du använder Tor. Det kan bero på att vissa utgångar ur Tor-nätverket är svartlistade av olika skäl. Du kan i så fall välja att byta utgångspunkt.



Klicka på ”Use a New Identity” i Vidalia. Kontrollera att du fått en ny IP-adress, exempelvis på http://whatismyipaddress.com.

För att öka säkerheten när du använder Tor finns ytterligare en del saker att tänka på:

Installera inga insticksprogram. Programmen har flera nackdelar. Framför allt kan flera av dem avslöja din IP-adress. De kan också bidra till att skapa en profil, som gör att du kan bli igenkänd även utan IP-adressen. Tor blockerar flera insticksprogram av de här skälen. Det gör att du exempelvis inte kan titta på YouTube-klipp. Läs på i manualen om du vill ta dig runt det problemet.

Öppna inga dokument som du laddar hem medan du är uppkopplad. Om dokumenten innehåller Internetkopplingar kan de gå förbi Tor – och din riktiga IP-adress avslöjas. Det bästa är att bara ladda hem dokumenten, och öppna dem senare på en dator som inte står i kontakt med nätet alls.