Internetguide #39

Kom igång med Tor!

internetguider.se

Anders Thoresson

I den här guiden lär du dig...

- ☑ Hur din dators ip-adress kan avslöja vem du är.
- ☑ Hur Tor kan hjälpa dig att tillfälligt ”låna” ip-adresser på ett säkert sätt.
- ☑ Hur du använder Tor Browser.
- ☑ Vilka fallgropar som kan avslöja dig även om du använder Tor Browser.

Innehåll

Vad är problemet?

Vad är problemet?

Vi är inte anonyma på internet. Istället lämnar vi gott om digitala fotspår efter oss. På många olika sätt.

Datorer som kopplas till internet får en så kallad ip-adress, nätets motsvarighet till den fysiska världens gatuadresser. Ip-adresserna behövs för att all data som skickas på nätet ska komma fram till rätt mottagare.

IIS webbplats www.iis.se finns exempelvis på ip-adressen 91.226.36.46. Det är från servern som svarar på den adressen, i en datorhall i Stockholm, som din webbläsare får text och bild när du surfar in på stiftelsens webbplats. Adressen med bokstäver finns helt enkelt till för att den är enklare att komma ihåg än en massa siffror.

Men för att servern i Stockholm ska kunna skicka den efterfrågade webbsidan till rätt dator måste den i sin tur veta till vilken ip-adress sidan ska levereras. Det är alltså inte bara webbservrar som har ip-adresser. Alla datorer, mobiltelefoner, surfplattor och andra prylar som ansluts till internet har en ip-adress.

En konsekvens av detta är att varje företag, organisation eller privatperson som driver en webbplats kan se vilka ip-adresser som besöker den. Ofta går det också att ta reda på vem det är som haft en viss ip-adress vid ett visst tillfälle. I Sverige och många andra länder, finns det lagar som reglerar hur dessa uppgifter får hanteras, men det finns inga tekniska hinder för att göra den kontrollen.

Ett sätt att försöka dölja sin identitet är därför att låna någon annans ip-adress. Grundprincipen är enkel: Istället för att ansluta direkt till webbplatsen man vill besöka går man via en annan dator.

För det här finns olika tekniska lösningar. Så kallade proxyservrar är en, VPN en annan.

Med en proxyserver tar trafiken helt enkelt en omväg: Din dator talar om för proxyn vilken webbsida den vill ha. Proxyn hämtar den, och visar då sin och inte din ip-adress, och skickar sedan sidan vidare till dig. Du kan tänka på proxy som att du surfar via en annan dator, en bulvan.

VPN, virtual private network, är en teknik som ursprungligen utvecklades för att anställda på ett säkert sätt ska kunna använda företagets nätverk när de är ute och reser. Med VPN skapas en krypterad förbindelse mellan den anställdes dator och företaget. Den som sedan surfar vidare ut på internet visar VPN-serverns ipadress i stället för sin egen – ett sätt att skaffa sig ökad anonymitet.

Ett mer vardagligt exempel är det som händer när du tar med din bärbara dator hem till en vän och kopplar upp dig mot det trådlösa nätverk som finns där. Det är fortfarande din dator du använder, men allt tjänsterna på nätet kommer att se är att de får en besökare från din väns internetanslutning.
Men de här lösningarna ger inte tillräckligt skydd för någon som har höga krav på anonymitet. Den som ansvarar för en proxy- eller VPN-server kan nämligen hålla koll på vilka webbplatser en viss användare besöker. Och att låna en väns internetanslutning riskerar att i stället orsaka denne problem.

Ip-adresser är inte heller det enda som sätter anonymiteten på internet ur spel. Cookies är en annan nätegenskap som kan avslöja en del om vem du är. Cookies är små filer som används för att följa användare mellan olika webbplatser. De utnyttjas bland annat som underlag i nätreklam, där personer som besökt vissa webbplatser sannolikt är intresserade av en viss typ av reklam.

Slutligen finns risken att någon avlyssnar vad du gör på nätet. Det kan handla om myndigheter, som NSA eller FRA, eller om någon som sitter på samma kafé som du och tjuvtittar på all trafik som skickas i det trådlösa nätverket som finns för gästerna.

Det här är Tor

Det här är Tor

Nätets bristande anonymitet beror alltså på en kombination av spårbarhet kopplad till ip-adresser och cookies samt risken för avlyssning.

Tor är ett anonymiseringsverktyg som löser den del av problemet som är kopplad till ip-adresser, men som till viss del även tar sig an de övriga två. Det finns likheter mellan Tor och ett VPN. I båda fallen krypteras trafiken så länge den befinner sig inne i tjänsten och dessutom får den uppkopplade datorn en annan ip-adress. Skillnaden mellan Tor och ett VPN är att det inte går att veta vem som fått låna en viss ip-adress.

Anledningen till detta är sättet som din dator får en ”låna” en ip-adress på. Tor är ett nätverk med några tusen datorer som skickar trafik mellan sig. När din dator kopplar upp sig skickas trafiken mellan tre av dessa och sedan vidare till slutdestinationen. All trafik som din dator skickar och tar emot via Tor krypteras i tre lager, på ett sätt som gör att ingen av de tre datorerna kan koppla trafiken till dig. (Det finns dock ett viktigt undantag som vi återkommer till i sista avsnittet!)

Tor har sina rötter i ett utvecklingsprojekt i den amerikanska marinen 1. Den ursprungliga idén var att skydda myndigheters kommunikation. Idag utvecklas mjukvaran, vars källkod är öppen, av en ideell stiftelse registrerad i USA. Finansiellt stöd kommer bland annat från svenska Sida och Broadcasting Board of Governors, den amerikanska paraplyorganisationen för radiostationer som Voice of America, Radio Free Europe och Radio Free Asia.

Att svenskt bistånd går till utvecklingen av Tor beror på att det är ett viktigt verktyg i länder med totalitära regimer. Med Tor får medborgarna möjlighet att använda internet utan att avslöja vilka de är eller för att undvika censur.

Så surfar du anonymt

Så surfar du anonymt

I det här avsnittet går vi igenom stegen som krävs för att komma igång med Tor Browser, vilket inte är en särskilt komplicerad process.

Men när du är klar med installationen finns det ett antal misstag du ska undvika för att inte röja din identitet trots att du använder Tor. Läs därför även nästa avsnitt noga!

1

Skaffa Tor Browser

Öppna din vanliga webbläsare och surfa till https://www.torproject.org

Här klickar du på den stora lila knappen, *Download Tor*.

2

Sannolikt känner webbsidan av vilken typ av dator du använder – Windows, Mac eller Linux – och med ett klick på *Download Tor Browser* kommer du hämta den version som passar din dator.

Om webbsidan inte lyckas avgöra vilket operativsystem du använder eller om du vill ladda ner Tor Browser för att köra programmet från en annan dator kan du klicka på rätt operativsystem till höger om knappen.

När installationsfilen har hämtats till din dator dubbelklickar du på den. Kör du Windows dyker en ruta upp där du får välja i vilken mapp på datorn Tor Browser ska hamna. Kör du Mac dubbelklickar du på den nedladdade filen och drar ikonen till din programmapp på hårddisken.

Kontrollera den nedladdade filen

På nätet finns alltid en risk att program du laddar ner är manipulerade, så att de exempelvis loggar allt du skriver på tangentbordet och skickar den informationen till en server på nätet.

Därför är det viktigt att du alltid laddar ner program från trovärdiga källor, i det här fallet Tors egen webbplats.

Förbindelsen till webbplatsen ska dessutom vara krypterad, så att adressen i din webbläsares adressfält inleds med texten https istället för http. På så sätt minskar du risken för att någon byter ut filen på vägen.
Instruktioner för hur du använder krypteringsprogrammet GnuPG för att kontrollera din kopia av Tor Browser hittar du på Tors webbplats[2].

Om du inte kommer in på Tors webbplats
Ibland händer det att möjligheten att besöka Tors webbplats är spärrad. I vissa länder är censurförsök anledningen, andra gånger handlar det om företag som vill hålla koll på hur de anställda använder nätet.

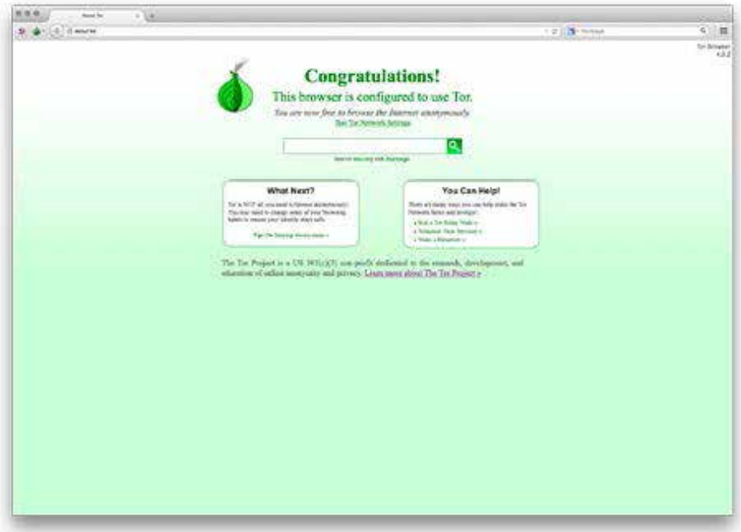
Oavsett anledning, om du inte kan besöka https://www.torproject.org finns det alternativa sätt att ladda ner Tor Browser.

Ett är att skicka ett mejl till *gettor@gettor.torproject.org* med help som enda text. Som svar får du då ett mejl med instruktioner om andra sätt att ladda ner Tor.

3

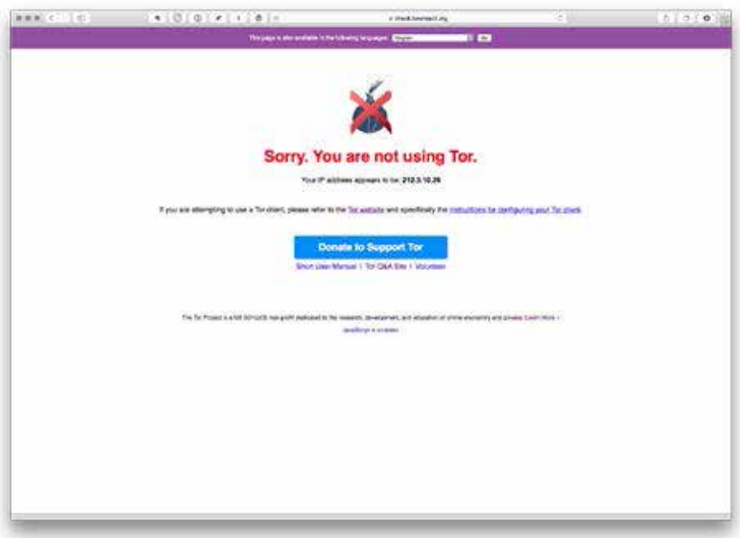
Använda Tor
När programmet finns på din dators hårddisk – eller ett usb-minne om du så vill – startar du Tor Browser på samma sätt som alla andra program: Med ett dubbelklick. Uppstarten tar dock lite längre tid än du är van vid. Anledningen är att Tor Browser först skapar en kryp-terad väg ut på internet. Tor Browser ansluter till nätet via tre andra datorer och får i sista steget ”låna” en ip-adress. Det är denna ip-adress och inte den som din dator fått från din internetleverantör som andra nu kommer att se när du surfar på nätet med Tor Browser.

När Tor Browser har startat ska du mötas av en webbsida som visar att du nu surfar via Tor.



4

Om du öppnar din vanliga webbläsare och surfar till adressen https://check. torproject.org får du se skillnaden.



5

Ett annat sätt att se hur Tor Browser skiljer sig från din vanliga webbläsare är att besöka webbsidan http://www.whatismyipaddress.com. Det är en webbsida som visar vilken ip-adress som din dator använder.

Knappar du in adressen i din vanliga webbläsare kommer ip-adressen från din internetleverantör att visas. Befinner du dig i Sverige kommer antagligen en punkt i din fysiska närhet att vara markerad på kartan. Undantaget är om du surfar via mobilnätet, då kan kartnålen istället sitta långt från den plats där du är.

6

Om du sedan besöker http://www.whatismyipaddress.com från Tor Browser kommer du se en helt annan ip-adress och en helt annan kartvy.

Det här är ip-adressen för den dator där din Tor Browser lämnar Tor-nätet och fortsätter vidare ut på internet. För andra på nätet ser det alltså ut som att det är härifrån du surfar.

7

Tor i mobilen
Har du en Android-telefon finns möjligheten att använda Tor även på den. Besök https://guardianproject.info för att få veta mer.

Det finns däremot appar som utger sig för att använda Tor. Var misstänksam mot dessa appar, och använda bara de du verkligen litar på. Använd helst bara Tor Browser på din dator, när det är möjligt

Fallgropar att undvika

Tor Browser må vara enkelt att installera. Men för att programmet ska fungera som det är tänkt är det viktigt att du använder det på rätt sätt. Annars finns en risk att du inte alls är anonym när du surfar på nätet.

Tor Browser är egentligen ett paket med flera olika program. Webbläsaren, i grunden en specialversion av Firefox, är det du ser. Men i bakgrunden finns bland annat program som ansluter din dator till nätverket Tor, det nätverk som ser till att du får ”låna” en annan ip-adress.

När din dator är ansluten till Tor finns plötsligt två vägar ut från den: Antingen den vanliga vägen, som exponerar den ip-adress som du fått tilldelad av din internetleverantör. Eller via Tor, med en lånad ip-adress.

Problemet är att bara de program som du uttryckligen ställer in att de ska använda Tor kommer att ta den vägen. Alla andra fortsätter som vanligt. Det fina med Tor Browser är att webbläsaren är inställd att använda Tor.

Utgå därför bara från att det är Tor Browser som är anonymiserad medan alla andra program, som din vanliga webbläsare och program för chatt och e-post, presenterar sig med din vanliga ip-adress. Det går att göra inställningar så att fler program än Tor Browser skickar sin trafik via Tor och därmed blir anonymiserad,men det tar vi av utrymmesskäl inte upp i det här materialet.

När du vill utnyttja Tor för att bli anonym på nätet är det första steget alltså att säkerställa att du verkligen använder ett program som skickar sin trafik via Tor – och det enklaste sättet att göra det är att använda Tor Browser.

Nästa steg är att förstå hur Tor gör dig anonym: Genom att förse din dator med en tillfällig ip-adress som inte går att koppla till dig. Men om du använder den tillfälliga ip-adressen för att exempelvis logga in på konton som går att koppla till dig riskerar du att avslöja vem du är. En bra grundprincip är därför att bara använda Tor Browser för sånt som kräver anonymitet, din vanliga webbläsare för allt annat. Genom att separera det du gör i två olika webbläsare och vara noggrann med att följa den principen minskar risken för att du gör något fel.

En annan 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 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 användare krypterade förbindelser, det vill säga https istället för http i webb-läsaren.

Slutligen kortfattat om några andra fallgropar som kan äventyra din anonymitet:

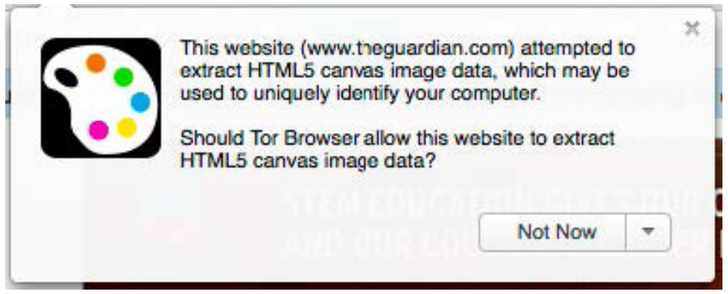
Installera inga tillägg i Tor Browser eftersom de kan luras att avslöja din ip-adress. Tor Browser saknar av den anledningen möjlighet att visa filmer och animerat innehåll som är gjort med Flash. Därmed är det inte säkert att allt innehåll på webben fungerar som det är tänkt.

Ladda inte ner filer med hjälp av fildelningstekniken BitTorrent. Din vanliga ip-adress kommer användas även om du ställt in att ditt torrent-program ska använda Tor. Se upp med nedladdade dokument, som pdf- och doc-filer. Det händer att de hämtar innehåll från nätet när de öppnas och kan då exponera din ip-adress. Om de nedladdade filerna är känsliga, öppna dem först när du kopplat ner datorn från internet.

Var medveten om att den internetoperatör som du använder för att ansluta till internet kan se att du kopplar upp dig mot Tor. Oftast är det inget problem, men i vissa situationer eller länder kan Tor-användning ses som något misstänkt.

Varningar om att dina användarkonton, exempelvis på Gmail, kan vara hackade kan bero på att du surfar via Tor när du loggar in. Eftersom du får en ny ip-adress från Tor varje gång du kopplar upp dig kommer vissa tjänster se att du loggar in från många olika ip-adresser vilket kan orsaka intrångsvarningen.

Om du får en fråga om att tillåta en webbplats att hämta ”HTML5 canvas image data”, svara nej. Det här är ett sätt som gör det möjligt att identifiera din webbläsare och på sikt även dig.[3].



Gömda tjänster

För att minska problemen med att Tor-trafiken avkrypteras i sista steget finns något som kallas *hidden services*. Det är webbservrar och andra tjänster som körs inne i Tor-nätet. Trafik till och från dem behöver därmed aldrig lämna Tor och blir därmed svårare att avlyssna.

Det här utnyttjas bland annat av en del redaktioner som vill göra det möjligt för allmänheten att lämna anonyma tips.

Tails – det Tor-ifierade operativsystemet

När du installerar Tor i din vanliga dator är grundinställningen att bara det du gör i Tor Browser går via Tor. Det är ett problem av två anledningar: Du vill kanske vara anonym även när du använder andra internettjänster än de du kommer åt via en webbläsare. Och du vill kanske minska risken för att slarva och råka använda fel webbläsare.

En lösning är Tails, en specialversion av Linux. En viktig del är att Tor är inbyggt och att all internettrafik går via Tor och därmed anonymiseras med en lånad ip-adress. Tails kan installeras på en usb-sticka, så att du kan andvända det på i princip vilken dator som helst.

Se mer på https://tails.boum.org

Lär dig mer

Lär dig mer om digitalt källskydd!

Det innehåll som du just läst hör ihop med Internetguiden ”Digitalt källskydd – en introduktion”. Det är en guide till ökat källskydd som riktar sig till journalister, arbetsledning och andra som arbetar redaktionellt. Innehållet är framtaget i samarbete med Svenska Journalistförbundet. Guiden är kostnadsfri att ladda ned eller läs mer på internetguider.se

Fotnoter

1. Tor: Overview – (https://www.torproject.org/about/overview.html.en)
2. How to verify signatures for packages – (https://www.torproject.org/docs/verifying-signatures.html.en)
3. Cross-Origin Fingerprinting Unlinkability – (https://www.torproject.org/projects/torbrowser/design/#fingerprinting-linkability)

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 Teknik-bloggen på dn.se. Han föreläser i samma ämnen, bland annat om digitalt källskydd för journalister och programmering i skolan för lärare och skolledare. Anders Thoresson har författat flera Internet-guider för IIS, exempelvis om programmering för barn, it-säkerhet, webbpublicering och omvärldsbevakning. Du hittar dem här: internetguider.se

Foto: Sebastian LaMotte CC-BY ND

Kom igång med Tor!
IIS Internetguide #39
Version 2.0 2016

IIS klimatkompenserar för sina koldioxidutsläpp och stödjer klimatinitiativet ZeroMission.

Författare: Anders Thoresson
Redaktör: Hasse Nilsson
Projektledare: Jessica Bäck
Formgivning: Detail Produktionsbyrå
ISBN: 978-91-7611-450-6

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. www.internetguider.se

Internetstatistik
Vi tar fram den årliga, stora rapporten ”Svenskarna och internet” om svenskarnas användning av internet och dessemellan ett antal mindre studier. www.soi2015.se

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 för 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. internetguider.se

---

Nya Internetguider!

Yttrandefrihet på nätet
Av: Nils Funcke

Det som enligt svensk lag får sägas och visas på internet är ett ständigt omdebatterat ämne. Det gäller även vad yttrandefrihet egentligen är och hur det fungerar på internet.

Nils Funcke är journalist, författare, debattör och utbildare som bland annat varit utredningssekreterare i Yttrandefrihetskommittén och tilldelats Stora Journalistpriset. Han reder ut begreppen både rent praktiskt och historiskt sett. Guiden avhandlar sådant som yttrandefrihetens grunder, vad som är yttrandefrihetsbrott, ansvar och skadestånd och förslag på lagändringar.

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.