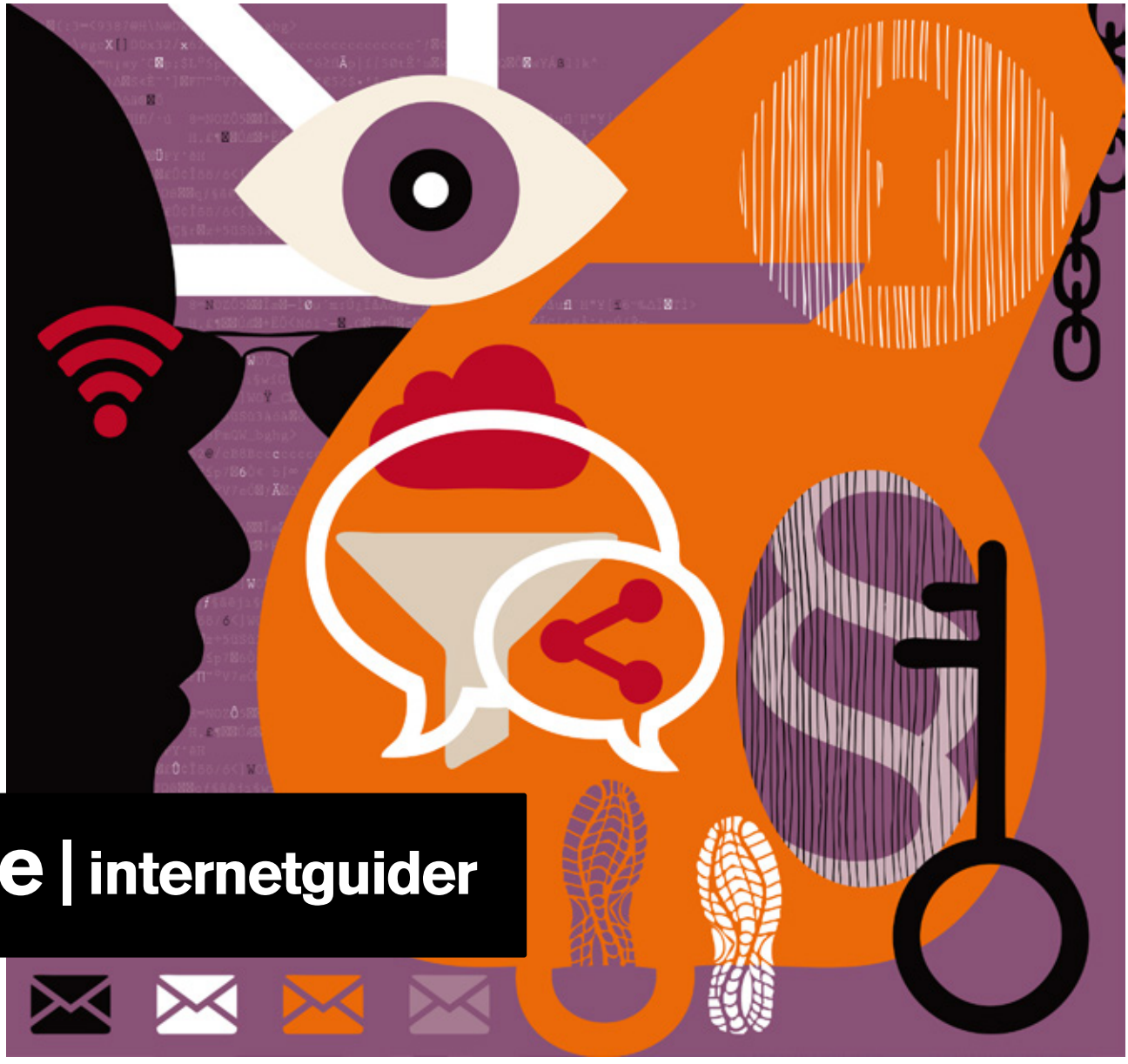
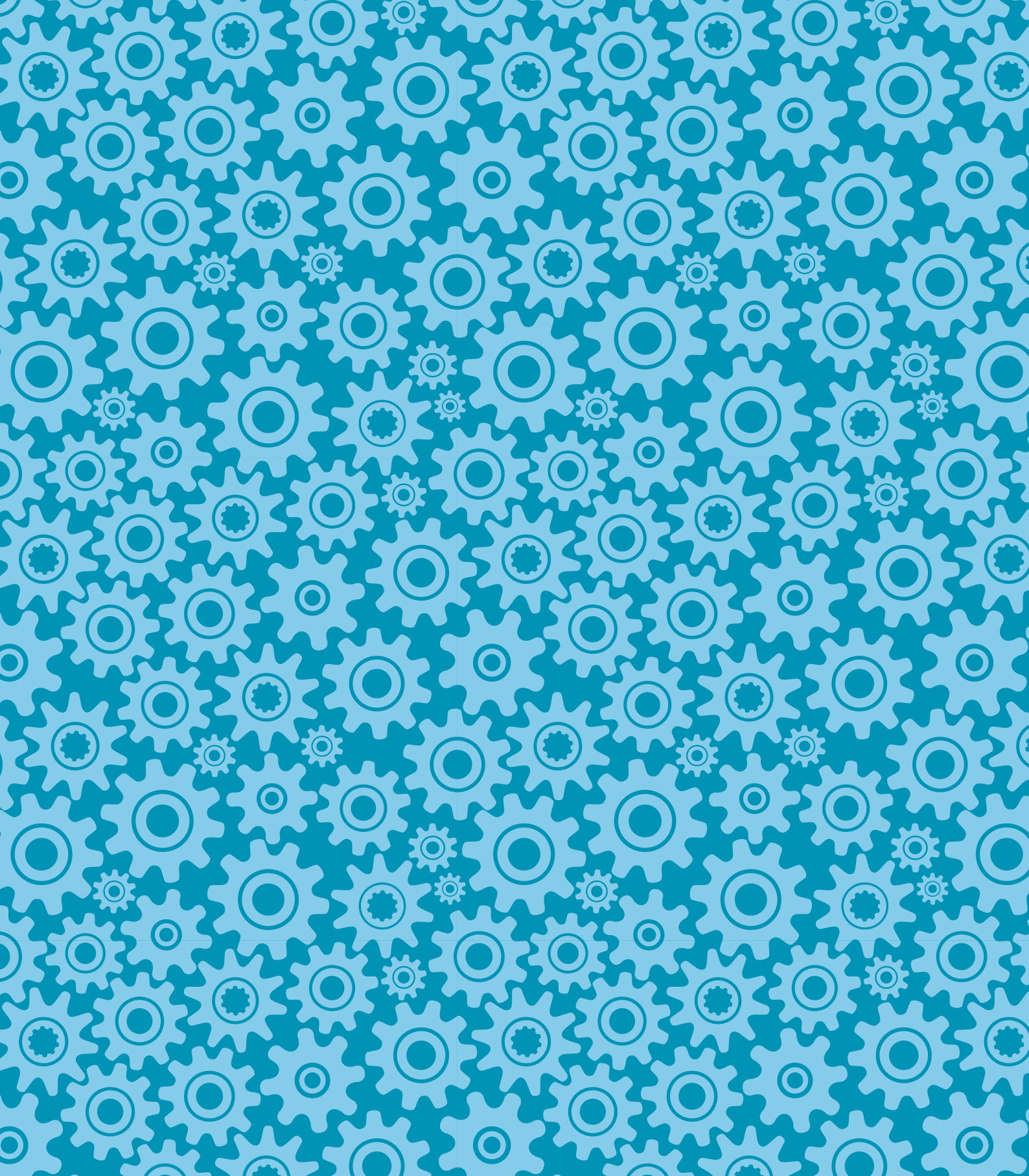
Martin Edström och Carl Fridh Kleberg

Digitalt självförsvar

– en introduktion



.se | internetguider



Martin Edström och Carl Fridh Kleberg

Digitalt självförsvar

– en introduktion

Digitalt självförsvar
.SE:s Internetguide, nr 36
Version 1.0 2015
Martin Edström och Carl Fridh Kleberg

.SE klimatkompenserar för sina koldioxidutsläpp och stödjer klimatinitiativet ZeroMission. Se www.zeromission.se för mer information om ZeroMission.

Författare: Martin Edström och Carl Fridh Kleberg
Redaktör: Hasse Nilsson
Projektledare: Jessica Bäck
Formgivning: Bedow
Omslagsillustration: Camilla Atterby
Första upplagan.
Tack till: Jonas Lejon, Eva Galperin, Sus Andersson, Anders Thoresson och Lennart Bonnevier.
ISBN: 978-91-87437-21-2

.SE (Stiftelsen för internetinfrastruktur) ansvarar för internets svenska toppdomän. .SE är en oberoende allmännyttig organisation som verkar för en positiv utveckling av internet i Sverige.

Alla .SE:s Internetguider
Du hittar alla .SE:s utgivna Internetguider på www.iis.se/guider.

Organisationsnummer: 802405-0190
Besöksadress: Ringvägen 100 A, 9 tr, Stockholm
Brevledes på .SE Box 7399, 103 91 Stockholm
Telefon: +46 8 452 35 00. Fax: +46 8 452 35 02
E-post: info@iis.se www.iis.se

Innehåll

Innehåll forts.

Förord

Den här boken ämnar ge dig kunskap och handfasta tips på hur du kan kommunicera säkrare på nätet. Vi vänder oss i första hand till människor som har information de vill ska komma ut till allmänheten – tipsare och uppgiftslämnare. Det kan handla om känslig information från en konflikt, ett skeende eller om ett missförhållande på en arbetsplats.

Det finns också mycket att hämta även för dig som kanske inte redan nu behöver lämna vidare ett tips, men ändå vill börja kommunicera på ett säkrare sätt. Och för dig som helt enkelt vill veta lite mer om hur internet fungerar och all kommunikation detta enorma nätverk rymmer.

Vi vill med denna guide ge dig en introduktion till säkerhet på nätet, och ge dig hjälp att med enkla verktyg lyckas skydda dig mot de hot som finns mot vår kommunikation och information på nätet.

En stor del av motivationen till att skriva denna bok kommer från de avslöjanden som gjordes under 2013, i samband med uppgiftslämnaren – även kallad visselblåsaren (från engelskans ”whistleblower”) – Edward Snowden. Med hans hjälp kunde medier avslöja att bland annat USA:s och Storbritanniens myndigheter genomfört omfattande övervakning av såväl toppolitiker som vanliga medborgare.

Framförallt hamnade ljuset på informationssamhällets brist på integritet, och hur vi i mångt och mycket står helt utelämnade till internets fällor och falldörrar. Detta gäller alla samhällsgrupper.

I frontlinjen för detta krig om informationen ligger de journalister och uppgiftslämnare vars kommunikation utgör en enormt viktig demokratisk funktion. Medborgares rättighet, och möjlighet, att slå larm om missförhållanden i sin omvärld är viktigare än någonsin. Men svårigheten i att kommunicera säkert, och därmed risken att bli avslöjad som uppgiftslämnare, är kanske värre än någonsin.

Vi tycker du har rätt att kommunicera och slå vakt om missförhållanden utan att riskera ditt arbete, din familj eller ditt liv.

01 Kunskap är makt

Du kan inte ta bra säkerhetsbeslut om du inte har god kunskap i ämnet. Ju mer du vet, desto mer välgrundade beslut kan du ta. Det gäller självklart också din arbetsgivare, myndigheter och andra organisationer som baserar sina säkerhetsbeslut på kunskap. Troligtvis sitter de oftast på mer information än du – varför det blir extra viktigt att du lär dig så mycket det bara går.

Den svagaste länken

Säkerhet på nätet fungerar precis som i det gamla ordspråket ”en kedja är bara så stark som sin svagaste länk”. Om du, likt i exemplen i denna guide, monterar ett extra lås på din dörr – men samtidigt har simpla fönster som en inbrottstjuv enkelt kan forcera – då har huset knappast blivit säkrare.

På samma sätt fungerar det med ditt kassaskåp eller din kryptering (som du ska få lära dig om nedan). Om du krypterar en fil innan du skickar den vidare, men samtidigt behåller en okrypterad kopia på din laptop som sedan blir stulen – då kan dokumentet knappast sägas vara hemligt.

Enklare är säkrare

Det bästa sättet att förvara information är troligtvis i huvudet. Ingen kan läsa den, ingen kan råka snubbla över informationen. Om du skriver informationen på en lapp, som du sedan gömmer under sängen, har systemet genast blivit lite mer komplicerat. Hur ska du kunna säkerställa att ingen letar under din säng?

På samma sätt blir saker och ting genast än mer komplicerade då du förvarar information på nätet eller kommunicerar via nätet. Men denna tumregel fungerar – ju enklare dina rutiner är, desto säkrare är de.

Dyrare lösningar är inte alltid säkrare

Tro inte att de dyraste lösningarna är bäst. Att investera i ett dyrt säkerhetssystem är sällan det smartaste man kan göra. Det finns oftast enkla förändringar, som går

att göra utan kostnad, som ändå leder till ett säkrare system i sin helhet. Sträva också efter att alltid säkra den svagaste länken i ditt system, inte den starkaste. Att rutinmässigt ta känsliga diskussioner vid ett fysiskt möte, istället för över e-post, är ofta enklare än att använda tjänster för e-postkryptering och leder troligtvis till säkrare kommunikation överlag. Det handlar bara om ändrade rutiner.

Öppen källkod

Faktum är att många av dagens bästa säkerhetslösningar, både till säkerheten och användarvänligheten sett, är gratislösningar. Många av dem är programvaror med så kallad öppen källkod (från engelskans open source).

Det betyder att källkoden till programvaran och dess byggstenar är öppna för allmän beskådan. Vem som helst kan ta en titt på koden som ligger till grund för dessa lösningar. Vem som helst kan också fortsätta bygga vidare på dem.

Detta gör att tusentals människor har ögonen på dessa programvaror. Till skillnad från kommersiella programvaror med stängd källkod kan därför programvaror med öppen källkod granskas av alla. Därmed blir det svårt att smyga in skadlig kod eller bakdörrar.

Flera av de programvaror och tekniker vi rekommenderar i kapitlet ”Att kommunicera säkrare” bygger på lösningar med öppen källkod, och de allra flesta av dem är gratis.

02 Det finns ingen perfekt säkerhet

Du måste hantera säkerhet på internet på ett sätt som är möjligt att genomföra på daglig basis. Självklart bör du anpassa dina åtgärder till din hotbild, men åtgärderna får inte sätta för stora hinder för ditt dagliga liv. Om din säkerhetspolicy är för jobbig att följa, riskerar du att inte orka följa den.

Det som är säkert i dag är inte säkert i morgon

Teknik förändras och förbättras varje dag. De som vill dig illa, eller de som vill åt din information, kommer alltid att kunna ligga steget före. Du bör veta detta och aldrig lita på att du vet tillräckligt. Det gör ingen. Men genom att uppdatera dina säkerhetsverktyg efter bästa förmåga kommer du en lång bit på vägen.

Det som är juridiskt svårt är tekniskt enkelt

Med dagens tekniska lösningar för övervakning ter det sig, från de exempel som kommit i ljuset av bland annat Edward Snowdens avslöjanden, väldigt lätt för myndigheter i exempelvis USA att titta på människors privata konversationer på nätet.

Tekniskt sett är det väldigt enkelt. Myndigheter kan med blott några knapptryck se hur, var, när och vad du kommunicerar.

Däremot är det juridiskt svårt för en myndighet att få tillstånd för den typen av övervakning. Det krävs ofta domstolsbeslut för att få övervaka någon enskild person.

Men på grund av att det är så tekniskt enkelt är det lättare för någon att utnyttja systemet – även utan tillåtelse. Bara det faktum att det så enkelt går att inleda övervakning gör att vi måste anta att systemet – på grund av den mänskliga faktorn – ibland utnyttjas utan tillåtelse.

Viktigt!

Uppdatera mera!

Det är av yppersta vikt att du uppdaterar ditt operativsystem och de program och appar du använder. I de allra flesta fall har operativsystemet (Windows, OS X, IOS, Android och så vidare) någon inbyggd funktion som letar upp och installerar en ny version när en sådan finns tillgänglig. Gör det till en vana att använda den en gång i veckan, exempelvis.

03 Avslöjanden som gjordes tack vare uppgiftslämnare

Vilket är världens mest kända journalistiska avslöjande någonsin? Tja, någon objektiv måttstock är svår att hitta men Watergateskandalen, de amerikanska journalisterna Bob Woodwards och Carl Bernsteins avslöjande om maktmissbruk på högsta nivå som 1974 tvingade president Richard Nixon att avgå, smäller högt. Men där hittar vi inte bara världens kanske största scoop, utan också världens mest kända uppgiftslämnare, ”Deep Throat”. Utan ”Deep Throat”, som senare visade sig vara FBI:s tidigare biträdande chef, hade det legendariska avslöjandet aldrig blivit av. Men det hade knappast varit möjligt för ”Deep Throat” att dela med sig av uppgifterna, om det inte var för att hans identitet kunde skyddas.

Ett drygt decennium senare pågår utredningen av mordet på Sveriges statsminister Olof Palme för fullt. En dag i mars kliver den dåvarande DN-journalisten Ann-Marie Åsheden in på polishuset för det första i en serie möten med spaningsledare Hans Holmér. Därefter kommer hon i nästan ett år att ”inbäddad” följa spaningarna efter Palmes mördare, ända fram tills Holmér tvingas lämna utredningen. Men stormen kring Holmér mojnar inte, och 1988 tvingar Justitiekanslern fram en bekräftelse från Ann-Marie Åsheden om att hennes källa varit Holmér. Trots detta ser många journalister tillbaka på den tiden med varm nostalgi. 1988 var det nämligen journalisten och branschens kollektiva hederskodex som garanterade källskyddet, och det var också därför det krävdes en ed för att avtvinga Åsheden källans identitet. I dag, 26 år senare, är det inte lika självklart att Åsheden ens behövt tillfrågas, och kanske ännu mindre självklart att alla journalister kan garantera källskyddet. Det stora flertalet journalister och deras chefer vet i dagsläget inte hur de ska värna källornas anonymitet på digital väg. En källa kan därför behöva välja både redaktion och journalist med stor omsorg.

I dag vet många vilka du kommunicerar med, och ibland även hur och när. Telefon- och datanätverk är inte alltid svåra att övervaka ens för en amatör, för att inte tala om den tillgång operatörer, myndigheter och arbetsgivare har.

Som ovan nämnt var ett av 2013 års största scoop Edward Snowdens avslöjande om den massiva övervakning USA och andra länder ägnar sig åt. Men Snowden var väl medveten om de risker som var involverade i avslöjandet, och arbetet med avslöjandet ställde enorma krav på digital säkerhet.

Man behöver inte ha ett avslöjande stort som Snowdens för att behöva kunna lite om digitalt källskydd. Inte heller behöver man hans expertis. Det vi kanske alla, i egenskap av möjliga uppgiftslämnare, kan komma att behöva någon gång är lite grundläggande verktyg och tankesätt med vilka vi kan skydda oss själva. Det är också därför den här handboken finns.

04 Vem tittar på dig och varför?

Big data

Begreppet ”Big data” (omfattande data) har blivit allt mer vanligt att läsa och höra talas om. Men vad betyder det?

Vi har skiftat våra arkiv från papper och pärmar till digitala filer och databaser. Det gäller allt. Banker, sjukhus, skolor, tågsystem, riksarkiv – allt håller på att digitaliseras. Det gäller inte minst dina egna privata data. I dag lagras allt från dina digitala foton till dina försäkringar och kreditkortsuppgifter på datorer och i mobilen.

Dessutom använder många webbaserade e-posttjänster och sociala medier, där ännu mer information om oss lagras. På Facebook finns dina foton, privata meddelanden och information om vad du gillar. I din e-post finns också massor av information – inte bara själva breven du skickar, utan dessutom information om varifrån och när de skickades.

När man räknar upp alla olika ställen där dina data finns lagrade blir det snart uppenbart hur beroende vi är av de digitala ettor och nollor som lagrar allt vi vill. Det står också klart att det finns en enorm mängd information om alla människor, sparat på hårddiskar runtom i världen – oftast utan att du riktigt vet var. Det blir snabbt både oöverskådligt och fullständigt ohanterligt. Det är här begreppet ”Big data” kommer in.

Naturligtvis finns det massor av anledningar till att personer, företag och myndigheter vill kunna sålla i all denna lagrade information. På samma sätt som en fotograf vill hålla koll på alla sina bilder – och kunna hitta rätt bild när den behövs – använder exempelvis polisen verktyg för att filtrera all information om kända brottslingar. Företag använder de omfattande mängderna data för att allt från personifierade erbjudanden till att utnyttja beteendemönster i kommersiellt syfte. I takt med att tillgången till information ökar blir verktygen också mer sofistikerade.

Trattmodellen

Tänk dig en stor tratt. Genom den stora öppningen kan tratten ta in all information, och genom rätt filter kommer bara den efterfrågade informationen ut på andra sidan.

Ju mer du slänger in i tratten, desto större chans att något intressant kommer ut. Genom sofistikerade filter kan tratten sålla fram bara precis det man vill veta.

Föreställ dig nu att det finns myndigheter i världen som har tillgång till stora delar av den information som finns lagrad om dig – delar av din e-post, dina kommentarer från Facebook, dina betyg i högstadiet och annat som du tänker på som privat. Om de kan slänga in all denna information i tratten, så är chansen större att de får ut den information de vill ha.

Det viktigaste att förstå här är den metod med vilken informationen samlas in, och de incitament som finns till att samla in mer.

Ju mer information du har tillgång till, och kan kasta in i tratten, desto mer kan du filtrera fram. För de myndigheter som exempelvis vill stoppa terrorister finns det därför ett stort incitament att samla in så mycket information som möjligt. Det ökar deras möjlighet att sålla fram rätt information, och därmed kunna sätta stopp för terroristerna. Ju mer information som lagras om oss alla desto mer omfattande blir övervakningen. Det är dock diskutabelt om den så kallade massövervakningen verkligen ger resultat jämfört med riktad spaning på individer och grupper av individer.

05 Hotbild och riskanalys

Då vi talar om digitalt självförsvar och hur man kan skydda sitt privatliv på internet är det första steget att göra en riskanalys. Det är ett helt avgörande steg. Om du inte etablerat vilket hot du kan behöva skydda dig ifrån, hur ska du då kunna skydda dig? Du kan likna ditt digitala självförsvar vid en bostad. Ett vanligt hus i ett område med många liknande hus, som inte sticker ut på något sätt. Vi ska nu titta på några olika hotbilder, och se vad du kan göra för att skydda dig på bästa sätt från potentiella hot.

Hotbild 1: Inbrottstjuvar

Ett första möjligt hot är förstås inbrottstjuvar. Inbrottstjuvar, som ofta väljer hus som är lätta att bryta sig in i, är ute efter något värdefullt att stjäla. Det värdefulla kan vara i princip vad som helst, men måste vara någorlunda lätt att komma över. Inbrottstjuvarna bryter sig hellre in i en dåligt skyddad villa än i ett säkert bankvalv.

Håll koll på dina egna vanor

En sak som är lätt att glömma bort när du av olika anledningar vill höja din digitala säkerhet är dina vanor och vad du gör på nätet. Exempelvis bör du inte söka efter den här guiden och liknande information på webben när du är på jobbet om du funderar på att läcka information till pressen om något som inte står rätt till. Vart du surfar, mejlar och med vilka program registreras och kan avläsas på din jobbdator och via arbetsplatsens nätverk. Givetvis gäller det även datorn eller annan utrustning som du har hemma. Det beror exempelvis på vem eller vilka som också har tillgång till ditt hem.

Viktigt

Lär dig mer om din egen it-säkerhet!

I Internetguiden ”It-säkerhet för privatpersoner – en introduktion” får du en grundkurs i allt från hantering av lösenord till hur virus och skadlig kod fungerar. Guiden innehåller matnyttiga tips om enkla åtgärder för att hålla din uppkoppling, e-post, ditt Facebookkonto och dina bankuppgifter i säkrare förvar. Innehållet kräver inga särskilda förkunskaper. Materialet laddar du ned kostnadsfritt från www.iis.se/guider

Att skydda sig mot inbrottstjuvar kan därmed vara relativt enkelt. Genom att sätta upp några extra lampor, som tänds automatiskt på kvällen när någon närmar sig huset, kommer huset att se mer säkert och svårforcerat ut än de andra husen på gatan. Man kan också skaffa ett extra lås till dörren, och därmed försvåra för inbrottstjuvarna. Genom dessa små förbättringar på huset kommer troligtvis inbrottstjuvarna välja ett annat hus att bryta sig in i. Hur gör du då det här digitalt?

Om du vill skydda dina filer på datorn eller i mobilen, så bör du börja med enkla skydd – precis som du skyddar din bostad. Genom att ha ett lösenord till datorn, och en pin-kod till mobilen, kan du skydda dig från de flesta obehöriga. De kommer troligtvis vända på tröskeln, eftersom dörren är låst.

Hotbild 2: Inbrottstjuvar som är ute efter något specifikt

Om inbrottstjuvarna är ute efter att stjäla från just din bostad blir det genast mer komplicerat. Kanske vet inbrottstjuvarna att det finns hemliga dokument förvarade i hemmet. Då räcker nog varken starka lampor eller ett extra lås för att skydda de hemliga dokumenten. Tjuvarna kommer att göra sitt yttersta för att ta sig in, trots dessa faktorer.

I det här fallet bör du nog skaffa dig ett ordentligt kassaskåp i vilket du kan förvara dokumenten. Även om inbrottstjuvarna kan ta sig förbi låset på ytterdörren kommer nog kassaskåpet att vara för svårt att forcera och för tungt att flytta.

Tips!

Lär dig mer om krypterad e-post!

Lär dig använda PGP!
Till den här Internetguiden medföljer XL-materialet ”Kom igång med PGP!”. I dokumentet får du lära dig grunderna och hur du använder PGP i praktiken, steg-för-steg. Materialet laddar du ned kostnadsfritt från www.iis.se/guider

Hur gör du då detta digitalt?
Genom att kryptera dina filer och digitala dokument kan du skapa dig ett digitalt kassaskåp. Även om någon kan bryta sig in i din dator, eller i din mobil, så kommer krypteringen fungera som ett kassaskåp – och utan rätt nyckel kan ingen öppna det.

Hotbild 3: Myndigheter och strukturell övervakning

Tänk dig nu att hemmet du skyddar i själva verket är helt oskyddat. Att myndigheter, eller någon annan kraft i samhället med resurser nog, byggt hemliga tunnlar till alla hus i området. Tänk dig att de placerat ut svagheter i dörrarnas och fönstrens lås som gör att det blir lätt att göra inbrott om de tycker att det behövs.

Hur skyddar du dig från detta? Det kommer inte hjälpa att sätta upp lampor eller montera ett extra lås på dörren om en myndighet vill komma in i huset. Ett kassaskåp kan hjälpa, eftersom det trots allt behövs en nyckel för att öppna det. Men tänk om tillverkaren av kassaskåpet har samarbetat med myndigheterna? Tänk om myndigheterna har tillgång till en universalnyckel, som öppnar ditt och alla andras kassaskåp?

I det här läget behöver du verkligen ha koll på vem som tillverkat kassaskåpet för att kunna lita på säkerheten. När vi talar om myndigheter och strukturell övervakning krävs det plötsligt en hel del kunskap och resurser för att försvara sig. Hur gör du då detta digitalt?

Det kommer aldrig att gå att skydda din information med hundra procents säkerhet, speciellt inte om du skickar den vidare. Men det finns åtgärder du kan vidta för att varken inbrottstjuvar eller myndigheter ska få tillgång till den. Framförallt måste du identifiera vem du inte kan lita

på, och bestämma dig för vilka säkerhetslösningar du bör använda.

- *Din arbetsgivare*, som vill förhindra att viss information sprids.
- *Hackare*, som är ute efter just dina eller ditt företags filer och dokument.
- *Hackare*, som slumpmässigt väljer offer och som hackar datorer och annan utrustning för att det är kul.
- *Privata aktörer,* som av olika anledningar vill komma åt just din kommunikation.
- *Dina närstående*. Är informationen väldigt känslig kanske du inte vill att en partner eller släkting ska kunna förstå vad det är du gör.

Din arbetsgivare – ett hot?

Din arbetsgivare kan mycket väl bli ett hot mot din digitala säkerhet, om du väljer att göra något som arbetsgivaren inte vill att du ska göra. Om du vill uppmärksamma ett missförhållande på din arbetsplats – där din arbetsgivare är boven i dramat – finns det troligtvis stor motivation för arbetsgivaren att stoppa detta.

Det som ofta komplicerar relationen mellan dig som uppgiftslämnare och din arbetsgivare, är att arbetsgivaren innehar en maktposition. Du arbetar i dess lokaler, ofta på en dator som tillhör arbetsgivaren. Nätverket, genom vilket du kopplar upp dig mot nätet, tillhör arbetsgivaren. Det gör också en stor del av den tekniska utrustning som står till ditt förfogande på jobbet.

Hur går vi då runt detta?

Det viktigaste är att aldrig kommunicera om sin arbetsgivares verksamhet från arbetsgivarens lokaler – från en miljö de kontrollerar. Om en miljö kan antas vara kontrollerad innebär det i praktiken att den kan vara avlyssnad och övervakad. Det gäller även data- och mobiltrafik från och till lokalerna. Skickar du ett e-postmeddelande från din arbetsgivares dator till en journalist finns det stort risk att arbetsgivaren kan hitta vem som skickat det. Det kan liknas vid att bjuda upp journalisten till arbetsgivarens fikarum för att diskutera ett missförhållande. Det kommer att uppmärksammas.

Fler konkreta tips hittar du i kapitlet *”Att kommunicera säkrare”*.

06 Vad du har att förlora

Varför är det viktigt att vi skyddar vår kommunikation egentligen? Frågan är grundläggande, utan att på något sätt vara banal, dum eller oviktig. Tvärt om, för att veta hur vi kan tänkas behöva skydda vår kommunikation, till exempel om vi vill lämna uppgifter om att något inte står rätt till, är det inte bara viktigt att veta vem som kan tänka sig vilja förhindra det, utan också vad som kan hända om vi blir upptäckta.

I Sverige skyddar grundlagen offentligt anställdas rätt att lämna uppgifter till journalister genom meddelarskyddet, och chefer får till exempel inte försöka ta reda på vem det är som lämnat ut en uppgift. Privatanställda har däremot inte alls samma skydd, och i praktiken finns det exempel på chefer för offentliga verksamheter som brutit mot lagen för att jaga rätt på källor.

Den som blir påkommen med att ha lämnat ut uppgifter riskerar inte bara att bli av med jobbet eller i värsta fall juridiska påföljder, utan också sociala konsekvenser som utfrysning på jobbet, misstänksamhet i professionella sammanhang eller trakasserier. Det kan också vara lätt att underskatta hur jobbigt det faktiskt är att befinna sig i en sådan situation, och därför är det i regel bäst att skydda sina uppgifter även om man inte är så oroad – det är alltid möjligt att vid ett senare skede träda fram, men svårare att backa bandet när man väl är känd. Vilka risker man utsätter sig för varierar naturligtvis också från fall till fall.

2007 hamnade till exempel en kvinna i Sverige i kläm sedan hennes arbetsgivare, ett privat företag, begärt ut listan över ringda telefonnummer från hennes tjänstetelefon och där hittat numret till en journalist på Dagens Nyheter. Ingen vet vad de två talade om, men att numret fanns där räckte för att kvinnan till slut skulle lämna sitt arbete.

Då handlade det om ett jobb, vilket är viktigt nog i sig, men i vissa extremfall kan det vara en fråga om liv och död. Trots detta har journalister misslyckats med att skydda källor med hemska konsekvenser. 2011 ”försvann” flera syriska aktivister som träffat en amerikansk dokumentärfilmare, som dessförinnan gripits och inte skyddat sina datorer.

2012 avslöjade Sveriges Radios Ekot hemliga dokument om svenska vapenavtal med Saudiarabien som del i den så kallade ”Saudiaffären”, varpå svenska myndigheter ansåg att det kunde handla om brott mot tystnadsplikten och försökte ta reda på vem som läckt uppgifterna. Totalförsvarets forskningsinstitut (FOI) lämnade då in en anmälan om brott mot tystnadsplikten, vilket kan leda till fängelse om källan avslöjas.

07 Allmänt om fotspår

Att du lämnar efter dig olika typer av fotspår när du använder internet, telefoner, datorer och annan teknik är något många i dag känner till. Men vilka spår, var hamnar de egentligen, och vad kan du göra för att sopa igen dem efter dig? Det är frågor som det kan vara bra att fundera på.

Rent allmänt kan man säga att det framförallt är två olika typer av spår vi lämnar efter oss. Den ena är i form av data på och från datorer, telefoner och surfplattor. Du kanske har märkt att datorer sparar webbadresser du besökt, inloggningsuppgifter som gör att du inte behöver skriva in ditt lösenord varje gång, men också filer du kanske inte ens vet att du laddar ned som tillfälligt eller permanent sparas på hårddisken. Det kan handla om bilder du tar med din kamera, där information om var och när bilden togs sparas i bildfilerna och sedan kan läsas. Sådan information kallas ofta för metadata. Det kan också vara svårare än vad man tror att radera till exempel en hårddisk eftersom metoderna för att återskapa data i dag är så avancerade, men mer om det strax.

Den andra typen är data som samlas in av olika personer som av ett eller annat skäl håller koll på vad för information som går genom nätverken vi använder oss av. De som övervakar nätverken kan vara väldigt olika personer inbördes och som också gör det av helt olika skäl. Om du till exempel är på din arbetsplats kan det för det första vara it-avdelningen som håller koll på arbetsplatsens nätverk och vad som händer i dem, internetleverantören som ser vilken information som passerar genom deras stora datanät, den som har sajten du besöker eller tjänsten du använder dig av och slutligen polisen, FRA och andra myndigheter som av ett eller annat skäl kan få tillgång till data om vår kommunikation. Dessutom kan utomstående, hackare eller andra, olagligt hålla koll på

Tips!

Meta-data: dina elektroniska fotspår

Pelles syster lever på hemlig ort och gömmer sig från sin våldsamma före detta sambo. Pelle träffar henne och tar en bild, som får gps-koordinater inlagda i meta-datan. Meta-data är information som osynligt bäddas in i digitala filer som dokument, bilder och så vidare. Sen publicerar han bilden på webben och gps-datan hänger med – vilket avslöjar exakt var hon finns. Det finns särskilda program som kan visa och även radera meta-data från filer och dokument. Använd dem innan du publicerar något på internet.

vad du gör om du inte försvarar dina datorer och din information mot obehöriga.

Det vi nog först bör fundera på är vad som sparas på apparaten vi använder oss av. Skälet till att det är ett bra ställe att börja på är att vi ofta vet rätt mycket om vår hårdvara, alltså prylen vi sitter och knappar på, jämfört med vad som händer i kablarna dina data färdas i. Samtidigt händer mycket inne i manickens program, alltså mjukvaran, som vi inte alltid ser eller känner till.

Det första du ska fundera på är vem som rent fysiskt har tillgång till datorn, telefonen eller surfplattan du använder. Vem tillhör den? Är det du som äger den, är det din arbetsgivare, är det en offentlig dator på en offentlig plats eller är det någon annan? Var lämnar du in den för service? Vem har använt den tidigare och vem om någon använder den i dag, förutom du?

Datorer sparar en massa filer om sajter vi besökt, filer vi laddat ned, och över hu-

vud taget vad vi gör. Om man tänker sig att man till exempel vill lämna uppgifter om missförhållanden på sin arbetsplats kan man snabbt räkna ut att det helst inte ska göras med hjälp av en dator som arbetsgivaren äger och någon gång nu eller i framtiden kan få tillgång till.

Att använda offentliga datorer som vem som helst kan använda kan vara ett lockande alternativ med uppenbara fördelar, till exempel att det är svårt att knyta just dig till den datorn. Men då är det också viktigt att datorn i fråga inte finns på en plats som lätt kan knytas till dig (exempelvis ett bibliotek där du kan springa på en kollega), eller att du lämnar några spår efter dig på den datorn som andra kan hitta. Det kan i sin tur vara svårare än vad man kan tro, beroende på hur medveten man är om vilka spår program lämnar efter sig på datorns hårddisk. Filer som du med en handvändning raderar från din egna hårddisk är du ofta helt utelåst från på en offentlig dator som vem som helst ska kunna använda. Sparade filer som ligger och skräpar kan kopplas till dig både av andra användare, och av den som äger den offentliga dator du använder. För den som ändå ser en offentlig dator som det bästa alternativet finns det verktyg som förhindrar att datorn sparar uppgifter på hårddisken, exempelvis det alternativa operativsystemet Tails – en skyddad verkstad i form av ett linuxsystem man bär med sig på exempelvis en usb-sticka. Det är dock för många överkurs, och vi nämner det bara för den som verkligen vill utforska detta i detalj.

I regel är helt enkelt det bästa alternativet att använda utrustning du själv äger som ingen annan kan göra anspråk på, där du själv kan radera filer och som arbetsgivaren inte kan kräva att du lämnar ifrån dig. Vill du verkligen inte att det ska finnas spår på din dator kan du använda exempelvis Tails-verktyget, som gör att du inte behöver lämna spår ens på din egen dator. Om du väljer att radera filer från exempelvis en hårddisk eller en telefon finns dessutom spår fortfarande kvar, som går att pussla ihop till de gamla filerna. Det åtgärdar du lättast genom att ”spela över” det tomma utrymmet med nytt material, ungefär som med ett vhs- eller kassettband. Installera annat på datorn så att det täcker utrymmet, eller spela hela hårddisken på datorn full med hd-video så att det tomma utrymmet (som alltså fortfarande innehåller spåren av det raderade innehållet) spelas över med nytt innehåll. Många webbläsare i dag har också inställningar för att radera filer som sparas i da-

torn som kan identifiera dig, exempelvis besökta sajter och så kallade kakor eller ”cookies”. Trots detta kan det vara värt att ha i åtanke att de som skapat programvaran du äger, exempelvis Apple eller Microsoft för att nämna två stora företag, kan lämna vidare information om vad du gjort i din dator eller telefon till myndigheter.

När vi konstaterat att det är bättre att använda en egen dator, och direkt oklokt att använda en dator eller telefon du har fått av din arbetsgivare, blir nästa fråga att ta ställning till vad som syns i nätverken du använder, vad som sparas och hur du undviker det.

I grund och botten kan man säga att det du gör på nätet syns av den som har de sajter du besöker eller tjänster du använder, av den som sköter din uppkoppling, alltså de som administrerar nätverken du använder, och den som av annat skäl har tillgång till din trafik.

Den första av dessa, alltså den som har sajten du besöker, kan se från vilken IP-adress du kommer från (alltså vilket ”telefonnummer” på nätet din uppkoppling har) och information om dig som vad du kommer från för sorts dator eller telefon, vilken webbläsare du använder och andra uppgifter. De kan i sin tur variera från vad du sökt på för att komma till sajten eller vad för sorts länk du klickat på för att komma dit, till ungefär var i världen du befinner dig. En del av det här kan också sparas av ett eller annat skäl för att se om du till exempel återkommande besöker sajten. En del sajter har funktioner som till exempel sparat IP-adresser till svenska medier och myndigheter så att de kan se om till exempel en viss tidning eller myndighet besökt sajten. På det sättet kan också den som tillhandahåller en sajt hålla koll på en del information om dig som besökare. Därför är det viktigt att både uppgiftslämnare och journalister (men även andra, till exempel poliser) funderar på vad de lämnar efter sig för identifierande spår när de besöker en sida

Att inte använda samma dator många gånger för att besöka en sajt kan därför vara en idé, eller så kan man använda andra verktyg som VPN-nätverk eller proxyservrar för att vara mer anonym, men då kan i stället den som levererar den tjänsten se din trafik. Mer om det längre fram. Uppgifter du sparar i olika onlinetjänster på nätet kan lämnas vidare bort till myndigheter.

Det andra handlar om vad din internetleverantör (till exempel Bredbandsbolaget, Telia eller Comhem) kan se. Om du inte använder någon teknik för att skydda

dig kan internetlevarantörer, som ofta benämns med den engelska förkortningen isp:er (internet service provider), se vad du gör och sedan lämna de uppgifterna vidare till myndigheter. Även här kan verktyg som VPN:er som krypterar din trafik skydda dina data. Frågan man får ställa sig är om isp:n kommer att lämna ut de uppgifterna till myndigheter kan de vara skyldiga att göra det, men kanske inte till de flesta arbetsgivare. Om du exempelvis använder en jobbtelefon kan däremot din telefonleverantör lämna ut en lista över exempelvis ringda nummer till arbetsgivaren som betalar räkningen, och det har också hänt i Sverige när arbetsgivare jagat efter uppgiftslämnare.

Om du sitter på exempelvis jobbet och surfar, eller på ett internetkafé, så kommer dessutom den nätverksadministratören se vad för trafik som går genom nätet. Det gäller för all del även ditt hemnätverk även om den som administrerar det oftast är någon i det egna hemmet. Ett hemnätverk behöver helt enkelt mer sällan hanteras men om någon av något skäl (till exempel en servicetekniker) kommer hem till dig för att hjälpa dig kommer de troligtvis se vad som händer där. Det här innebär att det än en gång finns starka skäl att aldrig lämna känsliga uppgifter via en jobbdator. Inte nog med att arbetsgivaren har tillgång till din hårdvara (som de kanske äger, eller står för reparationerna av), utan för att företaget också ser vad som händer i nätverkets trafik, vare sig det är besökta sajter eller e-post.

I mer ovanliga fall kan en annan tredje part se vad som händer i näten. Det vi pratar om då är i första hand myndigheter som signalspanar i nät (som svenska FRA), eller hackare. Tidigare, när krypteringen på trådlösa nätverk ofta använde den svaga krypteringen WEP var det mycket enkelt för en hackare som befann sig inom nätverkets räckvidd att ta sig in och övervaka trafiken i nätverket – alltså vad alla i det gjorde om de inte skyddade sig på något sätt. I dag används i regel starkare kryptering men fortfarande förekommer WEP, och det finns andra sätt för hackare att få tillgång till ditt nätverk. Att folk gör det kan ha en massa olika anledningar, ibland är det för att de verkligen vill åt dina uppgifter, ibland ren nyfikenhet. Oavsett finns alltid risken. För myndigheter är det naturligtvis lättare att antingen via direkt signalspaning eller genom att begära ut sparade uppgifter från internetleverantörer ta del av din internettrafik, men å andra sidan är det knappast något de kommer göra åt din

arbetsgivare om det inte finns brottsmisstanke. Om du vill lämna ut något särskilt känsligt och oroar dig för att det kan finnas en misstanke om brott (det behöver faktiskt inte vara brottsligt) är det dock vettigt att fundera på hur du kan skydda dig även mot svenska myndigheters övervakning.

För att summera: allt du gör på nätet lämnar i någon form spår, både på nätet och på datorn (eller vad du nu använder för manick) du surfar med. Som regel är då att man helst använder sådant som så få som möjligt förutom du har tillgång till och, om du exempelvis behöver registrera dig med en ny e-postadress för att skicka något, inte har med uppgifter som kan knytas till dig. Att använda en dator eller liknande verktyg på ett säkrare sätt handlar till stor del om att bara använda sådant du själv äger och försöka att ta bort känsliga uppgifter om du tror att någon kan se dem, exempelvis en servicetekniker. Att använda själva nätet är också lite knepigt eftersom din dator lämnar efter sig uppgifter till flera olika personer om vem du är och vad du besöker. Lyckligtvis finns det verktyg som gör det mycket säkrare, och det ska vi titta på längre ned där vi tar en närmare titt på både anonymiseringsverktyg och var våra data hamnar.

Viktigt!

Att läcka uppgifter kan vara straffbart

Den som begår brott mot rikets säkerhet av olika slag riskerar givetvis fängelse.
Notera även att lagen om företagshemligheter innebär en lojalitetsplikt som är mycket stark. Att läcka uppgifter är bara okej om företaget eller organisationen gör sig skyldigt till brott som kan ge mer än två års fängelse. Om du kan vara anonym kan du teoretiskt sett heller inte bli åtalad, men det är viktigt att känna till riskerna innan du avslöjar känsliga uppgifter till media.

08 Ger vi bort privata data frivilligt?

När vi talar om privata data, det vill säga uppgifter och information som du vill hålla för dig själv, finns det flera nya perspektiv att ha i åtanke. Som vi beskrivit ovan lagras dessa data bland annat på din dator, mobil och andra apparater. Bilder och dokument finns därmed lagrade på dina egna hårddiskar och minneskort.

Men en allt större del av dina privata data ligger nuförtiden också på servrar hos enorma (ofta amerikanska) företag, eftersom du valt att uppge dem i olika sammanhang. På Facebook, Twitter, Instagram och andra sociala medier.

Det ligger i de sociala mediernas natur att du delar med dig av ditt privatliv. Det är själva kärnan i de sociala aktiviteterna. Du samtalar öppet på Facebook och Twitter, om allt från världspolitik till lustiga händelser i kollektivtrafiken. Du delar med dig av dina bilder, visar stolt upp information från din joggingrunda och hittar tack vare de sociala mediernas räckvidd gamla vänner.

Lär dig mer om användarvillkor!

Varje gång du laddar ner ett nytt program, köper saker på nätet eller använder ett socialt nätverk sparas och sprids information om dig. Men behöver företagen verkligen så mycket information eller använder de den till saker du inte känner till? Guiden ”Användaravtalen som ingen läser – så använder företagen din information” ger dig handfasta råd om vad du ska tänka på innan du klickar i ja-rutan. Materialet laddar du ned kostnadsfritt från: www.iis.se/guider

Saken är att all denna information du delar med dig av sparas på tjänsternas servrar. Flera stora sociala medietjänster, däribland Facebook, spar inte bara det du aktivt skriver – utan loggar också vad du ”gillar” genom att spåra hur du använder dig av deras tjänster.

Den stora anledningen till att all denna information sparas är för att de sociala medierna ska kunna tjäna pengar på reklam. Genom att veta hur du surfar och vad du tycker om kan Facebook rikta reklam till just dig – något som annonsörerna är glada att kunna utnyttja. Om du tryckt på ”gilla” på flera Facebook-sidor som har med bilar att göra, då kan Facebook anta att du gillar bilar – och därmed låta bilannonsörer vända sig till just dig och liknande användare.

Baksidan av detta är just det faktum att massor av privat information om dig, och om hur du använder internet och sociala medier, ligger lagrat hos dessa tjänsteleverantörer. Ofta ligger dessutom informationen relativt öppet – om du inte själv valt att begränsa människors insyn på din information. Men även om du begränsar tillgången finns det en hel del data som fortfarande går att leta reda på. För att inte tala om dem som jobbar i de stora datorhallar där all information lagras.

Med ovan nämnda faktorer i åtanke finns det en viktig fråga att ställa sig. Var förvarar du dina känsligaste data? Var för du dina känsligaste konversationer, vars avslöjande skulle kunna vara jobbiga (eller rentav ödesdigera) för dig själv, dina närmaste eller dina medarbetare? Var kan man hitta vad du gillar, vad du pratar om och vilka människor du har kontakt med?

För de flesta av oss lyder nog svaret att en allt större del av vår kommunikation sköts via sociala medier och tjänsteleverantörer på nätet. Därmed har vi, kanske utan att riktigt vara medvetna om det, lämnat bort delar av våra privata data helt frivilligt. Hur dessa data kan användas är helt upp till tjänsteleverantören, som ju driver en kommersiell verksamhet med vinstintresse.

09 Att kommunicera säkrare

När du ska kontakta någon med känslig information är det första valet vilken metod du ska använda – ett personligt möte, ett telefonsamtal, ett e-postmeddelande eller någon annan digital samtalsform. Det första valet är också det viktigaste, som får absolut störst konsekvens för hur ditt säkerhetstänk kring kommunikationen bör formuleras.

Som vi tidigare har berättat kan den enklaste lösningen oftast vara den säkraste, därför är ett fysiskt möte ofta ett säkrare val än kommunikation över nätet.

Men alltför ofta är det digital information vi har att göra med. Det kan vara en fil, ett dokument eller en hel databas som vi vill lämna vidare. Det är då vi behöver tänka efter hur vi ska hantera den digitala säkerheten, på datorn och på internet.

Praktiska tips

Ett möte är alltid säkrast

Ju enklare ditt system är, desto säkrare. Detta är såklart en sanning med viss modifikation, men bör användas som en tumregel. När vi talar om kommunikation i dagens samhälle, där vi antingen kan träffa någon fysiskt (i verkligheten) eller över internet, då blir det väldigt enkelt att applicera denna tumregel.

Internet är ett extremt komplicerat nätverk, oavsett om vi besöker en hemsida eller chattar med en kompis. Vår information passerar flertalet servrar, maskiner och manicker – och gör informationsflödet svårt att överblicka och begripa sig på.

Ett möte i verkligheten är däremot någorlunda lätt att överblicka. Om du stämmer träff med någon på en plats du känner dig trygg på har du genast mer kontroll än du skulle ha i ett chattrum på internet.

Om du vill lämna vidare information om ett missförhållande på din arbetsplats, och därför stämmer träff med en journalist, kan det vara smart att inte mötas på din arbetsplats. På samma sätt kan det vara tillrådligt att inte träffas på journalistens arbetsplats

Skillnad mellan stad och land

På en mindre ort innebär hemliga möten praktiska svårigheter. Storstadens relativa möjligheter till anonymitet och större utbud av mötesplatser gör att det fysiska mötet är säkrare i storstadsmiljö. I ett mindre samhälle där exempelvis lokala reportrar och redaktörer kan vara kända till utseendet och det inte finns säkra platser att träffas på, kan elektronisk kommunikation och telefonsamtal vara säkrare för att undgå upptäckt.

– eftersom det då finns många personer som ser att du besöker redaktionen.

Detta belyser ett annat självklart problem med det fysiska mötet – det är väldigt svårt att vara anonym. Som du kommer läsa nedan finns det tekniska hjälpmedel som kan hjälpa dig uppnå en mycket högre nivå av anonymitet på nätet, i de fall där anonymitet är en viktig faktor.

Ett möte, helst på neutral plats, är oftast det allra säkraste sättet att kommunicera.

Telefon är säkrare än internet

På samma sätt som ett möte ofta är säkrare än kommunikation över telefon, är telefon ofta ett säkrare sätt att kommunicera än över internet. Att övervaka telefonsamtal kräver en riktad insats – där just ditt telefonsamtal avlyssnas. Självklart bör du inte lämna tips eller prata om känslig information över telefon om du tror det finns risk att telefonsamtalet avlyssnas. Och du bör alltid vara medveten om att även om ingen har spelat in samtalet, så finns det alltid information om att samtalet har ägt rum – i telefonbolagens samtalsloggar. Dessa loggar kan definitivt bevisa vilka två telefoner som använts, och därmed ibland vilka personer som samtalat. I vissa fall kan denna koppling vara nog så illa som information samtalet handlat om.

Kommunicera från en neutral miljö

Se till att kommunicera från en neutral miljö, där du har största möjliga kontroll. Om du skickar känsliga e-postmeddelanden från din arbetsplats är risken stor att din arbetsgivare kan se vem som skickat det – och vad du har skickat.

Om du därför ska skicka vidare information om din arbetsplats, bör du göra det exempelvis hemifrån från en privat dator. Ett ännu bättre alternativ kan vara

Tips!

Säkrare telefoni

Engångstelefoner, kontantkort och i den mån de fortfarande finns kvar, offentliga telefoner är beprövade metoder för att kunna ringa utan att enkelt bli spårad i efterhand. Det finns även appar som krypterar röstsamtal, men det går ändå att tekniskt spåra att två nummer varit i kontakt med varandra även om det inte går att avgöra vad som sagts. Som regel gäller att du som vill samtala anonymt aldrig kan använda din vanliga mobil. Den lämnar du hemma, helt enkelt.

Tips!

Lär dig utkasttricket

En beprövad metod om du vill meddela dig med någon utan att skicka e-post eller andra meddelanden går till så här. Registrera ett webbmejlkonto med en anonym ”hittepå”-adress. Välj ett långt och bra lösenord. Skapa sedan utkast till mejl, som du alltså inte skickar till någon. Förmedla lösenordet till den som du vill kommunicera med. Nu kan ni båda läsa meddelanden till varandra via utkasten utan att något mejl skickats i och med att båda parter loggar in på samma webbmejlkonto. Observera att själva informationen skickas till bådas datorer i och med att det går att läsa på skärmen, men att mejlen inte lagras lokalt på era datorer.

från en god väns dator (så länge din vän går att lita på, så klart), eller från ett allmänt bibliotek. Ju mer neutral miljö du väljer, desto svårare blir det att spåra informationen – och samtalet – till just dig.

Med begreppet neutral miljö menas både fysiska och digitala rum. Om du skickat ett e-postmeddelande hemifrån, men använder din arbetsgivares e-postsystem, så löper du fortfarande risk att avslöjas. Om du använder en privat e-post, och skickar meddelandet hemifrån, blir det däremot mycket svårare för din arbetsgivare att lista ut vem som har skickat informationen vidare.

10 Internetanvändning och anonymitet

När vi nu konstaterat att många olika personer av lite olika skäl kan se vad du gör på nätet – vare sig det är någon av dem som administrerar din uppkoppling, den som har sajten du besöker, myndigheter eller någon annan – är det viktigt att du också vet vad du kan göra för att skydda din identitet och internettrafik. Med andra ord hur du kan hålla dig anonym.

Att känna till några av verktygen för att skydda sin internettrafik är viktigt för många – ofta uppmärksammas till exempel brottslingars behov av att skydda sin trafik, men i själva verket används de här teknikerna av alla möjliga andra – poliser som jagar brottslingar, företag som vill skydda sina affärshemligheter, journalister, uppgiftslämnare, politiska dissidenter och helt vanliga nätanvändare som av någon anledning inte vill att deras trafik övervakas om de kan undvika det.

Bara en sådan sak som att en sajts ägare med hjälp av sparade ip-adresser ofta kan ta reda på vem som besökt deras sida gör att det kan vara bra att använda en mellanhand av något slag för att det ska vara svårare att se vilka sidor du besökt.

Flera olika typer av verktyg finns för att skydda din internettrafik. Vi ska titta på några av de vanligaste och enklaste att använda för en nätanvändare. Det är dock viktigt att komma ihåg att de bara kan bidra till att skydda eller anonymisera din nättrafik – om du drabbats av virus eller fått in något program i din dator som spionerar på vad du gör är de inte till lika stor hjälp.

Proxy

Ett av de enklaste och vanligaste sätten att dölja varifrån du besöker en sida, eller för att kringgå spärrar i vilka sidor man kan besöka på sitt nätverk, är en så kallad proxy-server, en mellanhand som man går via i stället för att besöka en sajt direkt. Det kommer då, för den som sköter ditt nätverk, se ut som att du besöker proxysajten och inte din slutdestination. För den som äger sajten du besöker ser det ut som att ditt besök kommer från proxyn och inte från din egentliga ip-adress.

Det finns en uppsjö av olika proxyservrar man kan använda sig av och det kan vara bättre än ingenting, men i allmänhet kommer inte en proxyserver att kryptera

eller på annat sätt skydda din trafik och därför kommer det ändå vara lätt för den som har tillgång till din nättrafik att kunna se vad du gör på nätet. Därför är det inte rekommenderat att bara använda en proxyserver om du verkligen vill vara anonym eller oroar dig för att någon ska se vad du har använt nätet till. Man vet sällan säkert vem den här mellanhanden är.

VPN

Ett kraftigare och mer avancerat verktyg som kan låta en nätanvändare skydda sin trafik är ett så kallat Virtuellt Privat Nätverk – ett VPN. VPN:er kommer i många olika former och låter datorer ansluta till, exempelvis, en arbetsplats intranät som om man var på plats på kontoret, trots att man sitter någon annanstans.

”Virtuellt Privat Nätverk” kan låta komplicerat och rullar inte direkt av tungan, men faktum är att många fler än vad man kan tro använder VPN:er till en massa olika saker. Det kanske absolut vanligaste användningsområdet handlar varken om affärshemligheter eller att lämna uppgifter till journalister. Många använder VPN-nätverk för att till exempel titta på filmer från livestream-tjänster i andra länder än där de själva befinner sig, till exempel för att titta på Netflix-filmer som egentligen bara är tillgängliga i USA trots att man är i Sverige. Det är möjligt därför att VPN:er inte bara skyddar din nättrafik utan många tjänster låter dig själv välja var ”utgången” i nätverket ska vara, alltså om det ska se ut som om du surfar från USA, Sverige, Kina eller Iran. Det finns också en uppsjö av olika kommersiella aktörer på VPN-marknaden att välja emellan. En del håller hårdare på skyddet av kunders personuppgifter än andra och därför är det vettigt att ta lite tid för att leta information om olika företag, vilka uppgifter de sparar och när de kan tänkas lämna ut dem.

Men VPN-nätverk kan också användas för att med hjälp av kryptering skydda nättrafik. Man kopplar upp sig mot VPN-nätverket och surfar sedan via det. VPN-nätverk kan skydda innehållet i din nättrafik och även vem du är, eftersom trafiken ser ut att komma från VPN-nätet. Det finns många olika kommersiella VPN-tjänster som kan låta en användare surfa snabbt och relativt säkert, många av dem relativt billigt. Kruxet är att den som administrerar själva VPN-nätverket potentiellt kan se vad man gör, och därmed också dela med sig av de uppgifterna. Hur sannolikt det sedan är att de gör det beror på – VPN-tjänster lovar ofta att inte dela med sig av användares trafik, men det är inte tekniskt omöjligt.

Tor

Ett annat verktyg som du kan använda för att skydda din nättrafik är Tor. Tor, som står för The Onion Router, är i dag relativt lätt att använda och mycket kraftfullt, och också gratis och lättillgängligt på nätet. Tor är i första hand designat för att göra din nättrafik anonym genom en sorts flerstegs-proxy där din nättrafik hoppar via flera (tre) olika punkter i Tors nätverk – därmed ser ingen enskild punkt samtidigt både vem du är och din slutdestination. Det är därmed rent tekniskt säkrare. Tor skyddar på det sättet inte bara din identitet utan också innehållet i din kommunikation. Tor utvecklades inledningsvis av amerikanska myndigheter, men finansieras numera av flera olika sponsorer inklusive svenska biståndsorganet Sida. Tor är också är fri och öppen programvara.

Den största bristen med Tor har i allmänhet varit att det är relativt långsamt. För en nätanvändare som är van vid de höga hastigheterna vi normalt ser i svenska nät kan den långsammare hastigheten vara frustrerande, men det är ett relativt lätt och tillförlitligt sätt att göra både trafikövervakning och övervakning av dina kommunikationers innehåll betydligt svårare. Tor kan heller inte dölja sista länken i kedjan utan bara trafiken inom sitt eget nätverk. Därför är det viktigt att skydda väldigt känsliga uppgifter på annat sätt. I vissa fall har det också visat sig att mycket avancerade organisationer, till exempel stora länders myndigheter eller vissa forskare kunnat komma åt delar av Tor-krypterad kommunikation genom att koppla upp sig mot nätverket med flera datorer och på så sätt få tillgång till flera länkar i den flerstegskedja som utgör Tor-surfning.

I grund och botten är dock Tor ett bra verktyg för dig som både vill kryptera din internettrafik och hålla dig relativt anonym på nätet. Inga verktyg är perfekta och att garantera att man är till hundra procent säker är i princip omöjligt. Att surfa via en dator som tillhör en arbetsgivare är till exempel ändå en mycket riskabel sak att göra – välj därför en privat dator. Med det sagt är Tor en av de saker man kan göra för att med små medel öka säkerheten avsevärt.

Lär dig använda Tor!

Till den här Internetguiden medföljer XL-materialet ”Kom igång med Tor!”. I dokumentet får du lära dig grunderna och hur du använder Tor i praktiken, steg-för-steg. Materialet laddar du ned från www.iis.se/guider

II Kryptering

Kryptering är att göra information svårläslig för alla som inte ska kunna läsa den, och har troligtvis funnits nästan lika länge som skriftspråket. Genom att använda ett kodsystem eller ett chiffer kastas bokstäver och siffror om, och texten blir oläslig. För att göra informationen läslig igen krävs dekryptering, som (i bästa fall) bara kan göras av de personer som texten är ämnad för.

I dag kan kryptering användas i många sammanhang. En grupp självklara användare är underrättelsetjänster världen över, som har behov av att skicka information kors och tvärs utan att den kan läsas av någon annan än dess egna instanser.

Idag är det en självklarhet att kryptering används av olika tjänster och webbsidor på nätet, i programvaror och i smartphones – för att skydda vår, ofta privata, information. De tydligaste exemplen på det är din internetbank och när du köper något från etablerade e-handelsplatser.

Men det finns fortfarande många tillfällen då vi själva behöver skydda filer och dokument, då vi aktivt behöver tillämpa kryptering.

Varför är Kryptering viktigt?

I kapitlet ”Vem tittar på dig och varför?” gick vi igenom det helt oöverskådliga nätverk vi i dag kallar nätet. Det är lätt att inse vilka känsliga vägar vi tar på nätet, då vi surfar och kommunicerar med andra. Vi har helt enkelt ingen aning om vem som tittar, vem som har tillgång till våra data eller var vår information passerar.

Framförallt finns det extremt många ställen där vår kommunikation är sårbar (rentav öppen för allmän beskådan) och där vår information är i fara att komma i orätta händer. Genom att kryptera vår kommunikation och våra filer kan vi vara säkra på att även om informationen kommer i orätta händer, vilket den förr eller senare kommer att göra, är den oläslig för obehöriga.

Exempel på tillfällen då kryptering kan vara viktigt:

En smartphone.
Smartphones är lätta att tappa bort, och är lovligt byte för ficktjuvar. Om din smartphone inte är krypterad är det lätt att komma åt bilder, sms och annan privat in-

formation. Om du har en krypterad smartphone kommer inte tjuven åt lika mycket.

Hemliga filer på en delad dator (hemma eller på arbetsplatsen).
Om flera har tillgång till datorn bör du kryptera de filer som bara är dina.

En laptop.
En bärbar dator som flyttas mellan olika platser är extra utsatt för stöldrisk – och kan rentav glömmas på bussen. Om hårddisken är krypterad, helt eller delvis, kommer ingen kunna komma åt dina filer.

Viktigt!
Din lösenkod

Att en mobil eller dator har en lösenkod som måste knappas in för att du ska kunna använda den är nödvändigt för din personliga integritets skull, men det innebär inte att innehållet i apparaten är krypterat. Det är med andra ord ett rätt svagt, men nödvändigt, skydd.

Kryptering av filer och kryptering av trafik

Det finns en viktig skillnad mellan kryptering av filer och av trafik, som vi kommer ta upp nedan genom ett flertal exempel.

Kryptering av filer kan liknas vid ett kassaskåp. Genom att kryptera filerna låser vi in dem i ett kassaskåp bara vi själva, eller en eventuell mottagare, har nyckeln till. På så sätt kan vi lagra eller skicka filerna utan att vara oroliga för att någon ska kunna öppna låset och titta på dem.

Kryptering av trafik kan liknas vid en privat tunnel på motorvägen, bara för dig. I det fria kan alla se vad du och andra gör på motorvägen, men i tunneln är du ensam. Dina data åker genom en krypterad tunnel, som bara du eller mottagaren på andra sidan kan avkryptera. Om någon tittar på din datatrafik då du är i tunneln kan de se att du surfar, men de kan inte se vad du surfar på eller vad du gör.

Viktigt att tänka på – kryptera trafiken eller filerna? Eller båda?
Det är viktigt att tänka igenom vilken del av din kommunikation som bör krypteras – och huruvida du ska kryptera filerna eller trafiken. I känsliga fall kan båda vara befogade.

Tänk dig att du åker bil. Om det viktigaste är att skydda ditt bagage (dina filer), då räcker det troligtvis med att kryptera

filerna. För även om någon ser att du åker bil kan de inte öppna ditt kassaskåp (dina krypterade filer). Det kan jämföras med att skicka krypterade filer över ett osäkert nätverk. Även om någon kan se och får tag på filerna, så kan de inte öppna och läsa dem.

Men om det snarare är viktigt att göra saker i hemlighet, så att ingen vet om att du åker bil eller vad du gör i bilen, då är det troligtvis smart att åka inuti tunneln. Genom att kryptera din nättrafik kan ingen utomstående se vad du gör inuti tunneln. Men notera att dina filer inte är krypterade inuti tunneln – det är enbart trafiken, var du klickar och vad du skriver, som är krypterat.

Om du därför inte litar på den som tillhandahåller tunneln, då kan det vara smart att också kryptera filerna som åker genom tunneln. På så vis kan ingen se vad du gör i tunneln, och även om självaste tunnelchefen skulle vända sig mot dig är dina filer säkra i kassaskåpet.

Detta är starkt förknippat med den teknologi och det tänk som används av tjänsten Tor, vars krypterings- och anonymiseringslösning ger ett av de bättre alternativen på säkra tunnlar på internet. Tor ger dock skydd i själva tunneln, men i ändarna är trafiken oskyddad. Många som är måna om sin säkerhet använder dessutom en VPN-tjänst (eller flera) för att maskera sin ip-adress.

Lokal kryptering

Den enklaste modellen av kryptering är lokal kryptering av filer. Det är vad du använder då du vill kryptera ett eller flera dokument, för att bara du eller en potentiell mottagare ska kunna öppna dokumenten.

Det går också att kryptera ett helt medium, likt hela hårddisken i en laptop eller en usb-sticka. Det sistnämnda kan vara ett väldigt smart sätt att lämna över information till någon annan. Att lämna en okrypterad usb-sticka vidare är inte särskilt säkert. Men om den är krypterad, och bara mottagaren har lösenordet, är det mycket säkrare. Eftersom usb-stickan kan överlämnas fysiskt behöver du dessutom inte skicka filerna över nätet.

Kryptering när du surfar

Ytterligare en viktig instans av kryptering sker då du surfar på sajter som använder kryptering. Det gäller absolut inte alla sajter, men de flesta stora banker, e-postleverantörer och sociala medier använder i dag krypterade anslutningar. Du vet att du surfar med en krypterad anslutning om det i adressraden står ”https://” istället för ”’http://”. Notera att det är ett extra ’s’ efter ’http’.

En krypterad anslutning kan som sagt liknas vid en tunnel på motorvägen. Kryp-

teringen gör så att dina data åker genom en tunnel, som bara du och webbplatsen kan avkryptera. Om någon tittar på din datatrafik kan de se att du surfar, men de kan inte tränga igenom tunneln – och därmed inte se exakt vad du gör.

Det är viktigt att inse vad detta skyddar mot, och kanske framförallt vad det inte skyddar mot. Om någon som surfar på samma nätverk som du försöker se vad du gör när du kollar din e-post i browsern – då skyddas du av tunneln. Personen kommer att se att du surfar, men inte vad du gör.

Däremot skyddar det självklart inte mot personer eller organisationer som har tillgång till tjänsten på andra sidan. Om du exempelvis surfar på Facebook så kan Facebooks personal självklart alltid se vad du gör, oavsett om du har en krypterad anslutning till Facebook eller inte.

Sakta men säkert börjar fler och fler sajter använda krypterade anslutningar, vilket hjälper användare att surfa krypterat i högre utsträckning. Men långt ifrån alla leverantörer använder https – kolla alltid i adressraden om du är osäker.

Dessutom finns det flera tjänsteleverantörer, däribland Facebook, i vars inställningar man själv måste välja om man vill surfa med https eller inte. Det är inte påslaget från början. Eftersom det knappast finns någon nackdel med att surfa krypterat kan det vara smart att undersöka huruvida dina olika tjänsteleverantörer har möjlighet att låta dig surfa krypterat.

Gör det till en vana att surfa med https.

Kryptering i molnet

Att förvara dina filer i molnet blir allt vanligare, både bland privata användare och företag. Tjänsteleverantörer som Google och Dropbox gör det supersmidigt att ha tillgång till dina filer var du än är – i datorn och i mobilen. Ett självklart problem med detta uppstår då du hanterar känsliga uppgifter. Eller rentav bara privata uppgifter, som du inte vill att någon obehörig någonsin ska se. Eftersom du förvarar dessa filer på ett företags servrar finns det full möjlighet för andra att titta på det. Som nämndes i inledningen: det som är juridiskt svårt är samtidigt tekniskt enkelt. Även om det är mot reglerna för en anställd på exempelvis Dropbox att titta på dina privata filer, så är det väldigt enkelt för dem att göra det. Litar du helt och hållet på företaget i fråga? Om svaret på frågan är nej, kan det vara smart att kryptera hela eller delar av din filsamling i molnet. Det finns flera bra lösningar på marknaden i dag, varav flera har en gratis grundnivå för privata användare, som gör

detta på ett smart och enkelt sätt. På så vis kan inte ens tjänsteleverantören i fråga se på dina filer, även om de har fysisk kontroll över servrarna där filerna ligger.

E-post

E-post blev i rasande fart en del av vår vardag. Oavsett om det gäller privata meddelanden eller kommunikation på jobbet är det något vi alla använder, mer eller mindre omfattande. Därmed finns det flera saker du alla bör tänka på, då du skickar våra brev ut på nätet.

Som ett vykort på posten

Att skicka e-post i dag är precis som att skicka vykort med posten. Den enda skillnaden är troligtvis att vykort är säkrare, och kan läsas av färre människor längs med vägen.

Ett vykort kan läsas av både brevbärare och diverse personer som arbetar med att hantera posten. Precis samma sak gäller för e-post. När du skickar ett e-postmeddelande passerar det förbi flera olika stationer på vägen till mottagaren, både hos olika internetleverantörer och olika e-postservrar. Den exakta vägen beror förstås på var du skickar meddelandet från, och vem du skickar det till.

Även om du skickar ett e-postmeddelande till någon på ditt eget företag – som arbetar på sin dator precis bredvid dig – är risken stor att ditt e-postmeddelande studsar runt i världen innan det når datorn bredvid dig. Om du exempelvis använder Gmail, från amerikanska Google, åker troligtvis ditt e-postmeddelande förbi USA en sväng – och därmed förbi de amerikanska myndigheterna. Så om meddelandet till din kollega är hemligt, kanske det rentav är värt att skriva ned det på en papperslapp istället och lämna över det vid dennes skrivbord.

Men även här finns det relativt enkla medel att ta till, för att kunna säkra sina meddelanden. Det kräver lite tålamod, men gör stor skillnad den dag någon obehörig vill komma åt din korrespondens.

PGP

Det finns i princip bara ett tillförlitligt sätt att kryptera sin e-post i dag, och det är att använda något som heter PGP (Pretty Good Privacy). Med hjälp av PGP kan du kryptera din e-post så att den enbart kan läsas av den tänkta mottagaren.

Enkelt förklarat fungerar PGP genom att alla användare genererar två nycklar, en privat och en publik nyckel. Den publika nyckeln kan man dela med sig av till alla, men den privata nyckeln behåller man för sig själv. Den publika nyckeln används för

att kryptera (låsa) e-post, och den privata används för att avkryptera (låsa upp) e-post.

Genom att byta publika nycklar med varandra, kan du därmed skapa ett nätverk av kontakter vars publika nycklar gör det möjligt att skicka e-post till dem i krypterad (låst) form.

På samma sätt kan alla andra skicka krypterad (låst) e-post till dig, som bara du kan avkryptera (låsa upp) med din privata nyckel.

Att på eget initiativ använda PGP resulterar i ett säkrare sätt att skicka e-post än du vanligtvis gör, då informationen är oläslig för alla utom mottagaren.

Viktigt att tänka på med PGP

Initiativet att använda PGP för krypterad e-post kan komma från dig själv och tekniken du använder ska också vara något du känner dig väl förtrogen med. Med andra ord behöver du inte lita på din arbetsgivares ord om att din e-post redan är säker i företagets system, eller lita på företagets egna lösningar. I synnerhet inte om du vill kunna skicka e-post som ska hemlighållas för arbetsgivaren.

En svaghet med PGP är att krypteringen bara gäller informationen, själva texten och filerna, i e-postmeddelandet. Men metadata om när och var e-posten skickades går fortfarande att se. Detta kan i många fall vara minst lika problematiskt. Om din arbetsgivare kan se att du skickat ett krypterat e-postmeddelande till en journalist, då spelar det troligtvis ingen roll vad som står i e-postmeddelandet.

Innan du använder PGP, läs på ordentligt och se till att du vet vad du gör. Vi passar på att igen nämna XL-materialet ”Kom igång med PGP!” som förklarar hur du går till väga.

Du kan skicka krypterade filer utan att kryptera själva e-postmeddelandet

Precis som vi ovan skiljer på krypterade filer och krypterad trafik, kan vi skilja på krypterade filer och krypterade e-postmeddelanden. Om du vill skydda all din text då du skickar e-post, då bör du använda PGP som beskrivits ovan. Om du däremot bara ska skicka en stor fil som är krypterad i sig själv, då kan du självklart skicka den med vanlig e-post. Då kommer all text i e-postmeddelandet att vara synlig vid ett eventuellt angrepp, men filen fortsätter vara skyddad av sin egen kryptering.

Lär dig använda PGP!

Till den här Internetguiden medföljer XL-materialet ”Kom igång med PGP!”. I dokumentet får du lära dig grunderna och hur du använder PGP i praktiken, steg-för-steg. Materialet laddar du ned kostnadsfritt från www.iis.se/guider

12 Din mobiltelefon och surfplatta

För inte så länge sedan var en telefon inte så mycket mer än en telefon. Du kunde skriva SMS, ta lite suddiga bilder och kanske till och med spela några MP3-låtar, men huvudnumret var att ringa. I dag är de telefoner de flesta av oss använder mer än så – de är avancerade minidatorer många använder både privat och i det dagliga arbetet.

Men förutom alla fördelar finns det för den som oroar sig för sin anonymitet och källskydd också risker. Telefoner sparar enorma mängder uppgifter om dig, din kommunikation, dina kontakter och var du befinner dig. Det är till och med, för exempelvis hackare eller myndigheter, möjligt att använda telefoner som raffinerade spionapparater. Därför är det viktigt att du funderar på hur du kan skydda information som finns i din telefon, eller till och med när du bör lämna telefonen hemma.

En mobiltelefon, eller för den delen en surfplatta, har flera unika identifieringsnummer. Det gäller både själva telefonen och det sim-kort du använder för att ringa och surfa. Om du inte har köpt din telefon och sim-kort anonymt är informationen kopplad till dig, och om det är en arbetstelefon också till din arbetsgivare.

Den första risken att tänka på är att telefoner både genom kommunikation med telefonmaster och genom de inbyggda platstjänster många av telefonens funktioner använder kan avslöja var du befinner dig. Den platsinformationen kan många olika appar och program ta del av, och den kan exempelvis sparas i bilder du tar med din kamera. Därför är det en bra idé att stänga av tillgången till platstjänster i telefonens inställningar, när du inte behöver använda dem. Om du behöver använda dem, tänk på vilka appar du ger tillgång till var du befinner dig. Det går också att ställa in på de flesta telefoner under enskilda appars inställningar.

Mobiltelefonkommunikationen som skickas genom luften är i regel krypterad. Det är dock inte telefonsamtal som går igenom kablar. En risk här är att det inte är du som kontrollerar om ett mobilsamtal avkrypteras – det styr mobiloperatören. Det är inte teknologiskt särskilt svårt att snappa upp telefonkommunikation, även om det juridiskt är betydligt mer långgående än med grundläggande information om vem du kommunicerar med och när – information som samtidigt kan vara komprometterande nog. Det finns vissa appar som säger sig erbjuda krypterad telefontrafik, något som dock kräver att alla telefoner i samtalet använder sig av den tekniken.

Den tredje, och kanske största frågan handlar om vilka data som sparas i din telefon och hos telefonoperatörer. Telefonen kommer att spara innehållet i meddelanden du skickar och tar emot, tidpunkter och telefonnummer när du ringer telefonsamtal och annan information som var du befinner dig. Det bästa man kan göra är ofta att manuellt ta bort den informationen och sedan använda telefonen – först när utrymmet ersätts med nya data skrivs den gamla informationen över; inte när du raderar den.

Det finns verktyg tillgängliga för att kryptera mobiltelefoner men det kan vara svårt att säga exakt hur säkra de är. Som regel kan man dock säga att de är mycket bättre än inget om någon skulle komma över din telefon, och du har väl lösenord på din telefon? Om inte, är det det första steget du bör ta.

Telefonoperatörer eller andra företag som förser din telefon med tjänster kan och kommer att spara uppgifter om vem du kommunicerar med och från var. Vilka samtal som rings, vilka sms som skickas, vilken datatrafik som sker med telefonen och var du befinner dig. Även mottagartelefonens operatör har tillgång till en del uppgifter.

Det finns exempel där exempelvis arbetsgivare begärt ut listor över ringda nummer och på så sätt upptäckt att anställda kommunicerat med journalister. Den bästa lösningen om du vill lämna en uppgift till en journalist eller någon annan granskare är att träffa den personen ansikte mot ansikte på en säker plats. Om det inte är möjligt, skaffa en enkel telefon utan avancerade funktioner utan att ditt namn registreras och köp ett kontant sim-kort utan att registrera några personuppgifter. Använd sedan den telefonen uteslutande för att kommunicera med den du vill lämna en uppgift till, och ring eller sms:a alltid från en neutral plats som inte kan spåras tillbaka till dig, alltså inte till exempel ditt hem eller din arbetsplats.

13 Källskydd och meddelarfrihet

Sveriges grundlag har ett särdeles starkt skydd för journalister, källor och deras kommunikation.

Källskydd, som också kallas tystnadsplikt, innebär att den person eller entitet (exempelvis en redaktion) som har tagit emot en uppgift eller ett tips inte får avslöja den uppgiftslämnare som vill vara anonym. Det är straffbart för den som tagit emot en sådan anonym uppgift att avslöja källan.

Det är viktigt att du som uppgiftslämnare uppger att du vill vara anonym, om så är fallet. Om du vid ett senare tillfälle av någon anledning vill röja din identitet, kan du självklart göra det.

Viktigt att veta är att källskyddet inte gäller vid grova tryckfrihetsbrott som spioneri, högförräderi och grov befattning med hemlig uppgift. I fall som dessa kan journalister genom domstolsbeslut tvingas att uppge sina källor.

14 Digitalt källskydd

På den tid då journalistik sköttes med penna, papper och tryckpress var det enklare att garantera källskydd. Genom att aldrig skriva ned namn och låsa in anteckningsböcker i ett kassaskåp på redaktionen kunde journalister rimligtvis garantera för sina tipsare att deras anonymitet och information var säker.

Källskydd på nätet är däremot svårare, och mer komplicerat än vad de flesta journalister vill erkänna. Med alla de oöverskådliga vägar vår information tar på nätet är det därför, enligt denna guides författare, näst intill omöjligt för en journalist att garantera källskyddet genom digital kommunikation.

Du bör därför aldrig fullt ut lita på en journalist eller redaktion, eller någon annan som säger sig kunna garantera ditt källskydd. Du måste själv vara medveten om de risker som finns, och kunna göra så mycket som möjligt för att skydda din anonymitet och den information du vill förmedla.

På följande sidor har vi samlat ett antal exempel som mycket väl skulle kunna vara hämtade ur verkligheten. I själva verket är de helt och hållet påhittade. ●

Lär dig mer om digitalt källskydd!

Du som funderar på att lämna information till medier kan ha stor hjälp av att läsa Internetguiden ”Digitalt Källskydd – en introduktion” som .SE producerat i samarbete med Svenska Journalistförbundet. Huvudsyftet med guiden är att introducera mediearbetare i Sverige och deras arbetsledning om vikten av att digitalt kunna garantera källors anonymitet.

Publikationen är dock bra läsning för dig som har frågor om hur redaktioner och enskilda journalister bör agera när du som uppgiftslämnare kontaktar en redaktion med känsliga uppgifter. Materialet laddar du ned kostnadsfritt från www.iis.se/guider

Tips!

Lita på journalister som krypterar

Lita inte på de medier som har en vanlig e-post adress, eller ännu värre, ett Twitter-konto, och skriver att du kan tipsa dem om nyheter eller lämna information. Det står ofta att de garanterar att du kan vara anonym. Detta är helt enkelt inte sant. Om du mejlar till en vanlig e-postadress är det snarare så att ingen kan garantera att du förblir anonym. Leta istället upp journalister/redaktioner som publicerar sina publika krypteringsnycklar eller medier som har säkra anonymiserande tjänster när du vill tipsa om något utan att avslöja vem du är.

Tips!

Lathund för tipsare

Till den här guiden medföljer en sammanfattande kom-ihåg-lista med det viktigaste som den som vill meddela sig säkrare med media bör tänka på.

Det går utmärkt att skriva ut lathunden och sätta upp på anslagstavlor, exempelvis. Lathund för tipsare finns att ladda ned kostnadsfritt på: www.iis.se/guider

15 Scenarier

Här kommer du att träffa familjen Andersen och deras vänner. Tillsammans hjälper de oss att få inblick i många olika situationer där digitalt självförsvar är viktigt, ibland till och med essentiellt.

Mamma Jessica Motobo

Mamma Jessica är statsvetare och jobbar på SIDA med utvecklingsfrågor och bistånd. Hon är medlem i fackförbundet ST. I sitt arbete möter Jessica många olika människor och hon reser ständigt kors och tvärs i världen, inte minst till Afrika. Större delen av hennes släkt bor också i Uganda.

En dag råkar Jessica av en slump märka att pengar som är öronmärkta till bistånd i Sydsudan har gått till att betala privata utgifter som inte har något med biståndsarbetet att göra. Nu vill hon uppmärksamma en journalist hon är bekant med på detta, men hon är osäker på hur hon ska göra för att inte röja sig själv på kuppen. Hon vill absolut vara anonym som uppgiftslämnare, inte bara när det gäller gentemot sin arbetsgivare, men även i kontakten med journalisten.

Efter att ha läst den här skriften som du läser nu, och andra guider på nätet, går hon till väga på följande sätt.

1. För Jessica är anonymiteten allra viktigast, och därefter att filerna inte hamnar i orätta händer. Hon försökte lära sig PGP, för att kunna skicka filer krypterat med e-post, men tyckte det var för svårt och ohanterligt. Därför valde hon att fysiskt skicka filerna till en journalist.
2. Eftersom Jessica arbetar med Sydsudan har hon redan tillgång till filerna som hon vill skicka. De finns på hennes jobbdator.
3. Hon funderar på huruvida filerna kan spåras tillbaka till henne. Men eftersom Jessica vet att flera andra på arbetsplatsen har tillgång till exakt samma filer känner hon sig trygg med att lämna dem vidare. Det skulle vara svårt att spåra dem till just henne.
4. För att kunna flytta filerna säkert krypterar Jessica ett usb-minne, så att det bara kan öppnas med ett lösenord. Hon krypterar det hemma på sin privata dator för att inte väcka uppmärksamhet.

5. På arbetsplatsen städar Jessica filernas egenskaper så att det inte direkt framgår vem som skapat dem och sist sparade versionerna. Hon gör det med program som tar bort meta-data och som hon laddat ned på nätet. Om Jessica misstänker att det går att spåra via kontorsnätverket vilka filer hon kopierar över till usb-stickan, skapar hon helt nya versioner som hon döper om till intetsägande filnamn. Sedan kopierar hon de känsliga dokumenten till usb-stickan. Nu vet hon att de ligger säkert, och att även om hon förlorar usb-minnet kan ingen annan än hon läsa dem.
6. Efter jobbet tar Jessica på sig handskar, går till Ica och köper ett kuvert och frimärken. Hon skriver journalistens namn och adress på kuvertet, lägger i usb-minnet och postar det. Utan att ta av sig handskarna. Hon har även torkat av usb-stickan ordentligt så att inga spår av henne finns där.
7. På sin privata dator, som hon själv köpt och installerat, installerar Jessica programvaran TOR som hjälper henne att surfa anonymt.
8. När hon kan surfa med hjälp av TOR registrerar hon en helt ny e-postadress, med ett namn som inte är hennes.
9. Genom den nya e-postadressen skickar hon ett e-postmeddelande till journalisten, och beskriver vad hon har hittat. Hon ger honom också lösenordet till det krypterade USB-minne som han kommer få på posten. Hon är noga med att inte avslöja några detaljer om sig själv.
10. Efter några dagar kopplar Jessica återigen upp sig via TOR och loggar in på sin hemliga e-postadress. Hon har fått svar av journalisten, som kommer med följdfrågor. Hon svarar, och efter några e-postmeddelanden fram och tillbaka har journalisten allt han behöver, och publicerar ett reportage om bidragsfusket i Sydsudan.

Pappa Pelle Andersen

Pappa Pelle är lärare i samhällskunskap, arbetar på Tvärforsskolan och är medlem i Lärarförbundet. Pelle är mentor för en klass på 30 elever och ansvarar dessutom för en lokal tennisklubb för gymnasieelever.

Pelle får höra av flera elever att rektorn på skolan fällt kränkande och rasistiska kommentarer och dessutom tagit hem flera surfplattor som skulle användas i skolan. Pelle tänker att lokaltidningen nog skulle vilja veta om det, men han vet inte riktigt hur kan ska bära sig åt och eftersom skolan inte är kommunal oroar han sig för att skolan

ska ta reda på vem som berättat om detta. Hans dator tillhör dessutom arbetsgivaren, vilket oroar honom. Om han installerar ny programvara för att exempelvis surfa anonymt finns det risk att skolans IT-avdelning kan se det.

1. För Pelle är det viktigaste att vara anonym. Han bedömer att informationen han vill lämna vidare inte är känslig för andra än rektorn på skolan. Det viktigaste är att ingen kan få reda att det är Pelle som talat om det för lokaltidningen.
2. Pelle läser på, och inser snabbt att han inte kan ta kontakt med någon om detta känsliga ämne från sin jobbdator. Han väljer därför att besöka ett bibliotek som har allmänna datorer som alla får använda.
3. Pelle vill använda verktyget TOR för att vara säker på att vara anonym, och laddar ned det på bibliotekets dator. Eftersom TOR inte behöver installeras på datorn är han igång på ett kick, och inom några minuter surfar han anonymt på nätet.
4. Sedan registrerar Pelle en ny e-postadress på Gmail, med ett påhittat namn. Från det e-postkontot skickar han ett meddelande till lokaltidningens redaktion, där han berättar om vad han hört och sett. Han är noga med att inte lämna vidare detaljer som skulle kunna avslöja honom som källa.
5. Efter några dagar går Pelle tillbaka till biblioteket, använder TOR och loggar in på sin fejkade e-postadress. Han har fått svar av journalisten, som undrar om Pelle kan ge en kommentar.
6. Pelle funderar igenom huruvida en kommentar från honom skulle kunna avslöja honom. Men eftersom skolan har närmare 50 lärare bedömer han risken som liten, och e-postar därför tillbaka en kommentar.
7. Lokaltidningen uppmärksammar problemet. Pelle är nöjd och känner sig säker på att ingen kan bevisa att det var han som tipsade tidningen.

Dotter Anna Andersen

Dottern Anna är läkarstudent och arbetar som AT-läkare på det stora sjukhuset i staden. Hon är medlem i Vårdförbundet. På fritiden reser Anna mycket och hon är dessutom aktiv i sociala medier. Anna tycker att det slarvas alldeles för mycket med patienterna på sjukhuset, trots alla regler. Hon funderar nu på hur hon ska kunna slå larm om detta utan att det spåras tillbaka till henne.

1. Anna funderar på huruvida hon bör kontakta en journalist digitalt eller om hon ska ringa personen. Vid närmare eftertanke tycker hon att ett samtal vore bäst, för att kunna svara på följdfrågor om journalisten undrar något. Då slipper hon hålla på med en massa tekniska lösningar.
2. Anna vill absolut inte kunna bli spårad, och vill därför inte ringa från sitt eget mobilnummer. Hon vill heller inte använda ett telefonnummer som kan spåras till någon familjemedlem eller vän.
3. Anna köper en billig mobil kontant i en affär och ett kontantkort, och med detta ringer hon upp journalisten. Hon ringer inte hemifrån utan från en plats som inte förknippas med henne.
4. Anna pratar med journalisten, som efter samtalen fått all information hen behöver. Efter samtalet förstör Anna både den billiga mobilen och kontantkortet och kastar skrotet i en kommunal soptunna. Därmed skulle det vara väldigt svårt att spåra samtalet till just henne.

Kusinen Yasmine

Yasmine är dotter till Pelles syster. I år sommarjobbar hon för första gången på ett café, men hon har sett att löner inte betalas ut som de ska. En del får ingen lön alls, andra har betalats svart och dessutom slarvas det med hygienen. Hon har tagit några bilder med sin mobiltelefon och vill föra dem vidare, men hon har hört att bilder kan spåras och vill inte att arbetsgivaren får reda på att det är hon som tagit dem så att hon kan få sparken.

1. Yasmine läser på om bilder, och förstår att det farliga med bilder från mobiltelefonen är att de innehåller massor av metadata – information om var, hur, och när bilden togs. Yasmine ser att bilderna hon tagit innehåller tidsangivelser om när de togs, vilket skulle avslöja henne om informationen kom i orätta händer.
2. Yasmine inser att hon måste ”tvätta” bilderna från metadata, och läser på internet om hur det fungerar. På så sätt lyckas hon ta bort tider och datumet från bilderna, och känner sig trygg med att skicka dem vidare.
3. Yasmine ringer upp en journalist från sin privata mobiltelefon, och ber om ett möte. På så sätt slipper hon skicka bilderna i ett e-postmeddelande, eftersom hon inte vet hur säkert det blir.
4. Då Yasmine träffar journalisten berättar hon om problemen på caféet, och ger honom bilderna på en usb-sticka.

Länklista

Electronic Frontier Foundation har utmärkta kostnadsfria guider på engelska om hur du skyddar dig och din information på nätet.
ssd.eff.org

TCO: Rätten att slå larm. En handbok om yttrandefriheten på jobbet.
Laddas ned gratis från:
www.tco.se

Kolla hur du blir spårad på nätet när du använder datorn:
trackography.org

Läs mer på nätet redan idag!

På Internetguidernas webbplats hittar du presentationer av alla 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, statistik och mycket mer. www.iis.se/guider

Digitalt källskydd - en introduktion

Den här guiden är producerad i samarbete med Svenska Journalistförbundet och är full av fallstudier, lösningar och konkreta tips på hur journalister, arbetsledning och andra som hanterar känslig information kan skydda källor i det dagliga arbetet. Introduktionen till digitalt källskydd är författad av de namnkunniga journalisterna Sus Andersson, Petra Jankov, Fredrik Laurin och Anders Thoresson.

It-säkerhet för privatpersoner – en introduktion

Vecka efter vecka fylls löpsedlarna av nyheter om stulna lösenord, skadlig kod och bedrägeriförsök. Kapade Facebook- och Twitterkonton likaså. Succéförfattarna Linus Larsson och Daniel Goldberg lär dig grunderna i hur du håller dig säkrare i den digitala världen. De bjuder på matnyttiga tips att hålla din uppkoppling, e-post, ditt Facebookkonto och dina bankuppgifter i tryggare förvar. Innehållet kräver inte särskilda förkunskaper.

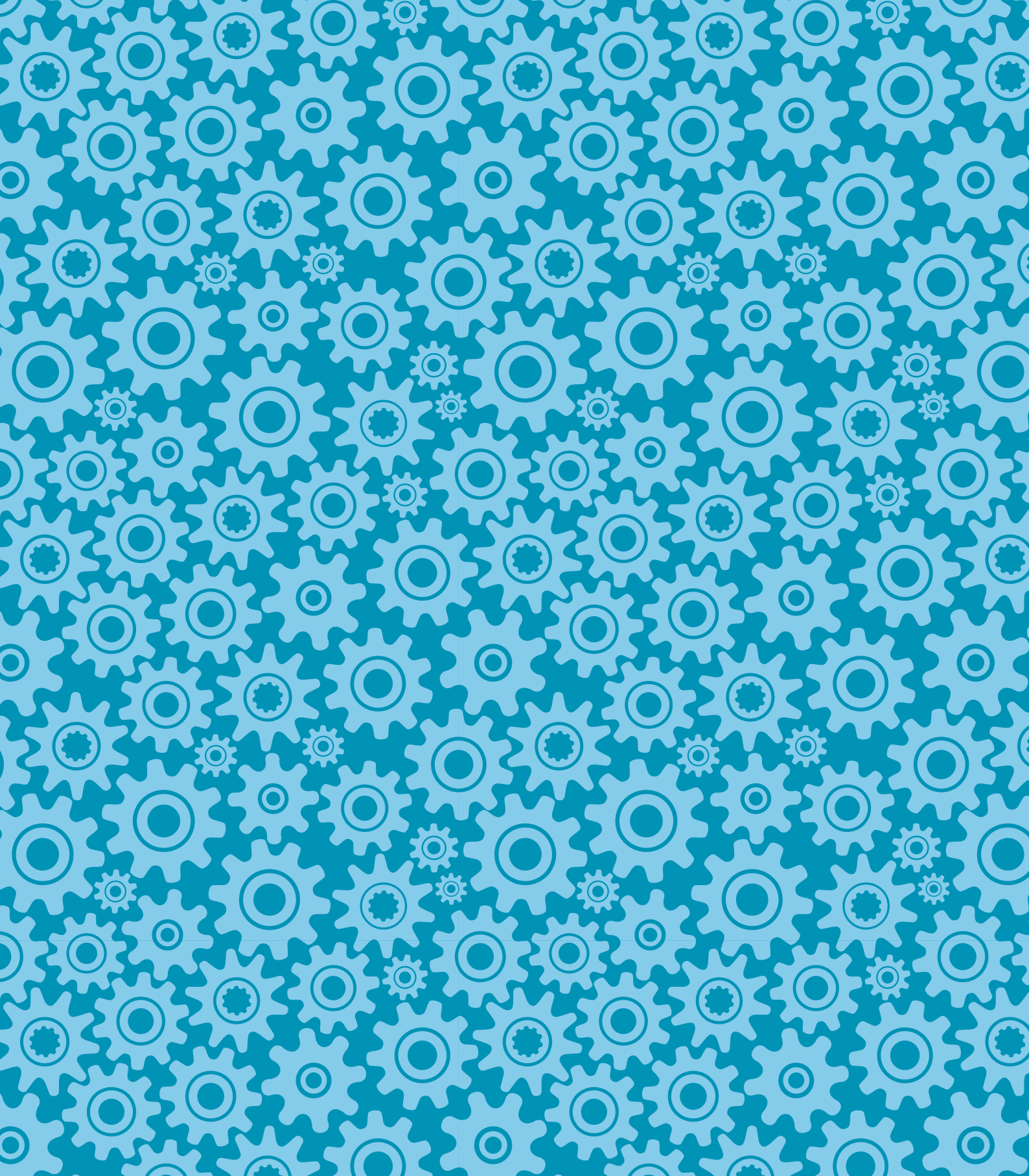
Till den här Internetguiden medföljer XL-materialen ”Kom igång med Tor!” och ”Kom igång med PGP!”. I dokumenten får du lära dig grunderna och hur du använder Tor och PGP i praktiken, steg-för-steg. Materialen laddar du ned gratis från www.iis.se/guider

Här hittar du alla Internetguider:

https://www.iis.se/guider

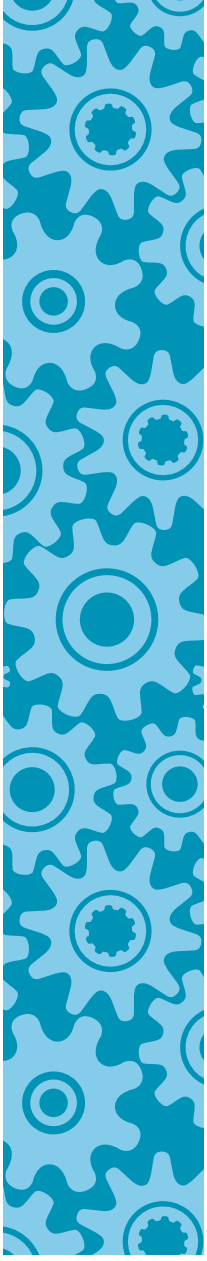
Varje ny .se-adress bidrar till utvecklingen av internet

.SE (Stiftelsen för internetinfrastruktur) ansvarar för internets svenska toppdomän och administrerar registreringen av domännamn under .se. Överskottet från registreringsavgifterna för domännamn investeras i internetutveckling som gagnar alla internetanvändare, bland annat den här Internetguiden!



.SE (Stiftelsen för Internetinfrastruktur) vill på olika sätt främja en positiv utveckling av Internet i Sverige. En av våra viktigaste målsättningar är att alla ska kunna ta tillvara på nätets möjligheter. Därför publicerar vi lärorika Internetguider inom olika spännande ämnen. Det finns praktiska guider för dig som vill börja blogga, teknikguider för dig som undrar hur mejlen du skickar når fram till rätt mottagare och guider som förklarar vem som egentligen bestämmer på nätet.

.SE:s Internetguider är gratis. Beställ eller läs dem online: www.iis.se/guider



ISBN 978-91-87437-21-2

.SE (Stiftelsen för internetinfrastruktur)
Box 7399, 103 91 Stockholm
Tel 08-452 35 00, Fax 08-452 35 02
Org. nr 802405-0190, www.iis.se

.se
Vi driver internet framåt