Internetguide #35
Digitalt källskydd

En introduktion

0100110
110010110101
0100101011101 1
0010111011001 01
1010101001010 1
1101100101 11
011001
0101011101 1
0010110101010010 11
0110110010111011001 01
1010101001010111011001

Sus Andersson, Petra Jankov Picha,
Fredrik Laurin och Anders Thoresson

internetguider.se

I den här guiden lär du dig...

- ☑ Om risker och konsekvenser vid bristande digitalt källskydd
- ☑ Att minimera risken att röja källor
- ☑ Hur du hjälper informationslämnare
- ☑ Använda internet och mobil kommunikation säkrare
- ☑ Praktiska tips och intressanta fallstudier
- ☑ Källskydd i sociala medier

Innehåll

Förord 4

Inledning 5

Alla har ett ansvar 6
Internet för journalister 7
Hjälp tipsaren att göra rätt! 10

1. Bristande källskydd: Lösenord 14

1.1 Case: Lätt att hacka lösenord på nätet 15
1.2 Skydda källan: Lösenor 16

2. Bristande källskydd: E-post 19

2.1 Case: Mediekontakter avslöjas genom e-posten 21
2.2 Skydda källan: E-post 22
2.3 Case: Greenwald höll på att missa tidernas scoop 26

3. Bristande källskydd: Telefon 28

3.1 Case: Att prata med källan i telefon 30
3.2 Skydda källan: Telefon 31

4. Bristande källskydd: Lagringsmedia 33

4.1 Case: Källan ”neo” röjs 34
4.2 Case: En kopierad hårddisk 35
4.3 Skydda källan: Lagringsmedia 36
4.4 Skydda källan: Radera säkert 37

5. Bristande källskydd: Uppkoppling 41

5.1 Case: Presidentvalet i vitryssland 43

6. Bristande källskydd: Molntjänster 44

6.1 Case: Reportern blev av med allt 45
6.2 Skydda källan: Minimera riskerna 46
6.3 Skydda källan: Brandvägg 48
6.4 Skydda källan: Surfa säkrare 50
6.5 Case: Lagen skyddar inte digitala källor 60

7. Källskydd och juridik 63

7.1 Skydda källan: Sociala medier 68
7.2 Case: Göteborgs-posten 70

8. Läs mer 72

Förord

Alla som lämnar en uppgift till media ska kunna garanteras anonymitet. Källskyddet är avgörande för journalistisk verksamhet och är därför inskrivet i svensk grundlag. Trots detta finns uppenbara hot mot källskyddet. Några exempel är FRA–lagen, fildelningslagen IPRED och lagen om elektronisk kommunikation, LEK, den bygger på ett direktiv som ogiltigförklarats av EU–domstolen som anser att direktivet är för integritetskränkande. Dessa lagar har försvårat för allmänheten att anonymt kontakta journalister. Därför behövs större vaksamhet och försvar av källskyddet, inte minst när nya övervakningslagar diskuteras.

Ansvaret för källskyddet ligger hos den som tar befattning med det källskyddade materialet. Det har aldrig varit en exklusiv utgivarfråga, vilket också Högsta Domstolen nyligen slagit fast i en dom mot journalister vid Göteborgs-Posten. Därför krävs att alla journalister har kunskap om och är medvetna om vikten att värna källskyddet. Arbetsorganisationen på redaktionerna måste göra det möjligt för journalisterna att leva upp till grundlagens krav om att de ska skydda källors rätt till anonymitet.

Alla redaktioner bör ha en källskyddspolicy, men få har det. Sammanslagningar av redaktioner som ska konkurrera med varandra, men som trots detta sitter i samma lokaler, kan innebära problem för att skydda respektive källor. Likaså intresset av att spara det redaktionella materialet i olika former av molntjänster utanför redaktionens direkta kontroll. Sociala medier och andra plattformar för tips, kommentarer, och möjlighet till direkt medverkan i nyhetsprocessen ökar yttrandefriheten, men skapar också problem med att även garantera digitalt källskydd.

Med den här guiden vill därför Journalistförbundet och IIS, Internetstiftelsen i Sverige ge tips och råd om hur vi i det dagliga arbetet skyddar oss och våra källor.

Jonas Nordling
Förbundsordförande Svenska Journalistförbundet.

Stephen Lindholm
Ordförande Journalistförbundets yttrandefrihetsgrupp, ledamot i förbundsstyrelsen.

Inledning

Även om journalister till vardags strävar efter största möjliga öppenhet, och källor som vågar stå för det de säger, finns det tillfällen när detta inte fungerar. Mutor och korruption, vanvård av gamla och sjuka, miljöskandaler – det finns en rad områden där det är uppenbart att det är viktigt att saker ska komma fram i ljuset. Samtidigt kan den som avslöjar problemen betraktas som illojal och därmed löpa stora risker. Källor i företagsvärlden kan få sparken och tvingas betala stora skadestånd, och i den undre världen eller i diktaturer kan människor som pratar med journalister i värsta fall sätta livet på spel.

Allt oftare inträffar allvarliga intrång i journalisters it-miljöer. Den syriske dissidenten ”Kardokh” och flera med honom fick fly hals över huvud när den brittiske journalisten Sean McAllister greps 2012, och hans utrustning hamnade hos den syriska säkerhetstjänsten. Under de senaste åren har svenska journalisters datorer stulits, hackats eller tagits i beslag av polisen. Lösenord till e-postkonton har läckt ut flera gånger. Enskilda frilansjournalister såväl som stora redaktioner med internationellt renommé har plötsligt upptäckt att någon varit inne i deras system. Stora företag har kammat igenom tusentals telefonloggar och e-postmeddelanden, i jakten på läckor till media. Och program som tar kontroll över din dator utan att du märker det kan vem som helst ladda hem från internet.

Respekten för redaktioners integritet och källskyddet är idag minimalt. Ett exempel var när TV4:s Anders Pihlblad misstänktes för bestickning efter att ha bjudit statssekreterare Ulrika Schenström på alkohol. Överåklagare Christer van der Kwast tyckte att det motiverade en husrannsakan på TV4-Nyheternas redaktion där kvittot för vin-kvällen förvarades. Vad olika länders massövervakning av människors kommunikation inneburit för möjligheten att skydda mediernas källor är omöjligt att ens överblicka.

Därför är det alla journalisters ansvar att vara extremt noggranna med alla uppgifter som kan vara känsliga. Med tanke på hur vi kommunicerar idag är risken stor att information ska komma på villovägar – antingen av misstag, eller för att någon är ute efter den.

Källskyddet omhuldas starkt av de flesta journalister. Alla ”vet” att de ska skydda sina källor. Att prata om en hemlig källas identitet är tabu och att glömma ett anteckningsblock på krogen en dödssynd. Det finns en idealbild av journalisten som är beredd att göra allt, inklusive att krypa i fängelse, hellre än att avslöja sina informatörer. Men så fort det rör sig om elektronisk kommunikation tycks den analoga världens spärrar släppa helt. Trots att e-post är att betrakta som internets vykort – faktiskt värre än vykort! – är det fortfarande

många redaktioner som uppmanar tipsare att använda just e-posten. Ett löfte om anonymitet i det läget är inte värt ett vitten.

Idag lämnar vi omfattande mängder digitala spår efter oss. Varje telefonnummer vi ringer, internetuppkoppling, e-post- och sms-kontakt sparas av teleoperatörerna. Google vet vad du försöker söka reda på. Facebook har full koll på ditt kontaktnät och massor av företag vet var miljoner svenskar befinner sig i varje ögonblick genom olika positioneringstjänster. Allt mer av våra spår sparas – en del för att det finns lagar som kräver det, annat för att det finns kommersiella intressen i att göra det. För den som har rätt verktyg finns stora möjligheter att snappa upp och avlyssna nätkommunikation.

Sist men inte minst finns stora risker bara i det att vi bär omkring apparater som innehåller känslig information. En dator eller telefon som glöms i en taxi kan innebära en katastrof om apparaten hittas av fel person. Är innehållet okrypterat är det fritt fram att botanisera i telefonboken, kalendern, researchen och i halvskrivna artiklar. De digitala möjligheterna gör det också allt svårare för journalister att skydda källorna.

Sedan den första utgåvan av den här boken har fler mediehus börjat vidta mått och steg för att skydda sina källor bättre. Men bristerna är fortfarande stora. Alltför få journalister och redaktioner kan ta emot krypterade meddelanden, man efterlyser tipsare i sociala medier utan att tänka på att kommunikationen är öppen även för andra, känslig information lagras i molntjänster som inte omfattas av svensk grundlag och många journalister går runt med en mobiltelefon som innehåller massor av känslig information – utan att ens ha en pinkod på telefonen. Dessutom arbetar allt fler journalister på frilansbasis, ofta helt utan tillgång till it-kompetens.

I den här guiden vill vi visa vilka risker källorna löper och att det är reella hot. Men framför allt vill vi ge exempel på vad man som journalist kan tänka på för att undvika att källorna avslöjas av misstag. För lösningar finns och förvånansvärt ofta är de enkla. Samtidigt är det viktigt att poängtera att det inte finns någon absolut säkerhet. Olika trick och program löser olika problem – men det finns inget system som löser allt. Dessutom är den digitala världen hela tiden föränderlig. I det program som var bäst igår kan någon ha hittat ett säkerhetshål idag. Därför krävs kontinuerligt arbete med källskyddet.

Alla har ett ansvar

Den enskilda journalisten har ett mycket stort ansvar för att skydda sina källor. Men källskyddet, så som det är formulerat i grundlagen, tvingar alla som på något sätt har med publiceringen att göra att hålla källorna hemliga. Kraven ställs alltså inte bara på journalisten, utan på alla som jobbar inom medierna: it-tekniker, växeltelefonister, tryckare och förlagsdirektörer.

Den enskilda journalisten, oavsett om det är en anställd eller en frilans, behöver tänka igenom sitt arbete och skaffa rätt verktyg. Det är också viktigt att försöka instruera källorna, så att de gör rätt från början. Berätta om riskerna med olika sätt att kommunicera och hur man kan skydda information.

För att källskyddet ska fungera krävs också betydligt större insatser från mediehusens ledningar. Även om grundlagens tystnadsplikt bara gäller dem som kunnat ta del av information om källorna handlar källskyddet idag också allt mer om ekonomi och organisation – att ha en it-säkerhets- och källskyddspolicy och att satsa på kompetensutveckling. Helt enkelt att ha bra verktyg för att verkligen kunna garantera källorna det skydd de ska kunna förvänta sig.

Internet för journalister

Den här guiden innehåller råd och tips om hur du som journalist kan minska risken att avslöja dig själv eller dina källor när du använder internet. Men för att verkligen förstå varför du ska vara försiktig när du använder det trådlösa nätverket på kafét eller varför du behöver kryptera känslig e-post behöver du också en grundläggande kunskap om hur internet fungerar.

Om du redan vet hur internet fungerar kan du hoppa över det här kapitlet. För alla andra följer här en kort genomgång av några av de egenskaper hos nätet som är särskilt viktiga ur källskyddshänseende.

Inga direktförbindelser

Internet är ett nätverk av nätverk. På redaktionen där du jobbar, eller på ditt frilanskontor, finns massor av it-utrustningar som är kopplade till varandra. Datorer, pekplattor, mobiltelefoner, skrivare, servrar och nätverkshårddiskar är anslutna till vad som kallas för routrar och switchar. En switch och en router är ett slags dataväxlar. Deras uppgift är bland annat att se till att trafik skickas till rätt mot-

Viktigt! Gör genast!

Det första du bör göra för att öka din it-säkerhet är:

- Använd starka lösenord.
- Använd aldrig samma lösenord på flera ställen.

(Läs mer om lösenord på sid 14)

tagare. Och redan här, i nätverket där dina prylar är uppkopplade, kan vi se att det inte finns några direktförbindelser: Ska du skriva ut en artikel på nätverksskrivaren skickas texten via åtminstone en switch eller router. På samma sätt är det när du skickar ett mejl. Det lämnar din dator, färdas via routern, vidare till nätverksutrustning hos din internetleverantör och därifrån i många steg fram till mottagarens e-postserver. Där ligger det och väntar tills dess att mottagaren kollar sin e-post. Då färdas det den sista biten till mottagarens dator eller mobiltelefon, via hens internetleverantör. När ett mejl skickas från person A till person B passerar det alltså många ställen på vägen. Och i varje enskild punkt kan de tekniker som har åtkomst till utrustningen också se trafiken som passerar.

Trafik i klartext

Kanske har du hört uttrycket "e-post är som vykort". Andemeningen är att brevbäraren och alla andra som hanterat vykortet du skickade från semestern kan läsa det – och att detsamma gäller för e-post. Att det är så beror på två saker. Det ena är just att det saknas direktkopplingar på internet. Det andra är att e-post ytterst sällan är krypterad. Tillsammans innebär det att de nätverkstekniker som vill också kan läsa e-post som passerar i deras system. Och detta gäller givetvis för all trafik som skickas okrypterad: Lösenord, chattmeddelanden, dokument och så vidare. Är det inte krypterat så är det som att skicka ett vykort. Dessutom är det enkelt att skapa kopior av

Viktigt! Vad är kryptering?

Kanske roade du dig med enkla chiffer som barn, där exempelvis alla bokstäver byts ut mot den som kommer efter i alfabetet. "Hej" blir då "Ifk". De krypteringslösningar som används av datorer är betydligt mer komplexa än så, men grundprincipen är ändå densamma: Ta en text och förvräng den på ett förutbestämt sätt. Förvrängningen sker enligt överenskomna matematiska regler och bara den som har tillgång till "nyckeln" (ofta ett lösenord) kan återskapa det begripliga originalet. För alla andra är innehållet inte annat än en härva av obegripliga teckenkombinationer.

all din internettrafik utan att du märker det. I dag, när vi ofta kopplar upp oss i trådlösa nätverk när vi exempelvis slår oss ner på ett kafé på stan, blir problemen extra stora. I ett trådlöst nätverk behöver man nämligen inte vara en behörig tekniker för att kunna titta på trafiken. Alla som befinner sig inom nätverkets räckvidd kan också titta på all trafik som skickas okrypterad.

Att trafiken ofta skickas i klartext innebär dessutom att den som sitter någonstans i kedjan mellan A och B också kan manipulera trafiken och ändra innehållet utan att du märker något.

Avslöjande adresser

För att utrustningen på internet ska veta vart ett mejl eller en webbsida ska behöver trafiken vara försedd med en mottagaradress. Det finns en tydlig parallell med en vanlig postadress: Utan den vet inte brevbäraren vart ett paket ska. På internet används så kallade ip-adresser. De är siffer-kombinationer av typen 91.226.36.46. När du surfar till IIS webbplats är det till den adressen som din webbläsare ansluter. Men också din dator har en ip-adress. När din webbläsare ansluter till IIS webbserver talar den om vilken adress den kommer ifrån, så att innehållet på webbsidan kan skickas tillbaka. Alla miljoner ip-adresser på nätet har en ägare, och det finns databaser där det går att ta reda på till vem en viss adress hör. När du kopplar upp dig via internetabonnemanget hemma får du tillfälligt låna en ip-adress som hör till din internetoperatör. Men en redaktion har

Viktigt! Sammanfattning!

Delar av de följande kapitlen är ganska tekniska och kan verka avskräckande för dig som inte är helt bekväm med nya termer och it-teknik i massor. Vissa läsare kanske också saknar mer detaljerade beskrivningar av hur de ska skydda sina källor. Vi har tagit fram extramaterial till den här guiden som förklarar hur du använder exempelvis kryptering i praktiken. Av utrymmesskäl, men även för att slippa trycka nya guider då programmen uppdateras, kan du läsa handfasta användarinstruktioner på adressen internetguider.se. Vi har döpt extramaterialet till ”*Kom igång med Tor!*”, ”*Kom igång med PGP!*”, "Kom igång med Tails!" och "Kom igång med säkrare mobiltelefon!".

Tips! Digitalt källskydd light

Snabba tips för dig som vill kommunicera lite säkrare:

- Tänk igenom värsta tänkbara scenario i ditt fall och agera efter det.
- Använd mobil med kontantkort. Förstörs efter avslutat projekt.
- Kommunicera inte med källan på dennes arbetsplats.
- Ha starka lösenord. (Läs mer om lösenord på sid 14.)
- Aldrig använda samma lösenord på flera ställen.
- Använd aldrig din vanliga e-post. Ett alternativ kan vara anonyma e-postkonton via en gratistjänst.
- Träffa de viktigaste källorna öga mot öga och skicka alla dokument med snigelposten.
- Inget av dessa tips fungerar i alla lägen, men är första steg på vägen.

sannolikt ett antal egna ip-adresser. Den som vet vilka ip-adresser som hör till redaktionen kan därför hålla koll på om någon från lokaltidningen exempelvis besöker företagets webbplats. Om du besöker ett företags webbplats i samband med att du gör research kan alltså företagets tekniker upptäcka detta.

Hjälp tipsaren att göra rätt!

Den kanske mest sårbara kontakten mellan en källa och en journalist är den allra första, den när källan är den som tar initiativet. Oavsett hur skicklig journalisten är på it-säkerhetkan ju källan använda en kontaktväg som är osäker. Ett stort problem idag är också att så få journalister och redaktioner hjälper källorna att göra rätt. Det är inte ovanligt att man ber om tips via e-post, Twitter eller Facebook. Många redaktioner har särskilda tipssidor på webben, där källorna kan skriva in sina tips eller ladda upp bilder. Men formulären skickas ofta helt öppet över internet; bara en handfull redaktioner har krypterade tipsformulär. Andra använder Google-formulär, som visserligen kan vara supersmidiga för exempelvis enkäter – men som samtidigt ger Google tillgång till information som kan vara känslig.

I andra kapitel i den här boken kan du läsa mer om riskerna med olika tekniker. Försök att utforma de kontaktvägar du har på ett sådant sätt så att du minimerar riskerna för källorna.

Hjälp tipsarna att förstå riskerna
Om du vill ha heta tips bör du ha en tipsarskola, exempelvis på webben, där det framgår hur källorna på bästa sätt kontaktar dig eller din redaktion samtidigt som de största hoten undviks. Berätta gärna om källornas rätt att vara anonyma, men var samtidigt tydlig med riskerna. Tala om hur man som tipsare undviker att lämna spår. Vad som ska ingå i tipsarskolan beror naturligtvis delvis på vilka kontaktvägar du själv kan bli nådd på, och vilken typ av information du vill ha. Enkla förslag som kan finnas med är att aldrig någonsin mejla känsliga uppgifter, att undvika att använda telefon och mejl på jobbet – och aldrig om tipsen gäller arbetet eller arbetsgivaren. Framhåll gärna tillfälliga, anonyma mejlkonton och ett oregistrerat kontantkort till mobilen – ett som bara används till tipset. Var tydlig med att ju känsligare ett tips är, desto viktigare är det att vara försiktig.

Viktigt! Sammanfattning.

Två saker som journalister som använder nätet behöver ha i huvudet: För det första är trafiken på internet ofta möjlig att avlyssna och manipulera. För det andra går mycket av det vi gör på nätet att koppla till oss som individer eller åtminstone till redaktionen.

Gör det lätt för tipsarna
Om man ska kommunicera digitalt är ett krypterat webbformulär den bästa kombinationen av enkelhet och säkerhet för källan. Till skillnad från krypterad e-post behöver källan inte installera några program, utan kan bara skriva in sitt tips i formuläret. Däremot behöver du eller din redaktion anlita en kvalificerad webbprogrammerare för att skapa den säkra webbsidan, som kommer att ha en adress som börjar med ”https” i stället för ”http”. Men även här finns stora skillnader mellan olika lösningar, och en dåligt krypterad tipsarsida kan invagga källorna i falsk säkerhet.

Känsliga uppgifter måste krypteras
Känsliga tips som skickas via nätet ska inte gå i klartext. Använd antingen krypterade formulär eller krypterad e-post. Om ni inte har möjlighet att kryptera: tala i alla fall om för källorna att de inte ska använda sådana osäkra kontaktvägar om de vill kunna förbli anonyma.
Allt fler redaktioner har nu också appar för att lämna tips eller skicka in bilder. Även dessa behöver naturligtvis vara konstruerade för hög säkerhet i överföringen av data.

Krypterat är inte detsamma som anonymt
Även om innehållet i ett webbformulär krypteras kan avsändaren spåras på flera olika sätt. Skickar du ett krypterat mejl står både avsändare och mottagare i klartext, även om själva innehållet i brevet ser ut som rappakalja.

Krypteringen kan därför behöva kombineras med anonymiseringsteknik, som anonyma mejladresser och internetuppkoppling via anonymiseringstjänster, som exempelvis Tor eller en VPN-tjänst. Det är också olämpligt med annonser på din tipsar-sida, eftersom du troligen ger annonsörerna möjlighet att se besökarnas ip-adresser och att placera kakor i deras webbläsare. Du bör inte heller analysera webbstatistik med hjälp av Google eller någon annan extern leverantör, eftersom du ger dem möjlighet att ta del av uppgifter om besöken på tipsarsajten.

Var tydlig
Tala om hur du eller din redaktion hanterar tips, och vad er lösning har för brister. Det hjälper källorna att göra rätt. Fullständig säkerhet finns inte, men om man vet var fallgroparna finns går de att undvika. Öppenhet med hur ni jobbar stärker också förtroendet för tipstjänsten. Däremot ska ni naturligtvis aldrig tala om sådana detaljer som gör det möjligt att hacka tipsen.

Viktigt! Instruera källan.

Den här guiden vänder sig i första hand till dem som jobbar inom media och hur de bör arbeta för att minska riskerna för källorna. En privatperson som vill lämna anonymt tips till en journalist har stor hjälp av att läsa Internetguiden ”*Digitalt självförsvar – en introduktion*” som finns att ladda ned kostnadsfritt från internetguider.se

Var noggrann

Trippelkolla hela kedjan innan du sjösätter din lösning. Låt externa it-säkerhetsexperter sätta den på prov. Slarva inte. Att till exempel publicera sin hemliga nyckel för PGP-kryptering istället för den publika är ett kardinalfel – men det begicks av Aftonbladet för ett par år sedan och upprepades igen våren 2015. Håll också kontaktsidorna aktuella vartefter. Att bara erbjuda en krypteringsnyckel till någon som slutat är inte heller lämpligt – något som inträffat på Svenska Dagbladet. Använd stark kryptering, och följ teknikutvecklingen. Nya säkerhetsluckor upptäcks hela tiden, och det som var bäst igår kan vara utdömt i dag. Tänk också på hur du hanterar och lagrar tipsen. Helst bör det ske på en dator som inte har kontakt med internet.

Krångla inte till det

Använd bara en lösning som är väl testad och som du vet att du behärskar. Det är ofta både enklare och säkrare för både källa och journalist att ses eller kommunicera med vanliga brev, än att ni använder en halvdan krypteringslösning som ingen av er riktigt klarar av. De här tipsen handlar bara om hur man som journalist hjälper källorna att ta en säkrare första kontakt. När du går vidare med ett tips behöver källorna få mer information om vilka spår de lämnar när de hjälper dig att få tag i uppgifter.

1. Bristande källskydd: Lösenord

Du kan begränsa åtkomsten till de flesta moderna arbetsverktyg med lösenord. Datorn, e-posten, mobiltelefonen, olika redaktionella system, bloggportaler, sociala medier – listan kan göras lång. Men på samma sätt som bra lösenord hindrar andra från att komma åt känslig information är dåliga lösenord ett allvarligt hot mot källorna. Det finns några klassiska fel som begås om och om igen. Ett av de vanligaste är att använda samma lösenord överallt. Då hjälper inte ett starkt lösenord. Om en bloggportal som inte haft tillräckliga säkerhetsrutiner blir hackad, är ditt lösenord likväl på vift – och hackarna kan komma åt din e-post eller logga in på ditt Facebook-konto. Alldeles för enkla lösenord är också vanliga. Genomgångar som har gjorts när olika sajter hackats visar att många använder varianter på sajtens namn, ibland med vissa bokstäver utbytta mot siffror – men alla i kombinationer som är lätta att gissa. Tangentbordssekvenser som ”qwerty” och liknande är också populära och därmed fullständigt förkastliga att använda som lösenord. En del använder mer personliga uppgifter och hoppas att de ska vara svårare att lista ut. Men alla bokstavskombinationer som finns i en ordlista går att testa sig fram till på några timmar om någon verkligen vill komma åt just din information. Ett mycket kort lösenord går att knäcka på några ögonblick. Även personliga sifferkombinationer går att lista ut. Ditt eller dina närmastes födelsedatum eller telefonnummer är lätta att hitta och testa om någon är ute efter ditt lösenord. På en del arbetsplatser är det it-avdelningen som skapar lösenorden och skickar ut dem. En del är rent ut sagt undermåliga: två bokstäver ur förnamnet, två ur efternamnet och sen året då personen började på företaget. Får utomstående tag på ett sådant lösenord har de snart knäckt hela redaktionens lösenord. Men även om de centralt distribuerade lösenorden är starka är de en säkerhetsrisk om alla lösenord skickas ut gemensamt – via e-post.

1.1 Skydda källan: Lösenord

Ett idealiskt lösenord är lätt att komma ihåg för användaren och svårt att lista ut för obehöriga. Samma lösenord ska aldrig återanvändas på flera tjänster med inloggning eller på olika apparater. Det viktiga är att hitta en teknik för att skapa lösenord som är smidig för dig. Grundprincipen är att lösenordet ska vara ganska långt. Statliga Post- och telestyrelsen föreslår minst tolv tecken. Men i sammanhang där information hanteras som är mycket känslig och där den som kan vara intresserad av att knäcka det har gott om pengar eller datorkraft kan det vara värt att överväga ett betydligt längre lösenord. Var man landar bör vara resultatet av en riskbedömning. Det finns litet olika skolor kring hur man konstruerar bra lösenord. Många hävdar att det är ett måste med en kombination av stora och små

Case: Lätt att hacka lösenord på nätet

Familjeliv, Spotify, Linkedin och Bloggtoppen är några av alla tjänster på nätet som de senaste åren fått sina medlemmars lösenord hackade och avslöjade. 2008 hackades lösenord till Aftonbladet av en grupp som kallade sig Vuxna förbannade hackare. En onsdagskväll i januari postade hackergruppen ett inlägg på nätforumet Flashback där man berättade att man hackat Aftonbladets intranät och gruppen lade även ut lösenord till journalisters inloggning i forumet. Detta ledde till att hundratals olika personer loggade in på flera journalisters konton och läste mejl och använde journalisternas e-post till att skicka ut falska meddelanden. Aftonbladet polisanmälde händelsen, men ingen kan svara på hur mycket källskyddat material som spreds eller hur många källor som avslöjades. Flera av journalisterna fick också sina Facebook-konton kapade på grund av att de använt samma lösenord till sin e-post på Aftonbladet som på Facebook. De upptäckte att deras profiler ändrades och att olämpliga bilder lades ut på deras sidor. Under hösten 2011 var det dags igen. Då nystades en stor hackerhärva upp som bara växte sig större och större när man avslöjade sajt efter sajt som hackats på lösenord. Totalt hackades 57 olika svenska sajter. De flesta var sociala nätverkstjänster som bloggtoppen och gratisbio.se men även nyhetssajterna dagensps.se, flamman.se och delar av norran.se drabbades. I samband med detta spreds riksdagsledamöters och kända journalisters lösenord på Twitter. Totalt uppskattades att 180 000 konton har drabbats. I januari 2012 kom 120 000 lösenord från en av Sveriges största mötesplatser, Familjeliv, på drift och i juni 2012 hackades Linkedin på 6,5 miljoner lösenord. År 2013 läckte 2,9 miljoner lösenord ut på nätet efter att Adobe hackades. 400 000 av dessa uppgavs vara svenska lösenord och 2014 hackades både Ebay och Gmail och över fem miljoner lösenord hamnade på drift. En billig försäkring är att aldrig någonsin använda samma lösenord på olika sajter utan ha unika inloggningsuppgifter för var och en.

Tips! Tvåfaktorersinloggning säkrast.

Förmodligen använder du redan tvåfaktors-inloggning till exempel för din internetbank. Där används ofta säkerhetsdosor med kort tillsammans med en kod eller ett lösenord. Det är en utmärkt idé att skydda även ditt e-postkonto med denna metod. Många mejltjänster har stöd för det. När tekniken är aktiverad använder du en engångskod tillsammans med ditt vanliga lösenord för att logga in. Mejltjänsten skickar engångskoden till dig antingen i ett sms eller via en särskild app.

bokstäver, siffror och specialtecken som #%&?+. Andra förespråkar långa fraser av vanliga ord. Om man använder den här tekniken är längden mycket viktig – 30 tecken kan vara ett riktmärke. Då blir det svårt för en angripare att testa sig fram, även om lösenordet är lätt för dig att komma ihåg. Undvik fraser som är kända, som ordspråk och litterära citat. Då är det bättre med en helt egen transkription av något uttryck på kalixbondska eller östgötska, eller bara en helt absurd mening. I en del sammanhang är längden på lösenorden begränsad. Om du exempelvis bara kan använda åtta – tio tecken är ”teckensoppa” nödvändig för att uppnå någorlunda säkerhet. Med så här korta lösenord är namn och ord ur ordlistor direkt olämpliga att använda. Program som används för att knäcka lösenord testar ofta igenom ordlistor på olika språk. Att ta ett känt ord och byta några tecken – ”Linkedin” omgjort till ”1!nked!n” är också sådant som är lätt att överlista. Utgå från en mening som du själv kommer ihåg. Sedan förvandlar du den till oigenkännlighet. Välj exempelvis frasen ”Äntligen stod prästen i predikstolen”. Ta de två första bokstäverna i varje ord. Låt den första bokstaven i varje ord vara versal: ÄnStPrIPr. Nu gäller det att få in några specialtecken och siffror. Välj gärna helt galna associationer – det blir ju svårare för andra att lista ut. Man kan byta ut bokstaven Ä mot siffran 4, bokstaven P mot # och lägga siffror efteråt som berättar hur många gånger bokstäverna T och S fanns med i den ursprungliga frasen. Då blir lösenordet 4nSt#rI#rt*4s*3. Poängen är att du inte behöver komma ihåg

”4nSt#rl#rt*4s*3”, utan ”Äntligen stod prästen i predikstolen” – och några regler. Reglerna kan du använda jämt, men låt fraserna vara unika för varje ställe. Lösenorden bör aldrig sparas i klartext. Skriver du upp dem: betrakta dokumentet som en värdehandling. Hur skulle du förvara 100 000 kronor? Knappast liggande löst på skrivbordet. Det finns krypteringsprogram som gör så att du får ett enda lösenord till en fil med många lösenord, men kontrollera att du kan lita på den som tillverkat det. Låt inte dina program som webbläsare och appar spara lösenorden i inställningarna. Om någon stjäl din mobil eller dator har den personen i så fall även omedelbar tillgång till alla dina program – och kan dessutom ändra lösenorden. Många webbsajter skickar ut nya lösenord till den e-postadress du har angett, ifall du varit glömsk. Ändra alltid detta nya lösenord till något som du själv väljer. Om någon snappat upp din e-post får annars den personen tillgång till sajten som lösenordet gäller för. E-postlösenord bör vara riktigt starka. Om någon får tag i dem kan han eller hon gå in och beställa nya lösenord i ditt namn på andra sajter. Till god lösenordshygien hör också att man byter dem med jämna mellanrum. Men för ofta är inte bra – då ökar risken att man förenklar dem, eller skriver upp dem, för att lättare komma ihåg dem. Några gånger per år kan vara ett riktmärke, eller om du använt det i ett osäkert sammanhang, som ett internetcafé. Lämna aldrig ut ditt lösenord. Radera som regel e-post som ber dig skicka lösenord eller som länkar någonstans där du ska logga in. Det är klassiska metoder för att lura av folk deras lösenord (så kallat nätfiske). Om du befinner dig på allmän plats bör du också tänka på att någon kan snappa upp ditt lösenord genom att kika över axeln på dig. Sitter du vid en publik dator bör du logga ut från tjänster och stänga webbläsaren innan du lämnar den.

Viktigt! Skaffa säkrare lösenord.

- Minst tio tecken, men gärna mer än 14 tecken långt.
- Ha aldrig samma lösenord på flera ställen.
- Byt lösenord en till fyra gånger per år.
- Byt lösenord när du jobbar med ett högriskprojekt.
- Byt lösenord när du exponerat det genom att använda en oskyddad uppkoppling.

2. Bristande källskydd: E-post

Tips! Kolla IP-numret.

Vem, vilka eller vad som står bakom en IP-adress kan du slå upp i så kallad Whois-tjänst. Ett exempel på en sådan hittar du på ping.eu

Mejlen är ett fantastiskt vardagsverktyg för journalisten – det går snabbt att skicka iväg ett meddelande till en person som inte svarar i telefon och det är enkelt att e-posta citat och textstycken för kontroll före publicering. Men enkelheten innebär också stora risker. Det är ett ögonblicks verk att skicka iväg ett mejl till fel person. E-posttrafik kan lätt snappas upp av obehöriga. E-postprogrammens adressböcker har flera gånger drabbats av virusattacker. E-post sparas hos avsändaren, hos mottagaren och hos förmedlaren. E-postloggarna hos myndigheter är offentliga handlingar. Därmed är alla e-brevskontakter med källor på myndigheter fullständigt öppna. Oavsett arbetsgivare kan kontakter mellan källan och journalisten alltid ses av källans arbetsgivare om breven går via arbetsgivarens e-postservrar.

Ett sätt att skydda kommunikationen kan vara att kryptera e-posten. Men även om en stark kryptering gör att den som snubblar över ett mejl inte kan läsa innehållet, finns ändå mycket information att vaska fram ur en mejlväxling. En del journalister skapar anonyma e-postkonton på gratistjänster. Men inte heller dessa är alltid helt anonyma. IP-numret, datorns ID-nummer, kan följa med i e-postmeddelandets brevhuvud. En journalist som e-postar från ett medieföretag med egna mejlservrar går då att avslöja med en enkel sökning på internet.

Skickas meddelanden exempelvis via Gmails webbsida följer dock inte IP-numret med och kommunikationen är anonym för den som råkar snappa upp den. Som med alla gratistjänster kan dock villkoren ändras när som helst. Ska du göra något känsligt bör du alltid kolla vad som gäller precis när du tänker använda en viss funktion eller tjänst. Om du läser e-posten på ett internetcafé, inte loggar

Case: Mediekontakter avslöjas genom e-posten

2009 avslöjade den tyska tidningen Der Spiegel att järnvägsbolaget Deutsche Bahn massövervakat de anställdas e-post. Syftet var att kartlägga Bahn-kritiker och deras nätverk, och inte minst deras mediekontakter. Uppemot 145 000 e-brev om dagen gick igenom ett filter, som sökte efter kända redaktioners domännamn – som spiegel.de.

Enligt uppgifter till tidningen skedde övervakningen på uppdrag av bolagets styrelse. Blev det en träff gjordes vidare efterforskningar runt den anställde som skickat e-breven.

Den här typen av efterforskningar är enkla att göra för organisationer och företag, som vill kontrollera sina anställda.

Men även reportrars e-post kan kontrolleras – exempelvis i samband med rättsprocesser.

Förfarandet att kräva in all möjlig dokumentation som bevisning är mycket vanligt i USA. Även e-post är något som rutinmässigt krävs in som bevis, också i civilmål. När David Kaplan, då reporter på den amerikanska veckotidningen US News and World Report, stämdes av en guldhandlare i Miami för förtal, var en av åtgärderna att kräva in Kaplans e-post. I ett mejl till bildredaktören skrev Kaplan skämtsamt nedsättande om guldhandlaren, en formulering som han kom att ångra när han av domstolen tvingades gå igenom och ta fram all korrespondens som hade med fallet att göra. Kaplan, US News and World Report och deras advokater slogs i två instanser i över ett år innan de lyckades vinna mot guldhandlaren.

– De begärde kopior av alla manusutkast, all e-post, allt som hade med artikeln att göra. Det är ett vanligt förekommande fenomen i amerikanska förtalsmål, säger Kaplan.

Fenomenet är så vanligt att vissa amerikanska journalister tagit för vana att inte ta emot känsligt material i sin egen e-post. Istället arrangeras en brevlåda i form av ett webbmejlkonto där avsändare och mottagare kan logga in och skriva och läsa utkast till e-post.

Viktigt! Undvik din vanliga e-post!

Om källans och journalistens ordinarie e-post-adresser används – eller en adress i stil med tipsa@redaktionen.se – kan ju en arbetsgivare som undrar vem som läckt information ganska lätt lista ut det. Detta genom att inspektera information från företagets eller organisationens e-postservrar. Eventuell kryptering från och till en ordinarie adress blir snarast en signal om att det är hemlig information som skickats. Använd därför i görligaste mån anonymiserade e-postadresser och instruera källan att göra likadant.

ut ordentligt och inte rensar webbläsaren efter dig, kan nästa användare komma åt all din e-post. Om du öppnar bilagor från e-posten sparas dessa som temporära filer på datorn – och kan ligga kvar för nästa användare att läsa. Rensa därför historik och återställ webbläsarens inställningar och undvik att öppna känsliga bilagor om du är på ett internetcafé eller lånar en dator på annat sätt.

2.1 Skydda källan: E-post

För att kunna skicka ett krypterat mejl mellan två personer krävs två saker: att båda har nyckeln som brevet är krypterat med och bägge har tillgång till samma krypteringsprogramvara. När Alice vill skicka ett brev till Bob, börjar man enklast med att bägge hämtar någon version av PGP, Pretty Good Privacy, exempelvis det öppna och fritt tillgängliga GnuPG. Både Alice och Bob installerar programmet och skapar sitt nyckelpar – en hemlig och en publik nyckel. De två nycklarna hänger intimt samman, men har två fundamentalt olika funktioner. Den publika nyckeln kan bara låsa och den hemliga kan bara öppna. Alice skickar sin publika nyckel till Bob och Bob skickar sin till Alice. Sedan kan Alice kryptera sina meddelanden till Bob med Bobs publika nyckel. Då är Bob den ende som kan läsa breven, eftersom Bob är den ende som har sin hemliga nyckel. Och vice versa.

Sedan över ett decennium är krypteringsprogrammet Pretty good privacy standard på internet för kryptering av e-post.

Tips! Lär dig mer om krypterad e-post!

Till den här Internetguiden medföljer material-et *”Kom igång med PGP!”*. I dokumentet får du lära dig grunderna och hur du använder PGP i praktiken, steg-för-steg. internetguider.se

Programmet förenar två viktiga byggstenar i en: en mycket stark kryptering och en finurlig lösning av det uråldriga problemet att hantera och distribuera krypteringsnycklar. Att kryptera e-post är numera en enkel process som tar ett par minuter att installera och sätta igång med. Till kända e-postprogram som Outlook och Thunderbird finns tilläggsprogram (plug-ins), exempelvis Enigmail, som sköter hela nyckelhanteringen och krypteringen genom knapp-tryckningar. Däremot är ett slarvigt valt lösenord och en hemlig nyckel förvarad på en öppen hårddisk enkla sätt att angripa en krypterad kommunikation. Eller det allra enklaste, att vänta på det misstag som alltför många gör, alltför ofta: att Bob svarar Alice utan att trycka på ”kryptera”-knappen och därmed skickar inte bara sitt svar, utan Alice ursprungliga brev i klartext och alltså avslöjar hela brevet i ett svep.

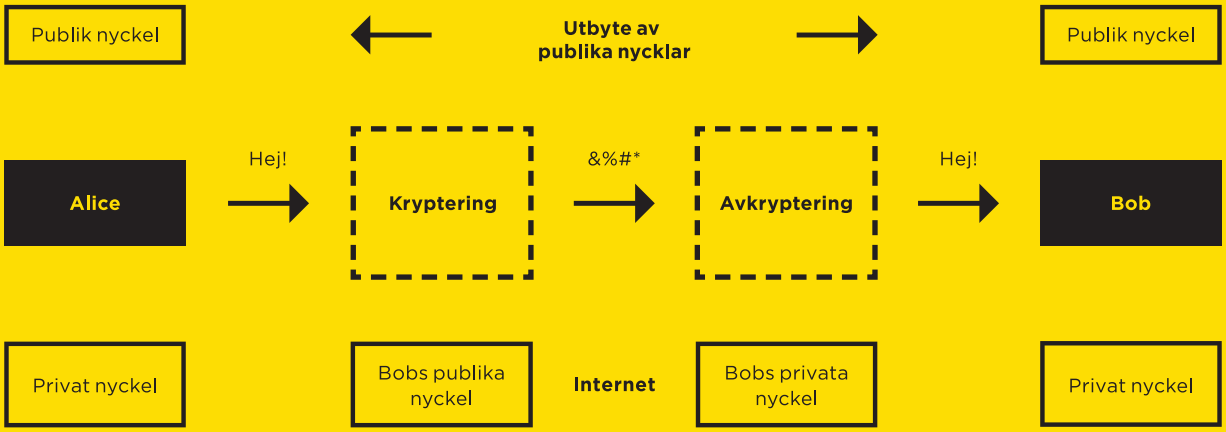
Det enklaste och kanske viktigaste sättet att säkra en viktig kommunikation är att dölja dess existens. Nätet erbjuder många enkla program som döljer ett meddelande bland annan datakod, så kallad steganografi, i till exempel en oskyldig bildfil. Ett krypterat meddelande som dessutom döljs i en bild blir svårt för ett otränat öga att upptäcka. Men i skarpa lägen, när känsligt material ska föras över gränser eller sändas från länder med auktoritära regimer, finns överhängande problem i form av reella hot om eller verklig misshan-del. Blir man tvingad att uppge lösenord och nyckel hjälper ingen kryptering. Utvecklarna av program som krypterar har tänkt på

Tips! Kolla spamfiltret.

Vissa e-postlösningar hanterar bifogade krypteringsnycklar i ett mejl som om innehållet i e-postbrevet vore oönskad skräpmejl, så kallad spam. Det finns även e-postfilter som hickar till och tror att krypteringsnycklar som bilagor är skadlig kod av okänt ursprung. Därför kan du behöva stänga av ditt spamfilter temporärt när du inväntar en nyckel i ett mejl från en kontakt. Alternativt kollar du i spamfiltrets folder regelbundet för att kolla att inte det mejl du väntar på fastnat där. Att e-postprogram städar undan mejl med nycklar i är inte jättevanligt, men vi nämner det för att det händer då och då och är lika irriterande varje gång.

människor i sådana situationer och skapat möjligheter för programmet att dölja krypterade enheter på en hårddisk eller ett usb-minne. Ytterligare ett sätt att dölja sin trafik tillämpades av aktivisterna bakom Wikileaks: tekniken ”Off-the-Record”-direktmeddelanden, OTR. OTR krypterar en chatt, en direktmeddelandetjänst, mellan två personer med en unik nyckel som upprättas vid varje chatttillfälle. Om angriparen kommer över nyckeln kan de inte läsa trafiken i nästa, eller tidigare, kommunikationer. Trafiken i OTR:s chatt-meddelanden är också konstruerad på ett sådant sätt att den kan ha kommit från vem som helst och inte kan knytas säkert till någon enskild person.

Så fungerar PGP:s nycklar



Case: Greenwald höll på att missa tidernas scoop

Ett halvår innan journalisten Glenn Greenwald satte sig på planet till Hong Kong för att träffa visselblåsaren Edward Snowden hade han fått ett märkligt mejl. Det kom från någon som kallade sig ”Cincinnatus”, som erbjöd sig att hjälpa Greenwald att installera krypteringsprogrammet PGP. Men Greenwald hade fullt upp, och hittade inget som kändes intressant nog i Cincinnatus brev – så han lät det vara. Trots flera kontaktförsök, till och med en videoinstruktion, blev det inget PGP för Greenwald, och ingen story då.

”På min ständigt för långa lista över saker att ta tag i, så hamnade installation av krypteringsteknik på uppmaning av denna okända person aldrig tillräckligt högt upp för att jag skulle lägga andra saker ifrån mig och fokusera på det”, skrev han senare i sin bok Storebror ser dig. Då visste inte Greenwald att det var Snowden som låg bakom signaturen.

Snowden kontaktade istället dokumentärfilmaren Laura Poitras, som kunde kryptera. Tidningen Washington Post fick tillgång till en del material, men Snowden tyckte att de var för fega. Så till slut var bollen tillbaka hos Greenwald, som via teknikexperten Micah Lee till slut fick till krypteringen.

”Så nära var jag att sumpa en av den amerikanska historiens största och mest betydelsefulla läckor”, konstaterade Greenwald när det senare uppdagades vem Cincinnatus var.

Greenwald fick inte bara lära sig PGP. I det paket han fick av Micah Lee fanns en usb-sticka med ett helt operativsystem, Tails, som är byggt för att öka säkerheten för den som använder det. Tails står för ”The Amnesic Incognito Live System”. Med stickan i datorn går det att använda datorn ungefär som vanligt – fast inte riktigt. Systemet har en rad program som är inställda för att lämna så få spår som

möjligt: webbläsare, chatt-, epost-, officeprogram och mycket annat. När stickan tas ut rensas alla spår av det som gjorts under sejouren bort från datorn. I och med att Greenwald fick till krypteringen vågade Snowden skicka de första smakproven av sina dokument. Och redan när Greenwald fick upp de första filerna blev han exalterad. Där fanns bland annat en powerpoint-presentation av övervakningsprogrammet PRISM, som gav den amerikanska säkerhetstjänsten NSA direkt tillgång till servrarna hos bland andra Microsoft, Google, Facebook, Skype och Apple. I den dokumentation han senare fick visade det sig bland annat att NSA samlat in 97 miljarder mejl och 124 miljarder telefonsamtal från hela världen – bara under en enda månad. Med tanke på vad det var för ett material var det kanske inte så konstigt att Snowden inte haft någon som helst lust att avslöja något om vem han var eller vad han hade att berätta, öppet över internet. Tillsammans med Laura Poitras och filmaren och fotografen Jeremy Scahill har Glenn Greenwald nu grundat The Intercept, en webbsajt som bland annat ska fortsätta att publicera utifrån Snowdens läckta dokument. Den ska också bedriva tuff och orädd journalistik om annat. Därmed har man också satsat på en hög säkerhetsnivå.

På The Intercept har 21 av de 24 anställda en publik krypteringsnyckel publicerad på tidningens kontaktsida. Och The Intercept använder en tipstjänst för källor som heter SecureDrop, ett system med både kryptering, anonymisering och en ”luftvägg” som inte dekrypterar inskickade dokument förrän de ligger på en dator som saknar kontakt med internet. SecureDrop har idag dryga dussinet användare världen över, bland andra The New Yorker, The Guardian och Washington Post. I boken ”Storebror ser dig” skriver Glenn Greenwald att alla internetanvändare borde använda krypteringsverktyg och anonymitetsskydd. ”Det här är extra viktigt för personer som arbetar med känslig information, som journalister”, skriver han.

3. Bristande källskydd: Telefon

De så kallade smarta mobiltelefonerna är kraftfulla arbetsverktyg. När du skaffar en ny modell går det snabbt och smidigt att fylla den med all information du behöver för att kunna jobba. I stort sett automatiskt kopieras telefonboken från datorn till telefonen. Sedan kommer insikten om vad som precis har hänt: hemliga mobilnummer till känsliga kontakter finns helt öppna på en apparat som är lätt att tappa bort och dessutom är stöldbegärlig. Om du inte kollat mobilens inställningar kan all information även ha kopierats till Apples eller Googles molntjänster. En smartphone med sin stora datorkapacitet, ständiga uppkoppling, positioneringstjänster, e-postprogram och sociala nätverksappar gör den till en guldgruva för den som försöker kartlägga en journalist och hans eller hennes kontakter. Många appar ger företagen bakom dem långtgående rättigheter att ta del av personlig information, som kontaktregister och var användaren befinner sig. Det finns också spionprogram, som exempelvis gör att telefonen kan utnyttjas för att avlyssna samtal eller för att ta reda på var du är. Men alla former av telefoni har sina särskilda risker. Att en källa kommunicerat med en journalist går att spåra på en lång rad sätt. Det framgår i klartext på telefonräkningen. 2008 avslöjades att flera stora tyska bolag, bland andra Deutsche Telekom och järnvägsbolaget Deutsche Bahn jagat interna läckor genom att gå igenom samtalsloggar. Loggarna sparas också hos operatörerna, där den som kommer åt informationen har långtgående möjligheter att spåra kontakter och beteenden genom de krav som EU:s datalagringsdirektiv ställer. Många redaktioner använder skyddade nummer när de ringer. Men det glöms ofta bort när journalisten använder mobiltelefonen eller ringer hemifrån. Vissa telefonväxlar skickar telefonsvararmeddelanden som e-post. Telefonnumret som ringde läggs i ärenderaden, och meddelandet ligger i en oskyddad bilaga. Den som kommer åt e-posten kommer då också åt telefonsvararen. Telefonen kan dessutom avlyssnas – legalt eller illegalt. Ett sätt att komma runt risken för avlyssning är att ringa via krypterad IP-telefoni. Det är något som bland andra Skype säger sig erbjuda. Men vid flera tillfällen har Skype visat sig ha buggar. Exempelvis har raderade samtalsloggar kunnat återskapas. Eftersom Skype inte använder transparent teknik går det inte att kontrollera om deras system innehåller bakdörrar. I samband med rättsliga utredningar lämnar företaget också ut samtalsinformation. Men så vitt det är känt är samtal via Skype fortfarande krypterade och därmed relativt svåra att avlyssna.

Case: Att prata med källan i telefon

Ett enda obetänksamt telefonsamtal kan ibland räcka för att avslöja att en journalist och en källa haft kontakt. Det vet bland annat UD:s förre kabinettssekreterare Hans Dahlgren. Under bråket om vem som gjorde vad i Regeringskansliet efter tsunamin i december 2004, åkte han personligen ut till Telias huvudkontor i Farsta för att ta del av sina egna telefonräkningar med samtalen från de aktuella dagarna. Syftet med Dahlgrens besök var inte att avslöja en källa utan att fastställa exakt när och vart han hade ringt. Men utan att begära in räkningarna till UD, eftersom journalister då hade kunnat begära kopior på dem. Telefonräkningen spelade dock en avgörande roll för källan 2007, när en kvinna på det privata vårdföretaget Maria Beroendecentrum blev avstängd från – och så småningom förlorade – sitt arbete. Efter publiceringen av en kritisk artikel i Dagens Nyheter om Maria Beroendecentrum på Söder i Stockholm, begärde arbetsgivaren in räkningarna för det egna företagets telefoner från teleoperatören och kunde därigenom hitta ett samtal från kvinnans tjänstetelefon till en reporter på DN. Reportern hade, efter att ha pratat med flera anonyma källor, skrivit ett stort antal artiklar om de miljonvinster vårdcentralens ägare hämtade ut ur bolaget.

De flesta på arbetsplatsen kände till att kvinnan var kritisk till vinstuttagen och när företagets ledning hittade numret till DN:s reporters privata mobiltelefon kallades kvinnan in till ledningen och fick lämna arbetsplatsen. Vad som sades i samtalet vet ingen annan än reportern på DN och hennes källa, men vetskapen om att hon och kvinnan haft kontakt räckte för att ledningen skulle stänga av kvinnan med motiveringen att hon agerat illojalt. Efter förhandlingar förlikades parterna och kvinnan lämnade företaget mot att hon fick 15 månadslöner. Om källan istället hade arbetat på en offentlig vårdinrättning hade hennes arbetsgivare begått ett lagbrott när hon tittade igenom telefonräkningen. För anställda på offentliga institutioner är efterforskande av källa ett brott enligt grundlagen, Tryckfrihetsförordningen. Men efterforskningsförbudet gäller inte privata företag, även om deras verksamhet finansieras med skattepengar. 2013 föreslogs en form av efterforskningsförbud för privatanställda inom offentligt finansierad vård, skola och omsorg. Men vid denna guides färdigställande har ännu inget lagförslag lagts.

Checklista! Säkrare smartphone.

- Kräv lösenord för att använda telefonen.
- Spara inga lösenord i telefonen.
- Spara inget känsligt i telefonen om den inte är krypterad.
- Kolla alla appar och vilka rättigheter du ger dem.
- Slå av positioneringstjänster och appar som använder dem.
- Undvik automatisk säkerhetskopiering till molntjänster.
- Synkronisera telefonen med din dator utan att vara uppkopplad på nätet.
- Stäng av mobilen helt och hållet vid känsliga möten. Om den inte går att stänga helt, vilket exempelvis inte går med en Iphone: lämna den hemma.
- Om du behöver extra säkerhet: skaffa tillfälliga kontantkort från olika mobiloperatörer, byt ofta, och kommunicera numren via krypterad kommunikation på nätet.
- Lämna den vanliga telefonen påslagen på ett säkert ställe när du går ut och använder din säkra telefon.

3.1 Skydda källan: Telefon

Några grundläggande tips för att minska möjligheten att spåra telefonkontakter är att använda dolt nummer, ställa in telefonen så att den rensar dina samtalsloggar och undvika att lämna telefonsvararmeddelanden om det finns minsta risk att fel personer kan lyssna av dem. Radera också sms. Ingen av de här åtgärderna ger dock någon högre grad av säkerhet. De hindrar att någon ser dina kontakter av en slump. Men om någon faktiskt försöker kartlägga dig räcker de inte till. För att ringa källor litet mer diskret finns två huvudalternativ, beroende på vad som är viktigast att skydda. Om det är själva kontakten, vem som pratar med vem, kan du använda anonyma mobiltelefoner. Om det viktigaste är att undvika avlyssning kan det finnas fördelar med IP-telefoni, eftersom samtalen krypteras.

Du kommer långt med två billiga mobiltelefoner med kontantkort, en till dig och en till källan. Telefonerna ska inte ha några finesser. Betala kontant, och registrera inte telefonkorten, även om det ger bonusar. Behövs högsta säkerhetsnivå bör ni vara på neutrala ställen när sim-korten stoppas in – platserna där de först användes

registreras av operatörerna. Använd telefonerna uteslutande till att ringa det andra, anonyma kontantkortet. Samtal till andra kan bidra till att identifiera dig eller din källa. Sitt inte på redaktionen när du ringer, eftersom platsen loggas av telefonbolaget. Använd inte samma telefon till olika projekt. Även om sim-korten byts ut kan telefonernas unika ID-nummer, IMIE-numren, länka samman dem.

Det finns en rad möjligheter att chatta och prata, med eller utan video, krypterat över internet, och nya program utvecklas vartefter. De flesta större program för IP-telefoni, som exempelvis Skype, krypterar överföringen och det finns chatt-program med off-the-record-funktion, OTR. Flera av dem duger gott i de flesta sammanhang, men det finns osäkerheter förknippade med dem alla. Innan de används i känsliga sammanhang bör du kolla upp deras dagsform. Kolla både deras egna integritetspolicyer och tekniska brister, som ofta går att hitta på diskussionsforum på internet.

Eftersom dagens smarta telefoner i princip är små datorer gäller mycket av det som skrivits i andra kapitel också telefonerna. Se upp om telefonens batteri plötsligt börjar ladda ur fortare än tidigare och håll koll på om datatrafik överförs utan att du själv gör något. Att verkligen säkra sin telefon är ett projekt som kräver tekniskt kunnande och tid. Läs i XL-materialet på webben om hur du går till väga.

4. Bristande källskydd: Lagringsmedia

Hårddisken på en vanlig bärbar dator rymmer med lätthet all e-post, alla dokument, manus, utkast, inspelade och utskrivna intervjuer som en journalist producerar under ett yrkesverksamt liv. För många är det en stor tillgång. Med hjälp av sökverktyg som Windows search eller Apples Spotligt går det att hitta det mesta på den egna hårddisken. Men digitaliseringens baksida är att allt blir extremt lättillgängligt även för polisutredare eller den som otillbörligt kommer över hårddisken. Och det händer ständigt. Bärbara datorer är stöldbegärliga och med dem försvinner också hårddisken med allt material. Att knäcka startlösenordet till de vanligaste operativsystemen är en manöver som tar max en timme med program som finns nedladdningsbara från nätet, färdiga att använda. Ett tappat USB-minne kan vara en katastrof om den kan läsas av personen som hittar den. Att använda någon form av kryptering av lagringsmedia är ett enkelt och nästintill nödvändigt sätt att skydda sina filer på datorn eller USB-minnet, om man inte vill göra dem tillgängliga för första bästa väskryckare eller nyfiken upphittare.

4.1 Skydda källan: Lagringsmedia

Lösningen på säkrare förvaring av data heter kryptering. Det är en funktion som blir allt vanligare och allt mer standardiserad. Kryptering kan ske av en enda fil, en mapp, en del av en hårddisk (som då dyker upp som en virtuell extra hårddisk på datorn) eller hela hårddisken – så kallad fulldisk-kryptering – som säkrar allt inklusive systemprogramvaran. Kryptering av hela hårddisken, eller i vart fall hela dokument-mappen, är en bättre idé än att bara skydda det som i nuläget bedöms vara känsligt. En fulldisk-kryptering skyddar även sådant som i ett senare skede blir känsligt. Ett USB-minne kan också enkelt krypteras och därmed bli en säker förvaringsplats. Tekniken är stabil och lätthanterlig även om det kan finnas en viss inlärningströskel.

Baksidan av krypteringen är en något nedsatt hastighet i dataöverföringen. Det kan vara besvärligt när stora filer, till exempel videomaterial, ska krypteras. Men för de flesta ändamål är prestandaförlusten knappt märkbar. Krypteringen gör också all form av dataåterställning omöjlig, eftersom ett förlorat lösenord till en stark kryptering innebär en förlorad hårddisk. Även om man har lösenordet kan trasiga hårddiskar bli mycket svårare, eller omöjliga, att restaurera om de är krypterade. Backup och rutiner för säkerhetskopiering blir alltså ännu viktigare. Krypteringen av data görs med mycket starka krypteringsalgoritmer, så starka att det, såvitt det är känt, inte går att knäcka de vanligaste algoritmerna utan mycket omfattande resurser. I praktiken krävs it-resurser som bara finns tillgängliga för statliga institutioner som Försvarets Radioanstalt, FRA, eller dess

Case: Källan ”Neo” röjs

När botten gick ur den lettiska lånetunnan 2008 och svenska storbanker som Swedbank och Nordea hotades av enorma kapitalförluster, ställde bland annat Sverige och Internationella valutafonden upp med nödlån. Men på hårda villkor. Villkor som gjorde att den lettiska regeringen lade ner sjukhus, sänkte löner för poliser och lärare med 30 procent och generellt skar i de offentliga utgifterna i en aldrig tidigare skådad omfattning. Lettlands BNP sjönk med en fjärdedel på två år. En grupp som klarade sig oskadda från nedskärningarna var dock högt uppsatta statstjänstemän, något som Ilze Nagla på lettisk tv kunde avslöja efter att hackaren ”Neo” försett henne med 7,5 miljoner inkomstuppgifter från det lettiska skatteverkets datorer. Det var uppgifter som i Sverige hade varit offentliga, men i Lettland ledde till att säkerhetspolisen i maj 2010 gjorde husrannsakan hos Nagla. Beslagtagna datorer och USB-minnen kunde ganska snabbt identifiera ”Neo” som Ilmārs Poikāns, medarbetare vid matematik- och datavetenskapliga fakulteten på Lettlands universitet. Ilze Nagla beklagar djupt att hennes hantering av uppgifterna från Poikāns så enkelt ledde till att han avslöjades och greps.

– Varför lärde ingen mig att kryptera? säger hon.

Case: En kopierad hårddisk

Efter uppgifter i pressen år 2010 om att Kung Carl XVI Gustaf varit otrogen, tilltog jakten på bilder och uppgifter om kungens sexuella kontakter. ”Mille” Markovic, före detta boxare, porrklubbsägare och dömd för en lång rad grova brott, uppgav våren 2011 att han hade bilder på kungen och kvinnor i komprometterande situationer. Sju reportrar, bland annat frilansjournalisten Nuri Kino, sades ha sett bilderna. ”Två kvinnor som har lesbisk sex, kungen tittar på”, berättade bland annat reportern Johan Stambro i TV4:s Nyheterna. Nuri Kino arbetade då med en dokumentär om skandalen för SVT:s ”Dokument inifrån”. Det projektet fick ett abrupt slut under sommaren 2011, då Nuri Kino fick klart för sig att informationen på hans hårddisk hade läckt ut. Stora delar av innehållet på disken – ingen vet hur mycket – hade kopierats. Ett stort material, hundratals bilder och känsliga, källskyddade uppgifter från Kinos pågående och tidigare reportage hade spritts till flera personer på USB-minnen. Bland annat överlämnade kungens nära vän Anders Lettström ett av USB-minnena till polisen och uppgav att han fått det med posten från en okänd avsändare. Enligt Nuri Kino kan kopieringen ha skett när som helst. Han hade bland annat lämnat datorn i bilen och på gymmet. Den hade ingen som helst kryptering. Inte heller använde han kryptering på det Gmail-konto som han använde. Förutom uppgifter från Nuri Kinos privatliv, innehöll datorn också anteckningar och uppgifter från kontakter med källor i flera tidigare och kommande reportage. Bland källorna fanns personer i kriminella kretsar i Sverige och personer med insyn i militanta islamistiska nätverk. SVT kontaktade Säkerhetspolisen som inte lyckades hitta några spår efter vare sig den som utfört eller beställt kopieringen av Kinos dator. Utredningen lades ned. Själv säger Nuri Kino:

– Från och med nu ska jag bara använda mig av anteckningsblock.

En annan reporter som också hade kontakt med Mille Markovic var frilansjournalisten Beata Hansson. Hon och författaren Deanne Rauscher arbetade under hösten 2011 med ett porträtt av Markovic som så småningom landade i boken: ”Mille Markovic. Biografin”. Men bokens mest intrikata del, de påstådda bilderna på kungen med halvnakna kvinnor, kom ut långt tidigare än författarna tänkt sig. Någon kapade, okänt hur, Hanssons Gmail-konto där bilden fanns och mejlade den vidare, varvid den publicerades i Expressen ett halvår innan Hansson och Rauschers bok kom ut.

amerikanska motsvarighet NSA. Istället sker de flesta försök att knäcka krypterade diskar genom att på olika sätt skaffa sig tillgång till hela eller delar av lösenordet. Till exempel försöker man placera programvara i datorn som känner av tangentbordstryckningar, så kallade trojanska hästar och tangentbordsloggare, eller så söker man igenom öppna delar av disken efter lösenord. Därför är det av stor vikt att ha uppdaterat virusskydd, undvika att öppna e-postbilagor från okända avsändare och inte installera okänd programvara. Skadlig kod är dock svår att skydda sig från. Även ett Word-dokument från en känd avsändare kan innehålla skadlig kod som har placerats där av någon annan. Den säkra lösningen är att lagra känslig information utan åtkomst från nätet, på datorer, USB-minnen eller hårddiskar som inte används till något annat än det aktuella projektet – och som aldrig ansluts till nätet. En grundläggande del av trovärdiga krypterings-produkter är att deras uppbyggnad, själva programmens källkod, görs tillgänglig för allmänheten, så att den kan undersökas och säkerhetshål, eller så kallade bakdörrar, kan upptäckas. Bakdörrar är medvetet inbyggda ingångar i ett krypterat system, avsedda att lura användaren att systemet är säkert när det egentligen är öppet för den som känner till var bakdörren finns. Kommersiella företag vill oftast inte publicera källkoden till sina program eftersom detta underlättar för andra programmerare att kopiera programmen. De har dessutom ofta färdiga överenskommelser med lagvårdande myndigheter om att information från användarna, inklusive krypteringsnycklar, ska kunna överlämnas till polis och domstol samt om hur detta ska gå till. Men vissa företag, som PGP, har offentliggjort den del av källkoden som hanterar krypteringen i programmet för att denna ska kunna kontrolleras. Program med helt öppen källkod, har här stora fördelar. Men 2014 lade utvecklarna av TrueCrypt, det program som varit såväl grävande journalisters som många dissidenters favorit i flera år, ner verksamheten. Några olika grupper utvecklar nu koden vidare, men många hävdar att den sista versionen av TrueCrypt än så länge är den bästa.

4.2 Skydda källan: Radera säkert

Känsliga uppgifter måste gå att radera när datorn kasseras, ett projekt är över eller gränser mellan länder ska passeras. Då måste speciella verktyg till. För informationen på en hårddisk av traditionell typ, med snurrande skivor där data lagras som magnetiska spår, är på intet sätt ”raderad” för att man slänger filer i papperskorgen eller ens efter en omformatering. För usb-minnen och andra minnen är situationen än värre. Minnena har ofta större kapacitet än vad de visar för användaren och information lagras utan att man vet om det i områden som inte kan raderas. Där är heldiskkryptering från start

Viktigt! Lär dig använda kryptering.

Kommersiella programvaror som PGP, Pretty Good Privacy, har erbjudit kryptering av hela eller delar av hårddisken i många år. Program med öppen källkod, som GnuPG, erbjuder samma funktion och starka kryptering som PGP för både Windows, Mac och Linux. Från och med Windows 7 Ultimate är funktionen Bitlocker standard. Den krypterar liksom PGP hela disken och kräver lösenord redan vid första inloggningen. Utöver det har Mac OS X en inbyggd funktion för skivavbildning med vars hjälp du kan skapa en fil som fungerar som en extra hårddisk. Där kan du lägga känslig information som sedan är krypterad från åtkomst med lösenord som måste anges för att ”hårddisken” ska monteras. Det fungerar på ett liknande sätt med förut nämnda Bitlocker.

eller fysisk förstörelse ibland de enda säkra lösningarna för att göra innehållet fullständigt oläsbart. På traditionella hårddiskar måste den exakta platsen på disken där känsliga data sparades skrivas över minst en och helst flera gånger med slumpvis genererad data. För det behövs ett program som på ett säkert sätt skriver över data på exakt rätt plats. Gratisprogrammet Ccleaner och PGP Desktop har en sådan funktion, liksom program med öppen källkod som Dban och Nwipe.

SSD-”hårddiskar” (lagringsmedia baserade på minneskretsar och inte på snurrande skivor), SD-minneskort, minneskort i telefoner och USB-minnen är betydligt svårare att radera säkert. I dessa tilldelas minnesplatserna slumpvis och inte enligt ett förutsägbart mönster. Det är därför mycket svårt att veta var man ska skriva slumpmässiga data för att kunna vara säker på att man skrivit över det som ska raderas. Detta utgör ett formidabelt problem eftersom dessa databärare ofta används för att flytta känslig information. En intervju inspelad på ett telefonminne, en känslig fil lagd på ett USB-minne, eller en bild sparad på ett SD-minneskort kan vara något som det finns stort behov av att radera säkert. Lösningen är att radera information på normalt sätt, slänga det i

papperskorgen, och på så sätt frigöra utrymmet för användning. Sedan använder man program som skriver över allt tillgängligt utrymme med slumpdata. För Androidtelefoner finns programmet Shredroid och för media som ansluts till en dator kan PGP desktop, Dban eller Nwipe användas. På Iphone gör användaren en återställning (reset) av hela telefonen som rensar allt innehåll och skriver över lagringsminnet som då är som ”nytt”. Problemet med all sådan överskrivning av tillgängligt minne – så kallad shredding – är att det tar tid. Ju högre säkerhet, desto längre tid tar det, ofta flera timmar. Att radera information som lagts upp på nätet – till exempel på Dropbox, Gmail, intranät eller en blogg – är nästintill omöjligt.

All data lämnar spår på de media där de lagras och dessutom kopieras data på servrar i lokala nät och på internet kontinuerligt av olika automatiska program och backup-processer. När grupperingen kring Wikileaks distribuerade materialet i ”Cablegate” mellan sig, använde man sig av en krypterad fil som lades öppet på internet. Filen innehöll det samlade materialet från de över 250 000 diplomatiska telegram som Wikileaks kommit över, men filen utgjorde inget hot förrän lösenordet till krypteringsnyckeln plötsligt publicerades i en bok. I det läget spelade det ingen roll att filen plockades bort.

Tips! Backup och säker lagring.

Det gamla niduttrycket om ”kontoret på fickan” är idag en realitet, särskilt för frilansande mediearbetare. Många använder sig av backuplösningar av olika slag och det är utmärkt eftersom en förlorad dator eller mobil annars kan leda till förlorad arbetsinkomst och stor frustration. Den som sköter sin egen bokföring är dessutom enligt lag tvungen att spara räkenskaperna i upp till tio år även om dessa sköts elektroniskt. Det gäller dock att skilja på vad du säkerhetskopierar och var du förvarar din information. Dina semesterbilder och liknande kan du gott lagra på en extern hårddisk i hemmet. Men när det gäller arkiverat redaktionellt material bör du vara betydligt listigare än så. Kryptera innehållet som du säkerhetskopierar och förvara sedan lagringsmediet på ett säkert ställe, gärna brandsäkert, eller i alla fall inte där det går att hitta på en minut. Du kommer att tacka dig själv den dagen då olyckan är framme och du blir av med en arbetsapparat eller den går sönder.

Det fanns redan kopior på många håll och med lösenordet kunde filen öppnas och telegrammen spridas med vinden. Med andra ord ska data som lämnar datorn som e-post, en fil på Dropbox eller liknande, kunna anses vara delad med resten av världen – som om texten låg på en webbsida. Företag som Google erbjuder gratis e-post med devisen ”släng inget, spara och sök istället”. De förbehåller sig också rätten att spara användarnas data och gör sedan själva en god affär av att söka i användarnas e-post efter mönster som de säljer till exempelvis annonsörer. Men de är också tydliga med att de lämnar ut uppgifter om lagvårdande myndigheter så kräver. Data som lämnats över till sådana tjänster har man således inte längre kontroll över. För att någon ska komma över data på den egna datorn, krävs att de får fysisk tillgång till disken eller att datorn kapas över sin nätanslutning. Det är betydligt krångligare och därmed är den egna datorn ett mycket säkrare ställe att förvara sin information på.

5. Bristande källskydd: Uppkoppling

Spår, avlyssning, intrång – nätet är en relativt osäker kommunikationskanal för den som inte aktivt skyddar sina källor. Själva datorn kan också stå mer eller mindre vidöppen för den som försöker ta sig in i den. Den som äger en webbplats loggar normalt besökarna, eller i alla fall deras datorers IP-adresser. Att en journalist från ett stort medieföretag varit på besök syns då tydligt. Men även den som döljer sitt IP-nummer kan identifieras. Det finns en rad uppgifter som går att vaska fram om dig när du surfar – vilka webbplatser du besökt innan, vilken version av webbläsaren du använder och många fler detaljer. Summan av dessa detaljer ger en unik profil som, om någon ger sig sjutton på det, kan kopplas tillbaka till dig. Nästan alla webbplatser idag placerar kakor, små filer med information, på din dator. De används exempelvis för att lagra olika inställningar du gjort, men kan också utnyttjas för djupgående analyser av ditt beteende på nätet. Via webbplatser eller genom bilagor i e-postmeddelanden eller chattar kan skadliga småprogram – virus, maskar och trojaner – ta sig in i din dator. De flesta är inte inriktade på att sabotera för journalister, utan sprids på internet till allmänt förtret. Men de kan mycket väl plocka dokument ur din dator och mejla iväg dem vart som helst. Beroende på hur du kopplar upp dig mot internet finns det olika möjligheter för en utomstående att ta del av trafiken – vilka webbplatser du besöker, innehållet i e-post eller de lösenord som skickas. Hackare kan fånga upp datatrafiken på vägen mellan din dator och den nätplats du tänkt besöka. Mest osäkra är trådlösa nätverk. Även nätverket med den starkaste krypteringen, WPA2, kan under normala omständigheter avlyssnas med program som finns allmänt tillgängliga på nätet. Okrypterad trafik på ett offentligt trådlöst nätverk – exempelvis på ett internetcafé eller i en hotellobby – är att betrakta som ett högljutt samtal på samma ställe. Det kan snappas upp hur lätt som helst, och du vet inte vem som lyssnar.

Case: Presidentvalet i Vitryssland

Den 20 december 2010 demonstrerade tusentals människor på Självständighetstorget i huvudstaden Minsk i Vitryssland. De var där för att protestera mot att den vitryska presidenten Alexsander Lukasjenko, genom valfusk, hade segrat i presidentvalet dagen innan. Demonstrationerna urartade i kravaller när polisen gick till attack, flera personer misshandlades och över tvåhundra aktivister greps direkt på plats.

Dagen efter blev många av demonstranterna som inte hade gripits uppringda av den vitryska säkerhetstjänsten KGB och kallade till förhör. Polisen hade nämligen kunnat se att deras mobiltelefoner varit på torget genom att mobiltelefonoperatörerna hade lämnat ut uppgifter om positionering. Mobiltelefonerna hade registrerats av de närliggande mobiltelefonmasterna. Polisen hade fått uppgifter om vilka som befunnit sig inom en radie av en kilometer från torget och tagit det som bevis för att personerna hade varit på plats för att demonstrera. Detta är inte tekniskt komplicerat, men såklart etiskt problematiskt. Det är mycket lätt idag att spåra och bestämma en mobiltelefons position. Genom att mäta signalstyrkan till mobilmaster kan man med god precision avgöra var en mobiltelefon befinner sig. Särskilt i en stad, där basstationerna ligger nära varandra.

Journalister i Vitryssland plockar därför numera ut batterierna ur sina mobiltelefoner när de går på möten där de diskuterar känsliga saker. Andrej Bastunets är ordförande i Vitrysslands oberoende journalistförbund. Han berättar för Dagens Nyheter i april 2012 att de inte längre litar på att de inte skulle vara avlyssnade eller kontrollerade.

– Vi pratar aldrig om viktiga saker i mobiltelefonerna, vi nämner inte möten eller adresser där vi ska träffas i sådana samtal. Det samma gäller mejl, säger Andrej Bastunets till DN.se

Ett av de inblandade mobiltelefonföretagen är Life som samarbetar med svenska TeliaSonera, men även andra svenska företag har intressen i bevakningen av vitryska medborgare och journalister. Bland annat har Ericsson sålt övervakningsutrustning till det helstatliga företaget Beltelecom som kontrollerar all datatrafik i landet.

6. Bristande källskydd: Molntjänster

Webbmejl och möjligheten att spara dokument i internetbaserade lagringstjänster som Dropbox är exempel på fenomenet molntjänster. Användningen av dessa växer blixtsnabbt. Stora företag som Google och Microsoft har ordbehandlare och kalkylprogram i molnet och än fler erbjuder lagringsplats, säkerhetskopiering, kalendrar, fotoalbum och adressböcker. Förutom att molntjänsterna ger bekvämlighet, anses de också vara billiga i drift. Men att flytta redaktionens viktigaste arbetsverktyg till en obestämd plats på internet kan kosta mer än det smakar. En redaktionell satsning på molntjänster i sin vidaste bemärkelse innebär att själva kärnan i journalistiken lämnas över till en extern leverantör. Allt från researchens rådata, via manus under arbete, till synkroniserade uppgifter från mobiltelefonen – inklusive telefonloggar och geodata om var ägaren har varit – ska lagras och hanteras av företag som redaktionen naturligtvis inte har kontroll över och där ansvarsfrågor som bäst kan betraktas som svårtolkade. Visserligen är de flesta stora aktörer på molnmarknaden väl medvetna om att det behövs en hög säkerhetsnivå. Inte bara medieföretag har ju anledning att skydda affärskritisk företagsinformation. Men en medvetenhet i teorin behöver inte betyda att säkerheten fungerar i praktiken. Du vet inte hur säkra molnföretagets säkerhetsrutiner är, du vet inte vilka människor som jobbar där – och du vet inte ens under vilket lands lagar som informationen kan begäras ut. Just för redaktioner är det sista ett extra stort problem – den grundlagsstadgade plikt som redaktioner har att skydda källors identitet och som hindrar myndigheter från att efterforska dem betyder ingenting utanför Sveriges gränser. Molntjänsten kan i princip ha servrar var som helst – i Finland lika väl som i USA. Och även om dessa fysiskt befinner sig i Luleå, kan en amerikansk domstol ändå hävda att information ska lämnas ut ifall det är ett amerikanskt företag som driver tjänsten. I användarvillkoren för de flesta tjänster framgår tydligt att data lämnas ut på begäran av domstol.

6.1 Skydda källan: Minimera riskerna

Kryptering, anonyma e-postkonton och kontantkort till mobilen – det finns massor av trick för journalister att ta till för att skydda sina källor. Men det viktigaste är egentligen inte de smarta lösningarna i sig eller att du har något speciellt program på din dator, utan att du har tänkt igenom vad du håller på med. Hundraprocentig säkerhet går inte att uppnå, utan det gäller att vara medveten om vilka risker man löper – och minimera de risker som leder till oacceptabla konsekvenser. Först och främst måste du se till att ha en allmänt god säkerhetsnivå.

Case: Reportern blev av med allt

En fredagseftermiddag i början av augusti 2012 stod plötsligt den amerikanska teknikjournalisten Mat Honan utan tillgång till vare sig Iphone, Ipad eller dator. Allt innehåll var raderat och han kom inte åt sitt Apple-konto. Hans Gmail-konto var avslutat och hans Twitter-identitet kapad. Allt genom att en hackare kommit åt Honans inloggning på Apples molntjänst Icloud. ”Jag hade faktiskt tur”, skriver Mat Honan i tidskriften Wired. ”Hackarna ville bara genera mig, ha lite kul på min bekostnad och reta upp dem som följer mig på Twitter”. Den som gjorde attacken kunde lika gärna ha tagit hans telefonbok, som innehåller kontaktuppgifter till ett antal inflytelserika människor i teknikvärlden, eller gått igenom åtta års sparad e-post på hans Gmail. Hackaren hade gått systematiskt till väga. Först lyckades han få internetbokhandeln Amazon att lämna ut de fyra sista siffrorna i Honans kreditkorts-nummer. Sen ringde han till Apple och påstod att han glömt sina inloggningsuppgifter. Genom att uppge e-postadress, hemadress och de fyra sista siffrorna från kreditkortet ansåg Apples support att han hade lämnat tillräcklig mycket personlig information för att de skulle tro på att hackaren var Mat Honan. Bedragaren fick tillgång till Honans konto. Genom kontot kunde hackaren använda fjärrstyrningsfunktionen i Icloud och i tur och ordning radera all information från Honans telefon, Ipad och dator. Eftersom Honan hade kopplat återställningen av sina Google-, Gmail- och Twitter-konton till e-postadressen hos Apple kunde hackaren utnyttja det, få nya lösenord och sedan göra vad han ville även med dessa konton. Honan trodde först att någon lyckats lista ut hans lösenord. Apples support berättade ingenting om att de hade lämnat ut hans kontoinformation bara en halvtimme innan Honan själv ringde. Det var först efter att hackaren kontaktat Honan och berättat hur han hade gjort som Honan även fick en bekräftelse från Apple. Hackaren lär ha sagt till Honan att han gjorde det för att uppmärksamma folk på säkerhetsproblem och förmå företagen att åtgärda dem. Hacket mot Mat Honan visar att molntjänster kan vara känsliga för intrång. I det här fallet räckte det med information som ett pizzabud har tillgång till för att komma åt en rad känsliga uppgifter.

- Ha starka lösenord. Aldrig samma på olika ställen och i olika apparater.
- Brandvägg och antivirusprogram är självklarheter.
- Uppdatera operativsystem, program och applikationer.
- Klicka aldrig på länkar som du inte vet vart de går och bilagor som du inte vet något om.
- Om det finns känsligt material på en dator eller mobiltelefon som du bär med dig, ska den vara krypterad. Vill du inte kryptera, ska informationen inte heller kånkas omkring, utan vara inlåst någonstans.
- Lämna aldrig en dator eller telefon utan uppsikt. Det tar ingen tid alls att stjäla den, och kort tid att installera ett program som anger din aktuella position eller avlyssnar dina samtal.
- Läs noga igenom villkoren och titta igenom alla inställningar på datorprogram och appar som du laddar hem till mobilen. Fundera på hur mycket du kan och bör dela med dig av när det gäller positionering, telefonbok och kalender – och vem som ska ha möjlighet att ta del av uppgifterna. Utgå ifrån att informationen kan sparas för evigt hos leverantören ifall inget annat anges.
- Ladda hem och installera nya versioner av program när det kommer säkerhetsuppdateringar.

När du väljer dina datorprogram och mobilappar kan det vara en fördel om det är öppen källkod, alltså att programkoden finns tillgänglig för alla att granska. Även om du inte själv kan avgöra hur säker den är, kan oberoende experter gå igenom den och hitta säkerhetsluckor samt publicera dem på nätet. Generellt kan du utgå ifrån att ju längre ett program har funnits, desto fler säkerhetsbrister är hittade och åtgärdade.

Stora, etablerade företags produkter har ofta säkerhetslösningar som är tillräckliga för de flesta användare. Men Snowden-avslöjandena visade att amerikanska myndigheter haft tillgång till data från ett antal av de stora programvaru- och tjänsteföretagen.

I grunden följer en riskbedömning enkla resonemang: om du står i begrepp att avslöja missförhållanden på ett privat företag är det sannolikt att källans chef kommer att kolla företagets mejl- och telefonlistor för att hitta källorna. Företaget har rätt att göra det och källan kan få sparken om den avslöjas. Alla kontakter via arbetsgivarens telefon- och it-system bör alltså undvikas. En kontakt via exempelvis Googles e-posttjänst Gmail fungerar däremot troligen ganska bra. Men så fort man hanterar något som berör en amerikansk part, som kan få ut Google-information i en rättsprocess, bör Gmail undvikas. Poängen är att hitta en lämplig säkerhetsnivå i det projekt du håller på med, utan att slå över i paranoia, vilket sannolikt kommer att hindra dig från att utföra ditt jobb på ett bra sätt.

Checklista! Snabb hotbildsanalys.

- Vem kan bli förbannad när din artikel eller ditt program publiceras?
- Vem kan förlora pengar eller trovärdighet på det? Och vem kan tjäna på att få fram läckorna?
- Vilka resurser har de som du granskar – i form av pengar, lagar och teknik?
- Vilka kommunicerar med varandra och hur? Inom redaktionen, och utanför?
- Hur bra är deras skydd och hur tar du reda på det?
- Var och hur sparas informationen? Vad krävs för att komma åt den?
- Vem kan komma åt informationen, exempelvis medarbetarna på it-avdelningen, städpersonal?
- Försök att bedöma hur allvarlig varje separat risk är.
- Fundera sedan på hur stor sannolikhet det är att den inträffar.
- Vidtag nödvändiga skyddsåtgärder.

Kanske är lösningen enkel: lägg alla projektdata på ett USB-minne. Idag finns minnen med färdiga, enkla krypteringslösningar att köpa. Glöm inte att gå igenom riskanalysen då och då. Har förutsättningarna ändrats – exempelvis genom att nya människor blivit inblandade – behöver kanske också skyddsåtgärderna ändras. Sist men inte minst, måste du komma ihåg att det tar tid att lära sig. Den dag du upptäcker att du skulle behöva kryptera ett mejl är det för sent att försöka förstå hur det fungerar. I det läget är det bättre att köra med gamla, analoga metoder än att invagga dig själv och källan i falsk säkerhet.

6.2 Skydda källan: Brandvägg

För att skydda din dator och mobiltelefon mot intrång och spionprogram finns två enkla regler: släpp inte in vem som helst och använd alltid skydd. Steg ett är att ha bra brandvägg och antivirusprogram. Det finns både kommersiella program och gratisprogram. Sök efter aktuella tester innan du bestämmer dig och se sedan till att alltid ha en aktuell version av programmet. Nya virus, maskar och trojaner utvecklas ständigt och skyddsprogrammen måste uppdateras därefter. Datorer med Microsofts operativsystem är

Tips! Bättre virusskydd.

Avinstallera, eller i alla fall avaktivera, Java och Flash om du inte vet att du behöver det. Dessa två program är skyldiga till många sårbarheter som kan utnyttjas av hackare och virus för att ta sig in på datorer. Om du måste använda filer i Adobe-format, till exempel Adobe Reader, se till att programmet alltid är uppdaterat till senaste versionen innan du öppnar några pdf:er. Detsamma gäller MS Word och Excel. Skadliga pdf:er och doc-filer används ofta vid riktade attacker.

mer utsatta för attacker, men det betyder inte att du som använder Apple-produkter kan strunta i brandvägg och antivirusprogram. Även Mac:ar drabbas i allt högre grad. Skyddsprogrammen klarar dock bara av redan kända hot. De stoppar alltså inte helt nya virus, men företag och användargrupper är ofta snabba med att identifiera färska digitala farsoter. En tröskel mot intrång får du genom att ställa in datorn så att du har flera användarprofiler: en normalanvändare och en administratör. Normalanvändaren använder du i ditt dagliga arbete, och denna profil ska inte ha rättigheter att installera nya program. Ifall skum kod följer med från en webbsida som du har besökt eller i någon e-postbilaga, så kan den då i alla fall inte installeras utan att du märker det. Men det gäller också att vara försiktig med vilka program och appar du laddar hem och vilka rättigheter du sedan ger dem. Kontrollera nya program innan du börjar använda dem. Hur ser användarvillkoren och integritetspolicyn ut? Vilka rättigheter ger du till programmet att gå in i exempelvis kontaktböcker och geodata? Känner du dig osäker kanske du hellre ska låta bli att installera programmet eller köra det på en separat dator eller mobil. Låt inte nätsidor köra skript eller lagra kakor på din dator om du inte vet hur de används. Stäng av funktioner som låter någon annan fjärrstyra din utrustning.

Tips! Hindra intrångsförsök.

- Ha brandvägg och antivirusprogram.
- Uppdatera program och operativsystem regelbundet.
- Surfa sällan eller aldrig till sajter som kan innehålla skadlig kod (pornografiwebbar, olagliga nedladdningssajter, et cetera).
- Var försiktig med att ladda ned program, bilder och dokument.
- Koppla inte upp dig som besökare på kontorsnät eller offentliga trådlösa nät om du kan undvika det.
- Koppla ned dig från nätet när du inte behöver vara uppkopplad.

Hackare söker också hela tiden efter luckor i program. Därför bör du alltid se till att du har den senaste versionen av alla dina program, applikationer och operativsystem. Ofta går det att ställa in att de ska hämtas automatiskt. I många operativsystem finns en automatisk uppdateringstjänst, som dock frågar om du vill installera uppdateringarna när de dyker upp. Använd dem. Om du har extremt känslig information ska den i princip inte förvaras på en enhet som är uppkopplad mot internet, eftersom det alltid kan finnas sätt att komma åt den.

6.3 Skydda källan: Surfa säkrare

Det går inte att ge råd som helt skyddar mot de problem som tas upp i de föregående kapitlen. Men med kryptering och "lånade" ip-adresser går det att göra en hel del för minska risken att bränna en hemlig källa eller avslöja dig som journalist när du surfar på nätet. En anslutning till en webbplats kan vara krypterad, du har säkert lärt dig att hålla ögonen öppna efter ett hänglås i webbläsarens adressfält när du använder ditt kontokort. Läs mer om https i rutan på sidan X. E-post, chattmeddelanden, videosamtal, dokument och så vidare går också att kryptera. Och grundregeln är enkel: Det som inte är krypterat är lättare att avlyssna. Ett typexempel där du

VPN för säkrare surfning

VPN för säkrare kommunikation med redaktionen

Tips! Skilj på VPN och Proxy.

På nätet finns något som kallas för proxytjänster. När du använder en proxy tar internettrafiken till och från din dator en omväg och lånar en tillfällig ip-adress. Däremot krypterar inte en proxytjänst trafiken, och därmed ger den inget skydd mot personer som vill titta på din trafik.

som journalist bör vara försiktig är när du sitter på ett kafé eller i en hotellobby och kopplar upp dina prylar mot det trådlösa nätverk som finns tillgängligt för gästerna.

Avlyssnade nät

Hur svårt det är att avlyssna trafiken till och från din dator eller mobiltelefon beror bland annat på hur den är ansluten till internet. Det som skickas i trådlösa nätverk, så kallade wifi-nät, är inte alltid krypterat. Om du inte behöver ange något lösenord första gången du ansluter dig till ett trådlöst nätverk innebär det att trafiken mellan din dator och det trådlösa nätverkets basstation är okrypterad. Då kan vem som helst som befinner sig i närheten avlyssna allt som skickas mellan basstationen och din dator. Om du då exempelvis skickar e-post utan att kryptera den innebär det att innehållet går att läsa. När du kopplar upp dig till trådlösa nätverk bör du därför alltid välja sådana som kräver lösenord, eftersom det är de nätverken som också krypterar trafiken. Men tyvärr räcker inte det. Äldre krypteringsmetoder har visat sig vara osäkra. En av de första som började användas heter WEP och anses idag vara mer eller mindre lika osäkert som ett okrypterat wifi-nät. Välj därför bort WEP-skyddade nät och även de som använder WPA. Anslut bara din dator och surfplatta till wifi-nät som använder den säkerhetslösning som heter WPA2.

När du kopplar upp din mobiltelefon eller dator till ett trådlöst nätverk innebär det också att du lämnar väldigt mycket information till den som sköter basstationen. Den personen kan om hon vill titta på all okrypterad trafik du skickar och tar emot via uppkopplingen, och ibland till och med knäcka krypteringen och avlyssna sånt som

du trodde var säkert. Det är dessutom lätt att sätta upp basstationer med namn som ser pålitliga ut, men där administratören i själva verket avlyssnar trafiken som passerar. Är du inte helt säker på att du kan lita på det trådlösa nätverket är det bättre att använda mobilnätet: Anslut din mobiltelefon till datorn med en usb-sladd och låt den fungera som modem.

VPN

Ett annat bra alternativ är att använda vad som kallas för VPN, virtual private network. Ursprungligen var VPN en företagsteknik. Det "virtuella nätverket" används bland annat för att skapa en säker förbindelse hem till företagets nätverk när anställda befinner sig på tjänsteresa. En så kallad VPN-tunnel är en krypterad förbindelse som sträcker sig från den anställdes dator till företagets nätverk. All trafik skickas via den krypterade förbindelsen och blir därmed svår för någon att avlyssna på vägen. Men en säker anslutning till företagets nätverk är bara ett användningsområde för ett VPN. Krypteringen innebär att det erbjuder ett bra skydd när du behöver koppla upp dig på nätverk som du inte riktigt känner att du kan lita på. VPN-förbindelsen gör det då väldigt svårt för någon att avlyssna trafiken från din dator till VPN-servern. Då spelar säkerheten i det trådlösa nätet plötsligt mindre roll eftersom du skapar en egen, säker förbindelse i det. En VPN-anslutning är alltså något du kan använda för att skydda dig mot avlyssning när du kopplar upp dig till ett trådlöst nätverk eller när du behöver ansluta till servrar på redaktionens nätverk. Ett VPN är däremot inte något som ersätter kryptering av e-post, https eller andra krypteringslösningar. Kryptering på internet finns i många lager: Innehåll och anslutning kan vara krypterad var för sig. Dessutom kan data vara krypterat eller okrypterat när det ligger lagrat på din dators hårddisk eller en server någonstans på nätet. Kryptering i de olika lagren ska inte ses som alternativ till varandra utan som kompletterande lösningar, särskilt om du handskas med riktigt känsliga uppgifter. Vill du surfa till en webbplats men inte vill att någon på samma kafé ska kunna se vilken förhindrar alltså en VPN-tunnel obehöriga från att snoka. Men från VPN-servern vidare till webbplatsen är din trafik bara skyddad om du dessutom ser till att använda https istället för http. Av den anledningen är det viktigt att fundera på vilken VPN-lösning du eller din redaktion använder. Är det ett företag som tillhandahåller VPN-tjänster, var medveten om att de har stora tekniska möjligheter att övervaka vad du gör på nätet.

Välj en VPN-lösning du kan lita på

Om du vill använda en VPN-tjänst för att försvåra för någon att avlyssna din trafik är det två saker du behöver fundera på:

- Välj en teknik som inte har några kända brister. En vanlig VPN-teknik heter PPTP, men den har flera kända säkerhetshål. Välj istället OpenVPN som är lättatt komma igång med och anses som säkert. På seriösa VPN-tjänsters sajter finns det alltid angivet vilken teknikom används.
- Om du inte jobbar på eller åt en redaktion somtillhandahåller en VPN-server behöver du själv välja vilkendu ska använda. Tänk då på att teknikerna på tjänsten du använder bland annat kan se vilka nättjänster du använder och eventuellt också innehållet i trafiken. Gör du en granskning i Ryssland, välj därför inte en rysk VPN-tjänst och så vidare.

Tor

Ibland är det inte bara avlyssning du som journalist behöver oroa dig för. Du kan behöva använda nätet anonymt, utan att någon kan koppla det du gör till dig. Vi har redan konstaterat att din dators ip-adress kan avslöja dig. Lösningen är Tor, en gratistjänst som utvecklas med stöd från bland andra svenska Sida. Tor används av journalister, människorättsaktivister och andra som behöver vara anonyma på nätet. Tor låter nämligen din dator tillfälligt låna en annan ip-adress. Och utlånet sker i en trestegsraket som gör det omöjligt för någon att koppla den tillfälliga ip-adressen till dig – så länge du använder Tor som det är tänkt. Om du surfar via Tor för att först kolla ditt Facebook-konto och därefter vidare till ditt hemliga e-postkonto på Gmail så finns möjligheten att någon kan göra kopplingen. På nätet är det viktigt att hålla vattentäta skott mellan det som ska vara anonymt och det som inte behöver vara det!

Trafiken som skickas via Tor-nätverket är krypterad och Tor kan därmed även användas för att skydda webbtrafiken när du är uppkopplad till ett osäkert wifi-nät. Men precis som med ett VPN är

Välj https istället för http

När du besöker en webbplats där du hanterar känsliga uppgifter, exempelvis ett webbgränssnitt till din e-post, kontrollera att det står https och inte http först i webbläsarens adressfönster. Förkortningen "http" står för hypertext transport protocol vilket är den teknik som används för att skicka webbsidor mellan server och webbläsare. Tillägget i "https" står för secure och betyder att kommunikationen mellan din webbläsare och webbplatsen är krypterad och därmed också svårare för obehöriga att avlyssna. Ta också webbläsarens varningar om felaktigheter i det så kallade SSL-certifikatet på allvar. SSL-certifikatet är nyckeln som används för att kryptera förbindelsen. En varning om att något inte stämmer kan innebära att någon försöker avlyssna trafiken.

För att minska risken för att du väljer en http-anslutning istället för https kan du installera tilläggsprogrammet HTTPS Everywhere i din webbläsare. Det är utvecklat av den amerikanska medborgarrättsorganisationen EFF och ser till att din webbläsare väljer en krypterad förbindelse varje gång en sådan finns tillgänglig. HTTPS Everywhere finns för Firefox, Chrome och Opera. Webbläsare som stöder htttps visar när en besökt sida är krypterad genom att en symbol med stängt hänglås syns i adressfältet eller längst ned i webbläsarfönstret.

trafiken bara krypterad fram till den punkt då den lämnar Tor. För att vara skyddad även därefter krävs andra former av kryptering, som https för webbtrafik eller PGP för e-post. Var också uppmärksam på att Tor bara skyddar det du gör i Tor Browser, Tors egen webbläsare. Om du av misstag råkar använda din vanliga webbläsare när du vill vara anonym kommer du att avslöja din ip-adress. För e-post, chatt och andra tjänster som du inte kommer åt via Tor Browser kommer du också att exponera din faktiska ip-adress.

Var också medveten om att du lämnar många andra spår efter dig när du använder internet och särskilt på webben. Där används exempelvis så kallade cookies för att följa hur du rör dig inom och mellan webbplatser. Normalt sett används de för att få sajten att fungera – som inköpskorgen på en webbshop – och i marknadsföringssyfte, men samma tekniska lösningar kan givetvis användas i andra syften också.

Uppdatera din webbläsare

Genom att uppdatera din webbläsare till den senaste versionen minskar du din riskexponering på webben. Äldre versionen har ofta många säkerhetshål som bland annat utnyttjas för att installera skadliga program i din dator. Du kan testa din webbläsare på https://www.ssllabs.com

Kryptering, lånade ip-adresser och igensopade spår

I det här kapitlet går vi igenom några av de åtgärder du som journalist kan vidta för att minska risken för att du av misstag röjer en källa som skulle förbli hemlig eller att du exponerar din arbetsplats ip-adress och därmed också avslöjar dig som journalist när du exempelvis besöker en webbplats. I grund och botten handlar alla lösningarna om tre olika saker:

- Vad gäller informationen du skickar på nätet, oavsett om det handlar om e-post, chattmeddelanden eller källdokument, kan den bara skyddas om den krypteras. Allt som skickas på nätet utan att vara krypterat kan läsas av utomstående som på ett sätt kan avlyssna trafiken.
- Vad gäller risken att avslöja dig som journalist handlar det delvis om att inte exponera arbetsplatsens ip-adress när du använder nätets tjänster. Det finns olika sätt att tillfälligt "låna" en ip-adress. Ett VPN är ett alternativ. En annan lösning är att surfa från ett mobilt bredband eller ett internetkafé. Men om du väljer det senare alternativet, var då medveten om de risker som du istället exponerar dig för!
- För riktig anonymitet, där det inte räcker med att dölja din yrkesroll som journalist med en lånad ip-adress, krävs mer eftertanke. Här är Tor ett bra verktyg. Precis som med ett VPN ger Tor dig en lånad ip-adress, men lånet administreras på ett sätt så att ingen kan knyta din lånade ip-adress till din faktiska ip-adress och därmed inte heller till dig.

Tails är ett Tor på steroider

Tails är en specialversion av operativsystemet Linux, utvecklat för att ge användaren maximal anonymitet på nätet. Tails installeras på en usb-sticka och när datorn startas från den skickas all nätverkstrafik via Tor. Installerar du Tor i din dator är det bara webbtrafiken från och till Tor Browser som går via Tor, medan exempelvis e-post och chatt inte gör det.

Tails har också den fördelen att det är lättare att skapa vattentäta skott till din anonyma nätanvändning. Ska du göra något som kräver anonymitet startar du om datorn med Tails-stickan i usb-uttaget. När du är klar startar du om datorn igen, till ditt vanliga operativsystem.

Därmed minskar risken för att du glömmer bort dig, gör något via Tor som du inte borde göra och därmed röjer din identitiet. Finns att ladda ned på: tails.boum.org

Kontrollera dina program

Utvecklingen på nätet står inte still. Och det gäller säkerhetsproblemen i lika stor utsträckning som allt annat. Många av de övergripande resonemangen i den här guiden kommer vara giltiga under lång tid framöver. Det gäller till exempel det faktum att okrypterad e-post är att jämföra med ett vykort, att vi lämnar många spår efter oss när vi använder nätet och att fler krypteringslager är bättre än färre. Men när det gäller de mer konkreta tipsen kring vilka program och tjänster du som journalist kan använda dig av för att minska riskerna för att röja dina källor går det tyvärr inte att säga något om livslängden. Nya säkerhetshål och andra brister upptäcks dagligen på nätet och de kan mycket väl finnas i de program som den här guiden tar upp.

Ett konkret exempel gäller Truecrypt, ett program för att kryptera filer eller hela hårddiskar. Det ansågs länge vara det bästa alternativet för den som vill spara information på ett säkert sätt på den egna datorn eller på ett usb-minne. Men i slutet av maj 2014 dök plötsligt en varning upp på Truecrypts webbplats: “Using TrueCrypt is not secure as it may contain unfixed security issues.”

Exakt vad som ligger bakom varningen är inte känt, men det finns gott om spekulationer. En handlar om att Truecrypt har en bakdörr som amerikanska myndigheter kan utnyttja. Utvecklarna själva säger att de handlar om att de inte längre vill jobba med projektet och inte litar på att andra skulle förstå koden och kunna fortsätta utveckla Truecrypt på ett säkert sätt.

Privat surf i webbläsaren

Kanske har du lagt märke till att din webbläsare har funktioner som heter Privat surf, Radera historik och liknande. Det är funktioner som i första hand gör det möjligt för dig att besöka webbplatser utan att någon som använder samma dator enkelt och i efterhand kan se vilka. Funktionen är däremot inte ett skydd mot de avlyssnings- och spårningsmöjligheter som finns på webben.

Huruvida äldre versioner av Truecrypt (specifikt den som heter 7.1a) fortfarande går att lita på eller inte råder delade meningar om. Men som följer av resonemanget i kapitlet om hotbilder är det inte säkert att den frågan har ett tydligt svar. Det beror istället på vad det är för information du behöver kryptera och vem det är du inte vill ska se den. Fallet med Truecrypt visar också att det är viktigt att hålla sig uppdaterad om vad som händer med de program du som journalist använder. Det generella rådet är därför att alltid använda den senaste versionen av ett program. I äldre versioner finns ofta säkerhetshål som kan utnyttjas på olika sätt. Så snart dessa blir kända för utvecklarna brukar de åtgärdas när en ny version släpps. Och om du inte behöver använda några av de här tjänsterna och programmen idag, men om några år jobbar med en artikel eller ett reportage som ställer höga krav på källskydd, kom då ihåg att det finns många fallgropar på nätet och skaffa dig aktuell kunskap om hur du bäst skyddar dina källor då. Du behöver också verifiera programmen du laddar ner, att de inte är manipulerade på något sätt. Hämta bara hem program från officiella webbplatser och följ de instruktioner som finns för att kontrollera att de så kallade hash-/checksummorna stämmer.

Hur ser hotbilden ut?

Edward Snowdens avslöjanden har satt fokus på den typ av övervakning och avlyssning som myndigheter som amerikanska NSA, brittiska GCHQ och svenska FRA ägnar sig åt. Men det är förhållandevis få svenska journalister som ägnar sig åt avslöjanden på den nivå som intresserar de myndigheterna. Men det innebär inte att du kan slappna av. En granskning av ett lokalt företag med en någor-

lunda duktig it-avdelning kan få för sig att läsa de anställdas e-post i smyg. Intervjuer med personer som flytt krigsområden kan få regimen i deras hemländer intresserad. Om du använder en VPN- eller proxytjänst, fundera då på vems ärenden företaget som erbjuder tjänsten kan tänkas gå. Granskar du hur USA agerar i en viss fråga ska du kanske inte välja en amerikansk VPN-tjänst. Utöver dessa risker som är kopplade direkt till ditt yrke som journalist finns mer allmänna hot. Sitter du på ett kafé i närheten av en teknisk högskola, vågar du lita på att studenterna som sitter med sina datorer i hörnet inte pluggar nätverkssäkerhet och just fått lära sig hur man avlyssnar trafiken i trådlösa nätverk?

Precis som säkerheten i de program du använder inte är statisk är inte heller hotbilden mot dig och dina källor det. Gör därför hela tiden nya överväganden om vilka åtgärder som är rimliga att vidta. Tyvärr innebär all kryptering och anonymitet på nätet en kompromiss med användarvänligheten. Det kan handla om lösenord som ska matas in, en långsammare surfupplevelse eller källor som måste utbildas. Allt är bökigt, tar tid, är mer eller mindre svårt att lära sig. Att kryptera all e-post och att alltid använda Tor för att surfa anonymt är därför inte realistiskt. Men vilka verktyg ska du använda när? Vissa åtgärder handlar om sunt förnuft och är sådana som du bör vidta med en gång, om du inte redan gjort det: Långa, bra lösenord till din e-post och andra känsliga konton (och som är unika för varje tjänst!), pinkod på din mobiltelefon, en vana att undvika okrypterade, trådlösa nätverk och inte spara känsligt material i någon av nätets molntjänster. På så vis har du en grundläggande, acceptabel säkerhetsnivå att utgå ifrån och behöver inte göra stora förändringar i din datoranvändning när det bränner till.

I övrigt handlar det om att fundera på hotbilden för varje jobb du håller på med. Ju mer högprofilerat jobb, desto mer genomgående åtgärder med kryptering av researchmaterial och försiktighet i källkontakterna behöver du. Men det räcker inte med att konstatera att du håller på med ett jobb som kan vara känsligt. Du behöver också fundera på för vem det är känsligt och vad det innebär för ditt val av tjänster och program. Är du ansvarig för it-frågorna på en redaktion bör du också ha med de här frågeställningarna i de upphandlingar som görs. Vilka företag får i uppdrag att sköta driften av exempelvis redaktionens interna nätverk eller mejlservrar? Vilka av företagets it-tekniker har tillgång till enskilda reportrars e-post?

Kryptering i flera steg

På internet förekommer kryptering i många olika nivåer. En anslutning i ett trådlöst nätverk kan vara krypterad eller okrypterad. Ett e-postmeddelande kan skickas krypterat eller okrypterat. Förbindelsen mellan webbläsaren i din dator och webbplatsen du besöker

Case: Lagen skyddar inte digitala källor

Den 19 september 2007 knackade två poliser på dörren till Kalla fakta-reportern Trond Sefastssons lägenhet på Östermalm i Stockholm. Sefastsson var misstänkt för mut- och skattebrott och poliserna skulle, på order av kammaråklagare Malin Palmgren, säkra bevis genom en husrannsakan. Med sig när de gick hade de förutom Sefastssons bokföring i pärmar, trots hans protester, också hans dator med material från mer än tio år av hans research, men även hans genomgångar av andra TV4-reportrars material.

Bland annat fanns där researchen om livstidsdömde Yasser Askar, friad av Högsta domstolen efter Sefastssons granskning av fallet, samt research om fallet med den morddömde romen Veija Borg. Bägge fallen hade fokus på rättsosäkerheten i polisens arbete, bland annat det som utfördes på just den avdelning som nu tog hand om den beslagtagna datorn. Trond Sefastsson och TV4, som han hade arbetat för i över tio år som reporter och juridisk konsult, begärde att beslaget skulle hävas, eftersom datorn innehöll material som omfattas av källskyddet i yttrandefrihetsgrundlagen. Sådant material har enligt rättegångsbalken särskilt skydd vid polisingripanden, som till exempel husrannsakan.

Men både tingsrätten och sedan hovrätten sade nej, och sedan Högsta domstolen i två beslut inte fann skäl att meddela prövningstillstånd vann beslaget laga kraft.

Lagstiftarens avsikt med rättegångsbalkens speciella regler för beslag av handlingar hos en journalist eller på en redaktion tillkom för att säkra att källornas identitet inte röjs, även om en journalist är misstänkt för brott. Men när lagen skrevs var begreppet ”skriftlig handling”, vilket domstolarna tolkade bokstavligt som papper. För elektroniskt lagrad information fanns inget skydd, menade de. ”Ärendet inrymmer … frågor av stor betydelse inte minst på yttrandefrihetsrättens område” ansåg Justitiekanslern, JK, som när han granskade ärendet i en genomgång av rättsläget fann inte mindre än sju utredningar av frågan. JK landade i att en lagreglering av även datalagrad information borde införas.

Förra justitieministern Beatrice Ask sade sig också vara bekymrad över läget, men ännu 2015 har ingen ny reglering kommit

till stånd. Enligt lagen kan ett beslag ske av en journalists digitala utrustning, utan att villkoren har prövats i domstol – och journalisten behöver inte ens vara misstänkt för något brott. Efter mordet på reporten Elin Falk vid Västerbottens folkblad togs hennes utrustning i beslag. Det hävdes till slut av hovrätten och dator och mobiltelefon lämnades tillbaka.

Efter att Sveriges Radios korrespondent Nils Horner skjutits till döds i Kabul i mars 2014 gjordes ett beslag av hans utrustning: datorer, mobiler, kameror och bandspelare.

Sveriges Radio överklagade beslaget med hänvisning till källskyddet. Beslutet hävdes inte, men det sattes villkor för hur utrustningen skulle gås igenom och att någon från radion skulle få vara med vid genomgången. Detta är dock inte någon rättighet som är reglerad i lagen.

I det här fallet sammanfaller sannolikt Sveriges Radios och polisens intressen av att hitta mördaren, utan att källor röjs. Men om datorns ägare är misstänkt för ett brott blir det naturligtvis en tydligare intressekonflikt om hen vid en genomgång säger att ”i de där mapparna får ni inte titta”. Ett annat exempel är att under utredningen av mordet på reportern Elin Falk vid Västerbottens folkblad i mars 2015, beslagtogs hennes utrustning av polisen. Beslaget hävdes till slut av hovrätten och dator och mobiltelefon lämnades tillbaka.

Datalagrad information om en källa som finns på redaktionen, i molnet eller hemma hos en journalist har idag inte på långa vägar samma skydd i lagen som information på papper. Vid denna guides tryckning finns ett förslag om en möjlighet att närvara när polisen går igenom it-utrustning som tagits i beslag. Men det ser inte ut att bli något krav.

Bäst är då att kryptera allt material som innehåller information som omfattas av källskydd – och att undvika att ha sådant som bokföring på samma dator som känsliga uppgifter om källor. Enligt Sveriges Radio fanns ”visst skydd” av innehållet i Nils Horners utrustning. Men det tog mer än ett halvår innan polisen hade lämnat tillbaka alla Nils Horners apparater till Sveriges Radio. Trond Sefastsson hade haft krypteringsprogrammet PGP, Pretty Good Privacy, installerat på sin dator i nästan på dagen tio år innan polisen knackade på dörren. Men han hade aldrig använt det.

kan vara krypterad eller okrypterad. Är det ena alternativet bättre eller sämre än det andra? Svaret är att de kompletterar varandra och att det finns en enkel grundregel: Ska du skydda en hemlig källa är fler krypteringslager bättre än få, eftersom varje krypteringslager gör det svårare för någon obehörig att komma åt det hemliga materialet. Om du skickar ett okrypterat e-brev via ett krypterat trådlöst nätverk minskar du risken för att någon som sitter på samma kafé kan läsa innehållet. Däremot kommer personer som har tillgång till den nätverksutrustning som ditt mejl passerar på vägen till mottagaren fortfarande kunna läsa det.

Om du däremot är uppkopplad till ett trådlöst nätverk som saknar kryptering när du skickar ett krypterat mejl är innehållet i det skyddat hela vägen fram till mottagaren. Däremot kommer de som finns på samma kafé kunna se mycket annat av det du gör på nätet. Och ibland omfattar det även vem du skickade ditt mejl till och vad som stod i ärenderaden – om anslutningen till och från e-postprogrammet i din dator inte är krypterad. Det är alltså viktigt att förstå att både anslutningen i sig, från din dator till nätverket och från programmen i din dator till respektive tjänst på nätet kan vara krypterad. Men även att innehållet som skickas via dessa anslutningar kan vara krypterat. Det ena utesluter inte det andra. Till krypterad förbindelse och krypterad överföring går dessutom att lägga en tredje typ av kryptering: Krypterad lagring. Ett exempel på när det kan vara relevant för en journalist att fundera på hur information lagras är Twitter. Tjänsten har en funktion som heter direktmeddelanden. Den gör det möjligt för två användare att kommunicera direkt med varandra utan att någon annan ser det som skrivs. Normala uppdateringar på Twitter kan läsas av alla, men direktmeddelanden bara av de två som deltar i samtalet. Twitter är en av de tjänster som aktiverat https och därmed är anslutningen från din dators webbläsare till Twitters webbplats krypterad och svår att avlyssna. Därmed kan det vara frestande att tro att Twitters direktmeddelanden också är en säker kanal för journalister och deras källor. Fel. Innehållet i Twitters direktmeddelanden är inte krypterat, på företagets servrar lagras de av allt att döma okrypterat. Det innebär att ett direktmeddelande kan vara krypterat när det transporteras till och från Twitters servrar och därmed vara svårt för någon att avlyssna på vägen. Däremot skulle de tekniker som har tillgång till Twitters servrar potentiellt kunna läsa dem. Krypterad förbindelse, krypterad transport och krypterad lagring är alltså tre typer av kryptering du som journalist behöver fundera på.

7. Källskydd och juridik

Svenska medborgare har enligt grundlagen rätt att inhämta och sedan lämna ganska mycket information till medier, utan att behöva vara oroliga för repressalier från staten – men rätten har också en rad begränsningar. Flera lagar ger också möjlighet att övervaka mediers kommunikation med källorna på olika sätt.

Källskyddet kan delas upp i två delar. Den ena är mediernas plikt att hålla källorna anonyma och den andra förbjuder myndigheter att jaga källor. Båda regleras i tryckfrihetsförordningen för tryckta skrifter och i yttrandefrihetsgrundlagen för radio, teve och internet.

Den som arbetar på en myndighet får inte ta reda på vem som lämnat information till medier, om det inte gäller kvalificerat hemliga uppgifter. Viktigt att komma ihåg är att det här efterforskningsförbudet riktar in sig på just myndigheter. Det är fritt fram för privata företag och organisationer att försöka ta reda på om deras anställda lämnar ut information.

Den som tar emot information från en källa har tystnadsplikt. I några fall gäller den dock inte. Det allra första undantaget är det mesta använda: om källan gått med på att identifieras. Att det är just ett undantag är en stark markering. Rätten att vara anonym är central.

Anonymiteten gäller inte vid vissa mycket allvarliga brott, exempelvis mot rikets säkerhet.

Det är inte bara journalisten som har tystnadsplikt, utan alla som ”tagit befattning med utgivningen”. Det innebär exempelvis att även en IT-tekniker som har hand om en journalists dator omfattas av förbudet att röja källor. Långt ifrån alla känner dock till detta, och det kan därför vara viktigt att ta upp det med alla som kan komma i kontakt med känsliga uppgifter – och reglera all hantering tydligt i avtalen, om man anlitar externa företag som kan stöta på uppgifter om källor.

Förutom grundlagen reglerar också personuppgiftslagen hur och vilka personuppgifter som får databehandlas. Många av de centrala paragraferna gäller inte för journalistiska ändamål. Reglerna om säkerhetsåtgärder gäller dock även för journalister.

Exakt hur långt en journalist eller medieföretaget måste gå för att inte avslöja sina källor är oklart, och usla it-rutiner har ännu aldrig prövats rättsligt. Överlag är det ovanligt att brott mot tystnadsplikten hamnar i domstol. Formellt kan straffet bli upp till ett års fängelse, men de som dömts de senaste åren har fått dagsböter i storleksordningen 40 000 kronor. Den journalist som avslöjar sin källa kan även bli avskedad. Man får inte vara oaktsam – man får exempelvis inte skicka iväg ett fax med en källas namn på ett sådant sätt att det hamnar i fel händer.

Bara det faktum att det finns en risk att källor avslöjas är dock inte straffbart. Det är först den dag en källa faktiskt blivit röjd som fallet

kan drivas rättsligt av Justitiekanslern. Då skulle det dock kunna vara försvårande om man utlovar ett starkt skydd, om man samtidigt använder teknik som innebär uppenbara risker – exempelvis genom formuleringar som ”Självklart är du anonym” eller ”Du är garanterad fullt meddelarskydd” på osäkra, okrypterade webbsidor för tipsare.

Lagar som gör det möjligt att hitta källor

Datalagrad information om en källa som finns på redaktionen, i molnet eller hemma hos en journalist har idag dåligt skydd i lagen. Vid en brottsutredning får polisen inte ta journalisters papper och pärmar i beslag enligt rättegångsbalken. Men digital utrustning, som datorer och mobiltelefoner, kan tas i beslag.

Trots att alla journalister borde känna till offentlighetsprincipen, att allmänna handlingar hos myndigheter i hög grad också ska lämnas ut, händer det att journalister skickar e-postmeddelanden till tjänstemän, som garanteras anonymitet om de ställer upp och berättar om något. Även om myndigheten inte får forska efter källan kan vem som helst begära ut e-postloggen – och kontakten mellan journalist och källa är röjd.

I det privata näringslivet gäller lagen om företagshemligheter. I princip är det arbetsgivaren som avgör vad som får berättas och vad som ska hållas hemligt. Arbetsgivaren får både ställa frågor om vem som läckt och leta igenom företagets it-system i jakt på uppgiftslämnare. Källan kan bli av med jobbet, riskerar att få betala skadestånd och kan dömas till upp till sex års fängelse. Undantaget är om avslöjandet i sin tur kan ge fängelse för det som avslöjas – vilket kanske inte alltid är så lätt att avgöra på förhand för den person som funderar på att tipsa media.

I och med att allt mer verksamhet som tidigare drevs i det allmännas regi numera är privatiserad eller bolagiserad har också förutsättningarna för meddelarskyddet ändrats. Vad som gäller regleras dels i avtalen med kommun eller landsting, dels i kollektivavtal. Anställda i statliga bolag har inte meddelarskydd.

En utredning som i skrivande stund inte lett till någon proposition föreslår stärkt meddelarskydd för privatanställda som jobbar inom vård, skola och omsorg, och som betalas med skattepengar. Annan offentligt finansierad verksamhet i privat regi skulle inte omfattas.

En annan utredning, ”visselblåsarutredningen”, riskerar att urholka meddelarskyddet. Enligt förslaget ska alla på hela arbetsmarknaden, även offentligt anställda, i första hand slå larm om missförhållanden internt, innan man går ut externt. Hur en sådan regel ska tolkas ifall att en journalist tar den första kontakten är oklart.

Under de senaste åren har flera lagar införts, som tillåter övervakning och tvingar teleoperatörer att spara trafikuppgifter. Motiveringen är brotts- och terroristbekämpning. Flera av lagarna

Viktigt! Meta-taggade bilder.

Meta-data är information som osynligt bäddas in i digitala filer som dokument, bilder och så vidare. När bilder publiceras på webben och hänger med meta-datat med – vilket avslöjar exakt var bilden togs med gps-information och allt. Det finns särskilda program, många av dem gratis, som kan visa och även radera meta-data från filer och dokument. Använd dem innan du publicerar exempelvis bilder på internet.

får långtgående konsekvenser för möjligheten att hitta kontakter mellan journalister och källor – och konsekvenserna för källskyddet har inte alltid analyserats ordentligt på förhand.

Den så kallade FRA-lagen ger Försvarets radioanstalt (FRA) rätt att avlyssna internettrafik som passerar Sveriges gränser. I praktiken innebär det att i princip allt kan fångas upp av FRA eftersom internet inte bryr sig om gränser. Ett e-postmeddelande från södra till norra Stockholm kan mycket väl ha tagit vägen via Tyskland, USA och Norge innan det når adressaten. Om det visar sig att sådana uppgifter har samlats in ska de enligt lagen förstöras – liksom meddelanden som omfattas av källskydd. Eftersom insynen i verksamheten är begränsad är det omöjligt att veta hur ofta journalisters kommunikation faktiskt snappas upp.

2012 införde Sverige EUs datalagringsdirektiv, som tvingar teleoperatörer att lagra trafikdata om människors telefon- och nätkommunikation för att denna information ska kunna användas i brottsutredningar.

I april 2014 dömde EU-domstolen ut datalagringsdirektivet, bland annat med hänvisning till att det inskränker grundläggande mänskliga rättigheter som yttrandefrihet och kommunikationsfrihet. Den dåvarande svenska regeringen ansåg dock att den svenska lagen gäller. Flera teleoperatörer har överklagat. I mars 2015 föreslog en utredning vissa mindre förändringar i reglerna kring polisens hantering av uppgifter – men kravet på att teleoperatörerna ska lagra kvarstår. I EU pågår en diskussion om en revidering av direktivet.

Dagens svenska lagring innebär att trafikuppgifterna sparas ett halvår av teleoperatörerna enligt lagen om elektronisk kommunikation, LEK. På ett par punkter går den svenska lagen längre än

Tips! Checka inte in.

Det kan verka självklart, men checka inte in på platser tillsammans om ni inte tidigare har en relation där det kan verka helt normalt att ni checkar in på samma plats. Gå igenom inställningarna på ditt konto på Facebook och de andra tjänsterna och kontrollera att inte digitala foton läses in och automatiskt adderar information om var och när de är tagna. Det viktigaste är att stänga av funktioner som utan ditt medgivande förser statusuppdateringar med platsinformation.

det ogiltigförklarade EU-direktivet. Alla försök att ringa någon ska lagras – även om det inte blev något svar. Dessutom ska den geografiska positionen för mobilsamtal sparas. Brottsbekämpande myndigheter kan sedan få tillgång till uppgifterna enligt LEK, rättegångsbalken eller inhämtningslagen.

Uppgifter kan tappas direkt från operatörernas system, eftersom LEK och inhämtningslagen inte kräver domstolsbeslut för att lämna ut uppgifterna.

Problemet med datalagringen är inte bara att ”storebror”, i form av myndigheter, medvetet eller omedvetet kan se kontakter mellan källor och journalister. I allt högre grad finns det anledning att fundera även över vilka ”småsystrar” som kan komma åt informationen.

När det gäller lagringen av trafikdata finns uppgifterna om mediers kontakter tillgängliga för en rad människor hos teleoperatörerna. Även om det ska råda sekretess kring det som sparas, finns ingen garanti för att ingen kommer att missbruka det faktum att journalisters och källors mobiltelefoner i praktiken blivit konverterade till spårsändare. Bevekelsegrunderna kan vara alltifrån ren och skär nyfikenhet till svartsjuka eller spelskulder. Att det är sådant som får folk att strunta i sekretessregler visar exempelvis alla de intrång som varje år sker i patientjournaler inom sjukvården.

Flera andra lagar ger polis och Säpo möjlighet att avlyssna telefonsamtal och lokaler. Även personer som inte är misstänkta för brott kan i vissa fall avlyssnas – även journalister. Lagen om hemlig rumsavlyssning förbjuder avlyssning av redaktioner, medan lagen om åtgärder för att utreda vissa samhällsfarliga brott inte hindrar det. Polisen kan också hjälpa utländsk polis med avlyssning.

Checklista! Sociala medier.

- Publicera inte något på sociala medietjänster som riskerar att röja din källa.
- Ge andra alternativ för kontakt via en skyddad e-postadress eller ett säkert telefonnummer.
- Checka inte in i någon positioneringstjänst tillsammans med dina källor.
- Gå igenom inställningarna för din profil och stäng av allt som kan tala om var du är, när och med vem.
- Bli inte ”vän” med dina källor eller följ dem inte, om ni inte är bekanta sedan tidigare.

7.1 Skydda källan: Sociala medier

Vi har sparat de sociala medierna till sist, främst för att de består av kombinationer av förut nämna tjänster på nätet, men även för att utvecklingen i skrivande stund är väldigt vital när det gäller mötesplatser på internet. Det gäller inte minst från ett redaktionellt perspektiv. Att använda sociala medietjänster har visat sig vara mycket användbart och tidsparande för många journalister. Facebook, Twitter, Linkedin, Instagram och andra nätverkstjänster är ett utmärkt sätt att bevaka olika händelser och går även att använda för research. Varannan svensk finns idag på Facebook. Tjänsten har därför snabbt blivit den ledande platsen på nätet för människor att samtala, interagera och knyta kontakter. I grupper, indelade på ämnesområden, kan man träffa likasinnade och diskutera specialintressen. Där finns också grupper där journalister kan efterlysa intervjupersoner för olika ämnesområden till reportage. Andra journalister frågar rakt ut i sina nätverk efter nyhetstips och förslag på intressanta intervjupersoner eller vinklar. De flesta sociala medier fungerar ungefär likadant. Man skapar ett konto och har en profil där man publicerar sina statusuppdateringar. Nästan alla sociala medier ger användare möjligheten att kontakta en journalist öppet eller via direktmeddelanden. En bra utgångspunkt när man publicerar något i sociala medier är att tänka att alla i hela världen kan se det. Även om du bara postar en uppdatering till dina vänner, kan någon alltid spara ner den, ta en skärmbild och sprida vidare. En källa kan höra av sig till journalisten direkt via direktmeddelande eller genom att svara

öppet i kommentarer på en social medietjänst eller ett diskussionsforum. Det är bra att alltid ge ett par olika alternativ för kontakt. Om du öppet söker ögonvittnen eller intervjupersoner i sociala medier, bör du alltid ge ett par olika valmöjligheter för kontakt, till exempel ett telefonnummer eller en e-postadress. Flytta alltid kontakten med källan utanför det sociala mediet. Det som publicerats i sociala medier, chattar eller diskussionsforum finns kvar för evigt och kraften i de sociala medierna är stark. Det finns många exempel när grupper av medlemmar i olika diskussionsforum tillsammans har avslöjat källor eller exempelvis misstänkta, men inte dömda, personer. Många tillsammans kan lätt dra slutsatser av de spår som du lämnar i de olika nätverkstjänsterna. Beroende på vilken relation du tidigare har haft till din källa kan man behöva agera olika för att han eller hon ska få så fullt skydd som möjligt. Om ni inte tidigare har varit vänner på Facebook eller följt varandra på Twitter finns ingen anledning att bli det nu heller, eftersom ni då lätt kan kopplas ihop. Om ni däremot redan tidigare har varit vänner eller Twitter-följeslagare är det dumt att sluta vara det, eftersom det också kan spåras och verka misstänkt. Att använda sig av tidningarnas kommentarsfält är ett dåligt sätt att hämta in eller lämna anonyma tips till tidningar. Många tidningar kräver att man uppger sitt riktiga namn och e-postadress innan man kommenterar. Andra använder sig av Facebook-inloggning, där ens namn och profil automatiskt länkas in. Kommentarsfälten skyddas heller inte av grundlagen när det gäller rätten att vara anonym, utan man måste lita på tidningens goda vilja.

Ett exempel är Kristianstadsbladet som inte förhandsmoderade sina läsarkommentarer vid den här tiden. I en artikel hade en person under pseudonym gjort uttalande som anmäldes för förtal. Kristiansbladets utgivare vägrade dock uppge personens namn utan hänvisade till deras policy som säger att de inte lämnar ut några uppgifter som kommer till tidningen oavsett vad som gäller. I ett omodererat kommentarsfält är det alltid den som skriver kommentaren som är ansvarig. Om man skriver ett inlägg och publicerar i eget namn eller pseudonym på en blogg, ansvarar man själv för sitt inlägg. I det här fallet höll tidningen fast vid källskyddet. Men i dagsläget är det oklart hur långt meddelarfriheten och källskyddet räcker. Än så länge finns ingen rättslig prövning av om tidningens plikt att skydda identiteten på källor även omfattar tips i kommentarerna.

Case: Göteborgs-Posten

När Samir Bezzazi arbetade på Göteborgs-Posten startade han tillsammans med kollegan Filip Kruse nätgrävet Bostadsfronten som låg bakom många avslöjanden om bostadsmarknaden i Göteborg. För att lyckas med detta använde de sociala medier.

– Jag har inte en offentlig Facebook-profil med mig som journalist, utan jag har andra konton under andra alias, mest i syfte för att gräva och kartlägga. Till exempel kunde vårt första avslöjande, om en tjänsteman på kommunen som gav en k-märkt lägenhet till sin bonus-son, avslöjas helt på grund av Facebook. Eftersom de inte var medlemmar i samma familj fanns inte kopplingen mellan dem, men när vi gick igenom vänlistor kunde vi binda tjänstemannen med hyresgästen, som visade sig vara en bonus-son, berättar han.

Han använder Facebook i gräv och för avslöjanden, men försöker hålla kontakten utanför. Han vill ha så kort kontakt i det sociala mediet som möjligt. Det är bättre att den flyttas till telefon eller mejl. Samir Bezzazi tycker att det har blivit svårare och mer problematiskt att skydda källor eftersom nätet är mycket lättare att övervaka än den riktiga världen.

– Det räcker med en kommentar eller ett meddelande i ett offentligt sammanhang på nätet för att man ska kunna spåra en tipsare till en journalist. Och det tänker inte många journalister på, och speciellt inte tipsaren, säger han.

Samir menar att journalistens ansvar har blivit större i och med utvecklingen på nätet och att man som journalist så tidigt som möjligt bör berätta för tipsaren vilka faror som finns.

– Jag hade till exempel en tipsare som i samma veva ville bli vän med mig på en sida. Jag tackade nej och kontaktade tipsaren och förklarade varför. Då visade det sig att tipsaren inte ens tänkt tanken på att det skulle bli lätt att spåra vår kontakt om vi blev vänner. För oss journalister kan en sådan sak vara ganska självklar, men inte för tipsaren.

En journalist måste utgå ifrån att tipsarens internetsäkerhet är usel, vilket den ofta är. Dåliga lösenord och mejl som synkas direkt till mobil gör att källan ofta är mycket mer sårbar än vad han eller hon tror. Det är väldigt sällan en källa kontaktar Samir via en social medietjänst.

– Om folk lämnar ett tips på sociala medier eller i en kommentar skriver jag alltid en hänvisning med information om hur de kan kontakta mig via telefon eller e-post. Men oftast väljer de att mejla eller ringa direkt. Det bästa är att alltid ha alla kontaktuppgifter nedskrivet i sin profil, menar Samir Bezzazi.

Han föredrar kontakt via telefon och det bästa är att källan använder ett kontantkort.

– Jag använder sociala medier mer för att snappa upp saker för att gå vidare på annat sätt. Risken att källan får sitt Twitter- eller Facebook-konto hackat är långt mycket större än att någon skulle lyssna av vårt telefonsamtal. Vill man verkligen vara säker, flyttar man konversationen så snabbt som möjligt från internet till verkligheten, avslutar Samir Bezzazi.

8. Läs mer

Electronic Frontier Foundation har utmärkta kostnadsfria guider hur du skyddar dig och din information på nätet. Delar av materialet riktar sig särskilt till journalister. ssd.eff.org

Comitee to Protect Journalists har omfattande säkerhetsguider för journalister. cpj.org

Tryckfrihetsförordningen (TF) 3:3.
Yttrandefrihetsgrundlagen (YGL) 2:3
Efterforskningsförbudet hittar du i TF 3:4 och YGL 2:4.
Lag (1990:409) om skydd för företagshemligheter.

Samtliga finns att läsa på lagen.nu

Anders R Olsson. Yttrandefrihet & tryckfrihet. Handbok för journalister. (ISBN 9144056761)

TCO: Rätten att slå larm. En handbok om yttrandefriheten på jobbet. Kan köpas från TCO eller laddas ned gratis från www.tco.se

Missa inte Internetguiden Yttrandefrihet på nätet av Nils Funcke. internetguider.se

Sus Andersson

Sus Andersson är skribent, researcher och föreläsare. Sedan många år är hon ledamot i Journalistförbundets yttrandefrihetsgrupp, där hon särskilt bevakar frågor som rör digitalt källskydd. Hon har jobbat med grävande journalistik inom teknik, miljö och naturvetenskap, bland annat under tio år på tidningen Ny Teknik och tre år i den egna webbtidningen Farad. Sus Andersson har bland annat granskat forskningsfusk, forskningsfinansiering, kemikaliepolitik och återvinning.

Foto: Rebecka Andersson

Petra Jankov Picha

Petra Jankov Picha är digital strateg och kommunikatör med bakgrund som journalist på bland annat Expressen och TV4. Hon jobbar sedan år 2001 med opinionsbildning, strategier, kampanjer, kommunikation och sociala medier i idéburen verksamhet, exempelvis på Svenska Journalistförbundet. Hon har även varit redaktör för boken Framtiden har redan varit här, om framtidens journalistik, och är författare till boken Konsten att bokblogga.

Foto: Ola Gäverth

Fredrik Laurin

Fredrik Laurin är journalist och arbetar som redaktör på Sveriges Television. Han har tidigare varit undersökande reporter på bland annat Uppdrag Granskning (SVT), Ekot (Sveriges Radio P1) och Kalla Fakta (TV4). Fredrik Laurin har tilldelats Stora Journalistpriset tre gånger för Årets Avslöjande. Han har även fått föreningen Grävande journalisters pris Guldspaden vid tre tillfällen. Laurin har dessutom mottagit internationella priser från Investigative Reporters and Editors (IRE) och Overseas Press Club of America.

Foto: Magnus Bergström CC-BY

Anders Thoresson

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

Foto: Sebastian LaMotte CC-BY ND

Digitalt källskydd
En introduktion
IIS internetguide, nr 35. 2016.
Sus Andersson, Petra Jankov Picha, Fredrik Laurin och
Anders Thoresson.

IIS klimatkompenserar för sina koldioxidutsläpp och stödjer klimatinitiativet ZeroMission.

Författare: Sus Andersson, Petra Jankov Picha, Fredrik Laurin
och Anders Thoresson.
Redaktör: Hasse Nilsson
Projektledare: Jessica Bäck
Formgivning: AGoodId
Tredje upplagan
ISBN: 978-91-7611-857-3

Du hittar alla IIS utgivna internetguider på internetguider.se

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 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!

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.

Kom igång med Tails!
Av: Anders Thoresson

Tails är ett portabelt operativsystem som är byggt för att skydda din integritet. All kommunikation går via Tor-nätverket, och all kommunikation som inte är anonym blockeras. Det installeras i regel inte på hårddisken utan till exempel på en usb-pinne. Det gör att du kan använda allmänna datorer på internetcaféer eller bibliotek utan att lämna spår efter dig.

I den här guiden lär du dig:
- Vad operativsystemet Tails är
- Hur Tails hänger ihop med anonymiseringsverktyget Tor
- Hur du installerar Tails
- Att använda Tails