Digital sikkerhed for journalister

Som journalister har vi et ansvar for at beskytte vores kilder, kommunikation og arbejde, også når det foregår digitalt. Dette kapitel giver en introduktion til, hvordan vi integrerer den digitale sikkerhed i vores journalistiske hverdag og vælger de rigtige værktøjer til at beskytte os mod overvågning og andre trusler.

Klokken er to om natten, og journalist Mads Ellesøe og hans kæreste er faldet i søvn på deres hotelværelse i Marokko, da det banker hårdt på døren. Udenfor står seks bevæbnede mænd. De er i civilt tøj, men siger, at de kommer fra de marokkanske myndigheder, og beordrer parret til at samle deres ting og følge med dem.

Mads Ellesøe er freelancejournalist, og blot to dage forinden har P1 Dokumentar sendt hans udsendelse om Marokkos besættelse af Vestsahara, et stærkt kontroversielt emne for det marokkanske styre. De seks mænd fortæller, at de har fulgt Ellesøes bevægelser allerede inden han samme dag igen ankom til landet. Denne rejse var egentlig bare en ferierejse, men nu bliver Mads Ellesøe og hans kæreste kørt væk og forhørt i flere timer.

Da solen begynder at stå op, bliver de fulgt til lufthavnen, hvor de får udleveret deres bagage, computere og telefoner med en kontant besked på at tage det næste fly hjem. Først her opdager Mads Ellesøe, at sim-kortet mangler i hans og kærestens telefoner, og at harddisken er fjernet fra deres computere.

“Jeg tænkte bare ‘fuck!’ Det var jo min eneste computer, så der lå alt muligt – interviews med lokale, arbejdsdokumenter og masser af private fotos. Jeg havde slet ikke tænkt på at kryptere den. Det var en enormt ubehagelig følelse, at de nu havde adgang til det hele,” fortæller han i dag.

Anholdelsen i Marokko var i 2010, og selvom både DR og Dansk Journalistforbund går ind i sagen, ser Mads Ellesøe aldrig harddiskene eller sim-kortene igen.

“Men efterfølgende begyndte jeg at kryptere min computer, og på et tidspunkt havde jeg også en særlig rejsecomputer, hvor jeg ikke havde alle mine andre filer på. Det var virkelig et wakeupcall,” siger Mads Ellesøe.

Hans fortælling er voldsom, men der er et enkelt element, der ikke er unikt. Mange journalister begynder nemlig først at tænke over deres digitale sikkerhed, når den er blevet kompromitteret – og så er det ofte for sent.

Dette kapitel handler om, hvordan du tænker den digitale sikkerhed ind i din journalistiske arbejdsproces til hverdag, så du ikke først skal tænke på den, når det brænder på.

Det er hverken særligt teknisk kompliceret eller besværligt, men snarere et spørgsmål om vane. Vi skal låse vores computer og kommunikation, lidt ligesom at vi skal huske at låse vores cykel, hvis vi vil være sikre på, at vi ikke mister den.

Indledning

Som journalister har vi pligt til at beskytte vores kilder, kontakter og materiale.

I dag, hvor langt det meste af vores kommunikation og arbejde foregår digitalt, er det derfor afgørende at vide, hvordan vi beskytter vores digitale kommunikation, research og materiale. Det gælder uanset om vi dækker lokalnyheder eller storpolitik eller om vi rejser i konfliktområder.

Den digitale sikkerhed er dog især vigtig for undersøgende journalister, der ofte arbejder med sensitive kilder og historier, hvor der er meget på spil, hvis kilder eller oplysninger bliver afsløret.

Samtidig er vores digitale sikkerhed under pres fra mange sider.

Arbejdsgivere, internet- og teleudbydere, it-kriminelle og firmaer bag de webtjenester, vi bruger, er blandt de aktører, der har adgang til information om hvad vi søger efter på nettet, hvem vi kommunikerer med, hvornår og hvorfra kommunikationen foregår og hvad den indeholder.

I Danmark har vi vidtgående logningsregler, som pålægger internet- og teleudbyderne at gemme, eller logge, oplysninger om brug af deres tjenester i mindst et år. Logningen omfatter oplysninger om, hvilke apparater der kommunikerer og hvor de er placeret, når kommunikationen finder sted, samt masteoplysninger om hvilke master vores mobiltelefoner bruger, når vi ringer, sms'er eller bruger internettet.

Politiet og PET kan kræve disse oplysninger udleveret fra internet- og teleudbyderne eller selv iværksætte målrettet overvågning af alle aktiviteter på udvalgte computere og telefoner. Det skal ske i forbindelse med en efterforskning og kan både rette sig mod mistænkte i en sag, og alle, der kan tænkes at kommunikere med mistænkte. Her er det vigtigt at huske på, at brud på tavshedspligten eller udlevering af fortrolige oplysninger også kan blive regnet som kriminelt.

Indgrebene kræver som udgangspunkt, at de bliver godkendt af en dommer, men politiet får meget sjældent nej til anmodninger om indgreb i meddelelsesfriheden, som det kaldes.

Kilder, kolleger og kontakter i andre lande kan arbejde under forhold med andre og endnu mere vidtgående overvågningskapaciteter.

Og på mange arbejdspladser har arbejdsgiveren adgang til de ansattes telefoner eller e-mails.

Uanset situationen skal vores kilder kunne stole på, at vi holder kommunikationen med dem fortrolig – også når den foregår digitalt. Derfor er det vigtigt, at vi ved, hvordan vi beskytter os selv og vores kilder mod overvågning og digitale fingeraftryk, der senere kan spore en afsløring tilbage til afsenderen. Hvis ikke vi ved det, bringer vi vores kilder i fare. Vi risikerer også, at de ikke tør komme til os, så vigtige historier måske aldrig kommer til offentlighedens kendskab.

Tip! Selvom den digitale sikkerhed er vigtig, er der mange journalister, der ikke helt har styr på den. Som nyuddannet journalist eller praktikant kan du derfor nemt blive first mover og bidrage med vigtig viden på redaktionen, hvis du sætter dig ind i emnet.

1. Sikkerhedsbevidsthed i hverdagen

Digital sikkerhed handler ikke først og fremmest om værktøjer.

Særligt efter NSA-whistlebloweren Edwards Snowdens afsløringer af global masseovervågning er der kommet en mængde nye programmer på markedet, som lover at løse alverdens sikkerhedsproblemer på forskellige måder; det kan være som en krypteret e-mail-tjeneste, en VPN eller andet. Selvom mange af dem sikkert fungerer fint, har de det tilfælles, at du som bruger skal sætte vores din lid til udbyderen. Det giver dig mindre kontrol over din data.

Samtidig er det vigtigt at forstå, at **forskellige situationer kræver forskellige værktøjer**. Der er ikke nogen enkelte værktøjer, der kan løse alle sikkerhedsproblemer på en gang.

I nogle tilfælde vil du måske bruge krypteret e-mail til at kommunikere med en kilde, men hvad hvis kildens største problem er, at hendes arbejdsgiver har adgang til hendes e-mailkonto? Så hjælper det ikke meget, at du har krypteret e-mailen. Så handler sikkerhed måske om noget så simpelt som at kilden skal lade være med at bruge sin arbejdsmail. Eller hvad hvis kilden er i et land, hvor alene det at have krypteringsværktøjer på sin computer er nok til at rette myndighedernes fokus mod én? Så må du tænke i andre baner. I andre tilfælde kan det være, at du skal beskytte data på en harddisk, mens du rejser i et konfliktområde, ligesom Mads Ellesøe. Eller skjule din færden, når du researcher på en bestemt hjemmeside.

Overvågningen og andre trusler mod den digitale sikkerhed forandrer sig hele tiden, og det samme gør de værktøjer, der kan beskytte dig.

Ofte har du slet ikke brug for teknisk komplicerede værktøjer, men for simple, logiske løsninger. Det kan være at lade telefonen blive hjemme, når du skal mødes med en kilde, eller huske kilden på at bruge noget andet end sin arbejdsmail til at kommunikere med dig.

Derfor er det væsentlige ikke, hvilke værktøjer du bruger, men at kunne forstå og analysere udfordringerne og lægge en realistisk plan for, hvordan du imødegår dem. Så bliver du i stand til at vælge den rigtige *type* af værktøjer.

Det er særlig vigtigt at vi som journalister vænner os til at tænke den digitale sikkerhedsbevidsthed ind i vores journalistiske hverdag.

Hvis du først begynder at tænke over din digitale sikkerhed, når du har en historie eller materiale, der kræver særlig beskyttelse, kan det allerede være for sent. Desuden kan dét pludselig at begynde at bruge en masse krypteringsprogrammer i sig selv være en adfærdsændring, der kan tiltrække uønsket fokus.

Derfor er det vigtigt, at du implementerer nogle sikkerhedsrutiner i din hverdag allerede nu. Det bør være rutiner, der er så overskuelige at følge, at du ikke begynder at finde nemme smutveje uden om dem, fordi de gør dit arbejde for besværligt.

Hvis du arbejder sammen med kolleger eller andre kontakter om en historie, kan det være en god idé at lægge en sikkerhedsplan, som alle er indforståede med og istand til at følge. Sikkerhed er kun så god som det svageste led i kæden.

Endelig skal du huske, at digital sikkerhed ikke kun handler om, hvad der sker på din computer og telefon, men også om din adfærd. Overraskende meget sikkerhed er blevet kompromitteret, fordi en journalist kom til at tale over sig på et værtshus, lade computeren stå åben på et cafébord eller logge på et ukendt hotspot under en rejse.

Fakta: Open Source
De fleste af de værktøjer, der anbefales i denne bog, er enten værktøjer, der følger gratis med dit styresystem, eller gratis open source-programmer. Det betyder, at dem, der har lavet programmet, har gjort kildekoden offentligt tilgængelig, så alle kan se, hvordan programmet er lavet, hjælpe med at opdage eventuelle sikkerhedsbrister og være med til at videreudvikle det. Når du vælger, hvilke sikkerhedsløsninger du vil bruge, er det altid en god idé at gå efter open source-programmer, som er gennemprøvede, har været på markedet et stykke tid og bliver jævnligt opdaterede. Tjek, hvordan programmet og firmaet bag bliver omtalt andre steder på nettet – får de positiv omtale fra andre, der

beskæftiger sig med digital sikkerhed, eller er de tidligere blevet kompromitterede eller har givet efter for pres fra efterretningstjenester?

Trusselsvurdering
Når du skal vælge, hvilke værktøjer du skal bruge for at beskytte din digitale sikkerhed, må du gøre dig klart, hvad du ønsker at beskytte og mod hvem.

Forskellige scenarier kræver forskellige værktøjer og sikkerhedsniveauer. Ved at lave en trusselsvurdering kan du vurdere hvilke værktøjer, der er brug for i din konkrete situation. Her er fem centrale spørgsmål til en god trusselsvurdering:

1. Hvad vil jeg beskytte?
2. Hvem vil jeg beskytte det imod?
3. Hvordan kan modparten tænkes at angribe?
4. Hvor sandsynlig er risikoen?
5. Hvordan kan jeg forhindre det?

Din trusselsvurdering kan du bruge som udgangspunkt, når du lægger en sikkerhedsplan, alene eller sammen med dine kolleger.

2. Beskyt dit udstyr

Vi går nu i gang med de konkrete værktøjer til digital sikkerhed. Det første, du skal tænke over, er at beskytte dit it-udstyr. Det er hardware, altså de fysiske dele som computer, telefon, eksterne harddiske, usb-drev og så videre, og software, altså programmerne på maskinerne.

At beskytte dit udstyr er lige så vigtigt som at beskytte din kommunikation.

For at sammenligne med sikkerhed i den fysiske verden: Din ven sender dig et fortroligt brev, som er lagt i en kuvert, for at postbudet ikke kan læse med. Men når du har åbnet kuverten og læst brevet, ligger det fremme på dit bord. Derfor er det også vigtigt, at du har en god lås på dit hus, så man ikke bare kan gå ind ad bagdøren og læse det åbne brev.

Fuld diskkryptering er det værktøj, du bruger til at låse dit udstyr – ligesom du har en lås på dit hus. Det gælder både for din computer og din telefon.

Selvom du har en adgangskode på din computer eller telefon, er der stadig mange måder at bryde ind i dem på, hvis du mister dem, også selvom det er slukket. Man kan for eksempel sætte din harddisk over i en anden computer og på den måde få adgang til alle dine filer alligevel, sådan som vi så de marokkanske myndigheder gøre med Mads Ellesøes harddisk i starten af dette kapitel.

Du kan sikre dig imod den type angreb ved at slå fuld diskkryptering til. Det betyder, at al data på din computer eller telefon er krypteret, når computeren eller telefonen er slukket.

Fuld diskkryptering på computeren
Når du slår fuld diskkryptering til på din computer, skal du bruge en adgangskode. Den giver dig adgang til den krypterede disk. Det gør det vigtigt, at du har en stærk kode, som man ikke kan bryde. Og så er det ekstra vigtigt, at du er *helt sikker* på, at du ikke mister eller glemmer din adgangskode. Hvis du glemmer din adgangskode, mens du har fuld diskkryptering slået til, mister du adgangen til dit materiale fuldstændigt.

Derfor er det en rigtig god idé at tage en backup af din data, inden du slår fuld diskkryptering til. Din backup kan også være krypteret.

Apples program til fuld diskkryptering hedder FileVault og kommer som en del af alle nyere versioner af styresystemet OS X.

På Apple-computere har du også mulighed for at lave en krypteret backup med systemets eget backup-program, Time Machine. Sørg for jævnligt at tage en krypteret backup på en ekstern enhed som for eksempel en harddisk og opbevar den et sikkert sted.

Det er desværre ikke helt så ligetil at lave fuld diskkryptering på Windows-computere som på Mac.

Nogle Windows-versioner har diskrypteringsværktøjet BitLocker inkluderet.

Du bør som udgangspunkt bruge en af disse versioner. Hvis du ikke har BitLocker på din Windows-computer, kan du i stedet styrke din sikkerhed en smule ved at skifte den adgangskode, du skal skrive, når du tænder computeren. BitLocker giver også mulighed for krypteret backup.

Hvis du har slået fuld diskkryptering til, har du forhindret Apple eller Windows i at få adgang til din data, hvis du mister computeren, samtidig med at du bruger krypteringsværktøjer, der kan lukke adgangen til din data. Derfor er backup endnu vigtigere end det plejer at være.

Fuld diskkryptering på telefonen
På de fleste nyere smartphones er fuld diskkryptering allerede slået til som standardindstilling. Du kan tjekke om din telefon er krypteret i dens indstillinger.

På ældre telefoner skal du slå fuld diskkryptering til manuelt. Det gør du også under indstillinger.

På nogle telefoner har har du også mulighed for at indstille telefonen til at slette dine data efter et bestemt antal mislykkede forsøg på indtastning af adgangskoden. Det er risikabelt, fordi du kan miste din data, hvis du selv for eksempel forsøger at logge ind flere gange med den forkerte finger. Men du kan for eksempel bruge funktionen, hvis du rejser i et område eller arbejder med en historie, hvor du har grund til at frygte, at nogen vil konfiskere din telefon og forsøge at bryde ind i den.

De fleste nye telefoner bruger biometriske adgangskoder såsom fingeraftryk, ansigtsgenkendelse eller iris-scanner. Det kan virke skræmmende, men for de fleste brugere er det faktisk mere sikkert end en almindelig adgangskode. Det skyldes, at du er bedre beskyttet mod at nogen aflurer din kode ved at kigge dig over skulderen mens du tasterne, eller gætter den, fordi den er for nem.

Som med al anden digital sikkerhed er det den konkrete situation, der afgør, hvad der er den mest sikre løsning.

Du kan være i en situation, hvor en modpart kan tvinge dig til at åbne din telefon, enten med fysisk magt eller trusler om retsforfølgelse. I sådanne tilfælde kan det være en fordel i stedet at slå en adgangskode manuelt til, hvis du mener, at du kan undgå at udlevere den. Det gør du under telefonens indstillinger.

I nogle lande har myndighederne også lovhjemmel til at tvinge dig til at åbne telefonen med ansigtsgenkendelse, men ikke til at udlevere din adgangskode.

Hvis du er i en situation, hvor du vurderer, at du kan blive tvunget til at låse din telefon op uanset om du bruger en manuel eller en biometrisk adgangskode, kan det i stedet være en fordel at slette det følsomme indhold fra telefonen og så åbne den, når du bliver bedt om det.

Hvis du er i en situation, hvor det er sikrest for dig at have en manuel adgangskode frem for biometrisk på din telefon, bør du bruge en kompleks kode på mindst otte cifre. De fleste modparter har udstyr som kan knække koder, og en standardkode på kun fire cifre er hurtig at knække.

Gode sikkerhedsvaner
Når du har installeret fuld diskkryptering på dit udstyr, er det vigtigt, at du også holder dit udstyr opdateret og beskyttet mod malware. Du skal have gode sikkerhedsvaner.

For det første skal du huske at opdatere dit styresystem på computeren og telefonen. På det meste nyere udstyr får du notifikationer, når det er tid til at installere en systemopdatering. Og selvom det sjældent kommer på et belejligt tidspunkt, så er det faktisk en af de bedste måder at sikre, at du har det nyeste og mest effektive bolværk mod virus og andre digitale angreb udefra.

For det andet skal du sørge for altid at opdatere til den seneste version af de kryptografiske værktøjer, de programmer og det styresystem, du bruger. Mange kryptografiske værktøjer fungerer slet ikke med forældede versioner af programmer og styresystemer, og producenterne tilbyder eksempelvis ikke sikkerhedsopdateringer til dem. Det er en god idé også at følge med i, hvad der bliver skrevet på nettet om de programmer og it-løsninger, du bruger, og i de opdateringer, som producenterne bag dem sender ud.

Det er også en god idé at slå din firewall til. En firewall er et program, som forhindrer uautoriseret adgang til og fra internettet på din computer. Den beskytter mod malware, som du ikke selv giver adgang, og mod at programmer udleverer data fra din computer til tredjeparter.

3. Stærke koder

At vælge stærke kodeord og bruge dem rigtigt er helt centralt i digitalt selvforsvar. Du skal bruge en stærk adgangskode til din computer, men du kommer også til at bruge stærke koder mange andre steder, på din e-mail-konto, dine sociale medier og så videre.

Desværre bruger mange i dag kodeord, som er meget nemme at gennemskue, fordi de skal være til at huske for den menneskelige hjerne. Computere er i dag så hurtige, at de kan bryde selv helt tilfældige kodeord, hvis de er kortere end 14 karakterer. Kodebrydningsprogrammer kan tjekke millioner af kodeordskombinationer i sekundet og arbejde i mange dage på mange simultane maskiner. De kan søge både på den computer, der er under angreb, og på offentligt tilgængelig information om ejeren, så hvis du på et tidspunkt har gemt kodeordet på din computer eller hvis du har brugt personlig information som eksempelvis din fødselsdato, er det nemt at knække. Programmerne bruger ordbøger på forskellige sprog og kender de gængse erstatninger med symboler i stedet for bogstaver, som @ for a, $ for s og så videre.

En stærk kodesætning er en, som denne proces ikke kan knække.

Her er tre hovedregler til stærke kodesætninger:

1. **Lang:** Din kodesætning skal være over 14 karakterer lang. Jo længere en kode er, jo sværere er den at knække. Derfor er det vigtigere, at koden er lang, end at den for eksempel er kompliceret med forskellige tegn og tal.
2. **Uforudsigelig:** Den skal kun være kendt af dig, og være nem for dig selv at huske og taste korrekt. Men også så uforudsigelig at den er umulig for andre at gætte – selv for folk, der kender dig godt.
3. **Unik:** Du bør undgå at genbruge kodesætninger flere steder for at minimere skaden, hvis en af dem bliver knækket.

Senere i dette kapitel kan du læse om, hvordan du bruger en password manager til at opbevare de fleste af dine koder. Men der er enkelte koder, som du er nødt til at kunne huske i hovedet. Det gælder koden til at åbne din computer, din password manager, dit backup drev og måske også særligt vigtige krypterede USB'er eller filer.

Det kan også være en god idé at kunne huske koden på den mailadresse, der bliver skrevet til, hvis du beder om nulstilling af dine koder på eksempelvis webtjenester, så du har en måde at genskabe koderne på.

Disse vigtige kodesætninger bør kun være gemt i din menneskelige hukommelse og skal derfor kunne huskes. Samtidig må de ikke være mulige at knække med et kodebrydningsprogram.

Box: Schneiers system

En af de mest brugte metoder til at komponere ubrydelige kodesætniger er Schneiers system, som er opfundet af den amerikanske kryptograf Bruce Schneier. Metoden går ud på at tage en sætning, man kan huske, og erstatte ordene med initialer, symboler og tal for at gøre det til en kodesætning. Sætningen bør indeholde både bogstaver, symboler og tal og være på mindst 14 tegn.

Du bør vælge en sætning, som er noget personligt, du kan huske, men som ikke er åbenlyst relateret til dig gennem offentligt tilgængelig data. Det kan for eksempel være en oplevelse eller en sang, som betyder noget særligt for dig.

For eksempel kan sætningen "Oppe i Norge, der boede tre trolde, Trolde-far og Trolde-mor og lille Olle-Bolle" blivet til "OiN,db3t,T-f&T-m&lO-B".

Du skal selvfølgelig undgå at vælge en sætning, der har været brugt før og sørge for at kunne huske, hvornår du har brugt store og små bogstaver og så videre.

En anden metode er Diceware-metoden, der er baseret på en lang ordliste med ord, som hver står ud for femcifrede numre sammensat af tallene 1 til 6. Ved at slå med en terning og følge listen kan du sammensætte en sætning af tilfældigt udvalgte ord, som er umulig at bryde, men nem for dig at huske.

Password manager

Vi bruger rigtig mange koder til alt fra Netflix til netbank, og det er umuligt at huske alle sammen. Derfor bør du bruge en password manager. Det er et program, som hjælper med at skabe og gemme et stort antal af stærke kodeord sikkert. Programmet hjælper også med at finde på stærke kodeord, som er så komplekse og tilfældige, at de er umulige at gætte.

Det fungerer samtidig som et slags krypteret pengeskab for alle dine kodeord, som det beskytter med et enkelt masterkodeord. Når du skal bruge et af kodeordene, kan du åbne pengeskabet og finde dem, men du behøver kun at huske det ene masterkodeord til password manageren. Det vil sige, at du i princippet kan nøjes med at huske to gode, stærke kodeord til din computer: Det, der lukker computeren op, og det, der lukker password manageren op.

Password manageren KeePassX er gratis og open source, og så adskiller den sig fra de fleste andre password managere ved at være opbevaret på din computer i stedet for i skyen. Det giver dig en smule mere kontrol over dataen. Omvendt kan det også gøre brugen mere besværlig, fordi den ikke kan synkronisere dine koder mellem for eksempel din telefon og computer, og brugerfladen på KeePassX fremstår en smule forældet.

Hvis du gerne vil bruge en skybaseret, mere brugervenlig password manager, kan du i stedet bruge LastPass eller 1password. Ingen af dem er open source, men de er begge alligevel anbefalet af mange sikkerhedseksperter. LastPass er gratis, mens 1password koster har et lille månedligt abonnement.

4. Beskyt din kommunikation

Når du har styr på at beskytte dit udstyr, kan du gå videre til at sikre din kommunikation.

Hvis du ikke krypterer din kommunikation, svarer det til at sende din besked afsted over nettet på et åbent postkort. Alle, der håndterer beskeden undervejs, kan læse med. Det gælder både den tjeneste, du bruger til at sende beskeden, din internetudbyder, modtagerens internetudbyder og eventuelle udefrakommende aktører, som opsnapper beskeden undervejs.

Når du krypterer beskeden svarer det til at lægge den i en lukket kuvert. Så er selve indholdet af beskeden skjult og forseglet, så kun du og modtageren kan læse med.

Den sikreste måde at kryptere sin kommunikation er med det man kalder end-to-end-kryptering. Det er en krypteringsform som sikrer, at det kun er afsenderen i den ene ende og modtageren i den anden ende, der kan læse den krypterede information.

End-to-end-kryptering bliver sikret med krypteringsnøgler, som opbevares lokalt på afsenderens og modtagerens udstyr. Et helt grundlæggende princip i end-to-end-kryptering er derfor, at begge parter skal have det samme slags krypteringsprogram for at kunne kommunikere med hinanden.

Et rigtig godt værktøj er den gratis end-to-end-krypterede app Signal. Du finder den i din App Store under Signal – Private Messenger.

Kommunikation med Signal foregår over internettet og ikke telefonnettet. Ligesom med al anden end-to-end-kryptering gælder det, at alle deltagere i kommunikationen skal have Signal installeret. Computere og telefoner kan sagtens kommunikere med hinanden, men begge parter skal bruge Signal.

Signal er udviklet af open source non-profit-firmaet Open Whisper Systems. Der er flere gode grunde til, at det er et rigtig godt værktøj.

For det første er det open source. Det betyder, at det er nemt for uafhængige it-sikkerhedseksperter at teste programmet, så man ikke risikerer fejl og sikkerhedsbrister.

For det andet er Signal virkelig nem at installere og bruge. Det betyder, at du let kan instruere kilder, kolleger og andre kontakter i at bruge Signal, og ikke risikerer at de skipper den sikre kommunikation, fordi værktøjerne er for besværlige. For eksempel kan du på din eller dit medies kontaktside skrive et telefonnummer på en telefon, der har Signal. Derefter kan du med ganske få linjer instruere potentielle kilder i at installere appen og sende dig følsomme oplysninger og lignende på det nummer.

For det tredje er den utroligt sikker. Vi ved fra afsløringer af fortrolige dokumenter, at end ikke USA's efterretningstjeneste NSA kan bryde Signals kryptering, og appen bliver anbefalet af Edward Snowden og en lang række andre sikkerhedseksperter.

Og for det fjerde – og næsten vigtigst: Signal gemmer meget lidt såkaldt metadata, meget mindre end andre krypteringstjenester. I 2016 forsøgte det amerikanske forbundspoliti FBI med en dommerkendelse at få Signal til at udlevere en række oplysninger om nogle af Signals brugere. Men af det udleverede materiale kan man se, at Signal kun opbevarer to oplysninger om deres brugere: Hvornår de første gang tog Signal i brug og hvornår de sidst brugte appen. Alle andre oplysninger – som navn, hvem der kommunikeres med, hvornår der kommunikeres, tilknyttede ip-adresser osv. – opbevarer firmaet simpelt hen ikke.

Når du bruger Signal er alt – både indhold, metadata og eventuelle vedhæftede filer eller billeder altså krypteret med end-to-end-kryptering.

Du kan bruge Signal til at ringe, videochatte og sende beskeder krypteret. Man kan vedhæfte filer og billeder og lave gruppesamtaler præcis som med en e-mail, og den kan bruges både på smartphones og i en desktop-version på computeren.

Tip! En nem måde at udveksle fortrolig information med en kilde, er hvis kilden åbner jeres samtale i Signal og tager et billede af dokumentet eller sin computerskærm med kamerafunktionen i appen. På den måde blive billedet ikke lagret i hverken hendes eller din kamerarulle, og hun undgår at sætte digitale fingeraftryk ved at printe eller sende dokumentet.

Der er også en del ekstra muligheder i Signals indstillinger, hvor du blandt andet kan sætte læste beskeder til at forsvinde efter et bestemt tidsrum, sætte en ekstra lås på programmet og tilføje andre sikkerhedslag.

Signal er på mange måder mere sikker end for eksempel krypteret e-mail, fordi den er lettere at bruge og gemmer mindre metadata.

Der kan dog også være situationer, hvor det ikke giver mening at bruge Signal. Det kan for eksempel være, hvis du eller din kontakt er i et land eller en situation, hvor alene det at have en app som Signal på sit udstyr kan være inkriminerende. Det kan også være, at du opererer i en situation, hvor dine kontakter ikke har råd til at have det relativt nye udstyr der skal til for at bruge Signal. Eller at dine kilde er så lidt tech-savvy, at selv det at installere Signal er for stor en mundfuld.

I sådanne situationer kan det være et alternativ at bruge for eksempel WhatsApp eller Messenger-appens "hemmelig samtale"-funktion, som du finder ved at klikke på navnet på den person, du chatter med i Messenger.

Begge disse løsninger bruger Signals krypteringsprotokol, så indholdet af samtalen er lige så sikkert, som hvis du bruger Signal. Problemet er, at de lagrer meget mere metadata. Det er for eksempel data om hvem du kommunikerer med, hvornår du kommunikerer med dem, og hvor du befinder dig, mens

du gør det. Det kan være langt mere afslørende end eksempelvis indholdet af kommunikationen. En anden ulempe er, at ingen af tjenesterne er fuldt ud Open Source-baserede. Det betyder, at det er sværere end hos for eksempel Signal at tjekke efter, om der for eksempel er skjulte bagdøre.

Det samme gælder Telegram, en tjeneste som er baseret i Dubai og udviklet af russiske it-folk. Her kan man vælge at kryptere sine samtaler med Telegrams egen krypteringsprotokol. Mange sikkerhedseksperter fraråder at bruge Telegram, blandt andet fordi de bruger en krypteringsprotokol, som der er fundet en række fejl i.

5. Beskyt din online færden

I takt med at vores datamængder stiger, bliver stadigt mere af vores data opbevaret i "skyen" hos tredjepartstjenester som Google, Facebook, Dropbox og lignende. Det er værdifuldt, og derfor er tredjepartstjenester også nogle af dem, der typisk bliver udsat for angreb.

Der er heldigvis meget du kan gøre for selv at beskytte dine online konti mod digitale angreb.

For det første kan du sørge for at have en stærk kodesætning og undgå at genbruge kodesætninger flere steder, som tidligere beskrevet i dette kapitel.

For det andet kan du sørge for, at holde dine online konti så sikre som muligt. Til det skal du bruge totrinsbekræftelse eller to-faktor-autentifikation (2FA), som det også er kendt som.

Totrinsbekræftelse betyder, at der er et ekstra trin med bekræftelse, når nogen forsøger at logge på en af dine online konti på en computer eller telefon, der ikke har været logget på disse konti før.

Dette ekstra trin finder sted på et andet medie, som hackeren ikke har kontrol med. Det kan for eksempel være, at der bliver sendt en SMS til din telefon med en bekræftelseskode, som du skal taste ind. Eller det kan være at du har et printet ark med bekræftelseskoder, som du skal bruge, ligesom du kender det fra nøglekortet til det offentlige Nem-ID.

Næsten alle store online-tjenester har en form for totrinsbekræftelse, som man kan slå til.

Surf anonymt
En anden situation, hvor du kan have brug for at beskytte din online færden, er når du besøger forskellige hjemmesider. Når du går på nettet med en almindelig browser som Chrome, Safari eller Firefox, bliver data om hvilke hjemmesider, du besøger, og hvad, du søger efter, registreret. Gennem din IP-adresse kan din færden på nettet spores tilbage til det kontor eller den café, du kobler på nettet fra. Det kan være et problem, hvis du som journalist for eksempel researcher på virksomheder eller organisationer, hvor du ikke har lyst til at enten de selv eller andre skal kunne se, at de har fået besøg fra den IP-adresse du sidder på arbejdsplads.

Det kan du beskytte dig mod ved at installere den anonyme open source-browser Tor.

Tor-browseren fungerer stort set som andre browsere, men trafikken bliver sendt krypteret gennem en række Tor-servere rundt omkring i verden i stedet for at foregå direkte mellem brugeren og de hjemmesider, hun besøger. Det betyder, at trafikken ikke kan spores tilbage til afsenderens ip-adresse. Når du går på nettet med en Tor-browser, kan ingen – heller ikke Tor-netværket selv – spore, hvilke hjemmesider du besøger, eller hvad du søger efter på internettet.

Tor anonymiserer, men krypterer ikke. Hvis du sender en email eller skriver en chatbesked, mens du bruger Tor, vil indholdet altså stadig være ukrypteret med mindre du gør noget for at kryptere det.

Husk, at det kun er din internettrafik, der bliver anonymiseret, når du bruger Tor. Hvis du bruger Tor-browseren til at logge ind på tjenester som Facebook eller Gmail, kan de sider eller firmaer naturligvis stadig se, hvad du foretager dig, mens du er logget ind – de kan blot ikke se, hvor du befinder dig.

Hvis du gerne vil sløre din IP-adresse, kan du også bruge en VPN-forbindelse. En VPN er en tjeneste, som du kan bruge til at koble på et netværk med en krypteret forbindelse, der slører din IP-adresse. Det betyder, at du kan omdirigere din trafik og for eksempel omgå de blokeringer, der kan være for bestemte typer indhold i bestemte lande. Den store forskel i forhold til Tor er dog, at VPN-tjenesten selv kan se al den internettrafik, der går igennem den.

6. Sådan bliver journalister hacket

Nu har du læst om, hvordan du beskytter dig, når nogen forsøger at "brute force" sig adgang til din data ved at knække dine koder, få tredjepartstjenester til at udlevere oplysninger og lignende. Men mange digitale angreb sker på en langt snedigere måde, nemlig ved at lokke dig til uforvarende selv at installere malware eller udlevere dine adgangskoder ved at fiske dem ud af dig. Det kalder man for phishing.

Du kan både blive udsat for bredspektret og målrettet phishing.

Den bredspektrede phishing er, når hackere sender den samme type besked ud til en hel masse mennesker, i håbet om, at nogle få bider på krogen. Den målrettede phishing kan være langt mere sofistikeret, og tage afsæt i din helt konkrete situation som journalist.

I 2016 skabte hackere en falsk online persona ved navn Safeena Malik for at infiltrere journalister og NGO'er, der dækker menneskerettighedssituationen i Qatar. Amnesty Internationals sikkerhedsekspert beskriver i en artikel, hvordan hackerne bag profilen interagerede med personer i NGO-miljøet på sociale medier og kommunikerede over flere år med ofrene for angrebet, inden de sendte et link til et delt Google-dokument, som man skulle logge ind på sin Google-konto for at se. Når folk fulgte linket blev de ledt ind på en side, der til forveksling ligner Google's log in-side. Her blev de så lokket til at udlevere deres e-mail og adgangskode.

Et andet eksempel er den (formodet russiske) hackergruppe, som på den aften, hvor Trump blev valgt, sendte mails til en lang række amerikanske journalister med et dokument, som angiveligt skulle indeholde dokumentation for valgsvindel. Hackerne udgav sig for at være en professor fra det prestigefyldte Harvard-universitet, og mailen var sendt fra en Harvard-mailadresse. I virkeligheden indeholdt dokumentet malware.

Typisk vil phishingangrebene enten forsøge at lede dig hen på en side, hvor du skal udlevere dine kodeoplysninger, eller forsøge at få dig til at downloade en fil, som så er inficeret med et spionprogram.

Disse angreb kan være særdeles svære at gennemskue. Og som journalister kan vi ikke altid bare ignorere tilsendte oplysninger, selvom de virker mistænkelige. Det kan jo være en god historie!

Der er heldigvis et par tommelfingerregler, man kan bruge til at beskytte sig mod phishing:

1. Hold øje med særlige kendetegn
Selvom phishing-forsøget er godt lavet, vil der være små kendetegn, der afslører, at noget er galt.

Det kan for eksempel været webadressen, eller URL'en. Hvis phishing-forsøget er designet sådan, at det skal lokke dig ind på en hjemmeside, der giver sig ud for at være noget andet end den – for eksempel log-in-siden til din Google-konto, Facebook-konto eller lignende – vil den typisk være designet som en nøjagtig kopi af disse sider. Men URL'en, altså adressen på hjemmesiden øverst i browseren, vil typisk være en lille smule anderledes.

Hvis du er i tvivl om hvorvidt et link er "phishy" er den sikreste måde altid at logge direkte på den tjeneste, du skal ind på. Hvis du for eksempel har fået et link til noget, der er delt i Google Docs tilsendt i en e-mail, skal du ikke følge linket, men i stedet åbne en browser og logge dig på Google Docs via Gmails' eller Googles normale login-side og logge på ganske som du plejer. Hvis der virkelig er tale om noget, der er delt med dig i Google Docs, kan du så se det her.

Andre særlige kendetegn kan være at du skal downloade et program for at kunne tilgå filen eller at der er underligt sprogbrug.

2. Luk filer op i skyen
Hvis phishing-forsøget er en fil, der er sendt til dig, som du skal åbne, kan det være inficeret med malware, som spreder sig til resten af din computer eller telefon. Men i stedet for at åbne filen på dit eget udstyr, kan du åbne det på andres.

Det gør du ved at downloade filen og uploade den til en sky-tjeneste, for eksempel dit Google Drev. Der sker nemlig ikke noget ved at downloade den inficerede fil – det er først i det øjeblik, du åbner den, at det går galt. Hvis du uploader filen til en sky-tjeneste som Google Drev og åbner den her, svarer det til, at du åbner den på Googles computere. Og de har kapaciteten til at håndtere vira og anden malware. I dit Google Drev kan du så trygt tjekke om filen er, hvad den giver sig ud for at være, og eventuelt derefter gemme den på din computer.

Når du bruger denne teknik, skal du selvfølgelig være opmærksom på, at du så giver Google adgang til den fil, du uploader.

Hvis først du er hoppet på krogen, kan du uforvarende komme til at lukke hackerne ind i ikke bare dit eget udstyr, men også på fælles netværk med dine kolleger. Der er altså god grund til at være meget påpasselig med phishingangreb.

7. Hvis du har brug for ekstra sikkerhed

I dette kapitel har du fået en introduktion til hvordan du kan sikre din kommunikation og dit arbejde digitalt i hverdagen. Hvis du sidder med den næste Snowden eller en anden kilde eller informationstype, der kræver et ekstra højt sikkerhedsniveau, har du brug for mere avancerede værktøjer.

Min bog Cryptoguide for journalister, Dansk Journalistforbund eller ekspertnetværket Cybernauterne er et godt sted at starte, og ellers har de fleste byer også netværk af søde og engagerede sikkerheds-nørder, som arrangerer såkaldte cryptoparties, hvor du ofte kan få hjælp gratis.

10 gode råd

1. Gør gode sikkerhedsvaner til en del af din hverdag og start før det brænder på
2. Gør sikkerhedsvanerne kollektive i dit team eller på din redaktion
3. Beskyt dit udstyr med fuld diskkryptering
4. Hold dine styresystemer opdaterede
5. Brug stærke kodeord, som kun du kender, til centrale koder som din computer og e-mail
6. Undlad at genbruge koder. Brug i stedet en password manager til mindre centrale kodeord
7. Beskyt din kommunikation med end-to-end-kryptering, for eksempel Signal
8. Beskyt din mail, dine sociale medier og andre online konti med totrinsbekræftelse
9. Pas på phishing. Vær påpasselig med at åbne dokumenter eller logge ind via links du får tilsendt, hvis du ikke kender afsenderen
10. Bed om hjælp fra eksperter, hvis du sidder med noget virkelig sensitivt

Videre læsning

- Freja Wedenborg: Cryptoguide for journalister https://www.cryptoguide.dk/
- Freja Wedenborg og Aslak Ransby: Digital sikkerhed på rejsen https://journalistforbundet.dk/digital-sikkerhed-pa-rejsen
- Electronic Frontier Foundation: Surveillance Self-Defense https://ssd.eff.org/
- The Committee to Protect Journalists: Safety kit https://cpj.org/safety-kit/
- Freedom House årlige landerapport om digitale rettigheder i forskellige lande: https://freedomhouse.org/explore-the-map

Kilder

Guarnieri, C (2014): Operation Kingphish: Uncovering a Campaign of Cyber Attacks against Civil Society in Qatar and Nepal.
https://medium.com/amnesty-insights/operation-kingphish-uncovering-a-campaign-of-cyber-attacks-against-civil-society-in-qatar-and-aa40c9e08852#.nyh6cefzv (hentet 07.06.20)

Lipton, Sanger og Shane (2016): The Perfect Weapon: How Russian Cyberpower Invaded the U.S.
https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html (hentet 07.06.20)

Freja Wedenborg er journalist og forfatter til bogen Cryptoguide for journalister. Hun arbejder som journalist og underviser med fokus på overvågning og digital sikkerhed i ekspertnetværket Cybernauterne. Hun sidder i hovedbestyrelsen for Dansk Journalistforbund.