Kaas & Mulvad | 20.09.21 | Undersøgende journalistik | Datasikkerhed

HUSKESEDDEL

Hvad	Hvorfor	Hvordan
Indfør faste retningslinjer	Start med at foretage en overordnet risikovurdering. Herefter kan du indføre faste retningslinjer for at gøre hverdagen nemmere. Der vil så være nogle situationer, hvor du må beskytte dig ekstra. Det vil være lettere at håndtere, fordi du har en fast praksis at gå ud fra – og kun behøver at justere den.	For eksempel er et råd, at du ikke skal tage mobilen med til møder med fortrolige kilder. Der vil være masser af ikke-fortrolige kilder, hvor du selvfølgelig har den med.
Beskyt renommé	Al din offentlige optræden kan bruges til at miskreditere dig og dine historier. Krav om uafhængighed og habilitet ser kun ud til at blive større med tiden. Det, der i dag virker OK, kan om nogle år være helt forkert.	Vær opmærksom på, hvad du udtaler dig om, og hvad du deler og liker på sociale medier – især Facebook. Ryd op. Tjek og rens dine beskrivelser på LinkedIn.
Krypter kommunikation	Dialog med kilder og samarbejdspartnere foregår over telefon og via chat/e-mail, hvor der kan være filer vedhæftet. Tidligere har krypterede e-mails og beskyttede samtaler været kompliceret og krævet brug af besværlig software. Programmet Signal har overtaget meget af det, men der vil stadig være situationer, hvor krypterede e-mails eller anden beskyttelse er nødvendig. Signal ejes af en nonprofit organisation.	Signal bruges til chat, filoverførsel og telefonopkald. Installer det som app på iPhone eller Android og på Windows PC / Mac. Opret dig som bruger på Signal med det samme, fordi dine kontakter kan se, hvornår du har oprettet dig – og det skal ikke være samtidig som en fortrolig kontakt. Der har tidligere været kritik af Signals manglende sikkerhed på pc'er, men den kritik er begrænset, efter at Signals Chrome-udvidelse er blevet erstattet af en App, der kører uden for browseren. I dag regnes Signal for bedre end WhatsApp, der ejes af Facebook. Se også her.
Slet overførsler	Computeren gemmer overførsler. Pas derfor på følsomme dokumenter, som du henter fra en database eller en anden server.	Husk at slette overførsler og tømme papirkurven, hver gang du slukker computeren.
Brug antivirus	Der er normalt ingen grund til at have særlige antivirus-programmer i dag.	For brugere af PC er Windows Antivirus helt tilstrækkeligt. For Mac-brugere er antivirus også indbygget i dag. Faktisk beskytter det nye Mac-styresystem også mod malware, lover selskabet.

HUSKESEDDEL

Tag ekstern backup	Gem dine filer på en ekstern harddisk som sikkerhed. Back-up i skyen kan være udmærket, men du er afhængig af et kommercielt firma. Køb en 2-4 TB stor harddisk. For eksempel Seagate Expansion Portable. En ekstern harddisk gør det også muligt at tilgå dokumenter uden at bruge wifi. Eksterne harddiske står dog af på et tidspunkt. Derfor lav også en kopi af den eksterne harddisk.	Windows: Brug den automatiske sikkerhedskopiering Klik på Windows -logoet i nederste venstre hjørne Klik på Indstillinger (gear) Klik på "Opdatering og sikkerhed" Klik på "Backup" Klik på "Flere indstillinger" Her kan du indstille, hvad der skal sikkerhedskopieres. Derefter: Sæt den eksterne harddisk i computeren Vælg "Sikkerhedskopier nu". Første gang tager det noget tid at få den grundlæggende kopi oprettet af hele maskinen. Men derefter tager det mindre end et minut. Opbevar den eksterne harddisk et andet sted end dit kontor - i tilfælde af brand eller lignende problemer.
Skjul IP-adresse med VPN	Når du bevæger dig på nettet, sætter du spor. Når du bruger et Virtual Private Network, går du fra din egen computer til en anden server. Du kan selv vælge, hvilket land den server er placeret i. Herefter ser det ud som din trafik kommer herfra. Det er ikke muligt at spore din computer.	Private Internet Access anbefales af flere eksperter. Det er ret billigt. Det samme abonnement kan bruges på flere enheder – herunder iPads og telefoner. Indstil privat internetadgang til at være konstant. Dvs. altid og automatisk. Så kan du altid slå det fra i særlige tilfælde. Der findes mange andre VPN's. Se her.
Krypter videomøder	I ethvert projekt er det nødvendigt med møder. I flere tilfælde foregår det som videomøder. De store leverandører (Zoom, Microsoft Teams, Google Hangout) leverer udmærkede løsninger, men der findes andre og i særlige situationer er kryptering af møder at foretrække.	Jitsi er ganske enkel. Du behøver ikke et abonnement. Du opretter et møde og sender bare et link via Signal. Et andet produkt, som kan det samme er collocall. Hvis man er mange, er GoToMeeting www.goto.com en god løsning (men ikke gratis).
Krypter dele af harddisken	Du skal kun kryptere de filer og biblioteker, der er nødvendige. Som rettesnor for journalister er det fortrolige undersøgelser og biblioteker med personoplysninger, der med GDPR-regler kræves beskyttet. Læg normalt hele biblioteker i den krypterede afdeling (fil), så alt er samme sted.	Microsoft har et indbygget krypteringssystem Bitlocker. Til undersøgende journalistik anbefales ofte VeraCrypt. Der er en enkel guide til VeraCrypt her. Inden du flytter biblioteker permanent til det krypterede område, så test, at du kan lukke og slukke maskinen - og åbne de krypterede biblioteker igen.

HUSKESEDDEL

	Husk at inkludere de krypterede filer i den automatiske backup.	
Anvend Password Managers	Som journalist har du behov for mange passwords. Du vil ikke kunne huske dem i hovedet. En fil på computeren med alle dine password bliver let fundet. En løsning er at have filer med password liggende på et USB-stick og med en kopi og have dem gemt sikre steder. Ikke det samme sted. En anden løsning er en password manager, der holder styr på alle passwords. Du skal kun huske et password for at få adgang til password manageren. I nogle tilfælde er en kombination af de to løsninger det bedste.	Lastpass kan bruges gratis på en enhed, men koster lidt, hvis du vil anvende det på flere enheder, inklusive mobilen, hvad der er langt det nemmeste. Sikkerhedseksperter siger, at KeyPassX er bedre, fordi det ikke gemmer dine data i nogen sky. Der findes også andre password managers, men LastPass er det mest brugervenlige.
Brug to-faktor godkendelse	To-faktor godkendelse bør du anvende overalt, hvor det er muligt. Der findes mange systemer til to-faktor godkendelse. De sender en kode til din email eller mobilnummer. Du skal slå op i en kodegenerator. Eller du får muligheden for at anvende Google Authenticator.	Google Authenticator kan du downloade som App til mobilen. Når du er inde på en webside, der benytter Google Authenticator, viser den gerne en QR-kode, som du kan lade din mobil læse, hvorefter det kører. Et særligt problem er at flytte authenticatoren til en ny mobil. Det kan være ret besværligt og sker normalt ved at klikke på glemt password og gentage opsætningen. Der er en video her. Andre steder skal du skifte til den nye telefon, ved at logge ind med den gamle og derefter på en eller anden måde få mulighed for at scanne en ny stregkode på den nye telefon, hvorefter den gamle ikke længere fungerer.
Gå dybere ned i datasikkerhed	Der er masser af yderligere råd om datasikkerhed. Arbejder du i en virksomhed, organisation eller et konkret projekt vil der normalt være specielle guidelines, som skal følges,	Om at lave en sikkerhedsplan: https://tinyurl.com/p5v3vsr En række sikkerhedsråd til journalister: https://cpj.org/2019/07/digital-safety-kit-journalists/#encrypt Snowdons råd til journalister (ligner denne huskeseddel):

HUSKESEDDEL

		https://theintercept.com/2015/11/12/edward-snowden-explains-how-to-reclaim-your-privacy/ Electronic Frontier Foundation er en nonprofit organisation fokuseret på digital beskyttelse og ytringsfrihed. Der er løbende gode artikler om datasikkerhed: https://www.eff.org/