

# DIN VEJLEDNING TIL DE DIGITALE FORSVARERE MOD DATAINDTRÆNGERE TAG KONTROL OVER DIT LIV PÅ NETTET PRIVATLIV FOR BØRN

[Overskrift]

Internettet. Det er sejt, hurtigt og globalt. Men også komplekst. Nogle gange kan det være svært at se, hvor vi er udsatte – og hvor vores private informationer online kan blive set og brugt af andre. I vores parallelle univers, hvor de DIGITALE FORSVARERE bekæmper de onde DATAINDTRÆNGERE, er det heldigvis nemt at se, hvem der er de gode og hvem der er de onde. [www.edri.org](http://www.edri.org)

[kolofon]

Redaktører for bladet: Kirsten Fiedler, EDRI Theresia Renhold, EDRI

Tegneserier: Gregor Sedlag

Grafik og design af: Gregor Sedlag Heini Jarvinen (EDRI-former illustrationer)

Bidrag af: ApTI Romania Bits of Freedom CCC / Chaos macht Schule Cryptoparty.in Digitale Gesellschaft e. V. EDRI (Brussels office) Open Rights Group Mediamocracy

Særlig tak til: Gloria González Fuster, VrijeUniversiteit Brussel (VUB) Hans Martens, Better Internet for Kids, EUN Partnership AISBL

Dette hæfte blev til takket være:

- Individuelle sponsorer på [GlobalGiving.com](http://GlobalGiving.com) – Tak til jer alle for jeres bidrag!
- Adessium-stiftelsen og Open Society-stiftelserne

Dette dokument gøres tilgængeligt under Creative Commons 2.0 (CC BY 2.0) <http://creativecommons.org/licenses/by/2.0/>

Dansk version opdateret 2019-12-01.

Kapitler:

Kapitel 1: Hvad er Internettet? Kapitel 2: Hvad er retten til privatliv? Kapitel 3: Top tre tips- og tricks Kapitel 4: Beskyt dig selv på sociale netværk Kapitel 5: Smartphones og sikkerhed Kapitel 6: Sikrere beskedtjenester Kapitel 7: Surfing på Internettet Kapitel 8: Kodeordsikkerhed Kapitel 9: Billed- og video-delning Kapitel 10: Programmer og værktøjer vi kan lide Kapitel 11: Praktisk vejledning til Signal

[Intro]

Internettet. Sejt, hurtigt og verdensomspændende.

Men også komplekst. Nogle gange kan det være vanskeligt at se hvor vi løber risici – og hvor vores private information kan læses og bruges af andre.

I vores parallelle univers, hvor Forsvarerne slås mod de onde Dataindtrængere, er det heldigvis nemt at se, hvem der er de gode og hvem der er de onde.

Forsvarerne vil vise dig nogle tips og tricks for at beskytte dig selv på nettet. De vil lære dig selvforsvar for at bekæmpe Indtrængerne.

Check dette blad ud, og vær klar til at blive en del af vores superheltehold, Forsvarerne!

Din ven,

Orv. Hold øjnene åbne for EDRi-former-spillet

Du vil finde rebuser rundt omkring i bladet. Hver rebus har kun eet rigtigt svar og vil give dig et bogstav. Sammen vil bogstaverne stave løsningsordet. Hint: Det er et ord som består af seks bogstaver. Skatten som kan låses op: EN MÆGTIG DIGITAL RUSTNING.

Når du har fundet ordet, vil du skulle gå til en hemmelig side på Internettet. Det gøres på følgende måde: 1 . Find den manglende del af linket: <https://efn.no/xxxxxx> . 2 . Erstat xxxxxx med løsningsordet (seks bogstaver), som du får fra rebuserne og skrivelse hele linket ind i din internetbrowser.

KAPITEL 1 Hvad er Internettet?

Internettet er et globalt netværk af enheder.

Når du bruger Internettet på din bærbare computer, tablet eller telefon, er de en del af netværket.

En af de specielle egenskaber med Internettet er, at mange forskellige teknologiske løsninger kan bruge samme netværk.

Vi kan endda bruge samme forbindelse til at downloade video, spille og chatte med vores venner samtidig.

Internettet er verdensomspændende, det er hurtigt, og det åbner en verden af muligheder.

Internettet er en utrolig og kraftfuld opfindelse. Før Internettet blev udbredt, fandtes der ingen enkel måde at forbinde mange mennesker på. Det var meget vanskeligere at lytte til musik eller at se en film. Internettet er også et fantastisk sted at lære, da størstedelen af information og viden deles på nettet.

Internetteknologi er lidt som en stor bakke, der er dækket af sne – vi kan bruge den til at stå på ski, snowboard eller til at bygge en snemand. Alt hvad vi behøver, er sne!

I den netbaserede verden svarer bakken til internetforbindelsen og sneen er det sprog, som netværket snakker – “internetprotokollen”!

Sociale netværk og andre netbaserede tjenester virker tilsyneladende som om, de er gratis – men vi betaler faktisk med personlig information, som vi deler på nettet. Information om hvad vi skriver, læser, eller ser, bruges af netbaserede virksomheder.

Hvordan kan vi bevare kontrollen over den information, vi deler på nettet?

Du finder svaret på det spørgsmål i dette hæfte.

## KAPITEL 2 Hvad er retten til privatliv?

Hvis privatlivet beskyttes, så har vi kontrol. Men hvad betyder det?

Retten til privatliv er vores ret til at bestemme, hvad vi deler om os selv, og hvem vi deler det med.

Det betyder for eksempel, at du har ret til at spørge Google, Facebook og andre om, hvilken slags information de har indsamlet om dig. Du kan også bede dem om at slette denne information.

Når vi beskytter vores ret til privatliv, kan vi føle os sikrere og tryggere, fordi det kan dreje sig om information, som kunne skade os, hvis det kom i de forkerte personers hænder.

Det kan være information, vi ønsker at dele med nogle som vores forældre eller lærere, men ikke med nogen andre.

Men vi kan også hjælpe andre, når vi beskytter vores eget privatliv, fordi de måske ønsker at dele noget med os, som ikke bør deles med nogen anden.

Vi har alle noget, vi ikke vil dele med andre.

At værne om vores eget privatliv har også meget at gøre med at passe på vores venner, fordi det bidrager til at gøre os frie, trygge og troværdige.

Vores forældre, venner eller andre som bruger computeren efter os, kan nogle gange se hvad vi søgte efter. Dette kan ske fordi vi glemte at logge ud, eller ganske enkelt fordi de kigger i computerens historik.

### » VIDSTE DU?

For bare 20 år siden havde de fleste hjem kun én telefonlinje, som kun en person kunne bruge ad gangen. Næsten ingen havde mobiltelefon, og kun få havde e-post.

» REBUS 1: INTERNETTET ER... [R]... et netværk af enheder. [S]... et effektivt fiskeriredskab for internationalt farvand. [T]... et socialt netværk.

## KAPITEL 3 Top tre tips og trick

### 1 . Ikke alle skal ikke vide alt om os

Lige som i den normale verden er det bedre at være omhyggelig når vi vælger, hvad vi ønsker at dele eller ej. Instinktivt deler vi nogle ting med nogle mennesker og ikke med andre. Internettet gør det nogle gange svært at foretage det valg.

Dette er delvis fordi, det ikke altid er klart, hvad der er privat på nettet og hvad der ikke er, og delvis fordi der på Internettet gælder andre regler end i den virkelige verden.

For eksempel: Vores venner vil tilgive en dum kommentar som vi er kommet med i vrede og forstår vores opførsel fordi de kender os. Hvis nogle andre læser

vores kommentarer på nettet, forstår de måske ikke, hvad vi mente og kan tro, at det var ondsindet ment.

## 2 . Tryghed og beskyttelse af privatlivet på nettet er ikke svært

Vi behøver ikke at være supernørder for at færdes sikkert online. Vi kan bruge en tablet, telefon eller en bærbar som vores klassekammerater ikke har adgang til, et kodeord ingen andet kan gætte, se videoer på nettet uden at blive sporet. Dette lader sig gøre på enkel vis.

## 3 . At vide hvad eller hvem vi beskytter os mod

Ligesom banker er nødt til at beskytte sig mod tyve, må vi også beskytte os selv - mod virksomheder som sporer os på nettet, klassekammerater som kan være sure på os over noget eller snusende forældre som er . . . snusende forældre.

Vi bør spørge os selv om, hvad de reelle trusler er og hvad kan gøre ved dem. Når vi først har tænkt over disse trusler, vil vi indse, at det reelt er muligt at sikre os selv og vores privatliv.

## KAPITEL 4 Beskyt dig selv på sociale netværk

Det kan være rigtigt sjovt at bruge sociale netværk. Her kan vi sludre med venner og familie, dele billeder, sende private beskeder og poste information offentligt.

I nogle lande har børn under 13 ikke lov til at bruge visse sociale medier. Hvis du ønsker at bruge sociale netværk, er det bedst at spørge familie og lærere for at være sikker.

Facebook, Instagram, Twitter, Snapchat, Diaspora og mange flere er alle sociale netværk.

Har du nogle favoritter? Hvorfor kan lide du dem?

Nogle sociale netværk gemmer endda beskeder vi ikke sender! Forestil dig, at når du skriver en besked til din ven på Facebook, som du ikke sender, så vil din ven ikke få kendskab til den. Men Facebook gemmer den!

Husk, at alt hvad vi gør på et socialt netværk bliver registreret på, eller går igennem, selskabernes computere. Det betyder ikke, at de har til hensigt at gøre noget dårligt med det - men du bør vide, at dette sker.

» VIDSTE DU?

De ting vi skriver ind i en søgemaskine, eller skriver i en chat til en ven, bliver ikke fuldstændig slettet. Virksomheder, som leverer populære tjenester (såsom YouTube, Facebook, Snapchat og så videre) kan registrere hvad vi skriver, de hjemmesider vi besøger og de ting vi søger efter på nettet.

» REBUS 2: BESKYTTELSE AF PRIVATLIVET ER VIGTIGT FORDI . . . [T] . . . det hjælper os til at se musikvideoer. [U] . . . det hjælper os med at være

frie og bevare kontrollen på nettet. [G] ... det hjælper os med at dele billeder med hele verden.

## DIGITALE FORSVARERE MOD DATAINDTRÆNGERE (I)

FR. ANONYMITET

HOLD: DIGITALE FORSVARERE

KRÆFTER: Statskontrollerede forsøg har forstærket hendes immunforsvar. Hun har også muligheden for at bruge sociale netværk anonymt, således at ingen ved, hvem hun egentlig er.

VÅBEN: Hun er dygtig til nærkamp

ID-TYV

HOLD: DATAINDTRÆNGERE

KRÆFTER: Hun kan se hvad du gør på nettet, for derefter at stjæle personlige oplysninger om dig. Hun lader som om, hun er dig og prøver at bruge dit navn, sociale medier og e-postkonti til kriminelle aktiviteter.

VÅBEN: Alfavirus – som hun bruger til at infiltrere computere og telefoner.

## KAPITEL 5 Smartphonesikkerhed

Vores telefoner er blevet meget vigtige for brugen af Internettet.

Vi bruger dem, når vi ønsker at kommunikere med venner og familie, når vi bruger sociale netværk, eller ganske enkelt for at surfe.

Men vores telefoner er også nyttige på mange andre måder - vi kan bruge dem som lommelygte, til at spille, eller for at tjekke næste busafgang.

Når du installerer en ny app, læser du så virkelig hvilke rettigheder, du giver programmet og hvordan det får adgang til informationen på din telefon? Har en lommelygte virkelig brug for adgang til din adresseliste?

Det er meget fristende bare at trykke «Godkend», men det er en god idé at stoppe op og tænke. Der er gode grunde til at ikke stole på et program, som spørger om adgang til ting, det åbenlyst ikke behøver.

Med blot nogle få klik kan vi også tjekke, og sågar begrænse vores telefoners rettigheder eller rettighederne for de programmer som allerede er installeret. På de fleste enheder kan vi finde disse under «Indstillinger». Undersøg indstillingerne på din telefon, det er nyttigt sætte sig ind i, hvordan den virker.

» Mange apps får adgang til dine personlige ting, som ligger på din telefon.

Vi kan begrænse adgangen til at kende vores position og til vores adressebog og vi kan låse telefonen med password eller fingeraftryksgenkendelse.

Det tager ikke lang tid at gøre vores telefoner sikrere og bedre i stand til at beskytte privatlivet. Sidst i dette hæfte finder du en række gode programmer, der har dette for øje.

» VIDSTE DU?

Hvis der er gode grunde til, at et program har rettigheder til ting - et fotoprogram, for eksempel, som har brug for adgang til dit kamera - er der ikke meget at bekymre sig over. Hvis du derimod tror, at programmet beder om for meget, kan du tjekke, om der findes andre programmer, eller versioner af programmet, som kræver færre rettigheder.

DIGITALE FORSVARERE mod DATAINDTRÆNGERE (II)

TANKEFRIGØRER

HOLD: DIGITALE FORSVARERE

KRÆFTER: Han kæmper for din ret til at bestemme, hvad du vil dele med hvem. Han har muligheden for at oprette et privat og sikkert miljø, hvor du kan sige, hvad du tænker.

VÅBEN: Hans sind.

MAND-I-MIDTEN.

HOLD: DATAINDTRÆNGERE

KRÆFTER: Han besidder mystiske kræfter til at opsnappe, hvad du gør på nettet. Han kan udgive sig for at være en faktisk person online og derefter bruge dette til at hacke sig ind i dine samtaler, til at læse dine beskeder, se dine billeder og dine videoer.

VÅBEN: Hans dragt og antenner.

KAPITEL 6 Sikrere beskedsforsendelse

De af os, der har mobiltelefon, bruger den til at sende beskeder til venner og familie.

Nogle beskedprogrammer læser indholdet i vores beskeder og sporer, hvem vi snakker med. Nogle programmer gør dette med henblik på at sælge informationen.

» Hvad du siger og gør online er meget værdifuldt for visse virksomheder.

De virksomheder, som laver beskedprogrammer, scanner ofte, hvad vi siger. De sporer, hvem vi snakker med, således at de kan vise reklamer for at få os til at købe noget eller for at dele informationen med andre selskaber. Du kan tjekke en liste over seje beskedprogrammer sidst i hæftet. Disse programmer sikrer også, at vi ikke modtager beskeder fra fremmede. Der er også en vejledning til installation af Signal i dette hæfte - Signal er et sejt program, som sørger for, at dine beskeder bliver sendt sikkert.

» REBUS 3: SOCIALE NETVÆRK ER FANTASTISKE FORDI... [Q] ... Jeg kan være sikker på, at de aldrig vil sælge eller bruge mine data. [S] ... Jeg kan holde kontakten med venner og familie. [N] ... Jeg kan være sikker på, at kun mine venner kan se de billeder, jeg lægger op.

KAPITEL 7 Surfing på Internettet

Når vi siger, at vi «bruger Internettet», er det ofte en browser, vi bruger.

» Man kan let komme til at glemme, at browseren også er et kraftfuldt stykke software.

Den er nogle gange det første, du åbner, når du tænder telefonen, tabletten eller din computer, og det sidste du lukker. Men der foregår meget inde i browseren, der kan være skadeligt (eller godt) for beskyttelsen af dit privatliv.

Når vi går på nettet for at købe noget, se videoer eller for at se, hvad vores venner har delt, efterlader vi digitale fodspor. Nogle websider og sociale netværk bruger disse fodspor til at spore os.

» Nogle netsider gemmer meget information om os!

Hvem vores venner er, hvad vi kan lide, hvad vi søger efter, og hvad vi lytter til, kan spores. Disse websider kan gøre dette ved at bruge små informationskapsler, (også kaldt «kager»/«cookies») i vores browsere. Disse informationskapsler er små filer, der gemmes på enheden.

De er usynlige for os, men når nok data er indhentet og kombineret med anden information om os, vil personlige detaljer, som vi opfatter som hemmelige, og sammenhænge vi ikke tænker på, blive kendt af mange personer og selskaber.

De fleste enheder kommer med en browser. På Windows kan vi bruge Internet Explorer og Edge, Apple kommer med Safari, og Android-enhedernes præinstallerede browser er som oftest Google Chrome. Men det er ikke nødvendigvis de browsere, der fungerer bedst for dig.

» VIDSTE DU?

Husk at sætte dig ind i de forskellige «privatlivsindstillinger» i din browser og ændr de forudvalgte indstillinger således at du overtager kontrollen - akkurat som Perfekt Bølge! Mange mener, at den mest sikre browser og den, der bedst værner om dit privatliv, er Firefox! Hvorfor? Fordi du kan tilpasse den, kontrollere den, og se hvordan den virker. Det er muligt, at den ikke er installeret på din computer, men den kan let downloades.

DIGITALE FORSVARERE mod DATAINDTRÆNGERE (III)

PERFEKT BØLGE

HOLD: DIGITALE FORSVARERE

KRÆFTER: Han kan navigere rummet, hyperspace og cyberspace med sit bræt. Perfekt Bølge har ikke brug for mad og drikke, han kan overleve ved at konvertere data til energi. Han er næsten fuldstændig usårlig.

VÅBEN: Surfbræt.

GAL SMÅKAGE

HOLD: DATAINDTRÆNGERE

KRÆFTER: Han er altid på udkig efter en slåskamp. Han hader alle forsvarerne, men synes, at Perfekt Bølge er hans værste fjende. Han har en vældig appetit efter dine hemmeligheder.

VÅBEN: Hans roterende robotarm.

» REBUS 4: NOGLE PROGRAMMER... [F] ... er så sikre, at jeg aldrig behøver at tænke på at beskytte mit privatliv, når jeg bruger dem. [L] ... er bedre end chokolade. [T] ... har adgang til mine kontakter, billeder og beskeder.

## KAPITEL 8 Kodeordssikkerhed

Kodeord er meget vigtige i den digitale tidsalder.

Faktisk uhyre vigtige. De udgør grundlaget for din sikkerhed og din beskyttelse af privatlivet. Og folks kodeord er sædvanligvis meget, meget svage - det mest brugte kodeord er «password» eller «12345».

At lave et sikkert kodeord er ikke særligt svært.

### 1 . Brug aldrig det samme kodeord to gange

Dette er faktisk en af de vigtigste regler! Men prøv i hvert fald at have forskellige versioner af det kodeord, du har oprettet.

Hvorfor? Som følge af at kriminelle (som Datasmugleren) har adgang til kodeordet på en tjeneste, prøver de ofte at komme ind på andre tjenester med samme kodeord. De ved, at folk har for vane at bruge samme kodeord flere steder!

### 2 . Brug aldrig et ord fra ordbogen

... uanset hvor langt det måtte være, eller hvor tilsyneladende kompliceret det ser ud.

Hvorfor? Fordi der findes computerprogrammer, som prøver hvert eneste ord i ordbogen for forsøge at «gætte» dit kodeord. Hver superhelt i vores hold af forsvarere har et stærkt og kreativt kodeord. Du kan blive en af dem – dit kodeord er dit våben for at undgå fare!

### 3 . Dit Kodeord bør være mindst 12 tegn langt

Dette er et mindstekrav. Desto længere et kodeord er, desto vanskeligere er det at gætte sig til det.

Hvorfor? Fordi desto længere det er, desto vanskeligere er det at gætte. Nogle eksperter siger, at det er OK at skrive det ned, bare man husker at skjule papiret godt!

DIGITALE FORSVARERE mod DATAINDTRÆNGERE (IV)

LÅSENE DRONNING

HOLD: DIGITALE FORSVARERE



KRÆFTER: Hun kæmper for retten til privatliv og sikkerhed. Hun deler kraftige private nøgler ud til folk, som er i fare, og hjælper dem med at sikre deres personlige information på nettet.

VÅBEN: Hendes hjelm - hun bruger den til at skyde energistråler fra øjnene. Hun kan skære lige igennem Finn Lurefiskers farlige net.

FINN LUREFISKER

HOLD: DATAINDTRÆNGERE

KRÆFTER: Han har overmenneskelig styrke, hurtighed og reflekser. Han bruger sine kræfter til at snige sig ind i din telefon og fiske dine hemmeligheder ud af den.

VÅBEN: Han kaster et elektrostatisk datanet for at overvælde sine modstandere.

» REBUS 5: NÅR JEG BROWSER PÅ NETTET [X] ... kan jeg gøre hvad jeg vil, jeg er tryk - det er ikke virkeligheden! [E] ... kan jeg beskytte mig selv ved at ikke tillade cookies og ikke gemme min browserhistorik. [Y] ... er det bare paranoidt at være forsigtigt, fordi jeg ikke har noget at skjule.

KAPITEL 9 Deling af videoer og billeder

Vi fortæller vores venner om det, vi gør til dagligt ved at dele billeder og videoer med dem på nettet.

» At dele er sejt - men billeder og videoer kan let kopieres.

Husk, at det altid er vigtigt at forsikre sig om, at man ikke deler med folk, man ikke ønsker at dele med. Folk kan komme til at både se og misbruge private billeder.

Hvad er problemet? Hvis vi sender et billede eller en video, sendes der en kopi af den fra vores enhed til vores vens enhed. Forestil dig at vores ven deler billedet videre med anden. Hver kopi kan kopieres igen uendeligt.

Hvis vi deler et billede eller en video på nettet, vil der altid være mange kopier af den på forskellige enheder. Selv om vi sletter det oprindelige billede fra vores egne enheder, vil de andre kopier stadig være at finde derude.

Når vi deler, kan vores ting komme andre folk i hænde, uden at vi havde til hensigt at dele med dem.

Nogle folk kan prøve at stjæle vores identitet ved at bruge vores billeder - akkurat som ID-tyv.

Snapchat er et spionerende program til deling af billeder, som tilsyneladende forsvinder hurtigt. Uheldigvis er det stadig muligt at lagre et billede ved brug af nogle tricks og dele det videre. Tusindvis af Snapchat-billeder er allerede blevet lagt ud på Internettet.

Dette betyder, at vi må leve med muligheden for, at vores sociale netværk kan bruges til både gode og dårlige formål. Vi er derfor nødt til at tænke, før vi

sender billeder og videoer via nettet! Vi bør spørge os selv, om vi ville have hængt dette billede op på en offentlig opslagstavle på skolen. Hvis ikke er det måske ikke en god idé at dele det på nettet.

Hvis vores billede viser andre mennesker eller deres ting, er vi nødt til at spørge dem om lov, før vi deler det, fordi de har ret til at bestemme selv. Råderetten er deres.

For billeder som vi ikke har taget selv, skal vi spørge ejeren om lov, før vi deler dem på nettet.

DIGITALE FORSVARERE mod DATAINDTRÆNGERE (V)

TROELS TILFÆLDIG

HOLD: DIGITALE FORSVARERE

KRÆFTER: Han blev født på planeten Entropia, i en afsidesliggende galakse langt borte. Som alle sine artsfæller, har han mulighed for at ændre form efter ønske. Han kan beskytte dine hemmeligheder med tilfældigt muterende kodeord.

VÅBEN: Hans hovedvåben er opladede kropsdele, som han kan kaste og hente tilbage når som helst.

DATASMUGLER

HOLD: DATAINDTRÆNGERE

KRÆFTER: Han er meget rig og hans evner overgår langt det, som er muligt for mennesker. Han er ekstremt fleksibel og besidder overmenneskelig styrke. Han samler dyrebare personlige data (som dine billeder og beskeder) og sælger dem på den sorte børs.

VÅBEN: Han har mange forskellige våben i sin mappe.

Kapitel 10 Programmer og værktøjer vi kan lide

SMARTPHONE APPS

Program | Hvad det gør | Sværhedsgrad

Signal | Chat, SMS og krypterede telefonopkald (alternativ til WhatsApp) | Let

Firefox | En privatlivsvenlig browser | Let

KeePass DX | Holder styr på alle dine kodeord | Let

F-Droid | Arkiv med programmer, der er fri software (alternativ til Google Play) | Let

K9 Mail | Mailprogram | Let

Transportr | Offentlig transport, check bus- og togtider | Let

Jitsi Meet | Sikre gruppevideopkald (alternativ til Skype) | Let

Tor Browser | Surf på nettet anonymt | Let

OpenKeychain | Til at kryptere emails med K9 Mail | Svært

## SOFTWARE TIL WINDOWS, MAC OG LINUX

Program | Hvad det gør | Sværhedsgrad

Firefox | En privatlivsvenlig browser | Let

Pidgin og OTR Plugin | Beskedprogram (kompatibelt med ChatSecure) | Mellem

Thunderbird | Mailprogram | Let

Enigmail | Tillægsprogram til at kryptere emails i Thunderbird | Svært

Tor Browser | Surf på nettet anonymt | Let

## BROWSER TILLÆGSPROGRAMMER, PLUG-INS OG UDVIDELSER

Program | Hvad det gør | Sværhedsgrad

Ublock Origin | Blokerer webreklamer og tracking | Let

Privacy Badger | Blokerer trackers | Let

HTTPS Everywhere | Tvinger websites til at kryptere datatrafikken, om muligt | Let

Self Destructing Cookies | Fjerner cookies, når de ikke længere bruges af åbne browser faneblade | Mellem

NoScript | Blokerer JavaScript | Svær

## KAPITEL 11 Vejledning til brug af Signal

Signal er et frit program til Android og iPhone. Det overvåger ikke, hvem vi snakker med og hvad vi siger. Vi kan bruge det til at sende tekst, ringe, og dele billeder, videoer og kontakter.

Det er ikke det eneste program, vi kan bruge til at kommunikere trygt, men det er et af de letteste at bruge. Her har du en vejledning på fem enkle skridt:

- 1 . Gå til Play-butikken (Android) eller App-butikken (iPhone). Søg efter «Signal». Vælg programmet «Signal Private Messenger» og tryk «Installer». Efter at Signal er installeret, åbner du programmet.
- 2 . Registrer dit telefonnummer med Signal ved at taste det ind og vælg «Registrer» eller «Bekræft din enhed». Du vil få en tekstbesked med en sekscifret kode. Tast den kode ind i Signal.
- 3 . Tryk på blyantsymbolet nederst til højre (Android) eller »+«-symbolet øverst til højre (iPhone) for at starte en samtale.
- 4 . Vælg personen du ønsker at sende en besked eller ringe til.
- 5 . Hvis du ønsker at veksle mellem sikre beskeder via din internetforbindelse og usikre SMS'er, hold da «Send»-knappen nede lidt længere.

Det er meget sikrere når, personen vi kommunikerer med, også bruger Signal. Det bruger vores internetforbindelse når vi kontakter en anden Signal-bruger, og normale SMS'er eller opkaldsminutter, når vi kontakter nogen, som ikke bruger Signal.

Husk! Du behøver ikke at få alle du kender til at begynde at bruge Signal. Bare fortæl dine nærmeste venner og de folk du kontakter oftest om at installere det også, og på den måde vil flere og flere af vores venner begynde at bruge det.

» REBUS 6: JEG BØR VÆLGE ET KODEORD SOM... [T] ... er en tilfældig kombination af bogstaver og specialtegn. [V] ... 123456789 - det er enkelt at huske. [D] ... det første ord jeg ser, når jeg åbner en tilfældig bog på en vilkårlig side.