DIN VEILEDER TIL DIGITALE FORSVARERE MOT DATAINNTRENGERE TA KONTROLL OVER DITT LIV PÅ NETTET VERN AV PRIVATLIVET FOR BARN

[omslagstekst]

INTERNETT. KULT, RASKT OG VERDENSOMSPENNENDE. Det er også komplekst. Noen ganger kan det være vanskelig å se hvor vi løper en risiko – og hvor våre private ting kan leses og brukes av andre. Heldigvis, i vårt parallelle univers, der de DIGITALE FORSVARERNE sloss mot de onde DATAINNTRENGERNE, er det enkelt å se hvem som er de snille, og hvem som er slemmingene. www.edri.org

[kolofon]

Redaktør for bladet: Kirsten Fiedler, EDRi Theresia Reinhold, EDRi

Tegneserier: Gregor Sedlag

Grafikk og formgivning av: Gregor Sedlag Heini Jarvinen (EDRi-former illustrasjoner)

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

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

Oversatt av: Ole-Erik Yrvin

Korrekturlesing: Ingrid Yrvin Petter Reinholdtsen Tom Fredrik Blenning

Dette heftet ble til takket være:

• Individuell kronerulling på GlobalGiving.com – Takk til dere alle for deres bidrag! • Adessium-stiftelsen og Open Society-stiftelsene

Bokmålsutgave basert på engelsk original oppdatert 2019-11-27.

Kapitler:

[Intro]

Internett. Kult, raskt og verdensomspennende.

Det er også komplekst. Noen ganger kan det være vanskelig å se hvor vi løper risiko – og hvor våre private ting kan leses og brukes av andre.

Heldigvis, i vårt parallelle univers, der forsvarerne sloss mot de onde datainntrengerne, er det enkelt å se hvem som er de snille, og hvem som er slemmingene.

Forsvarerne vil vise deg noen tips og triks for å beskytte deg selv på nett. De vil lære deg selvforsvar for å hanskes med Inntrengerne.

Sjekk ut dette bladet, og vær klar til å bli med på vårt superheltlag, Forsvarerne!

Din venn,

Hold øynene åpne for EDRi-former-spillet

Du vil finne oppdrag rundt omkring i bladet. Hvert oppdrag har bare ett riktig svar og vil gi deg én bokstav. Sammen vil bokstavene stave løsningsordet. Hint: Det er et ord som består av seks bokstaver. Utmerkelsen som kan låses opp: EN MEKTIG DIGITAL RUSTNING.

Når du har funnet ordet, vil du måtte gå til en hemmelig side på Internett. Dette er hvordan det gjøres: 1. Finn den manglende delen av følgende lenke: https://efn.no/xxxxxx . 2. Erstatt xxxxxx med løsningsordet (seks bokstaver) du får fra oppdragene, og skriv inn hele lenken i nettleseren din.

KAPITTEL 1 Hva er Internett?

Internett er et globalt nettverk av enheter.

Når du bruker Internett på din bærbare datamaskin, nettbrett eller telefon, er de en del av nettverket.

En av de spesielle egenskapene med Internett er at mange forskjellige teknologiske løsninger kan bruke samme nettverk.

Vi kan til og med bruke samme tilkobling til å laste ned video, spille, og prate med vennene våre samtidig.

Internett er verdensomspennende, det er raskt, og gir oss en hel verden av muligheter.

Internett er en utrolig og kraftig oppfinnelse. Før Internett spredte seg viden rundt, fantes det ingen enkel måte å koble mange folk til hverandre. Det var mye vanskeligere å lytte til musikk eller å se en film. Internett er også en flott plass å lære, siden mesteparten av informasjonen og kunnskapen deles på nett.

Internetteknologi er litt som en stor ås dekt av snø – vi kan bruke den til å kjøre ski, snøbrett eller å bygge en snømann. Alt vi trenger er snø!

I den nettbaserte verden, er åsen internettilknytningen vår, og snøen er språket nettverket snakker – “internettprotokollen”!

Sosiale nettverk og mange andre nettbaserte tjenester er tilsynelatende gratis – men vi betaler faktisk med personlig informasjon vi deler på nettet. Informasjon om hva vi skriver, leser, eller ser, brukes av nettbaserte selskaper.

Hvordan kan vi beholde kontrollen over informasjonen vi deler på nett?

Du finner svaret på dette spørsmålet i dette heftet.

KAPITTEL 2 Hva er rett til privatliv?

Hvis privatlivet vernes, så har vi kontroll. Men hva betyr dette?

Retten til privatliv er vår rett til å bestemme hva vi deler om oss selv, og hvem vi deler det med.

Dette betyr, for eksempel, at du har rett til å spørre Google, Facebook og andre om hva slags informasjon de har samlet inn om deg. Du kan også spørre dem om å slette denne informasjonen.

Vi er sikrere og tryggere når vi beskytter vårt rett til privatliv, fordi det kan dreie seg om informasjon som kan skade oss hvis det kommer feil person for øye.

Det kan være informasjon vi ønsker å dele med noen, som våre foreldre eller lærere, men ikke med noen andre.

Men vi kan også hjelpe andre når vi beskytter vårt eget privatliv, fordi de kanskje ønsker å dele noe med oss som ikke bør deles med noen andre.

Vi har alle noe vi ikke vil dele med andre.

Å verne vårt eget privatliv har også mye å gjøre med å ta vare på våre venner, fordi det bidrar til å gjøre oss frie, trygge og til å stole på.

Våre foreldre, venner eller andre som bruker datamaskinen etter oss, kan noen ganger se hva vi søkte etter. Dette kan skje fordi vi glemte å logge ut, eller ganske enkelt fordi de ser i datamaskinens historikk.

» VISSTE DU?

For bare 30 år siden, hadde de fleste hjem bare én telefonlinje som bare én person kunne bruke om gangen. Nesten ingen hadde mobiltelefon, og ikke mange hadde e-post.

» OPPDRAG 1: INTERNETT ER... [R]... et nettverk av enheter. [S]... et effektivt fiskeredskap for internasjonalt farvann. [T]... et sosialt nettverk.

KAPITTEL 3 De beste tre tips- og triksene

1. Du skal ikke vite alt om oss

Som i den vanlige verden er det bedre å være nøye i utvelgelsen av hva vi ønsker å dele, og hvem vi vil dele det med. Instinktivt deler vi noen ting med noen mennesker og ikke med andre. Internett gjør det noen ganger vanskelig å gjøre dét valget.

Dette er delvis fordi det ikke alltid er klart hva som er, og ikke er privat på nettet, og delvis fordi Internett har andre regler enn verden utenfor.

For eksempel: Våre venner vil tilgi en dum kommentar vi kom med i sinne, og forstår oppførselen vår fordi de kjenner oss. Hvis noen andre leser våre kommentarer på nettet, forstår de kanskje ikke hva vi mente og kan tro at vi mente å være slemme.

2. Trygghet og vern av privatlivet på nettet er ikke vanskelig

Din indre hacker beskytter deg på nett. Vi kan beskytte brett, telefon eller en bærbar slik at våre klassekamerater ikke får tilgang den. Vi kan bruke et passord ingen andre kan gjette og se videoer på nett uten å bli sporet. Dette lar seg gjøre på enkelt vis.

3. Vit hva eller hvem du beskytter oss mot

Slik banker må beskytte seg mot tyver, må vi også beskytte oss selv - mot selskaper som sporer oss på nett, klassekamerater som kan være sure, uvisst av hvilken grunn, eller snokende foreldre som er ... snokende foreldre.

Vi burde spørre oss selv om hva de reelle truslene er, og hva vi er i stand til å gjøre med dem. Når vi først har tenkt gjennom hva truslene utgjør, finner vi at det er muligheten for å beskytte oss selv og styre vårt vern av privatlivet.

KAPITTEL 4 Beskytt deg selv på sosiale nettverk

Det kan være veldig gøy å bruke sosiale nettverk. På dem kan vi prate med venner og familie, dele bilder, sende private meldinger og poste informasjon til offentligheten.

I noen land har barn under 13-årsalderen ikke lov til å bruke noen av de sosiale media-nettverkene. Hvis du ønsker å bruke sosiale nettverk, er det best å spørre familien din eller lærerene dine for å være sikker.

> Facebook, Instagram, Twitter, Snapchat, Diaspora og flere med dem, er alle sosiale nettverk.

Har du favoritter? Hvorfor liker du dem?

Noen sosiale nettverk lagrer selv meldinger vi ikke sender! Forestill deg at når du skriver en melding til din venn på Facebook, vil naturlig nok din venn ikke få kjennskap til meldingen, men Facebook tar vare på den!

Husk at alt en gjør på et sosialt nettverk blir registrert på, eller går gjennom, selskapenes datamaskiner. Det betyr ikke at de har til hensikt å snoke - men du bør vite at dette skjer.

» VISSTE DU?

Tingene vi skriver inn i en søkemotor, eller skriver i en tekstmelding til en venn, blir ikke fullstendig slettet. Bedrifter som leverer populære tjenester (som

YouTube, Facebook, og Snapchat) registrerer og tar vare på hva vi skriver, nettstedene vi besøker og de tingene vi søker etter på nettet.

» OPPDRAG 2: VERN AV PRIVATLIVET ER VIKTIG FORDI... [T] ...det hjelper oss å se musikkvideoer. [U] ...det hjelper oss å være frie og beholde kontroll på nettet. [G] ...det hjelper oss med å dele bilder med hele verden.

DIGITALE FORSVARERE MOT DATAINNTRENGERE (I)

FR. ANONYMITET

LAG: DIGITALE FORSVARERE

KREFTER: Myndighetsforsøk har forsterket immunforsvaret hennes. Hun har også muligheten til å bruke sosiale nettverk anonymt, slik at ingen vet hvem hun egentlig er.

VÅPEN: Hun er en dyktig på nærkamp

ID-TYV

LAG: DATAINNTRENGERE

KREFTER: Hun kan se hva du gjør på nettet, for så å stjele personopplysninger om deg. Hun later som hun er deg, og prøver å bruke ditt navn, dine sosiale medie- og e-postkontoer til kriminelle aktiviteter.

VÅPEN: Alfaviruset – som hun bruker for å infiltrere datamaskiner og telefoner.

KAPITTEL 5 Smarttelefoner og sikkerhet

Telefonene våre har blitt veldig viktige for bruken av Internett.

Vi bruker dem når vi ønsker å kommunisere med venner og familie, når vi bruker sosiale nettverk, eller ganske enkelt for å surfe.

Men telefonene våre er også nyttige på mange andre måter, vi kan bruke dem som lommelykt, til å spille, eller for å sjekke neste avgang på bussen.

Når du installerer ett nytt program, leser du hvilke tilganger du gir til programmet, og hvordan det får tilgang til informasjon på telefonen din? Trenger en lommelykt egentlig tilgang til adresselisten din?

Det er veldig fristende å bare trykke «Godta», men det er bedre å stoppe opp og tenke seg om. Det er gode grunner til å ikke stole på et program som spør om tilgang til ting det åpenbart ikke trenger.

Med kun få klikk kan vi også sjekke, og sågar begrense, tilgangene til våre telefoner eller programmer som allerede er installerte. På de fleste enheter kan vi finne disse i «Innstillinger». Sjekk rundt omkring på telefonen din, det er nyttig å lære seg hvordan den virker.

» Mange programmer (app-er) får tilgang til de personlige tingene som er lagret på telefonen din.

Vi kan begrense tilgang til posisjonen og adresseboken vår, og vi kan også legge inn passord- eller fingeravtrykksjekk for å låse opp telefonen vår.

Det tar ikke lang tid å gjøre telefonene våre sikrere og mer i stand til å verne privatlivet. På slutten av dette heftet finner du mange gode programmer med dette for øye.

» VISSTE DU?

Det er gode grunner til at programmer har tilganger til ting - et fotoprogram, for eksempel, som må ha tilgang til kameraet ditt - er lite å bekymre seg over. Hvis du derimot tror programmet spør om for mye, kan du sjekke om det finnes lignende programmer tilgjengelig som spør om færre tilganger.

DIGITALE FORSVARERE mot DATAINNTRENGERE (II)

TANKEFRIGJØRER

LAG: DIGITALE FORSVARERE

KREFTER: Han sloss for din rett til å bestemme hva du vil dele med hvem. Han har muligheten til å opprette et privat og sikkert miljø der du kan si hva du tenker.

VÅPEN: Hans tanker.

MANN-I-MIDTEN.

LAG: DATAINNTRENGERE

KREFTER: Han besitter mystiske krefter for å fange opp hva du gjør på nett. Han kan utgi seg for å være en faktisk person på nett, og så bruke dette til å bryte seg rett inn i samtalene dine, for å lese meldingene dine, se bildene og se videoene dine.

VÅPEN: Hans drakt og antenner.

KAPITTEL 6 Sikrere meldingsutveksling

De av oss med mobiltelefon bruker den til å sende meldinger til venner og familie.

Noen meldingsutvekslingsprogrammer (app-er) tar vare på alle meldingene våre og sporer hvem vi snakker med. Noen programmer gjør dette slik at de kan selge, tjene på, informasjonen.

» Hva du sier og gjør på nett er veldig verdifullt for selskaper.

Selskapene som lager meldingsutvekslingsprogrammer skanner ofte hva vi sier. De sporer hvem vi snakker med slik at de kan vise reklame, for å få oss til å kjøpe noe, eller for å dele informasjonen med andre selskaper. Du kan sjekke en liste over kule meldingsprogrammer på slutten av heftet. Disse meldingsprogrammene sikrer også at vi ikke mottar meldinger fra fremmede. Det er også en veiledning til installasjon av Signal i dette heftet - Signal er et kult program sikrer meldingene dine.

» OPPDRAG 3: SOSIALE NETTVERK ER FORTREFFELIGE FORDI... [Q] ... Jeg kan være sikker på at de aldri vil selge eller bruke mine data. [S] ... Jeg kan holde kontakten med venner og familie. [N] ... Jeg kan forsikre meg om at bare mine venner kan se bildene jeg poster der.

KAPITTEL 7 Surfing på Internett

Når vi sier vi «bruker Internett», er det ofte en nettleser vi bruker.

» Husk å ikke glemme at nettleseren i seg selv også er et mektig stykke programvare.

Det er noen ganger det første du åpner når du skrur på telefonen, brettet eller datamaskinen din, og det siste du lukker. Mye finner allikevel sted inne i nettleseren som du ikke ser, og det kan være skadelig (eller bra) for vern av ditt privatliv.

Når vi går på nett for å kjøpe noe, se videoer eller for å se hva våre venner har delt, etterlater vi digitale fotspor. Noen nettsider og sosiale nettverk bruker disse fotsporene til å spore oss.

» Noen nettsider tar vare på mye informasjon om oss!

Hvem vennene våre er, hva vi liker, hva vi søker etter, og hva vi lytter til kan spores. Disse nettsidene kan gjøre dette fordi det er informasjonskapsler, (også kalt «kaker»/«cookies») i nettleserne våre. Disse informasjonskapslene er små filer som langres på enhetene våre.

De er usynlige for oss, men når nok data er innhentet, og kombinert med annen informasjon om oss, vil personlige detaljer vi tenker på som hemmelige, og sammenhenger vi ikke tenker på, bli kjent for mange folk og selskaper.

De fleste enheter kommer med en dårlig nettleser. På Windows foreslås Edge, Apple-enheter kommer med Safari, og Android-enhetenes forvalgte nettleser er Google Chrome. Men disse er ikke nødvendigvis nettleserne som beskytter ditt privatliv best.

» VISSTE DU?

Husk å gjøre deg kjent med ulike «privatlivsinnstillinger» i nettleseren din, og endre de forvalgte innstillingene slik at du tar kontrollen - akkurat som Perfekt Bølge! Den nettleseren som best sikrer, og hegner om privatlivet ditt er Firefox. Hvorfor? Fordi du kan tilpasse den, kontrollere den, og se hvordan den virker. Det er mulig at den ennå ikke er installert på din datamaskinen, men du kan enkelt laste den ned.

DIGITALE FORSVARERE mot DATAINNTRENGERE (III)

PERFEKT BØLGE

LAG: DIGITALE FORSVARERE

KREFTER: Han kan navigere rom, kyberrom, og flere dimensjoner med brettet sitt. Perfekt Bølge trenger ikke mat og drikke, han kan overleve ved å omvende data til energi. Han er nesten fullstendig usårbar.

VÅPEN: Surfebrett.

GAL KAKE

LAG: DATAINNTRENGERE

KREFTER: Han er alltid på utkikk etter bråk. Han hater alle forsvarerne, men synes at Perfekt Bølge er sin verste fiende. Han har en uhorvelig appetitt for dine hemmeligheter.

VÅPEN: Hans roterende robotarm.

» OPPDRAG 4: NOEN PROGRAMMER... [F] ... er så sikre at jeg aldri trenger å tenke på å verne mitt privatliv når jeg bruker dem. [L] ... er bedre enn sjokolade. [T] ... har tilgang til mine kontakter, bilder og meldinger.

KAPITTEL 8 Passordsikkerhet

Passord er veldig viktige i den digitale tidsalder.

Faktisk uhyre viktig. De utgjør grunnlaget for din sikkerhet og ditt vern av privatlivet. Folks passord er vanligvis veldig, veldig svake - det mest brukte passordet er «passord» eller «12345».

Å lage et sikkert passord er ikke veldig vanskelig.

1. Aldri bruk samme passord to ganger

Dette er faktisk én av de viktigste reglene! Prøv i hvert fall å ha forskjellige versjoner av passordet du opprettet.

Hvorfor? Som følge av at hvis kriminelle (som Datasmugleren) får tilgang til passordet på én av dine konter, prøver de ofte å komme inn på andre tjenester med samme passord. De vet folk har for vane å bruke samme passord flere steder!

2. Bruk aldri et ord fra ordboka

... uansett hvor langt det måtte være, eller hvor tilsynelatende komplisert det ser ut.

Hvorfor? Fordi det finnes dataprogrammer som prøver hvert eneste ord i ordboka for forsøke å «gjette» passordet ditt. Hver superhelt i vårt lag av forsvarere har et sterkt og kreativt passord. Du kan bli en av dem – passordet ditt er ditt våpen for å unngå fare!

3. Passordet ditt burde være minst 12 tegn langt

Dette er et minstekrav. Desto lengre et passord er, desto vanskeligere er det å gjette seg til det.

Hvorfor? Fordi desto lengre det er, desto vanskeligere er det å gjette. Noen eksperter sier at det er OK å notere det ned på en papirbit, bare husk å skjule den godt!

DIGITALE FORSVARERE mot DATAINNTRENGERE (IV)

DRONNINGEN AV LÅSER

LAG: DIGITALE FORSVARERE

KREFTER: Hun sloss for retten til privatliv og sikkerhet. Hun deler ut kraftige private nøkler til folk som er i fare, og hjelper dem å sikre sin personlige informasjon på nett.

VÅPEN: Hjelmen - hun bruker den til å skyte energistråler fra øynene. Hun kan kutte Finn Lurefiskers nett tvert av.

FINN LUREFISKER

LAG: DATAINNTRENGERE

KREFTER: Han har overmenneskelig styrke, fart og reflekser. Han bruker sine krefter til å snike seg inn i telefonen din og fiske ut hemmelighetene dine.

VÅPEN: Han kaster sitt elektrostatiske datanett for å overvelde motstandere.

» OPPDRAG 5: NÅR JEG SURFER PÅ INTERNETT... [X] ... kan jeg gjøre hva jeg vil, jeg er trygg - det er ikke virkeligheten! [E] ... kan jeg beskytte meg selv ved å ikke tillate informasjonskapsler og ikke lagre min nettleserhistorikk. [Y] ... er det bare paranoid å være forsiktig, fordi jeg ikke har noe å skjule.

KAPITTEL 9 Deling av videoer og bilder

Vi forteller vennene våre om det vi gjør til daglig ved å dele bilder og videoer med dem på nett.

» Deling er kult - å ha kontrollen med kopier av bilder og videoer likeså.

Husk at det alltid er viktig å forsikre seg om at man ikke deler med folk man ikke ønsker. Folk kan komme til å både se og misbruke private bilder.

Hva er problemet? Hvis vi sender et bilde eller video, sendes det en kopi av den fra vår enhet til vår venns enhet. Forestill deg at vår venn deler bildet videre med andre. Hver kopi kan kopieres igjen uendelig.

Hvis vi deler et bilde eller en video på nett, vil det alltid være mange kopier av den på forskjellige enheter. Selv om vi sletter det opprinnelige bildet fra våre egne enheter, vil de andre kopiene fremdeles være å finne der ute.

Når vi deler, kan våre ting komme andre folk i hende, uten at vi hadde til hensikt å dele med dem.

Noen folk kan prøve å stjele vår identitet ved å bruke våre bilder - akkurat som ID-tyv.

Snapchat er et program for deling av bilder som raskt forsvinner ut av syne. Uheldigvis er det fremdeles mulig å lagre et bilde ved bruk av noen triks, og dele det videre. Tusenvis av Snapchat-bilder har allerede blitt lagt ut på Internett.

Vi må leve med det faktum at våre sosiale nettverk kan brukes til både gode og dårlige formål. Vi må derfor tenke før vi sender bilder og videoer via Internett! Vi bør spørre oss selv om vi ville puttet dette bildet på en offentlig oppslagstavle på skolen. Hvis ikke, er det kanskje ikke en god idé å dele det på nett.

Hvis bildet vårt viser andre mennesker, eller deres ting, må vi spørre dem om lov før vi deler det, fordi de har en rett til å bestemme selv. Råderetten er deres.

For bilder som vi ikke har tatt selv, spør vi eieren om lov før vi deler dem på nett.

DIGITALE FORSVARERE mot DATAINNTRENGERE (V)

TRULS TILFELDIG

LAG: DIGITALE FORSVARERE

KREFTER: Han ble født på planeten Entropia, i en avsidesliggende galakse, langt unna. Som alle hans artsfrender, har han mulighet til å endre form etter ønske. Han kan beskytte dine hemmeligheter med tilfeldig muterende passord.

VÅPEN: Hans hovedvåpen er oppladede kroppsdeler, som han kan kaste og hente tilbake når som helst.

DATASMUGLER

LAG: DATAINNTRENGERE

KREFTER: Han er veldig rik, og hans evner overgår langt det som er mulig for mennesker. Han er ekstremt fleksibel, og besitter overmenneskelig styrke. Han samler dyrebare personlige data (som dine bilder og meldinger), og selger dem på svartebørsen.

VÅPEN: Han har mange forskjellige våpen i stresskofferten sin.

KAPITTEL 10 Programmer og verktøy vi liker

SMARTTELEFONPROGRAMMER

Program | Hva det gjør | Enkelhet i bruk

Signal | Sikker meldingsutveksling og telefonsamtaler (WhatsApp-alternativ) | Enkelt

Firefox | En privatsfære-vennlig nettleser | Enkelt

KeePass DX | Håndterer alle passordene dine | Enkelt

F-Droid | Pakkebrønn med fri programvare (Google Play-alternativ) | Enkelt

K9-Mail | Håndterer e-postene dine | Middels

Transportr | Kollektivtransport, sjekk bussavganger og togtabeller | Enkelt

Jitsi Meet | Sikre gruppevideosamtaler (Skype-alternativ) | Enkelt

Tor Browser | Surf på nettet anonymt | Enkelt

OpenKeychain | Krypterte e-poster med K9 Mail | Vanskelig

PROGRAMVARE FOR WINDOWS, MAC og GNU/LINUX

Software | Hva den gjør | Enkelhet i bruk

Firefox | En privatsfære-vennlig nettleser | Enkelt

Pidgin og OTR Plugin | Meldingsutveksling (samvirker med ChatSecure) | Middels

Thunderbird | Håndterer e-postene dine | Middels

Enigmail | Utvidelse for å kryptere e-poster i Thunderbird | Vanskelig

Tor Browser | Surf på nettet anonymt | Enkelt

NETTLESERTILLEGG, INNSTIKKMODULER OG UTVIDELSER

Nettlesertillegg | Hva det gjør | Enkelhet i bruk

Ublock Origin | Blokkerer nettannonser og sporing | Enkelt

Privacy Badger | Blokkerer sporere på nettet | Enkelt

HTTPS Everywhere | Tvinger nettsider til å kryptere trafikken din, hvis mulig | Enkelt

Cookie AutoDelete | Fjerner informasjonskapsler som ikke lenger er i bruk av åpne nettleserfaner | Middels

NoScript | Blokkerer JavaScript | Vanskelig

KAPITTEL 11 Praktisk veiledning til Signal

Signal er et fritt program for Android og iPhone. Det holder ikke oppsyn med hvem vi snakker til og hva vi sier. Vi kan bruke det til å sende tekst, ringe, og dele bilder, videoer og kontakter.

Dette er ikke det eneste programmet vi kan bruke til å kommunisere trygt, men det er ett av de enkleste å bruke. Her har du en veiledning i fem enkle steg:

1. Gå til Play-butikken (Android) eller App-butikken (iPhone). Søk etter «Signal». Velg programmet «Signal Private Messenger» og trykk «Installer». Etter at Signal er installert, åpner du programmet.

2. Registrer telefonnummeret ditt med Signal ved å skrive det inn, og velg «Registrer» eller «Bekreft din enhet». Du vil få en tekstmelding med en sekssifret kode. Putt den koden inn i Signal.

3. Trykk på blyantsymbolet nederst til høyre (Android) eller »+«-symbolet øverst til høyre (iPhone) for å starte en samtale.

4. Velg personen du ønsker å sende en melding til eller ringe.

5. Hvis du ønsker å veksle mellom sikre meldinger via din internettilknytning, og usikrede SMS-er, hold nede «Send»-knappen litt lengre.

Det er mye sikrere når personen vi kommuniserer med også bruker Signal. Da brukes vår internettilknytning når vi kontakter en annen Signal-bruker, og vanlige SMS-er eller ringeminutter når vi kontakter noen som ikke bruker Signal.

Husk! Du trenger ikke å få alle du kjenner til å begynne å bruke Signal. Bare fortell dine nærmeste venner og folk du kontakter oftest om å installere det også, og dermed vil flere og flere av dine vennene begynne å bruke det.

» OPPDRAG 6: JEG BURDE VELGE ET PASSORD SOM... [T] ... er en tilfeldig kombinasjon av bokstaver, tall og spesialtegn. [V] ... 123456789 - det er enkelt å huske. [D] ... det første ordet jeg ser når jeg åpner ei tilfeldig bok på ei vilkårlig side.