JOUW GIDS TOT DE DIGITALE BESCHERMERS VS. DATAGRAAIERS VERKRIJG CONTROLE OVER JE ONLINE-GEGEVENS PRIVACY VOOR KINDEREN

[Omslagtekst]

HET INTERNET. HET IS COOL, SNEL EN OVERAL. Maar het is ook ingewikkeld. Soms kan het moeilijk zijn om te weten wanneer we gevaar lopen en wanneer onze persoonlijke informatie online kan worden gelezen en gebruikt door anderen. Gelukkig is het in ons parallel universum, waar de DIGITALE BESCHERMERS vechten tegen de gemene DATAGRAAIERS, wél makkelijk om te zien wie de goeie- en wie de slechteriken zijn. www.edri.org

[colofon]

Boekje bewerkt door: Kirsten Fiedler, EDRi Theresia Reinhold, EDRi

Strips: Gregor Sedlag

Illustraties & ontwerp door: Gregor Sedlag Heini Jarvinen (EDRi-former illustraties)

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

Met speciale dank aan: Gloria González Fuster, VrijeUniversiteit Brussel (VUB) Hans Martens, Better Internet for Kids, EUN Partnership AISBL

Dit boekje is mogelijk gemaakt door:

• Individuele sponsoren op GlobalGiving.com - bedankt voor jullie bijdrage! • De Adessium Foundation en Open Society Foundations

Revisiedatum: 2019-11-27.

Hoofdstukken:

Hoofdstuk 1: Wat is het internet? Hoofdstuk 2: Wat is privacy? Hoofdstuk 3: De 3 beste tips en trucs Hoofdstuk 4: Bescherm jezelf op sociale netwerken Hoofdstuk 5: Smartphonebeveiliging Hoofdstuk 6: Veilig berichten versturen Hoofdstuk 7: Surfen op het internet Hoofdstuk 8: Veilige wachtwoorden Hoofdstuk 9: Foto's en video's delen Hoofdstuk 10: Aanbevolen apps en hulpmiddelen Hoofdstuk 11: Handleiding voor Signal

[introductie]

Het internet. Het is cool, snel en overal.

Maar het is ook ingewikkeld. Soms kan het moeilijk zijn om te weten wanneer we gevaar lopen en wanneer onze persoonlijke informatie online kan worden gelezen en gebruikt door anderen.

Gelukkig is het in ons parallel universum, waar de DIGITALE BESCHERMERS vechten tegen de gemene DATAGRAAIERS, wél makkelijk om te zien wie de goeie- en wie de slechteriken zijn.

De Beschermers zullen je wat tips en trucs laten zien die je helpen om jezelf online te beschermen. Ze leren je zelfbescherming zodat je je kunt wapenen tegen de Graaiers.

Dus lees dit boekje en bereid je voor om deel te nemen aan ons superheldenteam, de Beschermers!

Je vriend,

OH, EN HOUD JE OGEN OPEN VOOR HET Edri-former SPEL

In dit boekje vind je zoektochten. Elke zoektocht kent slechts één juist antwoord. Het antwoord geeft je één letter. Met al die letters kun je een woord vormen dat leidt naar de oplossing. Hint: het woord bestaat uit zes letters. Met dit woord krijg je het volgende: EEN KRACHTIG DIGITAAL HARNAS.

Zodra je het woord hebt gevonden, ga je naar een geheime website. Zó doe je dat: 1. Zoek het ontbrekende deel van de volgende link: https://edri.org/xxxxxx . 2. Vervang xxxxxx door het zesletterwoord dat je hebt gevonden na het verzamelen van alle letters. Voer de volledige link in in je browser.

HOOFDSTUK 1 Wat is het internet?

Het internet is een wereldwijd netwerk van apparaten.

Als je internet gebruikt op je laptop, tablet of telefoon, dan ben je onderdeel van het netwerk.

Eén van de meest speciale functies van het internet. is dat verschillende technologieën kunnen worden gebruikt op hetzelfde netwerk.

We kunnen dezelfde verbinding gebruiken om een video te downloaden, een spel te spelen en te chatten met onze vrienden. Allemaal tegelijkertijd.

Het internet is wereldwijd, snel en biedt ons een zee van mogelijkheden.

Het internet is een geweldige en krachtige uitvinding. Voordat het internet wereldwijd werd uitgerold, was er geen eenvoudige manier om veel mensen met elkaar te verbinden. Het was véél moeilijker om naar muziek te luisteren of om een film te kijken. Het internet is ook een geweldige plek om informatie te verkrijgen en te delen.

Internettechnologie lijkt een beetje op een grote heuvel bedekt met sneeuw - we kunnen deze gebruiken om te skiën, snowboarden of om er een sneeuwman op te bouwen. Het enige dat we nodig hebben is sneeuw!

In de online wereld is de heuvel onze internetverbinding en de sneeuw is de taal die het netwerk spreekt - het “internetprotocol”!

Sociale netwerken en andere sociale diensten lijken gratis, maar stiekem betalen we er wél voor - met de persoonlijke informatie die we delen. Informatie over wat we schrijven, lezen of kijken wordt gebruikt door online-bedrijven.

Hoe kunnen we de baas blijven over de informatie die we delen?

Je zult het antwoord op deze vraag vinden in dit boekje.

HOOFDSTUK 2 Wat is privacy?

Als we privacy hebben, dan hebben we controle. Maar wat betekent dit?

Privacy is ons recht om te bepalen wat we delen en met wie.

Dit betekent bijvoorbeeld dat je het recht hebt om Google, Facebook en anderen te vragen wat voor informatie ze hebben verzameld over jou. Je kunt ze ook vragen om die gegevens te verwijderen.

Als we onze privacy beschermen, dan voelen we ons veiliger omdat er informatie tussen kan zitten die ons pijn kan doen als de verkeerde persoon deze in handen krijgt.

Dit kan informatie zijn die we willen delen met sommige mensen, zoals onze ouders of leraren, maar niet met iedereen.

Door het beschermen van onze privacy kunnen we ook anderen helpen omdat zij misschien iets willen delen met ons dat niet met iedereen mag worden gedeeld.

Iedereen heeft wel iets dat ze niet willen delen met anderen.

Zorgen voor onze eigen privacy heeft ook veel te maken met zorgen voor onze vrienden, want het helpt ons om vrij, veilig en betrouwbaar te zijn.

Onze leraren, vrienden of anderen die de computer na ons gebruiken, kunnen soms zien waar we naar gezocht hebben. Dit kan gebeuren als we vergeten uit te loggen of een kijkje nemen in de geschiedenis van de computer.

» WIST JE DAT?

20 jaar geleden beschikten de meeste huizen over één telefoonlijn die slechts door één persoon tegelijk gebruikt kon worden. Bijna niemand had een mobiele telefoon en weinig mensen hadden e-mail.

» ZOEKTOCHT 1: HET INTERNET IS... [A]... een netwerk van apparaten. [B]... een efficiënt hulpmiddel om te vissen op internationale zeeën. [C]... een sociaal netwerk.

HOOFDSTUK 3 De 3 beste tips en trucs

1. Niet iedereen hoeft alles over ons te weten

Net als in de echte wereld, is het beter om voorzichtig te zijn met wat we wel en niet delen. Instinctief delen we sommige dingen met sommige mensen maar niet met anderen. Het internet maakt het soms moeilijk om te kiezen.

Dit komt deels omdat het op internet niet altijd duidelijk is wat privé is en wat niet en deels omdat het internet andere regels heeft dan de echte wereld.

Voorbeeld: onze vrienden vergeven ons als we een stomme opmerking maken terwijl we boos zijn en begrijpen waarom we dat deden omdat ze ons kennen. Als iemand anders op internet onze opmerking leest, dan begrijpen ze mogelijk niet wat we bedoelen en denken ze dat we gemeen zijn.

2. Veiligheid en privacy op internet is niet moeilijk

We hoeven geen supernerds te zijn om onszelf te beschermen op internet. We kunnen een tablet, telefoon of laptop gebruiken waar onze klasgenoten geen toegang tot hebben, een wachtwoord dat niemand kan raden en video's bekijken zonder dat we worden gevolgd. Het is allemaal heel eenvoudig.

3. Weten wat en tegen wie we onszelf beschermen

Net zoals dat banken beveiliging nodig hebben om zich te beschermen tegen dieven, moeten wij onszelf beschermen tegen bedrijven die ons willen volgen op internet, tegen klasgenoten die ergens boos over zijn of tegen nieuwsgierige ouders die... nieuwsgierig zijn.

We moeten aan onszelf vragen wat de échte bedreigingen zijn en wat we er tegen kunnen doen. Als we hierover nagedacht hebben, dan zien we dat het helemaal niet moeilijk is om onszelf te beschermen en onze privacy te bewaken.

HOOFDSTUK 4 Bescherm jezelf op sociale netwerken

Het kan ontzettend leuk zijn om sociale netwerken te gebruiken. Op sociale netwerken kunnen we chatten met vrienden en familie, foto's delen, privéberichten sturen en openbare informatie plaatsen.

In sommige landen mogen kinderen jonger dan 13 geen gebruikmaken van sommige sociale netwerken. Als je sociale netwerken wilt gebruiken, vraag dan aan je familie of leraren of het al mag.

> YouTube, Facebook, Instagram, Snapchat, Twitter, Diaspora en vele anderen zijn allemaal sociale netwerken.

Wat zijn jouw favoriete sociale netwerken? En waarom vind je ze zo leuk?

Sommige sociale netwerken slaan berichten op, zélfs de berichten die we niet versturen. Stel je voor: je schrijft een bericht aan je vriend op Facebook en verstuurt het bericht niet. Je vriend weet niets van dat bericht, maar Facebook slaat het wél op!

Bedenk altijd dat álles wat we doen op sociale netwerken wordt opgeslagen op de computers van die bedrijven. Dit betekent niet per se dat ze er iets verkeerds mee gaan doen, maar het is belangrijk om te weten dát het gebeurt.

» WIST JE DAT?

De dingen die we typen in een zoekmachine of schrijven in een chatbericht aan een vriend worden niet volledig verwijderd. Bedrijven die de diensten aanbieden (zoals YouTube, Facebook, Snapchat, enz.) houden bij wat we schrijven, welke websites we bezoeken en de dingen die we zoeken.

» ZOEKTOCHT 2: PRIVACY IS BELANGRIJK, OMDAT... [T] ... het ons helpt om muziekvideo's te bekijken. [R] ... het ons helpt om vrij en in controle te zijn. [G] ... het ons helpt om foto's te delen met de hele wereld.

DIGITALE BESCHERMERS v DATAGRAAIERS (I)

MEVR. ANONIEM

TEAM: DIGITALE BESCHERMERS

KRACHTEN: Overheidstests hebben haar immuunsysteem versterkt. Ze heeft ook de mogelijkheid om sociale netwerken anoniem te gebruiken, zodat niemand weet wie ze werkelijk is.

WAPENS: Ze is een goed getraind vechter die vecht met haar handen

I.D.-dief

TEAM: DATAGRAAIERS

KRACHTEN: Ze kan zien wat je op het internet doet en je persoonlijke informatie stelen. Ze doet alsof ze jou is en probeert je naam, sociale media- en e-mailaccounts te gebruiken voor criminele activiteiten.

WAPENS: Het Alfa-virus - ze gebruikt dit virus om computers en telefoons binnen te dringen.

HOOFDSTUK 5 Smartphonebeveiliging

Onze telefoons zijn ontzettend belangrijk geworden om mee te internetten.

We gebruiken ze als we willen praten met onze vrienden en familie, als we sociale netwerken gebruiken of gewoon om te surfen op het internet.

Maar onze telefoons zijn ook handig voor veel andere dingen: we kunnen ze gebruiken als zaklamp, we kunnen er spelletjes op spelen of kijken hoe laat de volgende bus vertrekt.

Als je een nieuwe app installeert, lees je dan waarvoor je de app toestemming geeft en hoe de app toegang heeft tot informatie op je telefoon? Heeft een zaklamp-app écht toegang nodig tot je adresboek?

Het is erg verleidelijk om snel voorbij te gaan aan het »Accepteren«-scherm, maar eigenlijk is het een goed moment om even na te denken. Er zijn goede redenen om een app niet te vertrouwen als deze vraagt om machtigingen die niet nodig zijn.

Met slechts een paar klikken kunnen we controleren wat onze telefoon en apps allemaal mogen - en als we willen deze toestemming intrekken. Op de meeste apparaten vinden we die instellingen in de »Instellingen«. Kijk eens rond in de instellingen van je telefoon; dit is een mooie manier om te leren hoe je telefoon werkt.

» Veel apps krijgen toegang tot persoonlijke dingen die opgeslagen zijn op je telefoon.

Je kunt toegang tot je locatie en adresboek beperken, en een wachtwoord- of vingerafdrukcontrole toevoegen aan het vergrendelscherm.

Het veiliger en privacyvriendelijker maken van onze telefoons neemt nauwelijks tijd in beslag. Aan het eind van dit boekje vind je een lijst van geweldige apps waarmee je dit kunt doen.

» WIST JE DAT?

Als er een goede reden is om een app toegang te geven tot iets (bijv. een foto-app die toegang nodig heeft tot je camera), dan hoef je je weinig zorgen te maken. Maar als je vermoedt dat een app te veel machtigingen vraagt, dan kun je kijken of er andere versies van de app aanwezig zijn in de app-winkel die minder machtigingen vragen.

DIGITALE BESCHERMERS v DATAGRAAIERS (II)

GEESTBEVRIJDER

TEAM: DIGITALE BESCHERMERS

KRACHTEN: Hij vecht voor je recht om te beslissen wat je deelt en met wie. Hij heeft de mogelijkheid om een veilige privé-omgeving te creëren waar je alles kunt zeggen.

WAPENS: Zijn geest.

TUSSENPERSOON.

TEAM: DATAGRAAIERS

KRACHTEN: Hij heeft mystieke krachten om alles wat je op internet doet te onderscheppen. Hij kan zich voordoen als een legitiem persoon en zo inbreken in je gesprekken, je berichten lezen en je foto's en video's bekijken.

WAPENS: Zijn pak en antennes.

HOOFDSTUK 6 Veilig berichten versturen

We gebruiken allemaal onze telefoons om berichten te versturen aan vrienden en familie.

Maar sommige berichtenapps kunnen de inhoud van onze berichten lezen en bijhouden met wie we praten. Sommige doen dit om geld te verdienen aan deze informatie.

» Wat je op internet vertelt is waardevol voor bedrijven.

De bedrijven die berichtenapps maken, scannen regelmatig onze berichten. Ze houden bij met wie we praten zodat ze dat kunnen delen met andere bedrijven of om ons advertenties te laten zien om ons te verleiden iets te kopen. Aan het einde van dit boekje vind je een lijst met coole berichtenapps. Deze apps zorgen er ook voor dat we geen berichten ontvangen van vreemden. En er is een handleiding over het installeren van Signal in dit boekje. Signal is een coole app waarmee je je berichten veilig houdt.

» ZOEKTOCHT 3: SOCIALE NETWERKEN ZIJN GEWELDIG, OMDAT... [Q] ... ik zeker weet dat ze mijn gegevens nooit zullen gebruiken of verkopen. [M] ... ik in contact kan blijven met mijn vrienden en familie. [N] ... ik zeker weet dat alleen mijn vrienden kunnen zien welke foto's ik plaats.

HOOFDSTUK 7 Surfen op het internet

Als we internet gebruiken, doen we dat meestal met een browser.

» Het is makkelijk te vergeten dat een browser een klein stukje software is.

Soms is het het eerste wat je opent als je je telefoon, tablet of computer aanzet en ook het laatste wat je weer afsluit. Maar er gebeurt heel veel in de browser waar je je niet bewust van bent. En die dingen kunnen slecht (of goed) zijn voor je privacy.

Als we op internet gaan om iets te kopen, video's te bekijken of kijken wat onze vrienden onlangs hebben geplaatst, dan laten we digitale voetstappen achter. Sommige websites en sociale netwerken gebruiken deze voetstappen om ons te volgen.

» Websites verzamelen heel veel informatie over ons!

Wie onze vrienden zijn, wat we leuk vinden, waar we naar zoeken en luisteren: het kan allemaal worden gevolgd. Deze websites kunnen dat doen door middel van »cookies« in onze browsers. Deze »cookies« zijn kleine stukjes software.

Ze zijn onzichtbaar voor ons maar als er genoeg gegevens zijn verzameld en worden gecombineerd met andere gegevens over ons (persoonlijke gegevens waarvan we denken dat ze geheim zijn), dan worden ze bekend bij andere mensen en bedrijven.

De meeste apparaten hebben standaard een browser. Op Windows is dat Edge, op Apple-apparaten is dat Safari en op Android-apparaten is dat Google Chrome. Maar dit zijn niet per se de browsers die het beste zijn.

» WIST JE DAT?

Controleer de »privacy-instellingen« van je browser en pas de standaardinstellingen aan zodat jíj de baas bent, net zoals Perfecte Golf! Veel mensen vinden dat de beste browser omtrent privacy en veiligheid Firefox is! Waarom? Omdat je hem volledig kunt aanpassen, er volledige controle over hebt en omdat je kunt

zien hoe het werkt. Het kan zijn dat Firefox niet is geïnstalleerd op je computer, maar je kunt hem eenvoudig downloaden.

DIGITALE BESCHERMERS v DATAGRAAIERS (III)

PERFECTE GOLF

TEAM: DIGITALE BESCHERMERS

KRACHTEN: Hij kan navigeren in de ruimte, hyperruimte en cyberruimte op zijn plank. De Perfecte Golf heeft geen eten of drinken nodig; hij kan overleven door gegevens om te zetten in energie. Hij is bijna volledig onverwoestbaar.

WAPENS: Zijn surfplank.

GEKKE KOEKIE

TEAM: DATAGRAAIERS

KRACHTEN: Hij is altijd op zoek naar ruzie. Hij haat alle Beschermers maar beschouwt Perfecte Golf als zijn ergste vijand. Hij heeft een monsterlijke honger en zijn favoriete eten zijn jouw geheimen.

WAPENS: Zijn roterende robotarm.

» ZOEKTOCHT 4: SOMMIGE APPS... « [F] ... zijn zó veilig dat ik nooit hoef na te denken over mijn privacy als ik ze gebruik. [L] ... zijn beter dan chocolade. [O] ... hebben toegang tot mijn contactpersonen, afbeeldingen en berichten.

HOOFDSTUK 8 Veilige wachtwoorden

Wachtwoorden zijn ontzettend belangrijk in het digitale tijdperk.

Sterker nog: eigenlijk is er niks belangrijker! Ze vormen de basis van je veiligheid en privacy. De meeste mensen hebben heel, héél onveilige wachtwoorden. De meestvoorkomende wachtwoorden zijn »wachtwoord» en »12345».

Het creëren van een veilig wachtwoord is niet moeilijk.

1. Gebruik voor iedere dienst een ander wachtwoord

Dit is écht één van de belangrijkste regels! Probeer op zijn minst verschillende variaties van het wachtwoord te creëren.

Waarom? Als criminelen (zoals Gegevenssmokkelaar) toegang krijgen tot de wachtwoorden van een dienst, dan proberen ze die wachtwoorden ook te gebruiken bij andere diensten. Ze weten dat mensen de neiging hebben hetzelfde wachtwoord te gebruiken op verschillende sites!

2. Gebruik nóóit een woord uit het woordenboek

. . . hoe lang het ook mag zijn of hoe moeilijk het er ook uitziet.

Waarom? Omdat computerprogramma's elk woord uit het woordenboek proberen om je wachtwoord te »raden«. Elke superheld in ons Beschermers-team heeft een sterk en creatief wachtwoord. Ook jij kunt meedoen - je wachtwoord is je wapen om gevaar af te wenden!

3. Je wachtwoord moet minimaal 12 tekens lang zijn

Dit is het minimum. Hoe langer het wachtwoord, hoe moeilijker het is om te kraken.

Waarom? Omdat lange wachtwoorden moeilijker te raden zijn. Sommige experts zeggen dat het oké is om ze op te schrijven, maar verstop het papiertje dan goed!

DIGITALE BESCHERMERS v DATAGRAAIERS (IV)

KONINGIN DER SLOTEN

TEAM: DIGITALE BESCHERMERS

KRACHTEN: Ze vecht voor privacy en veiligheid. Ze geeft krachtige privésleutels aan mensen die gevaar lopen en helpt ze om hun persoonlijke informatie op internet te beveiligen.

WAPENS: Haar helm. Ze gebruikt haar helm om energieflitsen te schieten met haar ogen. Ze kan in een flits door het net van Finn Phisher breken.

FINN PHISHER

TEAM: DATAGRAAIERS

KRACHTEN: Hij heeft bovenmenselijke kracht, -snelheid en -reflexen. Hij gebruikt zijn krachten om stiekem je telefoon binnen te dringen en je geheimen op te vissen.

WAPENS: Hij gooit een elektrostatisch data-net uit om zijn tegenstanders te verzwakken.

» ZOEKTOCHT 5: ALS IK OP INTERNET SURF. . . [X] . . . dan kan ik alles doen wat ik maar wil. Ik ben veilig, het internet is niet echt! [U] . . . dan kan ik mezelf beschermen door cookies niet toe te staan en mijn browsergeschiedenis niet te bewaren. [Y] . . . té voorzichtig zijn is paranoïde; ik heb niks te verbergen.

HOOFDSTUK 9 Foto's en video's delen

We praten met onze vrienden over ons dagelijks leven door online foto's en video's met ze te delen.

» Delen is cool, maar foto's en video's kunnen makkelijk worden gekopieerd.

Onthoud dat het altijd belangrijk is om zeker te weten dat we niks delen met mensen waarmee we niet willen delen. Mensen kunnen soms onze privéfoto's zien en misbruiken.

Wat is het probleem? Als we een foto of video versturen, dan sturen we een kopie vanaf ons apparaat naar dat van een vriend. Bedenk nu hoe onze vriend de afbeelding deelt met anderen. Elke kopie kan opnieuw worden gekopieerd.

Als we online een foto of video delen, dan bestaan er altijd verschillende kopieën van op andere apparaten. Zelfs als we de originele foto verwijderen van onze eigen apparaten, dan zijn er nog steeds andere kopieën.

Als we iets delen, dan kunnen onze spullen in de handen komen van mensen met wie we niks willen delen.

Sommige mensen kunnen zelfs onze identiteit proberen te stelen door onze foto's te gebruiken - net als I.D. Dief.

Snapchat is een app om foto's te delen die snel weer verdwijnen. Helaas is het zelfs daarmee nog mogelijk om met een paar trucjes een afbeelding op te slaan en opnieuw te delen. Er zijn al duizenden Snapchat-afbeeldingen uitgelekt.

Dit betekent dat we ermee moeten leven dat het mogelijk is dat sociale netwerken zowel voor goede als kwade doeleinden gebruikt kunnen worden. We moeten dus nadenken voordat we iets plaatsen of foto's en video's versturen via het internet! We moeten onszelf afvragen of we de foto zouden willen ophangen op het prikbord op school. Als we dat niet willen, dan is het geen goed idee om deze online te delen.

Als er andere mensen op onze foto staan, dan moeten we ze toestemming vragen voordat we de foto delen. Het is hun recht om te beslissen of ze willen dat de foto gedeeld wordt.

Als we een foto niet zelf hebben genomen, dan moeten we toestemming vragen aan de eigenaar voordat we de foto online delen.

DIGITALE BESCHERMERS v DATAGRAAIERS (V)

JAN WILLEKEUR

TEAM: DIGITALE BESCHERMERS

KRACHTEN: Hij is geboren op de planeet Entropia, ergens in een sterrenstelsel ver hier vandaan. Net als de anderen van zijn soort kan hij zijn uiterlijk te allen tijde aanpassen. Hij kan je geheimen bewaren door middel van willekeurig wijzigende wachtwoorden.

WAPENS: Zijn belangrijkste wapens zijn de met energie geladen delen van zijn lichaam die hij op elk moment kan gooien en terughalen.

GEGEVENSSMOKKELAAR

TEAM: DATAGRAAIERS

KRACHTEN: Hij is behoorlijk rijk en kan dingen doen die mensen nooit zouden kunnen. Hij is heel flexibel en heeft bovenmenselijke kracht. Hij verzamelt waardevolle persoonlijke gegevens (zoals je foto's en berichten) en verkoopt deze op de zwarte markt.

WAPENS: Hij draagt verschillende soorten wapens bij zich in zijn koffer.

HOOFDSTUK 10 Aanbevolen apps & hulpmiddelen

SMARTPHONE-APPS

App | Wat de app doet | Moeilijkheidsgraad

Signal | Berichten en sms'jes versturen, en veilig bellen (alternatief voor WhatsApp) | Makkelijk

Firefox | Een browser die je privacy beschermt | Makkelijk

KeePass DX | Wachtwoorden beheren | Makkelijk

F-Droid | App-winkel met apps die open en vrij zijn (alternatief voor Google Play) | Makkelijk

K9-Mail | E-mailen | Iets moeilijker

Transportr | Openbaar vervoer: bekijk bus- en treintijden | Makkelijk

Jitsi Meet | Beveiligde videogesprekken (alternatief voor Skype) | Makkelijk

Tor Browser | Surf anoniem op internet | Makkelijk

OpenKeychain | Beveiligt e-mails die verstuurd worden met K9 Mail | Moeilijk

SOFTWARE VOOR WINDOWS, MACOS EN LINUX

Software | Wat de app doet | Moeilijkheidsgraad

Firefox | Een browser die je privacy beschermt | Makkelijk

Pidgin met de OTR-plug-in | Berichten versturen (compatibel met ChatSecure) | Iets moeilijker

Thunderbird | E-mailen | Iets moeilijker

Enigmail | Beveiligt e-mails die verstuurd worden met Thunderbird | Moeilijk

Tor Browser | Surf anoniem op internet | Makkelijk

BROWSERPLUG-INS, -ADD-ONS EN -EXTENSIES

Add-on | Wat de add-on doet | Moeilijkheidsgraad

Ublock Origin | Blokkeert reclame, advertenties en trackers op het internet | Makkelijk

Privacy Badger | Blokkeert trackers | Makkelijk

HTTPS Everywhere | Dwingt websites om, indien mogelijk, een veiligere verbindingsmethode te gebruiken | Makkelijk

Cookie AutoDelete | Verwijdert cookies als ze niet langer worden gebruikt door openstaande tabbladen | Iets moeilijker

NoScript | Blokkeert JavaScript | Moeilijk

HOOFDSTUK 11 Handleiding voor Signal

Signal is een gratis app voor Android en iOS. Signal kijkt niet mee met wat we zeggen of met wie we praten. We kunnen het gebruiken voor berichten, bellen en het delen van foto's, video's en contactpersonen.

Het is niet de enige app die we kunnen gebruiken om veilig te communiceren, maar het is één van de makkelijkste om te gebruiken. Hier is een handleiding voor Signal, bestaande uit 5 eenvoudige stappen:

1. Ga naar de Play Store (Android) of App Store (iOS). Zoek naar »Signal«. Selecteer de app »Signal Private Messenger« en druk op ›Installeren‹. Open Signal nadat de installatie voltooid is.
2. Registreer je telefoonnummer bij Signal door je telefoonnummer in te voeren en te drukken op ›Registreren‹ of ›Verifieer je apparaat‹. Je krijgt een SMS met een zescijferige code. Voer die code in in Signal.
3. Druk op het potloodje rechtsbeneden (Android) of op het »+«-symbool rechtsboven (iOS) om een gesprek te starten.
4. Selecteer de persoon die je wilt SMS'en of bellen.
5. Als je wilt wisselen tussen veilige berichten via je internetverbinding en onveilige SMS, dan moet je de »Versturen«-knop even ingedrukt houden.

Het is véél veiliger als de persoon met wie we contact opnemen ook Signal gebruikt. De app gebruikt onze internetverbinding wanneer we contact opnemen met een andere Signal-gebruiker en normale SMS of belminuten wanneer we contact opnemen met iemand die geen Signal gebruikt.

Onthoud: je hoeft niet iedereen die je kent over te laten stappen naar Signal. Vertel in ieder geval aan je beste vrienden en de mensen met wie je het meeste contact hebt om het te installeren, dan gaan vanzelf meer en meer vrienden het gebruiken.

» ZOEKTOCHT 6: IK MOET MIJN WACHTWOORD LATEN BESTAAN UIT . . . [R] . . . een willekeurige combinatie van letters en speciale tekens. [V] . . . 123456789, want dat is makkelijk te onthouden. [D] . . . het eerste woord dat ik tegenkom na het openen van een willekeurig boek.