4.

WIS JE SPOREN

De browser op je telefoon slaat veel informatie over jou op– waar je bent, wat je zoekt, welke websites je gebruikt – en kan die informatie weggeven. Je kunt de controle over een deel van die informatie terugkrijgen als je een aantal veranderingen doorvoert.

Telefoons, tablets en computers zijn vaak voorzien van een vooraf geïnstalleerde browser die minder privacyvriendelijk is. In plaats daarvan kan je **een browser downloaden en gebruiken** die **standaard meer privacy biedt** en die je beschermt tegen trackers.

En om je privacy nog beter te beschermen kun je add-ons en extensies installeren (dat zijn makkelijk te installeren mini-programmaatjes voor je browser die **je online activiteit nog beter afschermen**).

5.

ONT-TAG JEZELF EN ANDEREN

Heb je geholpen bij het opbouwen van de gegevensberg van je vrienden doordat je ze wel eens hebt getagd in foto's en berichten? Je kunt hun gegevensberg afgraven (en je geweten sussen) door die **tags te verwijderen** in zoveel mogelijk foto's en berichten.

Geef het door! Betrek je vrienden, familie en collega's ook bij het beheersen van die losgeslagen data. Als we allemaal samenwerken om onze datasporen onder controle te houden kunnen we elkaar beter helpen bij het detoxen.

Een product van

TACTICAL TECH

Ondersteund door

Firefox

datadetoxkit.org
#datadetox

Om spiedende advertenties en onzichtbare trackers te blokkeren, installeer je **uBlock Origin** (voor Chrome, Safari en Firefox) of **Privacy Badger** (voor Chrome, Firefox en Opera).

Om je verbinding met websites zo goed mogelijk te beveiligen, installeer je HTTPS Everywhere: een browserextensie die ervoor zorgt dat de communicatie tussen je browser en veel belangrijke websites wordt versleuteld en beschermd. Als je dit een nuttige functie vindt en Safari gebruikt, kies dan als standaard zoekmachine eentje die niet van Google is, zoals DuckDuckGo, die je automatisch omleidt naar een versleutelde verbinding.

HOUD CONTROLE OVER JE SMARTPHONEGEGEVENS

om je online privacy te vergroten

DATA DETOX KIT

Als je nadenkt over wat je gegevens prijsgeven over jou lijkt dat op het eerste gezicht niet belangrijk: wat boeit het iemand anders dat je groot fan bent van Nederlandse hits, dat je meer schoenen koopt dan je nodig hebt of dat je je vakantie een jaar van tevoren boekt?

Het probleem is wat er met die gegevens gebeurt. Als ze in de loop der tijd worden samengevoegd, **ontstaan er persoonlijke digitale patronen**: je gewoontes, locaties, relaties, voorkeuren, overtuigingen en geheimen worden tot in detail blootgelegd aan degenen die de gegevens **verzamelen en eraan verdienen**, zoals bedrijven en datahandelaars.

Met het volgen van deze afkickcursus word je ervan bewust hoe en waarom dit allemaal gebeurt en leer je praktische stappen te zetten om de **datasporen die je op het internet achterlaat te beheersen.**

Aan de slag!

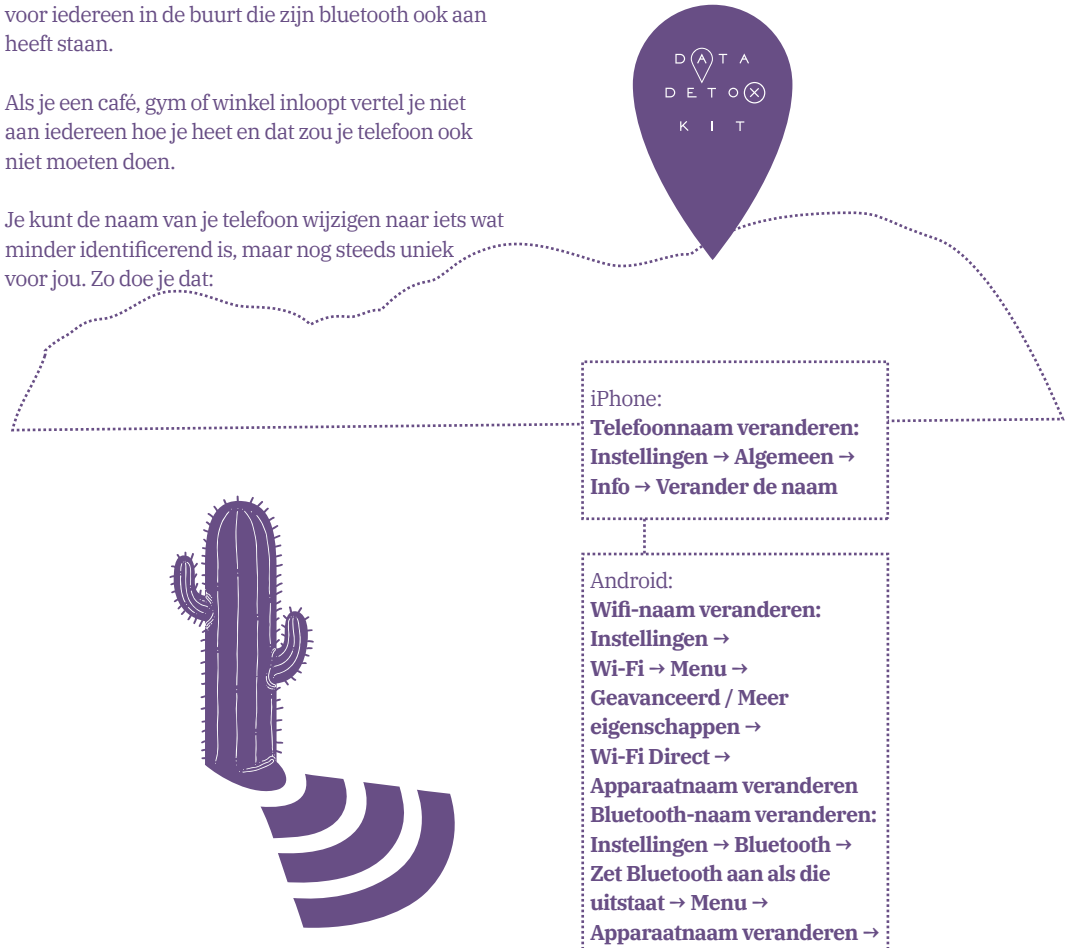
1.

VERANDER DE NAAM VAN JE TELEFOON

Het kan zijn dat je in het verleden je telefoon een naam hebt gegeven voor **wifi, bluetooth** of beide – of dat er automatisch een naam is aangemaakt tijdens de installatie. Dat betekent dat '*telefoon van Janneke Jonkman*' zichtbaar is voor de eigenaar van het wifi-netwerk en, als je bluetooth hebt ingeschakeld, voor iedereen in de buurt die zijn bluetooth ook aan heeft staan.

Als je een café, gym of winkel inloopt vertel je niet aan iedereen hoe je heet en dat zou je telefoon ook niet moeten doen.

Je kunt de naam van je telefoon wijzigen naar iets wat minder identificerend is, maar nog steeds uniek voor jou. Zo doe je dat:



iPhone:
Telefoonnaam veranderen:
Instellingen → Algemeen →
Info → Verander de naam

Android:
Wifi-naam veranderen:
Instellingen →
Wi-Fi → Menu →
Geavanceerd / Meer
eigenschappen →
Wi-Fi Direct →
Apparaatnaam veranderen
Bluetooth-naam veranderen:
Instellingen → Bluetooth →
Zet Bluetooth aan als die
uitstaat → Menu →
Apparaatnaam veranderen →
Zet Bluetooth uit

2.

WIS JE LOCATIESPOREN

De locatiedata lijken misschien willekeurige stukjes informatie, maar al die stukjes samen onthullen **belangrijke gegevens over jou** en je gewoontes, zoals je woonplaats, waar je werkt en waar je naartoe gaat met je vrienden. Daarom zijn die gegevens zeer gewild bij veel bedrijven en datahandelaars.

Je kunt **per app de instellingen beheren** en de **locatievoorzieningen uitschakelen**. Bekijk welke apps de locatievoorziening eigenlijk niet nodig hebben om goed te kunnen werken (moet een game echt weten waar je bent?) en voor welke apps je de locatievoorziening liever uitschakelt:

Android:
Instellingen →Apps →
Locatietoegang per app beheren

iPhone:
Instellingen →Privacy →
Locatievoorzieningen →
Locatietoegang per app beheren

3.

APPS OPRUIMEN

De apps die je gebruikt voor social media, games en het weerbericht hebben interesse in je gegevens... en de kans is groot dat ze veel van die gegevens verzamelen.

De apps die je nooit gebruikt kun je beter van je telefoon verwijderen, want het is een perfecte manier om je digitale ik te detoxen.

Bovendien krijg je met zo'n schoonmaakactie weer meer ruimte op je telefoon, je verbruikt minder data en je batterij gaat langer mee.

Android:
Instellingen → Apps →
Selecteer de app die je wilt
verwijderen → Verwijderen

iPhone:
Hou het app-icoontje ingedrukt totdat er een menu verschijnt.

Selecteer de optie app verwijderen.

Bevestig verwijderen van de app.

4.

BESCHERM JE VIRTUELE KOSTBAARHEDEN

Je geeft de waardevolle spullen in je huis een veilige plek en je zou hetzelfde moeten doen met de informatie die je virtueel bewaart – Of het nou om je financiële gegevens, scans van je paspoort of zelfs je adres of telefoonnummer gaat; het is geen overbodige luxe om na te denken over wáár en hóe je deze waardevolle persoon- lijke gegevens bewaart en beschermt.

Even **snel oppoetsen** is prima als je tijdens de koffie snel wat verbeteringen wilt doorvoeren. Zoek naar specifieke informatie in je e-mail of andere accounts en verwijder die: scans van je ID, bankgegevens of informatie over je zorgverzeke- ringen, om maar wat te noemen. Als het iets is wat je later weer nodig hebt kun je het altijd downloaden of printen voordat je het uit je e-mail account verwijdert.

Een **grote schoonmaak** gaat dieper en die zou je eens per jaar moeten doen. Archiveer alle gegevens in je e-mail of socialmedia-account, download die gegevens op je computer en verwij- der alle inhoud uit de accounts om weer met een schone lei te beginnen.

Tip: Als je het echt goed wilt doen, moet je niet alleen alles verwijderen, maar ook je prullenbak en tijdelijke bestanden leegmaken!

Je kunt zelf bepalen wat je het liefste doet: een back-up van je archieven en documenten in de cloud opslaan, of ze op een externe harde schijf of USB-stick bewaren. Hoe je de informatie ook opslaat, zorg ervoor dat je het niet kwijtraakt, dat je een sterk wachtwoord gebruikt en dat de methode bij je past.

Een product van
TACTICAL TECH

Ondersteund door
Firefox

5.

DOORGEVEN

Je zou het bijna vergeten, maar er is een reden dat we het internet het "web" noemen. **We zijn online allemaal met elkaar verbonden** door middel van verschillende netwerken, niet alleen als "vrienden" op social media, maar ook via de contacten in ons e-mailaccount en de foto's die we online delen. Als jij je accounts beveiligt, je wachtwoorden sterker maakt en je data opruimt ben jij niet de enige die daar baat bij heeft – **iedereen met wie je contact hebt, wordt zo een beetje veiliger door jouw inspanningen.**

Als je je e-mail en socialmedia-accounts opruimt bedenk dan wat je nog meer kunt downloaden en verwijderen om je vrienden en collega's te helpen: de bankgegevens van je zus, de toegangscode van het kantoor, de scan van het paspoort van je zoon zijn voorbeelden van gegevens die beslist niet in verkeerde handen mogen vallen.

Geef het door! Met een paar eenvoudige stappen kun je je digitale beveiliging verbeteren. Deel deze Data Detox met je vrienden, familie en collega's zodat ook zij hun gewoontes kunnen veranderen op een manier die bij hen past.

DATA DETOX KIT

VERANDER JE INSTELLINGEN

om je gegevens te beveiligen

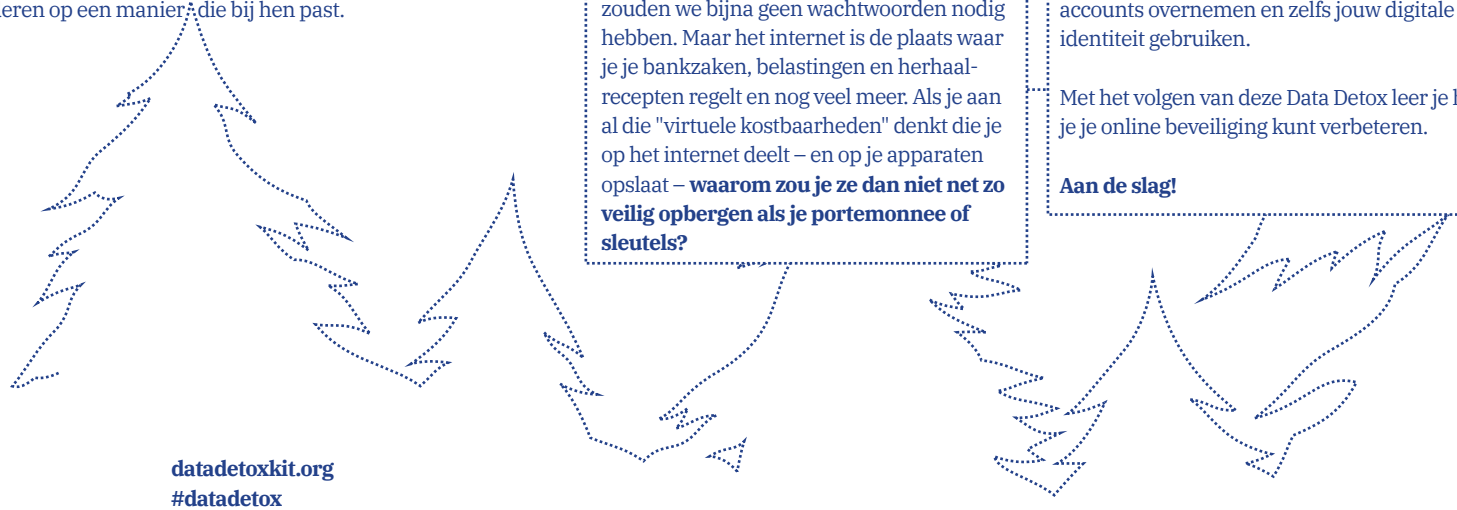
Als we op het internet alleen maar foto's van onze hond in rendierpak zouden delen, zouden we bijna geen wachtwoorden nodig hebben. Maar het internet is de plaats waar je je bankzaken, belastingen en herhaal- recepten regelt en nog veel meer. Als je aan al die "virtuele kostbaarheden" denkt die je op het internet deelt – en op je apparaten opslaat – **waarom zou je ze dan niet net zo veilig opbergen als je portemonnee of sleutels?**

Je kunt heel eenvoudig voorkomen dat anderen toegang krijgen tot jouw virtuele kostbaarheden: **zorg dat ze je wachtwoorden niet makkelijk kunnen raden**. Meestal hoeft iemand niet over gespecialiseerde technische vaardigheden te beschikken om in jouw account te komen – als ze goed kunnen raden, of een geautomatiseerd programma gebruiken, zijn ze zo binnen.

En als ze toegang hebben tot één account kunnen ze hetzelfde wachtwoord proberen voor je andere accounts; ze kunnen informatie verzamelen over jou en je gewoontes, je accounts overnemen en zelfs jouw digitale identiteit gebruiken.

Met het volgen van deze Data Detox leer je hoe je je online beveiliging kunt verbeteren.

Aan de slag!



datadetoxkit.org
#datadetox

1.

VERGRENDEL JE DIGITALE DEUR

Schermvergrendelingen: het wachtwoord, de vingerafdruk of gezichtsherkenning die je gebruikt om toegang te krijgen tot je apparaat zijn **prima verdedigingswerken** om te voorkomen dat iemand anders toegang krijgt tot je apparaat. Maar er zijn veel verschillende soorten vergrendelingen beschikbaar en het kan moeilijk zijn om te bepalen welke het beste werkt voor jou.

Iedere vorm van vergrendeling op je telefoon, tablet of computer geeft meer bescherming dan helemaal geen vergrendeling. En net als de verschillende soorten sloten die er voor deuren zijn, **zijn sommige schermver- grendelingen sterker dan andere.**

Van alle vergrendelingen die er bestaan zijn de lange, unieke wachtwoorden het sterkst. Dus als je je apparaat met een wachtwoord ontgrendelt, moet dat wachtwoord bestaan uit letters, cijfers en speciale tekens. Als je nu je telefoon opent door te vegen kun je de beveiliging verbeteren met het instellen van een lang wachtwoord. Gebruik je nu een bewegingspatroon? Dan zou je dat patroon langer kunnen maken. Gebruik je 1234 als pincode? Gooi eens zeven keer met een dobbelsteen en maak van die cijfers een pincode.

Met een kleine verandering kun je grotere controle krijgen over de beveiliging van je apparaten.

2.

EEN OPEN DEUR VOOR DE JUISTE PERSOON

Supergoede wachtwoorden maken is makkelijk. Je hoeft alleen maar wat basisprincipes te volgen. Kenmerken van een sterk wachtwoord:

Lang: **wachtwoorden moeten uit minimaal 8 tekens bestaan. Wil je het nog beter doen? 16 à 20 tekens.**

Uniek: **ieder wachtwoord voor iedere site moet anders zijn.**

Willekeurig: **je wachtwoord moet geen logisch patroon volgen of makkelijk te raden zijn. Wachtwoordmanagers kunnen je hierbij helpen.**

De sterkste wachtwoorden bestaan uit een combinatie van letters, cijfers en speciale tekens. Dit eeuwenoude advies is nog steeds van toepassing als het gaat om het maken van een sterk, moeilijk te raden wachtwoord. Helaas kun je in sommige wachtwoord- systemen geen gebruikmaken van speciale tekens (zoals @#$%-=+), maar een lange combinatie van letters en cijfers is nog altijd beter dan een korte.

Het is het beste als je een speciale wachtwoordmanager gebruikt om al je wachtwoorden te maken en bewaren. 1Password, LastPass en KeePassXC zijn wachtwoordmanagers die vaak worden aangeraden door beveiligingsexperts. Het zijn apps die je gebruikt om inloggegevens en andere gevoelige informatie te beschermen.

3.

MAAK EEN TWEEDE SLEUTEL

Als je tweestaps- of meervoudige verificatie instelt en iemand je wachtwoord ontdekt **beschikt die persoon waarschijnlijk niet over de extra informatie die nodig is om binnen te komen.**

Kijk eens naar de beveiligingsinstellingen van de sites en apps die je het meest gebruikt om te zien of je zo'n extra stap kunt instellen. Begin met de belangrijkste – bank-apps, of diensten zoals e-mail die je gebruikt als back-up wanneer je geen toegang krijgt tot je andere accounts.

Google:
Log in op: myaccount.google.com →
Beveiliging →
2-stapsverificatie →
Aan de slag

Facebook:
Menu →
Instellingen →
Beveiliging en aanmelding →
Tweestapsverificatie gebruiken

Tip: als je een tweede verificatiestap wilt instellen moet je een manier kiezen om te bevestigen dat jij het bent. Kies liever niet voor sms als tweede stap, want daar heb je niets aan als je je telefoon bent verloren. E-mail is een betere optie.

4.

LAAT JEZELF HOREN

Je kunt verschillende dingen doen als je niet blij bent met de verslavende ontwerpen of persuasive designs of desinformatie op websites die je bezoekt of in apps die je gebruikt: je kunt e-mails sturen, Tweets schrijven en bedrijven laten weten dat je het niet eens bent met hun praktijken. Als bedrijven door hun meest waardevolle bezit – hun gebruikers – onder druk worden gezet om actie te ondernemen, is er een kans dat ze veranderen.

En als je het gevoel hebt dat de feedback niet serieus wordt genomen, kun je een krachtig statement maken: een andere website of app gaan gebruiken. Als je hebt gecommuniceerd dat je niet blij bent met iets wat een website of app doet en je stopt met het bezoeken van die website of je die app verwijdert – en als er maar genoeg mensen zijn die dat ook doen – **dan moeten ze wel iets gaan doen met die feedback.**

5.

ZEGT HET VOORT!

Doorgeven! Deze tip vergeet je makkelijk, maar doorgeven van kennis kan veel effect hebben. Vertel je vrienden, familie en collega's over de dingen die je zijn opgevallen en vraag of ze met je willen meedoen aan deze detox! Iedereen worstelt met vervelende telefoongewoontes. Het belangrijkste is dat je een manier vindt die goed voelt en past bij je leefstijl. Experimenteer met de verschillende mogelijkheden totdat je iets vindt wat bij jou past. Er is niet één bepaalde oplossing die voor iedereen werkt.

En tenslotte: bespreek je technologiekeuzes met de mensen om je heen. Als je bijvoorbeeld iedere dag vanaf acht uur 's avonds niet meer bereikbaar bent via Messenger, omdat je schermvrije tijd dan begint, vertel dan dat ze je vanaf dat moment alleen nog kunnen bellen.

Blijf erover praten, stel vragen, leef een evenwichtig online leven dat bij jou past.

DATA DETOX KIT

ONTSNAP AAN DE STANDAARD

om je digitale gezondheid te verbeteren

Wanneer heb jij jezelf voor het laatst "ontkoppeld" en een dag, of zelfs een uur, geen technologie aangeraakt?

Als je continu online bent, ben je niet de enige. We tikken, klikken en swipen gemiddeld 2.600 keer per dag op onze telefoon (bron). Als je ergens zoveel tijd aan besteedt wil je ook dat het de moeite waard is. Hoe kun je ervoor zorgen dat de tijd die je doorbrengt met je apparaat ook kwaliteitstijd is?

Wil je een gezond evenwicht vinden tussen je online en je offline leven? Dan komt dit onderdeel van de Data Detox goed van pas.

Aan de slag!

Een product van
TACTICAL TECH

Ondersteund door
Firefox

datadetoxkit.org
#datadetox

1.

MET BEIDE BENEN OP DE GROND BLIJVEN STAAN

Deze tip is moeilijker dan hij klinkt. Erbij blijven vereist dagelijkse oefening. Het is als een spier in je hersenen die je regelmatig moet trainen om kracht op te bouwen. Eerst moet je inzicht krijgen in het soort relatie dat je hebt met de technologie die je gebruikt.

Hoeveel tijd breng je door op je telefoon?

Als het antwoord je niet aanstaat zijn er instellingen en strategieën die je kunt inzetten om meer controle te krijgen over je telefoongebruik.

Als je minder tijd op Facebook, Instagram of Twitter wil doorbrengen verander je de instellingen en machtigingen van die apps zodat ze beter voor je werken.

Sommige apps, zoals Instagram, bieden zelfs een optie waarbij de app je er vriendelijk aan herinnert dat je je dagelijkse limiet hebt bereikt.

Instagram:
Profiel → Menu → Instellingen→ Account → Je activiteit → Dagelijkse herinnering instellen

Als je vindt dat je gesprekken in het echte leven worden verstoord door de bliepjes, piepjes en lichtjes van je telefoon, kun je hem tijdelijk op stil zetten, met het scherm naar beneden wegleggen of hem in je zak of tas stoppen zodat hij buiten beeld is.

2.

ZOEK DE ONTWERPTRUCS

Met persuasive design (letterlijk: overtuigend ontwerp) wordt je beslissingsproces beïnvloed. De ontwerpen zijn gebaseerd op de menselijke psychologie en proberen je te verleiden om iets te ondertekenen of te kopen of meer persoonlijke informatie te geven dan je van plan was.

Veelvoorkomende ontwerpduwtjes en aansporingen zijn bijvoorbeeld specifieke kleuren, opvallende knoppen, onduidelijke teksten of incomplete informatie. Soms zijn deze trucjes overduidelijk, maar ze zijn ook vaak moeilijk te herkennen. Je zag ze misschien wel eens als je je ergens registreerde of online winkelde. De reden dat je die ontwerptrucs overal ziet is dat ze werken – we klikken, abonneren, kopen vaker en blijven terugkomen. Als je weet dat deze subtiele duwtjes en manipulaties in websites zijn ingebouwd kun je er ook slimmer mee omgaan.

Herken het duwtje: Stap één is dat je je bewust bent van deze technieken.

Screenshot delen: Maak een schermafbeelding als je online persuasive designs tegenkomt en deel ze met je vrienden (vergeet niet eerst je persoonlijke gegevens te verwijderen of te blurren - privacy voor alles!). Je kunt ook aan bedrijven vragen of ze hun manier van werken willen bijstellen.

Blijf kalm: Als er op een verkooppagina een aftelklok staat, vraag je dan af, "Heb ik dit product echt dringend nodig?" Als je merkt dat je op een knop klikt terwijl je dat eigenlijk niet wilde, bekijk dan wat er op de knoppen staat of welke kleuren er worden gebruikt. Als je in de war raakt denk dan niet automatisch dat het aan jou ligt – kijk met een kritische blik naar de woorden die de website of app gebruikt, want misschien zijn die wel onduidelijk.

3.

MEDIA, NIEUWS EN VERSTAND

Je kunt nu de functies en ontwerpen die bedoeld zijn om je continu te laten scrollen en klikken te slim af zijn. Hetzelfde geldt voor misleidende nieuwsberichten: gebruik je verstand en je trapt er niet in.

Het kan niet anders of je hebt wel eens gehoord van 'desinformatie', 'fake nieuws' en 'nepnieuws'. Je kunt desinformatie leren filteren als je er een gewoonte van maakt om kritische vragen te stellen bij het nieuws dat je ziet en leest, vooral als het er ongewoon, bizar of veel te leuk uitziet.

Eigenlijk wil je kunnen vaststellen of nieuws echt is of nep – vooral als je het nieuws wilt delen met familie en vrienden.

Waar komt deze website vandaan?
Wie heeft dit artikel geschreven?
Wat staat er eigenlijk in het artikel als je verder kijkt dan de kop?
Naar welke bronnen wordt verwezen?

Als je denkt dat het onjuiste informatie is en je wilt voorkomen dat het verder wordt verspreid, hebben de meeste platforms een knop om het bericht te rapporteren. Je kunt je ook afvragen of je de account die het heeft gepubliceerd wilt blijven volgen.

DATA DETOX KIT

5.

OP ZOEK NAAR DE WAARHEID OP INTERNET

De term "nepnieuws" of "fake nieuws" wordt gebruikt om te verwijzen naar een breed scala aan onjuiste of misleidende informatie, zoals satire, slecht onderzochte of niet-gecontroleerde content, hoaxen en scams. Nepnieuws wordt niet altijd met slechte bedoelingen verspreid, maar het resultaat is over het algemeen hetzelfde: de mensen die het nieuws ontvangen denken dat iets wat niet waar is juist wél waar is of dat er iets is gebeurd wat nooit gebeurd is.

In het beste geval gaat het om een grappige meme. In het slechtste geval gaat het om onjuiste gezondheidsinformatie of verkeerde politieke voorlichting.

Ook al doe je zo goed mogelijk onderzoek naar de artikelen en stel je kritische vragen, je kunt er toch van in de war raken als je ze leest. Maar: je bent niet alleen!

Alle hens aan dek
Ook al erkent een website zijn fouten niet, dan betekent dat niet dat ze geen fouten maken. Eigenlijk komen de meest betrouwbare publicaties van bedrijven die extra voorzichtig zijn met de waarheid en die mensen of hele afdelingen in dienst hebben die zich alleen maar bezighouden met feiten checken.

Zoek naar bronnen die rectificaties plaatsen als ze het mis hebben. Het mooiste is als de rectificatie boven aan het artikel staat en op social media wordt gedeeld, zodat je er niet eindeloos naar hoeft te zoeken.

6.

JE FILTERBUBBEL DOORPRIKKEN

Als websites en apps een profiel van je interesses hebben samengesteld kun je terechtkomen in een filterbubbel. Dan komen er meer verhalen en afbeeldingen in je nieuwsoverzicht die lijken op de items die je al eerder hebt aangeklikt. Dat beperkt en verandert wat je ziet en hoort, maar hoe?

Als je in een filterbubbel zit, zie je soms heel andere verhalen, nieuwskoppen, artikelen en advertenties dan de mensen om je heen. Dat wordt uit de doeken gedaan in het interactieve artikel Blue Feed, Red Feed (graphics.wsj.com/blue-feed-red-feed).

Als je weet dat de content die je in je apps en op websites ziet specifiek voor jou wordt bepaald door een algoritme, dan is de vraag: hoe kun je uit je filterbubbel stappen?

Verander van koers en hussel je nieuwsberichten door elkaar
Een goede manier om je filterbubbel door te prikken is je abonneren op diensten die nieuws en informatie uit verschillende bronnen samenvoegen en verschillende invalshoeken belichten. Met RSS-feeds, forums en mailinglijsten die ruimte bieden aan veel verschillende meningen en onderwerpen wordt het makkelijker om buiten je bubbel te kijken.

DATA DETOX KIT

ZES TIPS OM ONLINE UIT DE BUURT VAN DESINFORMATIE TE BLIJVEN

Apps, websites en online media kunnen essentieel zijn om toegang te krijgen tot nieuws, lifehacks en entertainment. Maar met die grote hoeveelheid content kan het moeilijk zijn om langs alle afleidingen te navigeren en te vinden wat je eigenlijk zoekt. Sterker nog, het kan moeilijk zijn om het verschil tussen feit en fictie te onderscheiden als je een video, afbeelding of artikel online ziet. Van persoonlijkheidskwisjes die een profiel van je proberen te schetsen tot schokkende krantenkoppen en bewerkte foto's of video's die je proberen te overtuigen van een compleet andere werkelijkheid: wat je online ziet, is niet altijd wat het lijkt.

Het stellen van kritische vragen is de beste verdediging, zodat je kunt leren wat het verschil is tussen een onschadelijke parodie en een hoax, tussen content die opzettelijk misleidend is en content die domweg slecht onderbouwd is en hoe je alarmbellen en onbetrouwbare bronnen kunt herkennen.

datadetoxkit.org **#datadetox**

Een product van
TACTICAL TECH

Projectpartners
Save the Children 100 ANNI
IFLA

Funded by the European Union

1.

JE HEBT DE MACHT OM REURING TE VEROORZAKEN

Liken, sharen, retweeten, kopiëren – al deze acties beschrijven hoe je interactie is met wat je online ziet – en jouw interacties hebben grote impact. Als er genoeg mensen zijn die iets doen met een afbeelding, video of bericht verspreidt die zich razendsnel en gaat viraal.

Sta even stil bij de vraag: "Welke impact heb ik online?" Wanneer heb je voor het laatst shockerende of grappige artikelen, kranten-koppen, video's of afbeeldingen gezien en die in een fractie van een seconde doorgestuurd naar je vrienden? Onderzoekers hebben vastgesteld dat juist de verhalen en afbeeldingen die angst, weerzin, verbijstering, boosheid of bezorgdheid oproepen viraal gaan. Heb je vanmorgen nog een bericht gedeeld? Maak je geen zorgen!

DATA DETOX KIT

Delen is lief
Delen is een vorm van meedoen. Als je iets deelt ben je een radertje in de kans dat iets viraal gaat. Als het nepnieuws blijkt te zijn zou je dan willen dat je naam en reputatie ermee verbonden zijn? Bedenk, voordat je een link deelt, of je misschien bijdraagt aan de verspreiding van onjuiste, destructieve of gemene dingen.

2.

DENK TWEE KEER NA VOORDAT JE DIE PERSOONLIJKHEIDSTEST DOET

Wanneer heb je voor het laatst een quiz voorbij zien komen (in tekst- of fotovorm) met titels zoals:

- Welk decennium ben jij?
- Welk dier ben jij?
- Welke Disney-boef ben jij?
- ... het gaat maar door!

Het kan een leuke quiz zijn over een leuk onderwerp, maar het is ook mogelijk dat de vragen zorgvuldig zijn samengesteld om **gegevens te verzamelen en een profiel van je te maken** op basis van zogenaamde psychometrische patronen.

De antwoorden die je geeft in een quiz zoals "Welk Simpsons-karakter ben jij?" en bepaalde gewoontes die je hebt die in de gaten worden gehouden door je browser, app of bijvoorbeeld een klantenkaarten zijn een bron van informatie. Het geeft data-analisten een idee van het soort persoon dat je bent, wat je leuk vindt, en hoe je te beïnvloeden bent om een bepaald soort schoenen te kopen ... Ze zouden zelfs een profiel van je kunnen maken om te bepalen op welke manier ze

Meer geheim houden
Als je denkt aan privé-informatie komen je wachtwoorden, BSN en pincode misschien als eerste in je op. Maar informatie over waar je bang voor bent, wat je irriteert en wat je ambities zijn, zijn net zo persoonlijk. Deze gegevens zijn van grote waarde voor data-analisten, want ze maken duidelijk waar jij als persoon gevoelig voor bent. Denk twee keer na voor je dergelijke informatie weggeeft in een enquête of quiz.

3.

HAP NIET TE SNEL

Clickbait is een term die wordt gebruikt voor sensationele, oneerlijke of verzonnen titels die als enig doel hebben dat mensen worden verleid om op de kop of link te klikken. Hoe meer aandacht er voor een artikel, video of afbeelding is, hoe meer geld ermee wordt verdiend. De makers trekken daarom alles uit de kast om jou zover te krijgen dat je klikt op hun content en die deelt.

Op basis van het profiel dat platforms (zoals Facebook en Instagram) van jou samenstelden krijg je koppen die op jou zijn afgestemd en **inspelen op jouw emoties**, zodat je erop klikt.

Clickbait kan hand in hand gaan met desinformatie, maar dat is niet altijd het geval. Als je clickbait-koppen leert herkennen, zie je ze opeens overal op YouTube, in blogs en in de roddelbladen..

Ga naar de bron
Als je wordt geconfronteerd met clickbait, kijk dan verder dan de koppen. Als de link veilig lijkt, klik dan naar het artikel en zoek uit wie het heeft geschreven, wanneer het is gepubliceerd en naar welke bronnen wordt verwezen. Het kan zijn dat er in het artikel een opmerking staat dat de content een advertorial is of dat het wordt beschouwd als opiniestuk. Deze informatie helpt om te beslissen of je energie wilt steken in het betreffende stuk.

4.

PAS OP VOOR DEEPFAKES

Deepfakes zijn video's, geluidsfragmenten of afbeeldingen die digitaal veranderd zijn, vooral om een gezicht of bepaalde bewegingen te vervangen of om iemands woorden te veranderen. Hoewel de term "deepfakes" nog maar kort wordt gebruikt, bestaat het fenomeen al jaren. De zogenaamde cheapfakes zijn nog makkelijker te maken – het is misleidende content die zonder geavanceerde technologie gecreëerd kan worden door gewoon een verkeerde titel bij een foto of video te zetten of verouderde content te gebruiken als illustratie bij een actuele gebeurtenis.

Het lijkt misschien onmogelijk om nepnieuws volledig te bestrijden, maar er is iets belangrijks wat je kunt doen ... laat je niet gek maken.

Laat je niet gek maken en ga op onderzoek uit
Net als wanneer je te maken hebt met clickbait moet je niets op het eerste gezicht accepteren. Als een video of foto er verrassend of bizar uitziet moet er een alarmbelletje gaan rinkelen. Hou er rekening mee dat er meer aan de hand is dan je op het eerste gezicht ziet. En als je ziet dat dezelfde afbeelding telkens weer in je nieuws-overzicht verschijnt, of meerdere keren met je gedeeld wordt, kan dat een reden zijn om de echte bron te achterhalen.

Dat is het moment dat je meer vragen moet gaan stellen: wie heeft het gepubliceerd (welke website, wie heeft het geschreven)? Wanneer is het gepubliceerd? Als het om een afbeelding gaat, zoek dan omgekeerd naar afbeeldingen op TinEye en zoek uit waar je de afbeelding nog meer ziet. Controleer andere geloofwaardige nieuwsbronnen voordat je aanneemt dat het wel waar zal zijn en voordat je de informatie of de afbeelding deelt met je familie en vrienden.