Browsen op je mobiele telefoon (praktijk)

www.data-detox.nl

DATA DETOX KIT

Aan de slag:

Omschrijving workshop
Eerst bekijken wat er via je browser met anderen wordt gedeeld en hoe dat werkt. En daarna concrete stappen nemen om het browsen meer privé en veiliger te maken.

Overzicht

1. Inleiding (10 min.)
2. De browser is tweerichtingsverkeer (60 min.)
3. Tracking in de browser (30 min.)
4. Browsen op je mobiele telefoon: praktijk (60 min.)
5. Zoekmachines (20 min.)
6. Strategieën (30 min.)
7. Afronding (20 min.)

Tijdsduur
200 minuten (pauzes niet meegerekend).

Ideaal aantal deelnemers
Splits de deelnemers op in twee groepen, aan de hand van het soort besturingssysteem dat ze gebruiken, iOS of Android. Er moeten dus ook minimaal twee trainers aanwezig zijn en het liefst een derde om zo nodig bij te springen.

- 2-20 deelnemers: 2-3 trainers
- 20-28 deelnemers: 4 trainers

Leerdoelen

Kennis

- Inzicht dat je browser misschien niet zo veilig is als je dacht en zien wat er onveilig is.
- Begrijpen wat “encryptie” betekent, hoe het internet werkt (infrastructuur) en op welke manier en waarom online tracking een voedingsbodem is voor advertenties.
- Weten wat er wordt bedoeld met “online anonimiteit” en in grote lijnen begrijpen wat Tor is.

Vaardigheden

- Weloverwogen besluiten nemen over welke browser je gebruikt.
- Datasporen die via de browser achterblijven beperken.
- Android: leren hoe je Firefox kunt installeren en aanpassen, en leren hoe je Orbot en Orfox installeert en gebruikt.
- iPhone: leren hoe je Safari aanpast om tracking te beperken.

Redenen

- Je kunt keuzes maken en eenvoudige stappen nemen om tracking te beperken.

Referenties

- Download het "Referentiedocument mobiele telefoons":https://data-detox.nl/wp-content/uploads/2020/01/verwijzing-REFERENTIEDOCUMENT-MOBIELE-TELEFOONS.pdf
- Het diagram van EFF over https en Tor: https://www.eff.org/pages/tor-and-https
- Trackography (Tactical Tech): https://trackography.org/
- Lightbeam: https://addons.mozilla.org/en-US/firefox/addon/lightbeam-3-0/
- Panopticlick (EFF): https://panopticlick.eff.org/

Benodigde materialen en apparatuur

- Telefoons van de deelnemers
- Tools kiezen - blanco raster: https://data-detox.nl/wp-content/uploads/2020/01/choosingtools_emptyframework.pdf
- Referentiedocument mobiele telefoons: zie boven
- Computer
- Projector
- Flip-over
- Markeerstiften
- Pennen
- Overzicht van "De Strategieën van het Verzet": https://data-detox.nl/wp-content/uploads/2020/01/verwijzing-DE-STRATEGIEËN-VAN-HET-VERZET-.pdf

Optionele materialen en hand-outs

- Pocket Privacy Guide - Mobile:https://data-detox.nl/wp-content/uploads/2020/01/pocket-privacy-mobile_en_complete.pdf.

Opbouw van de les

Stap 1: Inleiding (10 min.)

1. Vertel kort iets over jezelf en de les, doe een voorstelrondje en laat de deelnemers antwoord geven op de volgende vragen:
- Welke browsers gebruik je en waarom gebruik je juist deze browsers?
- Wat wil je in deze les leren?

2. Houd de verwachtingen van de deelnemers in gedachten als je een kort overzicht geeft van de les, noem de doelstellingen, vertel wat er wordt behandeld (en wat niet) en hoeveel tijd jullie daarvoor hebben.

Stap 2: De browser als tweerichtingsverkeer (30 min.)

De browser geeft ons toegang tot het internet, maar biedt tegelijkertijd anderen de toegang tot heel veel informatie over óns.
Deze activiteit geeft een overzicht van hoe het internet werkt en laat zien welke informatie derden kunnen zien als je aan het browsen bent of e-mail verzendt. Daarna zie je wat anderen kunnen zien als je het internet gebruikt via https en via Tor.
Activiteit: "Https en Tor"

Voorbereiding

1. Als de deelnemers een computer hebben (één per groepje), geef dan de URL voor het diagram van EFF en informatie over https en Tor: https://www.eff.org/pages/tor-and-https
2. Je kunt het diagram ook uitprinten in elke modus (http, https, Tor) - één setje per groepje.

Onderzoek https en Tor (10 min.)

1. Splits de deelnemers op in kleine groepjes.
2. Geef de groepjes wat tijd om het diagram over Tor en https te bekijken en laat ze hun bevindingen met elkaar bespreken.

Feedback en discussie (20 min.)

De groepjes doen verslag van hun bevindingen. In de discussie moeten de volgende onderwerpen worden besproken:

1. Wie heeft toegang tot je datasporen?
2. Wat is het verschil tussen http en https?
3. Wat is Tor?
4. Hoe anonimiseert Tor het browsen en hoe blokkeert hij online tracking?

Stap 3: Tracking in de browser (30 min.)

Tracking in de browser is vaak onzichtbaar. Met deze activiteit kunnen de deelnemers zien hoe tracking werkt.
Activiteit: "Tracking in de browser visualiseren"

Voorbereiding

1. Zorg dat je vertrouwd bent met Trackography en Lightbeam. Meer informatie kun je in het "Referentiedocument browser" vinden.
2. Zorg dat er genoeg computers zijn - één per klein groepje. Lightbeam kan niet worden geïnstalleerd op een mobiele telefoon en Trackography werkt alleen op een groter beeldscherm.
3. Schrijf de links voor Trackography en Lightbeam op het bord of projecteer ze op een scherm.
4. Als de internetverbinding zwak is, kun je de film over Trackography van tevoren downloaden en een schermafbeelding van Lightbeam laten zien.

Kennismaken met Trackography & Lightbeam (15 min.)

1. Verdeel de deelnemers tussen Trackography en Lightbeam, maak zo nodig nog kleinere groepen.
2. De deelnemers moeten de twee tools onderzoeken en hun bevindingen bespreken.

Feedback en discussie (15 min.)

De groepjes doen verslag van wat ze hebben ontdekt. Vul eventuele leemtes op en geef zo nodig uitleg. De volgende onderwerpen moeten worden behandeld:

1. Wat is tracking?
2. Welk soort data wordt er verzameld en door wie?
3. Wat is profielbepaling?
4. Hoe kunnen bedrijven me langs verschillende websites volgen? Wat is een browse-vingerafdruk? (Demo EFF's Panopticlick.)
5. Volgroutes: hoe gegevens over het internet reizen.
6. Vertel zo nodig hoe het internet werkt.

Stap 4: Browsen op je mobiele telefoon: praktijkles (60 min.)

Behandel in deze praktijkles de volgende onderwerpen (gedetailleerde informatie vind je in het "Referentiedocument mobiele telefoons"):

1. Vergelijken, kiezen en aanpassen

- Geef een overzicht van de verschillende browsers die er zijn voor het besturingssysteem dat je gaat bespreken. Daarna:
- Android: Firefox installeren en aanpassen (Firefox is de enige browser voor Android waarin de instellingen kunnen worden gewijzigd).
- iPhone: Safari aanpassen (Safari is de enige browser voor iPhone waarin de instellingen kunnen worden gewijzigd).

2. Installeer een VPN of Tor

Android:

- Installeer Orfox en Orbot.
- Bespreek alternatieve appstores en help de deelnemers bij het configureren van hun telefooninstellingen, zodat ze apps uit andere bronnen kunnen accepteren als ze die alternatieven willen gebruiken.

iPhone:

- Omdat Tor (via Orfox en Orbot) niet kan worden gebruikt met een iPhone is een VPN de beste optie. Laat de deelnemers zien hoe je een VPN kunt installeren en geef ze de mogelijkheid een VPN op te zetten.

Tips: "Hoe geef ik een praktijkles"

Voorbereiding

1. Test alle tools en instellingen die je in de les gaat installeren en/of gebruiken.
2. Zoek of maak hulpmiddelen waarmee de deelnemers zelf-lerend aan de slag kunnen.

Stappen

1. Splits de groep op naar gelang het aantal deelnemers, het aantal trainers en, als het aan de orde is, het besturingssysteem (bijv. Android of iPhone). Er is voor ieder groepje minimaal één trainer.
2. Leid ieder groepje stapsgewijs op een interactieve manier door het proces. De instructies kun je op de muur projecteren of printen.

Stap 5: Zoekmachines (20 min.)

Gebruik deze activiteit om de deelnemers te laten zien wat de belangrijkste verschillen tussen commerciële en "alternatieve" tools zijn; leg de nadruk op zoekmachines.

Activiteit: "Tools kiezen"

Voorbereiding

1. Print voor iedere deelnemer een beoordelingsraster "Tools kiezen" - zorg ervoor dat het blanco rasters zijn!
2. Download een raster dat al is ingevuld met specifieke tools:https://data-detox.nl/wp-content/uploads/2020/01/choosingtools_chatapps.pdf
Je kunt ook zelf een raster invullen, afhankelijk van welke tools en diensten je gaat bespreken in de les (bijv. zoekmachines of berichten-apps). Je kunt het ingevulde raster printen voor de deelnemers of het op de muur projecteren.

Brainstorm over apps en tools (5 min.)

1. Vertel kort iets over de activiteit en geef alle deelnemers een blanco tools-raster.
2. Richt je op een bepaald soort dienst (zoekmachines, berichten-apps, enz.), splits de deelnemers op in tweetallen en laat ze in de eerste kolom invullen welke namen van diensten/apps ze kennen (bijv. voor berichten-apps: Whatsapp, Snapchat, Signal).

Neem het beoordelingsraster door (20 min.)

1. Gebruik een van de diensten/apps (bijv. Whatsapp) als voorbeeld en neem samen met de groep stapsgewijs iedere categorie door. Leg uit wat de begrippen betekenen en beantwoord eventuele vragen.
2. De deelnemers gaan weer in tweetallen werken en krijgen tijd om de rest van het raster in te vullen.
3. Geef ze een ingevuld raster om te vergelijken met hun eigen raster en beantwoord eventuele vragen.

Discussie: Hoe besluit je welke tool het best bij jouw behoeften past? (10 min.)

Bespreek in een discussie het volgende:
1. Als je een tool kiest, is het belangrijk om na te denken over welke gegevens je wilt "beschermen". Het kan handig zijn om hierbij uit te gaan van vier categorieën: identiteit, sociale netwerken, content en locatie.
2. Een tool beschermt bijvoorbeeld je content met versleuteling, maar vereist ook toegang tot specifieke informatie zoals je telefoonnummer, waardoor het onmogelijk wordt de tool anoniem of onder pseudoniem te gebruiken. Als je een pseudoniem of anonimiteit nodig hebt, sluit een andere tool wellicht beter aan op je behoeften.

Stap 6: De Strategieën van het Verzet (30 min.)

Met deze activiteit maken de deelnemers kennis met de belangrijkste strategieën om meer controle te krijgen over de data die ze delen met commerciële bedrijven. Pas de activiteit aan zodat hij aansluit op browsen.

Activiteit: "De Strategieën van het Verzet"

Voorbereiding

1. Bereid je voor op de presentatie van de vier verzetscategorieën. Zorg dat je een uitgebreide lijst met voorbeelden hebt voor ieder categorie.
2. Maak een keuze voor het gebied waarop de groep zich gaat richten (bijv. browsertracking, locatie-tracking, mobiele telefoons in het algemeen, enz.).

Vier soorten verzet (15 min.)

1. Vraag de deelnemers op welke manieren ze hun online privacy hebben geprobeerd te verbeteren. Schrijf er een aantal van op het bord.
2. Gebruik de voorbeelden op de flip-over om te laten zien wat in grote lijnen de vier verzetsstrategieën zijn:

- Minderen (minder internetten)
- Een rookgordijn optrekken (verwarring zaaien, herrie maken)
- Opdelen in compartimenten (dingen van elkaar scheiden)
- Verdedigingswerken opwerpen (de speurders tegenhouden)

Brainstorm over de strategieën (20 min.)

1. Splits de deelnemers op in vier groepen en geef iedere groep één van de vier strategieën: Minderen, Een rookgordijn optrekken, Opdelen in compartimenten, Verdedigingswerken opwerpen.
2. Bepaal het aandachtsgebied (bijv. browsen, apps).
3. Ieder groepje gaat brainstormen over de manieren waarop ze hun gegevens op dit gebied kunnen verminderen, versluieren, opdelen en/of verdedigen.

Feedback: presentaties (15 min.)

Ieder groepje doet verslag aan de rest van de groep met behulp van een 2 à 3 minuten durende presentatie.

Discussie (10 min.)

Houd een korte discussie over de voordelen en beperkingen van iedere strategie, geef zo nodig voorzetjes.

Stap 7: Afronding (15 min.)

1. Kijk of er nog dingen onduidelijk zijn en beantwoord vragen.
2. Wijs de deelnemers de weg naar extra informatie.
3. Als je de "Pocket Privacy Guide - Mobile" van Tactical Tech hebt, kun je die uitdelen.