

Instellingen mobiele telefoon (praktijk)

130 minuten

Voorkom dat anderen toegang hebben tot je data door een aantal belangrijke instellingen te wijzigen.

Aan de slag:

Omschrijving

Voorkom dat anderen toegang hebben tot je data door een aantal belangrijke instellingen te wijzigen.

Overzicht

1. Inleiding (10 min.)
2. Waarom is je telefoon onveilig? (20 min.)
3. Praktijk (60 min.)
4. *Optioneel: De Strategieën van het Verzet (30 min.)
5. Afronding (10 min.)

Tijdsduur

130 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

- Weten welke soorten gegevens standaard worden verzameld via mobiele telefoons.

Vaardigheden

- De beveiliging van je mobiele telefoon kunnen verbeteren.
- De telefooninstellingen kunnen configureren om standaard dataverzameling te beperken.

Redenen

- Mobiele telefoons zijn standaard behoorlijk onveilig, maar er zijn eenvoudige manieren om de controle over je gegevens te vergroten.

Referenties

- Toolbox Internetvrijheid Bits of Freedom: iOS: <https://toolbox.bitsoffreedom.nl/overzicht/formfactor/mobiel/platform/ios/>
- Toolbox Internetvrijheid Bits of Freedom: Android: <https://toolbox.bitsoffreedom.nl/overzicht/formfactor/mobiel/platform/android/>

Benodigde materialen en apparatuur

- Computer
- Projector
- Mobiele telefoons van de deelnemers
- Referentiedocument mobiele telefoons: <https://data-detox.nl/wp-content/uploads/2020/01/verwijzing-REFERENTIEDOCUMENT-MOBIELE-TELEFOONS.pdf>

- Flip-over
- Markeerstiften
- Overzicht van “De Strategieën van het Verzet”: <https://data-detox.nl/wp-content/uploads/2020/01/verwijzing-DE-STRATEGIEËN-VAN-HET-VERZET-.pdf>
- 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.)

Vertel kort iets over jezelf en de les, doe een voorstelrondje en laat de deelnemers antwoord geven op de volgende vragen:

- Waar gebruik je je telefoon voor?
- Wat wil je in deze les leren?

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. Waarom is je telefoon onveilig? (20 min.)

Neem deze vragen door met de groep:

1. Hoe worden datasporen gecreëerd op je mobiele telefoon?

- De infrastructuur van mobiele communicatie brengt met zich mee dat bepaalde soorten data automatisch worden gecreëerd, zoals data over je precieze locatie.
- Er worden nog veel meer datasporen gecreëerd als we de telefoon en apps (bijv. Google Maps, Facebook, e-mail, andere apps) gebruiken.

2. Wat gebeurt er met deze sporen nadat ze zijn gecreëerd?

- Veel van die sporen worden in de telefoon zelf opgeslagen, wat gevolgen kan hebben als je telefoon in handen van andere mensen valt.
- Veel datasporen worden echter zonder jouw nadrukkelijke toestemming verzameld door bedrijven en instellingen.

3. Kun je controle uitoefenen op je datasporen?

- Het goede nieuws is dat je een béétje controle hebt over de gegevens die worden gecreëerd en verzameld. Met privacy en digitale veiligheid bestaat er geen alles of niets: ieder klein stapje telt. Het belangrijkste is dat je er mee aan de slag gaat en het voor jezelf zo goed mogelijk regelt.

Stap 3: Praktijk (60 min.)

Vraag de deelnemers om hun mobiele telefoon te pakken en maak twee groepen: Android & iPhone.

Neem de checklist voor praktijklessen door (zie het “Referentiedocument mobiele telefoons”) en laat met name het volgende aan de orde komen:

1. Controleer de basisbeveiliging en -privacy
 - E-mail
 - “Telefoonnaam”
 - Versleuteling
 - Simkaartvergrendeling
 - Wifi & bluetooth

- Wachtwoorden
- Locatie-instellingen
- Back-up maken & resetten

2. Beperk toegang & machtigingen van apps

- Controleer en beperk machtigingen van apps.
- Evalueer geïnstalleerde apps en verwijder onnodige apps.
- Meld je af voor op je profiel gebaseerde reclame (Android)

3. *Optioneel: Verander van browser, wijzig instellingen in je browser & en verander de manier waarop je toegang hebt tot netwerken.

In dit onderdeel moeten de volgende onderwerpen aan bod komen:

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).

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 4: *Optioneel: De Strategieën van het Verzet (30 min.)

Doe een oefening met de strategieën van verzet, eventueel in aangepaste, verkorte vorm, om de kennis van de deelnemers te toetsen. In het “Referentiedocument mobiele telefoons” vind je goede voorbeelden.

Activiteit: “De Strategieën van het Verzet”

Vorbereiding

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 5: Afronding (10 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.