Activité - L'empreinte numérique

TOUTES LES FICHES

par Nothing 2hide

PUBLIC	PARTICIPANTS	ANIMATEURS	NIVEAU	PRÉPARATION	ACTIVITÉ

Description

Cet atelier permet de prendre conscience que les navigateurs ont comme les mains une empreinte digitale unique qui permettent à des services en ligne de nous identifier de manière unique.

Objectifs

Empreinte numérique
Données personnelles
Identité numérique

Matériel

Ordinateurs
Smartphones ou tablettes
Une connexion à Internet

Contenus utilisés

https://amiunique.org/

Pré-requis

Aucun

WORKFLOW

1 Introduction

Les comportements en ligne sont tracés et enregistrés soit pour augmenter le ROI (retour sur investissement) d'un site de vente en ligne, soit pour savoir quels articles on lit le plus sur un site, soit (et c'est souvent le cas) pour vous proposer de la publicité ciblée en fonction de vos habitudes de surf.

Attention, les trackers n'utilisent pas seulement les cookies. Nous allons voir comment certains sites arrivent malgré les bloqueurs de publicité à quand même nous tracer grâce à notre empreinte numérique.

Conseil médiation :

Vous pouvez également compléter cette activité par l'activité "Introduction au tracking publicitaire" et par un débat mouvant sur la thématique des données personnelles et de la vie privée.

Pour avoir de plus amples informations sur ce sujet, nous vous conseillons de vous référer à la fiche outil "Les données personnelles".

2 Les marqueurs techniques

Pour faire comprendre aux participant.e.s ce qu'est l'empreinte numérique, diviser en petits groupes selon le type de téléphone ou d'ordinateur qu'ielles utilisent, puis selon la taille d'écran, puis selon la marque, puis selon l'endroit d'où ielles se connectent, etc.

Parcourir tous les marqueurs techniques susceptibles de les identifier et les diviser en autant de groupes différenciés par ces attributs. À la fin de cette partie de l'atelier déconnecté, tous les participant.e.s devraient se retrouver non plus en groupe, mais isolés tant ces marqueurs sont discriminants et précis. Procéder comme suit pour les smartphones :

- Demander aux participant.e.s "qui a un Iphone ? qui a un Android". Répartissez les participant.e.s dans ces groupes là
- Répartir les participant.e.s de chaque groupe déjà formé en nouveaux sous-groupes (iOS 9, iOS7, iOS10, Android 6, Android 7 etc.) : Pour obtenir la version de l'OS :
    - sur Android : paramètres, à propos, informations logicielles
    - sur Iphone : réglages > Général > Informations
- Demander ensuite aux participant.e.s de se diviser à nouveau en sous-groupe

en fonction du modèle de leur smartphone.
    - Pour les Iphones :5, 5c, 5S, 6, 7 8 X, Xs etc. La liste des modèles est disponible en ligne (il y a fort à parier que les possesseurs d'Iphone connaissent leur modèle de toute façon)
    - Pour les Android : commencer par le constructeur : Acer, Lenovo, Sony, Samsung, HTC, etc. (un liste ici)
        - puis séparer encore une fois les participant.e.s en fonction de leur modèle (Galaxy, Galaxy note, OHTc one, etc.). Vous trouverez une liste des marques et modèles par marque sur wikipédia (on trouve vraiment tout sur wikipédia)
- S'il reste encore des groupes de plus d'une personne, demander alors de lister leurs lieux de connexion. La plupart se sont forcément connecté.e.s au moins une fois chez eux.elles et à moins d'habiter ensemble, il ne restera plus que des individus épars et plus un seul groupe.

Sur ordinateur faire la même chose avec les critères suivants :

- Demander quel OS les participant.e.s utilisent : Windows, Mac OS ou Linux
- Demander quelle version de l'OS,
    - Windows (menu Démarrer, paramètres, système, à propos de) XP (!), Windows 8, Windows 10, etc.
    - Mac OS X (cliquer sur le menu pomme en haut à gauche de l'écran puis "à propos de ce mac") Leopard, snow leopard, Muntain lion, Sierra, Mojave etc.
- Demander quelle est la taille de leur écran (17 pouces, 19, 4:3, 16:9)
- Quel est le navigateur qu'ielles utilisent, chrome, firefox, safari, Internet explorer, edge
- Quelle version du navigateur
    - sur mac : safari, firefox ou chrome > en haut à gauche, menu pomme > à propos de safari
    - sur Windows
        - chrome : dans le menu en haut à droite de la barre d'adresse > Aide et à propos puis sur À propos de Google Chrome
        - firefox : dans le menu à droite de la barre d'adresse, cliquez sur l'icône représentant un point d'interrogation puis sur À propos de Mozilla Firefox.
        - Internet explorer : il suffit de cliquer sur ? dans le menu du haut d'Internet Explorer puis sur À propos d'Internet Explorer.
        - Edge : dans Windows 10, sélectionner Autres actions en haut à droite, puis Paramètres puis À propos de cette application.
    - Sur linux, manipulations identiques à Windows pour Safari et chrome.
- Demander alors de lister les plugins installés sur leur navigateur. Si les listes sont identiques, séparer les en plusieurs groupes.
- Enfin s'il subsiste des groupes, demander de lister leurs lieux de connexion. La plupart se sont forcément connecté.e.s au moins une fois chez eux.elles et à moins d'habiter ensemble, il n'y aura plus que des individus épars et plus un seul groupe.

Expliquer que tous ces marqueurs techniques sont envoyés aux sites visités chaque

fois qu'il y a une connexion. Résultat, certaines régies publicitaires qui ont des bouts de scripts installés sur les sites qui affichent de la pub avec leurs outils ont la possibilité de traquer un.e internaute et de l'identifier en fonction de ces paramètres techniques.

3 Amiunique.org

Dans la deuxième partie de l'atelier, en mode connecté cette fois, l'objectif est de montrer un site qui leur permet de visualiser l'empreinte numérique de leur téléphone ou de leur ordinateur.

Si des ordinateurs et une connexion Internet sont à disposition, ou si les participant.e.s ont des smartphones (ce qui est certainement le cas sinon cet atelier ne fonctionne pas trop), demander de se connecter sur le site https://amiunique.org/ . Ce site va dire à chaque personne qui s'y connecte si ses empreintes numériques permettent de l'identifier de manière unique.

Il sera possible de voir dans la page de détails d'autres marqueurs techniques non abordés dans cette fiche (ex : utilisation de flash ou non, mise en place du mode do not track, langue locale utilisée).

4 Conclusion

Il faut bien comprendre que lorsqu'on navigue sur Internet, on y laisse une empreinte numérique sur tous les sites que l'on visite, un peu à la manière d'un voleur qui cambriolerait une maison sans mettre de gants et qui laisserait ses empreintes digitales un peu partout. Certains services qui savent les collecter peuvent les utiliser.

Comme l'explique wikipédia sur son article sur les empreintes numériques :

"Certains fournisseurs de services (par exemple, des institutions financières ou des fournisseurs de services de courrier électronique) mémorisent les empreintes des ordinateurs fréquemment utilisés par leurs clients. Par la suite, lorsque quelqu'un tente de se connecter au service à partir d'un autre ordinateur, les fournisseurs demandent des preuves supplémentaires d'identité à la personne qui essayent de se connecter pour s'assurer qu'il ne s'agit pas d'un fraudeur. De même, lorsque l'on coche une mention semblable à *Je réutiliserai fréquemment cet ordinateur pour me connecter à ce service*, on demande à notre fournisseur de mémoriser l'empreinte de votre ordinateur et de se méfier de communications qui proviendraient d'un autre ordinateur. Il ne faut pas être surpris qu'un fournisseur nous demande des preuves supplémentaires d'identité.

Des régies publicitaires utilisent aussi des empreintes d'appareil pour reconnaître un internaute sur plusieurs sites, amasser de l'information sur ses intérêts et lui proposer

de la publicité ciblée. Certaines personnes considèrent qu'il s'agit là d'une violation de la vie privée parce que des informations sont accumulées sur les internautes à leur insu."

On laisse les participant.e.s juges de l'intérêt de laisser ses empreintes en ligne ou non. Pour celleux qui veulent effacer leur empreinte numérique et mettre des gants lors de leur navigation, il est possible d'utiliser un outil comme Tor qui non seulement change votre adresse IP mais prend également soin de vous attribuer une empreinte numérique standard, faisant ainsi en sorte de vous fondre dans la masse et de vous rendre très difficile à identifier. On vous explique son fonctionnement en détail dans la fiche d'activité un chemin Tortueux.