Atelier 1 : Vie privée et anonymat sur le web

Vue d'ensemble des traqueurs, des cookies tiers et de Tor. Veuillez étoffer votre rapport de captures d'écran en plus de répondre aux questions posées.

Cet atelier vous permettra d'en savoir plus sur la façon de protéger votre vie privée sur le Web. Effectuez les étapes ci-dessous sur votre ordinateur personnel.

Partie 1 : Consultez vos données

Plusieurs grandes entreprises vous permettent de vérifier et d'examiner les données qu'elles détiennent sur vous. Cela peut être très révélateur.

Utilisez ce lien pour apprendre à télécharger vos données à partir d'un ou de plusieurs des services suivants :

- Facebook (fortement recommandé)
- Instagram
- Google (si vous utilisez Gmail ou Google Drive, sachez que les téléchargements peuvent être volumineux)
- Instagram (si vous utilisez Gmail ou Google Drive, notez que les téléchargements peuvent être importants)
- LinkedIn
- Pinterest
- Twitter

Vous pouvez également consulter les liens ci-dessous pour télécharger vos données auprès de ces entreprises :

- Amazon
- Apple
- Snapchat

Si vous n'êtes pas client de l'une de ces entreprises, essayez de vérifier vos données auprès d'une autre entreprise que vous utilisez.

Question 1 : quels types d'informations ces services en ligne ont-ils collectés à votre sujet ?
Question 2 : les données vous concernant vous ont-elles surpris ?

Question 3 : inclure dans votre rapport une capture d'écran des fichiers que vous avez obtenus des services en ligne. Ne soumettez pas de capture d'écran du contenu de ces fichiers.

Partie 2 : Bloquer les traqueurs de publicité sur le web

Bien que les traqueurs de publicité semblent être omniprésents sur le Web, la bonne nouvelle est que les versions les plus récentes des principaux navigateurs Web, tels que Firefox, Brave et Safari (pour les appareils Apple), intègrent des protections de la vie privée.

Configuration de Firefox

Pour cette section de l'atelier, vous allez configurer Firefox sur votre ordinateur portable afin de bloquer et d'examiner les différents types de traqueurs Web.

1. Regardez cette vidéo d'une minute sur les protections de la vie privée dans Firefox
2. Assurez-vous d'avoir au moins Firefox 70
   - Si vous n'avez pas encore Firefox, téléchargez la dernière version de Firefox
   - Si Firefox est déjà installé sur votre ordinateur, vérifiez que vous avez installé Firefox 70 ou une version plus récente.

     Pour ce faire, visitez la page "À propos". La visite de cette page permet de télécharger toutes les mises à jour disponibles :
     - Sur Mac, allez dans le menu Firefox et sélectionnez "À propos de Firefox"
     - Sur Windows, allez dans le menu "Aide" et sélectionnez "À propos de Firefox"

     Si une mise à jour a été téléchargée, cliquez sur le bouton "Redémarrer pour mettre à jour Firefox".
3. Activez le blocage des empreintes digitales.
   - Ouvrez les préférences de Firefox en cliquant sur l'icône avec trois lignes horizontales (l'icône dite "hamburger") dans le coin supérieur droit de Firefox.
   - Sélectionnez "Confidentialité et sécurité"
   - Sous "Enhanced Tracking Protection", sélectionnez "Custom" et assurez-vous que les quatre cases sont cochées ("cookies", "Tracking content", "Cryptominers" et "Fingerprinters").

Utilisez Ghostery pour en savoir plus sur les traqueurs Web

Firefox bloque désormais les cookies tiers et les techniques d'empreintes digitales. Cependant, pour obtenir plus d'informations sur les traqueurs web, vous devrez ensuite installer Ghostery, une extension de navigateur qui bloque les publicités et les traqueurs.

1. Visitez le site https://www.ghostery.com/ghostery-ad-blocker et installez l'extension Ghostery dans Firefox.
2. Dans "Customize Setup", sélectionnez "Block Everything" et cliquez sur le bouton "Next". Décochez la case permettant d'envoyer des données analytiques anonymes à Ghostery.
3. Naviguez sur vos sites préférés et cliquez sur l'icône Ghostery après chaque chargement de page. Lequel de vos sites favoris utilise le plus de traqueurs web ?
4. Cliquez sur l'icône Ghostery et sélectionnez l'onglet "Detailed View". Cliquez sur le nom barré d'un traqueur publicitaire et, le cas échéant, cliquez sur "Continue to full tracker profile" pour en savoir plus sur le traqueur publicitaire.
5. Recherchez sur Google "politique de confidentialité" (ou "privacy policy") et le nom de l'un des traqueurs que vous avez identifiés pour en savoir plus sur la politique de confidentialité de ce traqueur.

Question 4 : quel est le nom du traqueur tiers dont vous avez entendu parler et quels types d'informations sa société recueille-t-elle à votre sujet ?

Partie 3 : Empreinte du navigateur

Visitez le site Coveryourtracks.eff.org et cliquez sur le bouton "Test your browser". Ne décochez pas l'option "Test with a real tracking company".

Question 5 : votre navigateur bloque-t-il les annonces de suivi ?
Question 6 : votre navigateur bloque-t-il les traqueurs invisibles ?
Question 7 : votre navigateur est-il protégé contre le "fingerprinting" ?

Dans la section "Detailled Results" du rapport, examinez les différents types de mesures pour voir combien de bits d'informations d'identification chacune fournit.

Remarque : le nombre de bits d'informations d'identification signifie que votre navigateur peut être identifié de manière unique à partir d'un ensemble de 2^bits d'informations d'identification. Un score plus faible est préférable, car il signifie que vous pouvez être identifié avec moins de précision. En voici un exemple :

"Nous observons que la distribution de notre empreinte digitale contient au moins 18,1 bits d'entropie, ce qui signifie que si nous choisissons un navigateur au hasard, au mieux nous nous attendons à ce qu'un seul navigateur sur 286777 partage son empreinte digitale. Parmi les navigateurs qui prennent en charge Flash ou Java, la situation est pire, puisque le navigateur moyen

contient au moins 18,8 bits d'informations d'identification. 94,2 % des navigateurs équipés de Flash ou de Java étaient uniques dans notre échantillon".

https://coveryourtracks.eff.org/static/browser-uniqueness.pdf

Question 8 : combien de bits d'informations d'identification Coveryourtracks.org rapporte-t-il pour votre navigateur ?

Partie 4 : Navigation anonyme sur le web

Attention ! A travers cet atelier, je ne cautionne aucune activité illégale.

Il arrive parfois que l'anonymat sur Internet soit souhaitable. Ce n'est pas la même chose que la confidentialité sur Internet. Avec la confidentialité, il n'est pas possible pour les oreilles indiscrètes de lire le trafic web. Avec l'anonymat, le trafic web ne peut pas être relié à son origine.

Le protocole HTTPS assure la confidentialité du trafic web, mais uniquement du contenu de la requête. Les éléments du trafic web tels que l'adresse IP source et de destination et les requêtes DNS sont publics. Cela signifie que si un militant politique utilise un ordinateur dont l'adresse IP est 192.0.2.1, qu'il se connecte à https://securedrop-pour-les-journalistes.exemple.com/soumettre/quelquechose/compromettant et soumet des documents ayant fait l'objet d'une fuite, les informations suivantes devraient être cryptées (confidentielles) :

- les informations de connexion
- les documents soumis
- le fait que le chemin demandé était /soumettre/quelquechose/compromettant

Cependant, https ne peut pas protéger les informations suivantes :

- L'adresse IP source 192.0.2.1
- La requête vers securedrop-pour-les-journalistes.exemple.com

Tester si la navigation privée anonymise les adresses IP sources

1. Rendez-vous sur le site https://whatismyip.com/ et notez votre adresse IP.
2. Activez le mode de confidentialité de votre navigateur (par exemple, "Mode Incognito" dans Chrome, "Navigation privée" dans Firefox et Safari).
3. Allez à nouveau sur https://whatismyip.com/ et notez votre adresse IP.

Notez que votre adresse IP n'a pas changé. Pourquoi n'a-t-elle pas changé ?

Question 9 : si votre véritable adresse IP peut toujours être vue par les serveurs web, que fait le mode de confidentialité de votre navigateur ? (Demandez à Internet si vous n'êtes pas sûr).

Tester si Tor anonymise les adresses IP source

Dans cette section, vous utiliserez le navigateur Tor.

1. Installez Tor si nécessaire : disponible pour Linux, Mac, et Windows ici.

   Remarque : si vous utilisez un Mac et que MacOS refuse d'ouvrir l'application Tor Browser parce qu'elle provient d'un développeur inconnu, maintenez la touche de contrôle enfoncée et cliquez avec le bouton droit de la souris sur l'application Tor Browser, puis sélectionnez "ouvrir". Cela créera une exception pour l'application Tor Browser et l'ouvrira.

2. Lancez le navigateur Tor.
3. Visitez https://whatismyip.com/ à l'intérieur du navigateur Tor et vérifiez que votre adresse IP a changé.
4. Déterminez votre adresse IP en utilisant trois sites web différents (par exemple, https://www.whatismyip.com/ , https://www.whatsmyip.org et https://whatismyipaddress.com/). Notez les adresses IP que chaque site signale à votre navigateur.
5. Recherchez l'emplacement de chaque adresse IP que vous avez notée à l'étape 4 à l'aide d'un service tel que https://www.wolframalpha.com/.

   Question 10 : à quelles régions du monde appartiennent les adresses IP que vous avez relevées à l'étape 4 ?

6. Lisez cette page sur ce que Tor peut et ne peut pas faire pour protéger votre anonymat : https://support.torproject.org/faq/staying-anonymous/

Visiter un serveur .onion

Comme indiqué précédemment, Tor permet également d'accéder à des serveurs qui ne sont accessibles que via le réseau Tor. C'est ce que l'on appelle familièrement le "dark web". S'il est vrai qu'il existe de nombreux sites fournissant des services illégaux sur le dark web, il existe également des utilisations légitimes du dark web.

Lisez ce court article sur le dark web : https://www.wired.co.uk/article/what-is-the-dark-web-how-to-access/

Accéder à des services Tor légitimes

Accédez à certains services Tor légitimes en utilisant le navigateur Tor :

SecureDrop : de nombreux organismes de presse utilisent SecureDrop pour "accepter en toute sécurité des documents provenant de sources anonymes", comme les lanceurs d'alerte. Visitez la FAQ de SecureDrop pour en savoir plus sur le fonctionnement de SecureDrop.

Ensuite, utilisez l'annuaire SecureDrop pour trouver et visiter les sites de dépôt de chacun des organismes de presse suivants :

- Le New York Times
- Le Washington Post
- ProPublica

Facebook : si vous avez un compte Facebook, vous pouvez accéder à Facebook en utilisant le service TOR :

https://www.facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion/

Facebook explique pourquoi il fournit une adresse en oignon :

Considérez Tor : Tor remet en question certaines hypothèses des mécanismes de sécurité de Facebook – par exemple, sa conception signifie que, du point de vue de nos systèmes, une personne qui semble se connecter depuis l'Australie à un moment donné peut, l'instant d'après, sembler se trouver en Suède ou au Canada. Dans d'autres contextes, un tel comportement pourrait suggérer qu'un compte piraté est accessible par l'intermédiaire d'un "botnet", mais pour Tor, c'est normal.

Remarque : Facebook affirme qu'en avril 2016, plus d'un million de personnes accèdent à Facebook via Tor.

The Federalist Papers : publiés à l'origine sous pseudonyme en 1787-1788 :

http://kx5thpx2olielkihfyo4jgjqfb7zx7wxr3sd4xzt26ochei4m6f7tayd.onion/book/9K0biYYOZKvPBokZ

Moteur de recherche DuckDuckGo :
https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion

Le service Tor officiel de la CIA :
http://ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion

OnionShare : envoyez et recevez des fichiers, chattez et hébergez des sites web de manière anonyme via le réseau Tor à l'aide d'OnionShare :
http://lldan5gahapx5k7iafb3s4ikijc4ni7gx5iywdflkba5y2ezyg6sjgyd.onion/