Comment bien cuisiner ses cookies ?

TOUTES LES FICHES

par MarieAnne Willefert

PUBLIC	PARTICIPANTS	ANIMATEURS	NIVEAU	PRÉPARATION	ACTIVITÉ

Objectifs

A la fin de cette formation, les participants sauront définir les termes techniques tels que « donnée personnelle » et « cookie ». Ils seront sensibilisés au fait que la moindre donnée est stockée et réutilisée, parfois à leur détriment, et donc qu'ils doivent apprendre à faire attention à ce qu'ils mettent sur le net. Nous leur apprendrons à identifier les différents cookies et à différencier ceux qui servent au bon fonctionnement d'une page web de ceux qui sont utilisés pour créer de la publicité ciblée. Enfin, les participants auront une liste de leurs droits et de conseils pour protéger leurs données de personnes malintentionnées.

Avec la première activité déconnectée, les participants sauront croiser les informations trouvées sur une personne sur un réseau social pour créer une publicité qui pourrait intéresser cette personne. De plus, lors de la deuxième activité déconnectée, ils réfléchiront sur la démarche à suivre selon une certaine situation.

Matériel

– connexion internet (identifiant sur Coggle) + diapo
OU
– crayons pour tableau blanc/craie
OU
– grandes feuilles blanches + crayons
– faux cookies en papier

Compétences travaillées

– Définition de termes techniques
– Découverte des différents cookies et de leurs différents rôles
– Savoir utiliser des informations sur une personne pour créer une publicité ciblée
– Comprendre comment les données sont récupérées
– Savoir se protéger

Pré-requis

Aucun pré-requis

WORKFLOW

1 Etape 1 : Présentation :

Se présenter aux participants et expliquer le déroulé de l'activité. Demander aux participants de se présenter et leur demander s'ils ont l'habitude d'utiliser internet et par quel(s) outil(s) : ordinateur, portable, tablette,… Nous leur demanderons également ce qu'ils attendent de cette formation.

Il faut bien préciser que cette fiche permettra aux participants d'acquérir des connaissances de base pour pouvoir suivre une formation plus poussée. Nous définirons avec eux les termes « données personnelles », « identité numérique », « cookies »,… Nous leur montrerons qu'il existe plusieurs cookies avec des rôles bien précis. Après avoir bien différencié les cookies, nous nous intéresserons aux droits qui protègent les utilisateurs d'internet, en particulier le règlement de l'Union Européenne sur les droits des données personnelles en 2018.

Au cours de cette formation, ils sauront définir une donnée personnelle et lister les risques qu'ils encourent à ne pas les protéger. Après avoir défini les risques, nous listerons quelques conseils clés pour éviter que les informations que nous partageons se retournent contre nous. Ensemble, nous identifierons quels sont les sites web qui récoltent nos données. Cela nous permettra de décrire le rôle des data-broker dans le business des données personnelles. Enfin, nous discuterons des différents droits qui protègent les utilisateurs.

2 Etape 2 : C'est quoi une donnée personnelle ?

1. **« Donnée personnelle » VS « identité numérique » : où est la différence ?**

Demander aux participants s'ils ont un compte sur un réseau social, une boîte mail, un jeu en ligne, un blog ou autre site web ? Si non, est-ce qu'ils connaissent quelqu'un qui utilise un réseau social ou autre ? Si oui, le(s)quel(s) ?

Leur demander s'ils ont dû donner des renseignements lors de leur inscription. Pour ceux qui n'ont pas de compte, leur proposer de réfléchir à ce qu'un site pourrait leur demander pendant une inscription (nom, adresse,…).

N.-B pour l'animateur : écrire sur un tableau, une grande feuille ou utiliser Coggle et projeter les réponses avec une diapo.

Avec les réponses des participants, définir avec eux une donnée personnelle.

Définition de la Cnil : « Toute information identifiant directement ou indirectement une personne physique (numéro de téléphone, photos, date de naissance, adresse physique/électronique, numéro sécurité sociale,…) ».

Contrairement à la donnée personnelle qui correspond aux informations qui ne sont pas visibles par tous (coordonnée bancaire), *l'identité numérique* correspond à toutes les traces que vous laissez consciemment (photos, vidéos, commentaires,…). Mais aussi les publications des autres dans lesquelles vous êtes cités. Pour faire simple, il s'agit de tout ce qui peut être visible par tous les utilisateurs du web et qui peut nous identifier.

2. **Identifier les requins qui menacent nos données** :

Nous avons tous au moins un espace client sur un réseau social, une messagerie électronique ou le site web de notre banque ou de notre assurance. Les jeunes prennent beaucoup de plaisir à surfer sur internet pour regarder leur clip préféré ou rencontrer d'autres jeunes avec qui ils partagent des centres d'intérêts. Mais nous nous ne méfions pas souvent des requins qui rôdent dans cet océan numérique, prêts à voler nos données les plus précieuses, transformant nos moments de plaisirs et de détente en véritable cauchemar.

Ces personnes malintentionnées veulent voler vos informations pour acheter des choses en lignes ou poster des photos/vidéos que vous souhaitez garder privée. La diffusion de certaines photos ou certaines vidéos peuvent mettre les victimes dans l'embarras et peut les poursuivre pendant des années. Certaines personnes peuvent être victime de *cyberharcèlement* !

Prenez-garde aussi au *phishing* (hameçonnage, en français), n'importe qui peut se faire passer pour une grande société (votre banque, votre assurance, …) pour voler vos identifiants et mots de passe. Par exemple, on vous envoie un mail pour vous raconter qu'il y un souci quelconque et on vous invite à vous connecter à votre espace personnel via un lien. De cette manière, ils vous volent votre identifiant et votre mot de passe. Si vous recevez un mail de votre banque et que vous avez un doute sur la véracité de ce mail, n'hésitez pas à la contacter, vous éviterez bien des tracas.

Nous pouvons également citer *l'usurpation d'identité en ligne*, « suite » du phishing, qui consiste à utiliser, sans votre accord, vos informations pour faire des achats en ligne, faire des abonnements ou commettre des actes répréhensibles.

Quand on utilise des données pour nuire à votre e-réputation ou celle d'un tiers, il s'agit de *diffamation* et peut avoir des impacts négatifs aussi bien sur votre vie réelle que votre vie virtuelle.

Ce n'est pas tout, même les réseaux sociaux, les moteurs de recherches et autres sites web enregistrent et stockent vos données. Pour ceux qui sont habitués aux réseaux sociaux, vous êtes-vous déjà demandé comment les créateurs des réseaux

sociaux peuvent être riches, alors que leur création est gratuite ? C'est parce que les données que vous partagez sont revendues aux publicitaires. De nombreux sites collectionnent nos données, il y a même des entreprises qui en ont fait leur activité principale. Ce sont les *Data broker (ou courtier de données)*. Mais comment font-ils pour récupérer ces données ?

3 Etape 3 : Recettes de cookies aux données personnelles :

1. **Un cookie, c'est quoi ? Ça se mange ?**

A chaque fois que vous vous connectez à un site, vous laissez des traces de votre passage (parfois involontairement). Ces traces sont les *cookies*, des petits fichiers textes déposés sur le disque dur de l'internaute par le serveur du site visité ou un serveur tiers (publicitaire,…). Parfois, lorsque vous allez sur un site web, un message apparaît et vous indique qu'il utilise des cookies. Leur « durée de vie » est de treize mois.

2. **A quoi ça sert ?**

Un cookie a plusieurs fonctions, mais il est surtout connu pour son rôle clé dans le marketing, l'analyse du comportement des usagers et dans le ciblage. Ainsi, dès que vous aimez une vidéo ou que vous visitez un site, ces informations sont enregistrées. Ne soyez pas surpris de voir le lendemain, une pub correspondant à vos recherches. Cet usage du cookie soulève beaucoup de questions et fait l'objet de recommandation et d'obligations émises par la Cnil (https://www.cnil.fr/fr/recherche/cookie).

Les cookies sont également utilisés pour reconnaître l'ordinateur d'un utilisateur (et pas l'inverse) lorsqu'il revient sur un site web. Ils permettent aussi de retrouver une page personnalisée automatiquement, même sans s'identifier, ou d'identifier des revisites.

Il existe de nombreuses sortes de cookies, tous avec des rôles bien définis.

3. **Des cookies par millier :**

Le cookie de session ou temporaire :
C'est un cookie dont la durée de vie est limitée à une session de navigation. Il est surtout utilisé pour la gestion des paniers d'achat sur les sites marchands.

Le cookie tiers :
C'est un cookie qui est placé sur l'ordinateur de l'internaute par le serveur d'un domaine distinct de celui du site visité. Les cookies tiers permettent un suivi comportemental sur un réseau de sites. Ils sont par exemple utilisés pour le ciblage

comportemental, car ils permettent de « reconnaître » un internaute sur un ensemble de sites distincts.

Le cookie post-view :
Un cookie post-view est un cookie placé par une régie publicitaire ou une plateforme d'affiliation pour mesurer l'impact d'un élément publicitaire qui est vu mais non cliqué. Il permet de connaître les visites par la mémorisation d'une offre publicitaire. Aujourd'hui, il est dominé par les cookies post-clic (cookie qui est déposé sur le poste de l'internaute après que celui-ci ait cliqué sur un lien publicitaire).

Les cookies des réseaux sociaux :
Les boutons de partage des réseaux sociaux (« j'aime » de Facebook) fonctionnent de la même manière que les autres cookies publicitaires. Quand un internaute se rend sur une page internet où se trouve l'un de ses boutons, le site peut associer cette visite à votre profil. Cela fonctionne même si vous ne cliquez pas sur « partagez », « j'aime » ou que vous n'êtes pas connecté sur le réseau. Le site peut ainsi adapter les publicités, vous inviter à rejoindre un groupe qui partage les mêmes centres d'intérêts, par rapport aux sites que vous avez visités.

N.-B : pour rendre cette partie de l'atelier un peu plus attractif, l'animateur peut créer des dépliants en forme de cookies. Un participant peut en choisir un au hasard, l'ouvrir et annoncer quel cookie il a pioché. Il peut essayer d'expliquer à quoi correspond ce cookie. S'il n'y arrive pas, les autres peuvent en discuter avec l'animateur.

4 Etape 4 : Atelier déconnecté : « Dans la peau d'un cookie » :

Après avoir découvert quelques cookies, les animateurs vont se mettre dans la peau des publicitaires. Selon le nombre de participants, vous pouvez former des groupes. Prévoir des feuilles blanches, des stylos, voire des crayons de bois et de couleurs.

Ils vont piocher au hasard une (ou plusieurs) page de renseignement sur un (ou plusieurs) utilisateur de Facebook. Ils étudieront les centres d'intérêts de l'internaute et ils créeront une ou plusieurs publicités qui pourraient plaire à cet internaute.

Par exemple, un utilisateur aime les motos et est fan d'une page Facebook consacrée à Johny Hallyday. De plus, il passe régulièrement du temps au cinéma. On peut créer de nombreuses publicités pour cet internaute : une publicité sur un CD des meilleures chansons de son chanteur préféré, des réductions du prix des places de cinéma, gagner un concours aux Etats-Unis en moto, …

Les participants pourront faire preuve d'imagination et créer les publicités les plus folles.

5 Etape 5 : Pêche interdite ou comment protéger ses données :

1. **La loi et les cookies** :
   Le fait que nos moindre faits et gestes soient ainsi enregistrés et réutilisés pour nous noyer sous des tonnes de publicités (parfois, sans que nous l'ayons demandé), fait grincer des dents. C'est pourquoi la loi oblige les sites internet de demander votre consentement avant le dépôt de ces cookies, vous indiquer à quoi ils servent et comment vous pouvez vous y opposer. En pratique, un message doit apparaître quand vous vous connectez au site pour la première fois pour vous indiquer comment accepter ou au contraire refuser les cookies. Il existe également des outils qui peuvent vous permettre de bloquer certains cookies lors de votre navigation. La Cnil a mis un au point un outil appelé CookieViz, pour vous permettre de visualiser en temps réel l'ampleur du phénomène des cookies ainsi que le nombre impressionnant d'acteurs qui interviennent pour analyser votre navigation.

Vous pouvez également trouver des conseils pour mieux protéger vos données, par exemple, comment se mettre en navigation privée.

2.**Vos droits** :

Que faire lorsque nous trouvons une vidéo gênante de nous pendant une soirée ? Dans ce moment-là, on se sent très seuls, on se dit que personne ne peut nous aider et que notre vie est finie. Pourtant, il y a une organisation qui veille que nos données personnelles soient respectées et protégées : la Cnil.

Sur le site de la Cnil, nous pouvons trouver des conseils pour protéger nos données, nos droits et les étapes pour toute démarche « administrative », par exemple, que faire contre des spams ou comment supprimer son compte Facebook.

Vous ne le savez sans doute pas, mais nous avons beaucoup de droits pour protéger notre vie privée.

Il y a *le droit d'accès*. Il consiste à avoir le droit de demander à un organisme (banque, site internet,…) s'il détient des informations sur vous et de demander à ce qu'on nous les communique. Ce droit permet ainsi de contrôler l'exactitude des données, les faire rectifier ou supprimer.

Le droit de rectification est une suite au droit précédent. Si nous remarquons une information inexacte ou incomplète nous concernant, nous pouvons demander à la rectifier.
Il y également le droit d'opposition qui permet de s'opposer à tout moment à ce qu'un organisme utilise certaines données pour un objectif précis. Par exemple, demander à ne plus recevoir de publicités.

Enfin, *le droit de déréférencement* (ou *droit à l'oubli numérique*) qui nous autorise à

demander aux moteurs de recherche de ne plus associer un contenu qui nous porte préjudice (délai entre 1 et 3 mois). Mais ce droit à des limites, telles que cette suppression ne signifie pas l'effacement de l'information du site internet source, ou que la personne qui a diffusé cette information refuse d'effacer cette information. Dans ce cas, il faut porter plainte auprès de la Cnil soit en ligne, soit par courrier.

N.B : ne pas hésiter à faire participer le public en lui demandant s'il sait à quoi correspond chaque loi. De plus, il serait intéressant d'utiliser une grande feuille blanche (ou Coggle) pour faire le lien entre les lois et leurs conséquences. Par exemple : « droit de déréférencement » = « droit à l'oubli » = « effacement d'un contenu nous concernant » = « limites ».

3.**Quelques conseils** :

La Cnil a mis au point une petite charte en 10 points (voir ci-dessous) pour que les internautes puissent mieux protéger leurs données. Avec les participants, vous pouvez créer la vôtre.

- Respectez les autres,
- Faites attention à ce que vous publiez sur le net,
- Ne dites pas tout,
- Protégez vos comptes (paramétrez vos profils sur les réseaux sociaux pour garder le contrôle sur vos informations),
- Créez plusieurs adresses mails,
- Ne publiez pas de photos ou de vidéos gênantes,
- Utilisez un pseudo,
- Faites attention à vos mots de passe,
- Nettoyez vos historiques,
- Vérifiez vos traces (tapez votre nom sur Google).

6 Lexique :

Blog : Site web ne nécessitant pas de connaissance particulière en programmation sur lequel un internaute tient une chronique personnelle ou consacrée à un sujet particulier. Les articles (ou billets) sont généralement affichés dans l'ordre chronologique inversé et ouverts aux commentaires des visiteurs du blog.

Cnil : (Commission Nationale de l'Informatique et des Libertés) : Veille à ce que l'informatique respecte les libertés, les droits, la vie privée des internautes.

Cookies : Fichier contenant des informations sur nous, lors de notre visite sur un site (nom d'utilisateur, mot de passe,…).

Cyber-harcèlement : Diffusion de textes, d'images ou de films diffamatoires via un moyen de communication moderne pour calomnier, compromettre ou harceler quelqu'un.

Data broker : personne ou entreprise dont l'activité est basée sur la revente de

données à des entreprises de marketing ou des annonceurs.

Diffamation : C'est le fait de s'exprimer de façon injurieuse sur une personne que l'on connaît ou pas, mais qui est reconnaissable. Elle peut être raciste, homophobe ou sexiste.

Données personnelles : Toutes les informations relative à une personne, permettant de l'identifier (nom, adresse, téléphone,…). A ne pas confondre avec l'identité numérique.

Droit d'accès : Droit obligeant le gestionnaire d'un fichier informatique doit permettre à toute personne qui en fait la demande, d'accéder aux informations qui la concerne et de faire modifier ou annuler certaines de ces informations.

Droit de déréférencement (Droit à l'oubli numérique) : Droit qui existe suite à une décision de la Cour de justice de l'Union européenne. Il permet aux européens de demander la suppression de résultats présents sur les moteurs de recherche qui sont obsolètes, excessifs, ou inappropriés portant atteinte à leur e-réputation.

Droit à l'image : Droit qui permet à toute personne de s'opposer ou non à la diffusion de photos, de vidéos,… où elle apparaît.

Droit d'opposition : Droit permettant, à toute personne qui le souhaite, de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Droit de rectification : Droit permettant à chaque individu a le droit de faire corriger des erreurs le concernant. Les informations corrigeables sont celles qui sont inexactes, incomplètes, équivoques ou périmées.

E-réputation (ou réputation électronique) : C'est l'ensemble des informations disponibles sur internet concernant un internaute. Ces informations peuvent prendre plusieurs formes : commentaires, « J'aime », photos, vidéos,…

Facebook : Réseau social en ligne qui permet à ses utilisateurs de publier des images, des photos, des vidéos, des fichiers et documents, d'échanger des messages, joindre et créer des groupes et d'utiliser une variété d'applications.

Identifiant : Code personnel permettant d'accéder à un service informatique.

Identité numérique : Correspond à toutes les traces que vous laissez consciemment : photos, vidéos, commentaires. Peut-être visible par tous les utilisateurs du site, comme un commentaire sur Youtube. A ne pas confondre avec la donnée personnelle.

Instagram : C'est à la fois une application, un réseau social et un service de partage de photos et de vidéos disponibles sur plates-formes mobiles de type iOS, Android et Windows Phone.

Mot de passe : Mot d'identification pour accéder à un compte personnel. Pour plus de sécurité, il doit être composé de majuscule, de minuscule, de chiffres et de caractères spéciaux (@, !, ?, …).

Navigation privée : Fonction complémentaire de plusieurs navigateurs web, permettant de naviguer sur le web sans que les données de navigation comme la partie historique ou les cookies soient conservées.

Phishing (ou hameçonnage) : Technique utilisée par les escrocs sur internet pour obtenir des informations personnelles. Ils se font passer, par exemple, pour votre banque et demande vos coordonnées bancaires.

Réseau social : Site internet qui permet aux internautes de se créer une page personnelle afin de partager et d'échanger des informations, des photos ou des vidéos avec leur communauté d'amis et leur réseau de connaissances.

Snapchat : C'est une application de photographie pour smartphones disponible sur iOS et Android. Elle a la particularité de permettre la publication de clichés ou de vidéos éphémères.

Twitter : C'est un réseau social permettant à l'utilisateur d'envoyer gratuitement des messages brefs appelés « tweets ».

Usurpation d'identité : Fait de voler l'identité numérique de quelqu'un pour faire des achats ou arnaquer d'autres personnes.

WhatsApp : Application mobile qui fonctionne grâce à une connexion internet et se présente comme une alternative aux SMS et MMS : un moyen de communiquer gratuitement à l'étranger lorsqu'on dispose d'une connexion wifi.

Wifi : Permet de relier sans fil plusieurs appareils informatiques et mobiles (portable, tablettes,…) au sein d'un réseau informatique afin de permettre la transmission de données entre eux.