

Thème : Web

ACTIVITE: Sécurité et confidentialité

Découverte des cookies et des traces laissées sur les postes.

1. Présentation de la CNIL :

La CNIL est une autorité indépendante et impartiale (composée de parlementaires, hauts magistrats...), qui doit promouvoir, faire respecter et faire évoluer la loi « informatique et libertés » en :

- **Informier et protéger les droits** en informant les personnes physiques et les responsables de traitement de leurs droits et obligations. Toute personne peut s'adresser à la CNIL en cas de difficulté dans l'exercice de ses droits en lui adressant une plainte.
- **Accompagner la conformité, conseiller** en veillant à ce que les traitements de données à caractère personnel soient conformes à la loi. La mise en conformité constitue l'objectif prioritaire du régulateur qu'est la CNIL.
- **Anticiper et innover**, dans le cadre de son activité d'innovation et de prospective, la CNIL s'intéresse aux signaux faibles et aux sujets émergents.
- **Contrôler et sanctionner** en donnant des avis sur des traitements et en proposant des mesures législatives ou réglementaires en fonction des évolutions des technologies de l'information. En cas de manquements constatés, elle peut décider de les mettre en demeure ou de les sanctionner.

2. Regarder la vidéo de la CNIL sur les cookies.

Consulter le site de la CNIL et visionner la vidéo (3mn35) : [Tutoriel – Qu'est-ce qu'un cookie ?](#) sur Daylimotion ou [Tutoriel – Qu'est-ce qu'un cookie ?](#) sur Youtube

3. Débat : Faut-il supprimer les cookies ?

4. Faut-il effacer l'historique de navigation ?

Consulter l'article sur le site de la CNIL à ce sujet et rédiger une synthèse individuellement:

<https://www.cnil.fr/fr/faites-regulierement-le-menage-dans-l-historique-de-navigation>


Observer les traces laissées sur un poste suite à la navigation sur le Web.

5. Quelles informations obtenons-nous en consultant cet historique ?


6. Même question pour les téléchargements. Quelles informations confidentielles peut-on obtenir ? Et si on déplace ou supprime un fichier téléchargé, apparaît-il toujours dans la liste des téléchargements ? Si on supprime la liste des téléchargements, supprime-t-on le fichier téléchargé ?

7. Supprimer les cookies de son navigateur pour ensuite consulter des sites marchands et vérifier ce qui est à nouveau installés.

Effacer les cookies avec Google Chrome

- Cliquer sur l'icône  en haut à droite de la fenêtre pour ouvrir le menu de réglage et choisir **Paramètres**.
- Dans la fenêtre qui s'affiche, cliquer sur "Paramètres avancés" puis sur **Effacer les données de navigation**.
- Cocher la case **Cookies et autres données de site** et cliquer sur **Effacer les données**. Fermer ensuite la fenêtre des réglages.

Supprimer les cookies avec Firefox

- Cliquer sur l'icône  en haut à droite de la fenêtre pour ouvrir le menu de réglage et choisir **Options** puis **Vie privée et Sécurité** puis dans la partie Historique, cliquer sur **Effacer les données**.
- Dans la fenêtre qui s'affiche, cocher la case **Cookies** et cliquer sur **Effacer maintenant**.

Effacer les cookies avec Internet Explorer

- Cliquer sur la roue dentée en haut à droite de la fenêtre pour faire apparaître le menu **Outils** et sélectionner **Options Internet**.
- Dans la fenêtre qui s'affiche, sélectionner l'onglet **Général** puis, dans la rubrique **Historique de navigation**, cliquer sur le bouton **Supprimer...**
- Cocher la case **Cookies et données de sites Web** et cliquer sur **Supprimer**. Cliquer ensuite sur **OK** pour fermer la fenêtre de réglages.


Consulter une page web de e-commerce et ajouter des produits dans le panier

- Fermer le navigateur
- Retourner sur les paramètres d'affichage des cookies
- Vérifier ceux nouvellement installés

Paramétrer les navigateurs pour ne pas garder les traces de navigation.

1. Repérer l'historique des sites web visités dans le navigateur et consulter l'historique avant de le supprimer.
 - Onglet **historique**
 - Cliquer sur **afficher l'historique**
2. Supprimer l'historique de navigation :

Effacer l'historique avec Google Chrome

- Cliquer sur l'icône  en haut à droite de la fenêtre pour ouvrir le menu de réglage et choisir **Paramètres**.
- Dans la fenêtre qui s'affiche, cliquer sur "Paramètres avancés" puis sur **Effacer les données de navigation**.
- Cocher la case **Historique de navigation** et cliquer sur **Effacer les données**. Fermer ensuite la fenêtre des réglages.

Effacer l'historique avec Firefox

- Cliquer sur l'icône ≡ en haut à droite de la fenêtre pour ouvrir le menu de réglage et choisir **Options** puis **Vie privée et Sécurité** puis dans la partie Historique, cliquer sur **Effacer l'historique**.
- Dans la fenêtre qui s'affiche, cocher la case **Cookies** et cliquer sur **Effacer maintenant**.

Effacer l'historique avec Internet Explorer

- Cliquer sur la roue dentée en haut à droite de la fenêtre pour faire apparaître le menu **Outils** et sélectionner **Options Internet**.
- Dans la fenêtre qui s'affiche, sélectionner l'onglet **Général** puis, dans la rubrique **Historique de navigation**, cliquer sur le bouton **Supprimer...**
- Cocher la case **Historique** et cliquer sur **Supprimer**. Cliquer ensuite sur **OK** pour fermer la fenêtre de réglages.

Présenter les informations qu'un site Web peut obtenir grâce à l'adresse IP

1. Préciser et faire vérifier que dans le cas du lycée, tout le monde est identifié par la même adresse IPV4 en faisant CheckIP (exemple outil libre tel que *Network stuff* présent sur la liberkey (<https://www.liberkey.com>), onglet *Computer's IP*).

Lancer l'outil Network stuff, onglet Computer's IP.

Tous les élèves d'une même classe ont la même adresse « Outside IP » et une adresse du réseau interne « Local IP(s) » différente.

2. Contrôler l'utilisation d'un proxy pour accéder à Internet en utilisant le lien suivant : <https://www.whatismyip.com/proxy-check/>

Cet outil permet d'indiquer qui fait la demande de requête : Un proxy (mandataire pour plusieurs clients) ou un poste individuel ?

Le proxy est un serveur mandataire qui permet de centraliser les demandes clients. A l'origine il permet de mettre en mémoire cache les réponses des serveurs (pages statiques, images...) de façon à optimiser les temps de réponse lors de requêtes identiques.

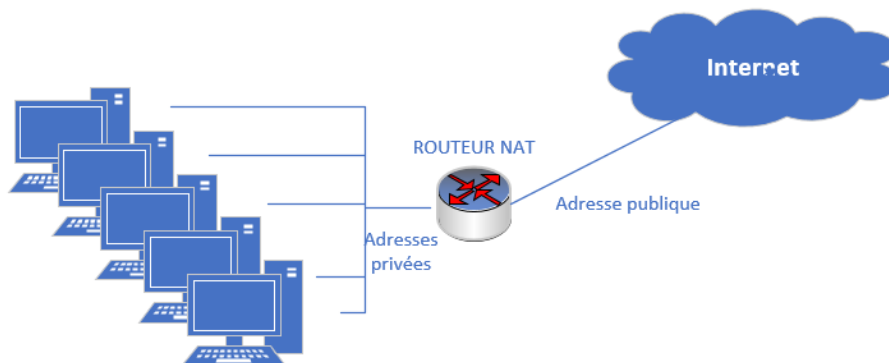
Par exemple lorsque les élèves d'un établissement ont la page Google affichée par défaut lors du lancement de leur navigateur. La page est demandée pour les centaines d'élèves qui se connectent en même temps. Le proxy mémorise la page d'accueil de Google et la renvoie sur les postes clients-élèves sans aller chercher la page chez Google à chaque fois.

Aujourd'hui on profite de ce passage obligé pour ajouter des fonctionnalités contrôle, comme le filtrage d'URL (exemple : contrôle parental, contrôle des sites accessibles dans un établissement scolaire...).

Le proxy d'un établissement enregistre toutes les transactions dans un journal.

En raison du manque d'adresses IPV4 disponibles, chaque réseau contient un routeur permettant de faire correspondre des adresses IP interne à une adresse IP publique. C'est la fonction d'un routeur NAT (*Network Address Translation*) d'attribuer plusieurs adresses IP (postes) du réseau interne à une

seule adresse publique. Seul le routeur NAT sait qui fait une requête vers un site web externe et à qui il faut retourner la réponse sur le réseau interne.



C'est pour cette raison qu'il est très facile de retrouver l'utilisateur grâce à son adresse IP interne au réseau lorsqu'il y a un problème. A l'adresse IP d'un poste est associée une machine. Grâce aux journaux, il est alors possible de savoir quel jour et à quelle heure s'est connecté un utilisateur sur cette machine et quelles requêtes Web il a effectué grâce au proxy !

3. Consulter son adresse IP et les informations associées au navigateur

<https://www.iplocation.net/find-ip-address>.

Cliquer sur [details] sur la ligne *IP Location* pour avoir la géolocalisation de l'adresse IP.

Observer : Quelles sont les informations utiles pour les applications Web ?

4. Quelles informations sont laissées par les autres acteurs du Web ?

Rechercher sur un moteur de recherche votre nom et prénom.

Que constatez-vous ? Est-ce vous qui avez laissé ces informations sur le Web ?

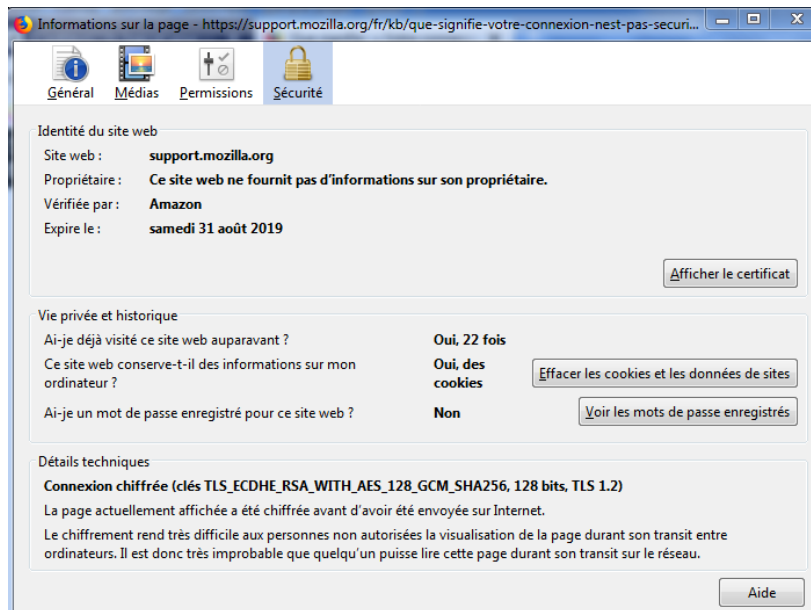
Consulter le certificat d'un site.

1. Les certificats valides et non valides.

Les certificats valides sont de couleur verte :

  <https://s>

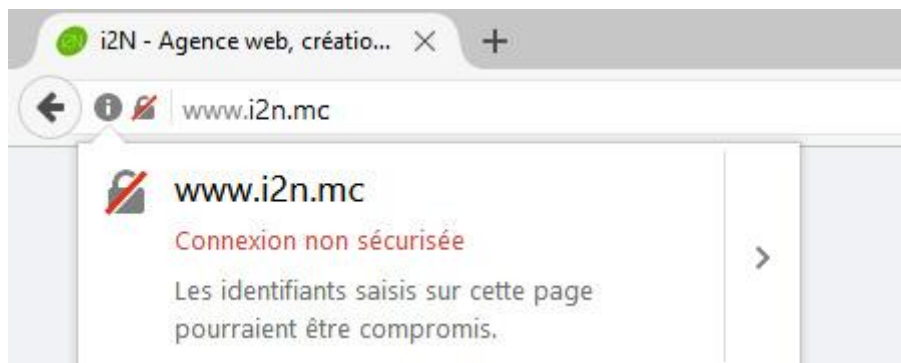
En double cliquant sur le cadenas et en demandant des renseignements supplémentaires on obtient la boîte de dialogue suivante :



Des éléments importants du contrat de sécurité apparaissent :

La date d'expiration du certificat. Dans cet exemple le site est considéré comme sécurisé.

En revanche lorsque l'on trouve le cadenas barré en rouge comme ici, il faut éviter de consulter ces sites:



Le cadenas barré en rouge signifie que ce site n'utilise pas HTTPS mais HTTP, protocole qui est de moins en moins utilisé sur Internet. Le site n'est pas sécurisé, qu'il n'utilise pas de certificat. Les communications entre les clients et les serveurs ne sont pas chiffrées, un hacker peut donc intercepter et utiliser les données de communication.

Les certificats sont émis par des autorités de certification (tiers de confiance), il en existe plusieurs sur Internet. Ce service est payant, mais il garantit la sécurité des échanges de données. Les autorités de certification surveillent la validité des certificats. En cas de perte ou de vol des clés de chiffrement (permettant de chiffrer et de déchiffrer les données), il faut avertir les autorités le plus rapidement possible afin de demander la révocation des certificats compromis. Cette révocation est diffusée à travers une black-list qui permet de bloquer l'accès aux sites qui utiliseraient ces certificats volés.

Présentation des pop-up et de l'hameçonnage (phishing).

1. Observer les pop-up et les cases cochées lors des téléchargements de logiciels gratuits.

A partir d'un site web Télécharger un logiciel comme Notepad++ et observer les *pop-up* qui s'affichent sur la page Web et si elles existent les cases cochées/décochées lors de l'installation.

2. L'hameçonnage peut être caché sous forme d'hyperlien Web envoyé par email ou affiché sur un lien d'un site Web.

Ne pas cliquer sur les liens dont le nom de domaine n'est pas en lien avec le site consulté. Passer la souris sur le lien ci-dessous sans cliquer :

<https://www.cnil.fr/fr/phishing-detecter-un-message-malveillant>

En réalité ce lien renvoie sur un site fictif (qui n'existe pas) qui pourrait être réellement un site d'escroquerie. En passant le curseur de la souris sur le lien sans cliquer, vous avez l'adresse réelle cachée par l'hyperlien.