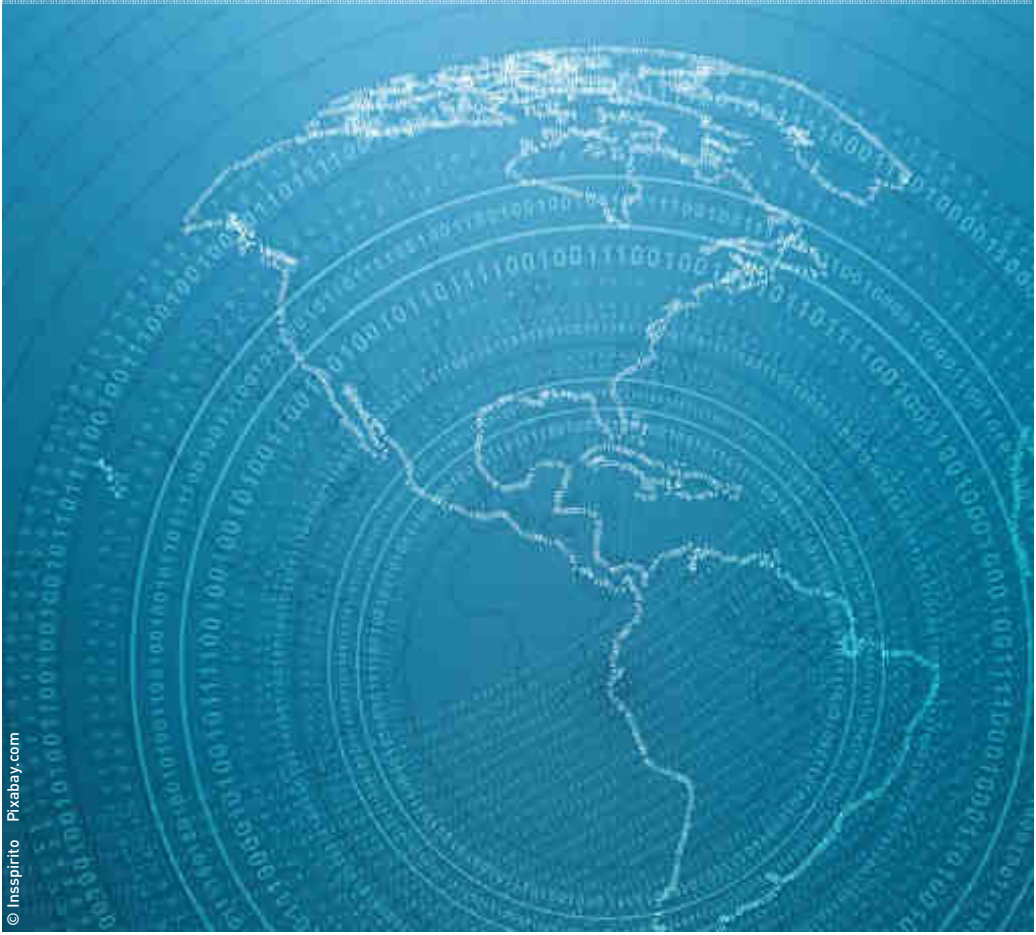
Centre Culturel Communautaire des Cordeliers

SURFEZ TRANQUILLE !

Astuces pour bien profiter de la toile sur tablette, smartphone et ordinateur.



Soyez discrets sur le net

Les navigateurs, moteurs de recherche, réseaux sociaux et sites internet veulent tout savoir sur vous. Leur but, **définir au plus juste votre profil de consommateur** pour pouvoir vendre ces précieuses informations à d'autres sites et entreprises qui vous proposeront des publicités ciblées.
L'outil de recueil de données le plus connu et le plus exploitable à l'heure actuelle est le **cookie**. Mais il faut savoir que vos « **like** », vos requêtes auprès des **moteurs de recherche** ou tout simplement les informations que vous avez échangées sur les **réseaux sociaux** sont capitalisés dans le même but commercial.

BOÎTE À OUTILS

- Configurez votre navigateur.

⇒ En vérifiant les paramètres de confidentialité : **supprimez régulièrement votre historique** et veillez à bien cocher la case ***cookies.***
Vous pouvez aussi **paramétrer le navigateur** pour que ces informations s'effacent à chaque fermeture.

⇒ Contrôlez tous les onglets des paramètres relatifs à la vie privée, les mots de passe et formulaires, la géolocalisation… Décochez tout ce qui vous paraît superflu (la plupart des options !).

Pour vous guider **2 liens vers des tutoriels** :

◊ http://www.linternaute.com/hightech/encyclo-pratique/internet/divers/4450/supprimer-les-cookies-mode-d-emploi.html

◊ http://www.internetsanscrainte.fr/espace-jeunes/parametrer-son-navigateur

- Activez la fonction « Do Not Track » intégrée dans votre navigateur.

Cette fonction permet d'indiquer aux sites que vous visitez que vous ne souhaitez pas être pisté.
Pour vous aider à l'activer : http://www.futura-sciences.com/tech/questions-reponses/internet-activer-fonction-do-not-track-son-navigateur-internet-6290/

⇒ Installez une **extension « anti-traceurs ».**

Ces extensions sont de **petits logiciels utilitaires** que vous installez dans votre navigateur même et qui bloquent les cookies et autres mouchards des sites que vous visitez. Ils sont **simples à configurer** même si les instructions ne sont pas toujours traduites.

Il en existe plusieurs : *Disconnect*, *Ghostery*, *TRUSTe Tracker Protection*, *TrackMeNot*, *Https Eveywhere*...

⇒ Bloquez les **boutons de partage des réseaux sociaux**.

Ces boutons informent les réseaux sociaux des sites que vous visitez. Si vous souhaitez stopper cette collecte de données, **installez l'extension « Share me not »** : http://sharemenot.cs.washington.edu/

- **Utilisez un moteur de recherche qui ne vous trace pas :**
  - **Qwant** : https://www.qwant.com/
  - **Startpage** : https://www.startpage.com/
  - Ou autre : http://korben.info/wiki/les_moteurs_de_recherche_anonymes_libres_et_decentralises

- **Installez des logiciels pour nettoyer votre ordinateur** tels que **Ccleaner**, **Glary Utilities**, **OnyX** (pour Mac OS). Il existe des applications spécifiques pour **tablettes** et **smartphones**.

- **Protégez votre connexion.**

L'adresse IP, c'est la **carte d'identité de votre connexion** sur Internet. Votre fournisseur d'accès est capable de faire le lien entre votre adresse IP et votre identité bien réelle. Masquer ou brouiller la provenance de son adresse IP, c'est donc surfer discret.

Pour cela, 3 solutions :

1. Installez un **proxy** : http://www.commentcamarche.net/contents/610-serveur-proxy-et-reverse-proxy
2. Utilisez un **Réseau Privé Virtuel** (VPN) : http://www.wefightcensorship.org/fr/article/virtual-private-network-vpn-ou-reseau-prive-virtuelhtml.html
3. Utilisez le **réseau Tor** : https://securityinabox.org/fr/tor

Pour aller plus loin :
http://www.leblogduhacker.fr/etre-anonyme-sur-internet/

Choisissez un mot de passe complexe

Notre quotidien est envahi par les mots de passe et autres codes d'accès. Ce trop plein nous incite à opter pour des **codes simples**, faciles à retenir. Or c'est **une erreur** car s'ils sont faciles à retenir, ils sont surtout faciles à deviner par n'importe qui, et surtout par les pirates.

BOÎTE À OUTILS

- **Faites attention à sa longueur :** une chaîne de huit à douze caractères est un bon compromis entre sécurité et facilité de mémorisation.
- **Utilisez une diversité de caractères** comme des majuscules, minuscules, chiffres, et divers caractères de ponctuation…
- **Utilisez des mots de passe différents** selon les sites, surtout s'ils sont « sensibles » : banque en ligne, PayPal, impôts, EDF, opérateur téléphonique…
- **Changez régulièrement.**
- Et si vous êtes en manque d'inspiration, il existe des **générateurs de mots de passe** qui vous en suggèrent en fonction de vos préférences : https://www.generateurdemotdepasse.com/

FAITES L'EXPÉRIENCE : testez la « force » de votre mot de passe !

https://howsecureismypassword.net/

http://password-checker.online-domain-tools.com/

Pour aller plus loin :
http://www.police-nationale.interieur.gouv.fr/Actualites/Dossiers/Cybercrime/Comment-choisir-ses-mots-de-passe

Sécurisez vos paiements en ligne

Les **escroqueries** et **abus de confiance** sur Internet ne cessent de progresser chaque année. Le piratage des données personnelles et bancaires reste le principal risque associé aux achats en ligne.

BOÎTE À OUTILS

- Protégez votre ordinateur, tablette ou smartphone avec un antivirus. Vous **évitez** ainsi **toute installation de programmes malveillants** (*trojan*, cheval de Troie) capables de copier vos coordonnées bancaires lorsque vous passez une commande.
- N'achetez pas n'importe où, renseignez-vous sur le site avant de conclure la transaction. Soyez méfiants, si l'affaire est trop belle, malheureusement, c'est qu'elle est louche... (une paire du dernier modèle d'Adidas à 30€, sérieusement ?)
- Ne communiquez vos données de paiement que sur les sites web sécurisés de commerçants fiables et reconnus. Sur un site web sécurisé figurent un **cadenas** ou une **clé** et la mention **https://** devant l'adresse web.
- N'enregistrez jamais les données de votre carte de crédit, mots de passe ou codes dans votre ordinateur ou smartphone. Un hacker peut facilement les trouver et s'en servir à votre détriment.
- Renseignez-vous auprès de votre banque, votre carte de crédit possède peut-être une fonction comme **3D Secure,** ou autre.
- Contrôlez régulièrement vos extraits de compte pour détecter directement les transactions douteuses.
- Choisissez un mode de paiement alternatif si vous êtes un e-acheteur régulier: **Paypal**, **carte prépayée**...

Pour aller plus loin :
https://www.cnil.fr/fr/carte-bancaire-et-banque-en-ligne-comment-securiser-leur-utilisation

Maîtrisez votre identité numérique

Internet est un **espace public.** Tout est accessible ou presque. En tout cas, tout ce que vous diffusez et tout ce que d'autres diffusent sur vous. C'est pour cela qu'il est essentiel d'en révéler **le moins possible** sur vous-même.

BOÎTE À OUTILS

- **Utilisez un pseudonyme** si ce n'est pas professionnel.
- **Utilisez un avatar** autre que votre photo d'identité.
- **Renseignez des généralités.** Il est inutile de répondre aux questions non précédées d'une * (non obligatoires) sur les formulaires d'inscription.
- **Interrogez-vous sur le pourquoi** des demandes d'information. Est-il utile de communiquer son adresse personnelle pour devenir membre d'une communauté en ligne ?
- **Ne renseignez pas fidèlement les informations dans votre profil** si cela n'est pas nécessaire.
- **Paramétrez vos comptes de réseaux sociaux** correctement pour vous assurer un maximum de confidentialité. Visitez vos différents profils en tant que visiteur anonyme, pour vérifier quelles informations sont visibles à ceux qui ne sont pas vos « amis ».
- **Soyez vigilants quant à vos publications**, qu'elles vous concernent directement ou une tierce personne, et ce quelque que soit la plateforme (réseau social, blog, forum, sites...). N'oubliez pas que les écrits restent...

Pour aller plus loin :

http://eduscol.education.fr/internet-responsable/communication-et-vie-privee/maitriser-son-identite-numerique.html

Contrôlez régulièrement votre e-reputation

Que vous soyez une entreprise ou un particulier, il est indispensable de **suivre un minimum sa réputation** sur Internet. En tant qu'**entreprise** car les clients se renseignent sur le web avant d'acheter et les avis postés influencent grandement les achats. En tant que **particulier** car n'importe qui peut réaliser une « googlelisation » sur votre personne et beaucoup d'informations anodines regroupées peuvent vous être préjudiciables.

BOÎTE À OUTILS

- Google : c'est l'incontournable !

Il suffit de taper votre **nom / marque / produit** dans Google et de voir ce qui sort dans les résultats **web**. N'oubliez pas d'aller cliquer sur les autres onglets : **Images, Vidéos et Actualités.**

- Talkwalker Alertes : gratuit, il se paramètre très facilement.

Vous pouvez créer jusqu'à **100 alertes différentes** et choisir de les recevoir par **courriel** ou de les consulter **via un lecteur de flux RSS**. Seul inconvénient, il ne brasse que les sites, blogs et forum. Vous ne serez donc pas au courant de ce qui se dit sur les réseaux sociaux.

- Social Mention : gratuit, plus complet que Talkwalker Alertes.

Il fonctionne comme un **moteur de recherche classique** mais en se focalisant sur les médias sociaux (blogs, sites participatifs comme les wikis, les forums de discussion, bookmarks, Twitter, Youtube, Facebook...).

- Netvibes : gratuit, mais nécessite la création d'un compte utilisateur.

C'est un **lecteur très complet de flux RSS** qui permet de se faire sa propre veille informationnelle et documentaire à partir de mots-clés, comme votre propre nom ou celui de votre entreprise.

Pour aller plus loin :

http://www.conseilsmarketing.com/e-marketing/8-outils-pour-surveiller-et-travailler-son-ereputation

Méfiez-vous du phishing

Le **phishing** est une technique utilisée par les hackers pour **usurper votre identité**. Généralement, ils se font passer pour une société connue et vous demandent de confirmer vos coordonnées bancaires ou vos identifiants.

BOÎTE À OUTILS

- Posez-vous les questions suivantes :

1. Ai-je communiqué à cet établissement **mon adresse de messagerie** ?
2. Le mail reçu possède-t-il des **éléments personnalisés** permettant d'identifier sa véracité (numéro de client, nom de l'agence...) ?

- Ne cliquez jamais sur le lien contenu dans le mail !
  Saisissez vous-même l'**URL d'accès au site officiel** de l'entreprise concernée. Si le mail est authentique, vous le retrouverez alors sur votre espace client.

- Méfiez-vous des formulaires demandant des informations bancaires. Si vous avez un doute, n'hésitez-pas à contacter votre agence par téléphone. Ce type d'informations n'est JAMAIS demandé ni par courriel, ni par téléphone.

- Assurez-vous que votre navigateur est en mode sécurisé lorsque vous saisissez des informations sensibles. L'adresse dans la barre du navigateur commence par ***https*** et un **petit cadenas** ou **une clé** est affiché dans la barre d'état.

- Préférez un navigateur équipé d'un système anti-phishing comme *Firefox* ou *OpenDNS*.

- N'hésitez-pas à signaler toute tentative de phishing sur le site www.phishing-initiative.fr. Ainsi, chaque site dont la fraude est confirmée sera bloqué par un message d'avertissement.

Pour aller plus loin :
http://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/Phishing-hameconnage-ou-filoutage

Osez dire non à la géolocalisation

Si cette technologie s'avère séduisante et parfois très utile, il est important de mesurer les conséquences de son utilisation. **Être géolocalisé, c'est rendre publique vos déplacements,** c'est-à-dire dévoiler vos habitudes et donc vos centres d'intérêts. Et vous n'êtes jamais à l'abri de sociétés peu scrupuleuses ou d'individus malveillants qui exploitent ces données à des fins commerciales de spam et autres actions de marketing ciblé non sollicitées : *dites-nous où vous êtes, nous saurons quoi vous vendre !*

BOÎTE À OUTILS

- **Avant d'accepter la géolocalisation,** demandez-vous si elle est nécessaire au bon fonctionnement de l'application.
- Sachez qu'un **simple commentaire posté révèlera votre position** géographique si la géolocalisation est active sur votre appareil.
- Sur les services de réseaux sociaux géolocalisés, **choisissez attentivement vos amis.**
- Dans tous les cas, **ne l'activez pas de façon permanente.**

Le **même principe** s'applique à la **fonction Bluetooth**, qui, toute confortable qu'elle soit, fragilise sensiblement votre sécurité numérique.

Pour aller plus loin :
https://www.educnum.fr/fr/maitrisez-les-reglages-vie-privee-de-votre-smartphone

Mettez-vous à la cryptographie

Un **e-mail transite par plusieurs ordinateurs** entre le moment où vous l'envoyez et celui où votre destinataire le reçoit. À chaque fois, il est **copié sur des disques** et cette copie est conservée pendant **un an** par les fournisseurs d'accès Internet. Un e-mail non crypté et envoyé sur Internet est donc comme **une carte postale sans enveloppe** : un inconnu peut le lire sans que vous le sachiez.

BOÎTE À OUTILS

- Sur votre **ordinateur**, réunissez **les applications suivantes** :

* Thunderbird, client de messagerie **libre** et **gratuit ;**
* GPG4Win (ou **GPGSuite** pour **Mac OS**), qui **chiffrera** et **déchiffrera** votre courrier ;
* Enigmail, qui reliera **Thunderbird** et **GPG4Win.**

Pour vous guider **2 liens vers des tutoriels** :

◊ http://www.numerama.com/tech/128179-comment-chiffrer-ses-mails-windows-pgp.html

◊ http://www.wefightcensorship.org/fr/article/assurer-confidentialite-ses-emails-thunderbird-et-pgphtml.html

- Sur **tablette** et **smartphone**, il existe également des applications spécifiques, notamment :
  - sous **Android** : **OpenKeychain** pour le chiffrement des données et **K-9 Mail** pour la messagerie.
  - sous **Mac OS : iPGMAil** et **oPenGP**.

Pour vous guider :

◊ https://openclassrooms.com/courses/echangez-par-e-mail-en-toute-securite/gpg-votre-smartphone

Pour aller plus loin :
http://www.justgeek.fr/les-meilleurs-outils-gratuits-pour-crypter-vos-donnees-45833/

Méfiez-vous du Cloud computing

Le **Cloud computing** est **l'informatique dans les nuages**. Vous n'archivez plus vos données sur votre ordinateur mais utilisez Internet comme moyen de stockage. Pratique, cela vous donne la possibilité d'accéder à vos fichiers n'importe où, du moment où vous avez accès à Internet. Mais il faut savoir que **vous perdez ainsi en partie le contrôle vos données**. En dehors de la possibilité de mauvaise manipulation de votre part, il existe le risque non-négligeable de piratage.

Les précautions à prendre sont une synthèse des points précédents.

BOÎTE À OUTILS

- **Sécurisez vos appareils et votre connexion.**

Cela passe par l'installation :

1. d'un **antivirus**. Il en existe de nombreux **gratuits** et **efficaces** pour ordinateur, tablette et smartphone.
2. d'un logiciel **anti-malware**, tel que **Malwarebytes**.

Pour le télécharger : https://fr.malwarebytes.com/products/

3. d'un **pare-feu**.

- **Choisissez un mot de passe efficace.**

- **Sélectionnez ce que vous envoyez en ligne.** N'oubliez pas que le prestataire hébergeant vos données peut être tenté de les exploiter.

- **Faites une sauvegarde** de vos données sur un disque dur physique. Un problème technique ou un vol pourraient entraîner la perte définitive de vos données sans aucune possibilité de récupération.

- **Cryptez vos fichiers** à l'aide de logiciels ou applications spécifiques (**AxCrypt**, **TrueCrypt**).

Pour aller plus loin :
http://www.capital.fr/art-de-vivre/high-tech/comment-utiliser-le-cloud-sans-risque-1017776#

Internet et ses dangers sont en **constante évolution**. C'est la **course permanente du gendarme et du voleur**, dans laquelle le voleur a toujours une longueur d'avance. D'où deux dernières recommandations :

* **tenez-vous régulièrement au courant de ces évolutions pour vous protéger !**
* **préférez toujours les liens vers les sites officiels !**

Les incontournables :

- La Commission Nationale de l'Informatique et des Libertés (**CNIL**) : https://www.cnil.fr/
- L'Agence Nationale de la Sécurité des Systèmes d'Information (**ANSSI**) : http://www.ssi.gouv.fr/
- Le site de la **Hack academy**, à l'initiative du Club Informatique des Grandes Entreprises Françaises (CIGREF) : https://www.hack-academy.fr/
- Le kit de survie numérique du site **WeFightCensorShip** : http://www.wefightcensorship.org/fr/online-survival-kithtml.html
- La **Quadrature du net** : https://www.laquadrature.net/fr
- **WikiHow** catégorie Ordinateurs et l'électronique et toutes ses sous-catégories (Internet, Réseaux...) : http://fr.wikihow.com/Cat%C3%A9gorie:Ordinateurs-et-l'%C3%A9lectronique
- **Educnum** : https://www.educnum.fr/

Centre Culturel des Cordeliers
7 rue des Cordeliers
39000 LONS LE SAUNIER
Contact : contact-4c@ecla-jura.fr
http://4c-lons.ecla-jura.fr

Conception et impression : Centre Culturel Communautaire des Cordeliers