

Fiche n°7 : Ils doivent se méfier.

ÉTHIQUE ■ ■ ■

VALIDITÉ ■ ■ ■

IDENTITÉ ■ ■ ■

NOTIONS

De quoi parle-t-on exactement ? Des définitions simples pour des idées claires !

« Avec Internet, il est facile d'envoyer un message à des millions de destinataires, sans dépenser d'argent. » Du coup, nous sommes envahis de messages sans les avoir sollicités (= **spams** ou **pourriels**). Certains s'apparentent à des messages publicitaires, d'autres commerciaux voire malhonnêtes. Une autre technique nous menace celle du **filoutage** ou **hameçonnage** ou **phishing**. Une escroquerie qui s'apparente à des **courriels** ou des sites frauduleux et qui a pour but de récupérer des données personnelles. Pour lutter contre les spams et obtenir un suivi sur votre action, vous pouvez signaler les spams que vous recevez sur ce site : <https://www.signal-spam.fr/>

Pour en savoir plus : **Lutter contre les courriers indésirables** (Col.« Se protéger ») - Cité des Sciences – Disponible sur : <http://www.universcience.fr/fr/carrefour-numerique/contenu/c/1239022827640/fiches-pratiques/>

Pour en savoir plus : **Fiche méthodologique n°6 : Reconnaître les spams et les éviter** – CNIL - Disponible sur : <http://www.jeunes.cnil.fr/fileadmin/documents/Jeunes/cnilmethodo10.pdf>

Pour la petite histoire : Les Monty Python ont leur part de responsabilité dans le choix du terme spam. Voir la vidéo sur : http://www.dailymotion.com/video/x1q97s_spam-spam-spam_fun

Les **hoax** (rumeurs ou canulars) participent également au **pollupostage** des **messageries électroniques** et des réseaux. Sans représenter de réels dangers pour votre ordinateur, vos finances ou votre vie, ils constituent cependant des risques de désinformation, d'atteinte à l'image, de fausses alertes ou d'encombrements des réseaux. Pour lutter contre les hoax, connectez-vous au site Hoaxbuster pour les rechercher, vérifier et éviter de propager des canulars : <http://www.hoaxbuster.com/>

Pour en savoir plus : **Complément d'Enquête : La vérité est ailleurs** - France 2, 1/12/2008 – Disponible sur : http://www.dailymotion.com/video/x7px9i_internet-la-verite-est-ailleurs_webcam

Quand on navigue sur Internet, on laisse **à notre insu** des **traces** de notre passage : les sites que l'on visite laissent des traces sur notre ordinateur (= les **cookies**) ou conservent des **données personnelles** (adresse IP, fournisseur d'accès,...), les moteurs de recherche mémorisent nos **préférences**, très pratique pour la **publicité ciblée**, prospection commerciale ou **teen-marketing**. Rien n'est gratuit sur Internet, et des sites apparemment gratuits comme Facebook ou Google gagnent beaucoup d'argent en vendant nos traces !

Pour en savoir plus : **Protection des données personnelles : où est le problème ?** - CNIL - Disponible sur : http://www.dailymotion.com/video/x7px9i_internet-la-verite-est-ailleurs_webcam

Pour en savoir plus : **Marketing ciblé sur Internet : vos données ont de la valeur** – CNIL – Disponible sur : <http://www.cnil.fr/dossiers/internet-telecoms/fiches-pratiques/article/marketing-cible-sur-internet-vos-donnees-ont-de-la-valeur/>

Il faut toujours **penser à se déconnecter, effacer son historique de navigation voire à refuser les cookies**.

Pour en savoir plus : **Fiche méthodologique n°10 : Découvrir et effacer ses traces sur Internet** - CNIL- Disponible sur : <http://www.jeunes.cnil.fr/fileadmin/documents/Jeunes/cnilmethodo10.pdf>

Internet est un outil incontournable qui pose donc le problème de la **sécurité des données** : choix des **mots de passe**, vérifier que les **achats en ligne** sont sécurisés et se protéger des **virus** en installant un **logiciel antivirus**.

Pour en savoir plus : **Fiche méthodologique n°4 : Surfer en toute sécurité** – CNIL - Disponible sur : <http://www.jeunes.cnil.fr/fileadmin/documents/Jeunes/cnilmethodo4.pdf>

OBJECTIFS CITOYEN

L'essentiel est de **protéger ses données** et de **sécuriser son environnement informatique** contre les menaces du web.

Quelques sources

■ Kredens, Elodie ; Fontar, Barbara - **Comprendre le comportement des enfants et adolescents sur Internet pour les protéger des dangers** – Fréquence écoles, 2010 – Disponible sur : <http://www.frequence-ecoles.org/ressources/view/id/37c48d9366cfe18d321ef6e1db77cd38>

■ Réseau Éducation Médias - **Jouer sans se faire jouer (jeu en ligne + guide de l'enseignant)** – Disponible sur : http://www.media-awareness.ca/francais/jeux/jouer_jouer/index.cfm

■ Académie d'Orléans-Tours – **Vie numérique : Le Dico du Net** – Disponible sur : http://www.ac-orleans-tours.fr/vie_numerique/usages/pratiques_de_classe/internet_responsable_et_citoyen/le_dico_du_net/

Groupe TICE Documentation – <http://documentation.tice.ac-orleans-tours.fr/>

OBJECTIF Savoir se protéger.■ **Un peu de ménage s'impose !**

→ **Faire le tri dans sa messagerie** : « La chasse aux mots », les élèves recherchent en ligne les définitions et les synonymes (anglais-français) des mots suivants : messagerie électronique, pollupostage, spam, pourriel, courriel, filoutage, hameçonnage, hoax, e-mail, webmail, adresse électronique, netiquette, phishing, authentification.

↳ **Ressources utiles** : Les dossiers : « *Qu'est-ce que le filoutage (Phishing) ?* » et « *Qu'est-ce que l'authentification ?* » + La rubrique : « *Glossaire* » – Surfez intelligent - Disponible sur : <http://surfez-intelligent.dgmic.culture.gouv.fr/>

→ **Conseils d'usage** :

- Ne répondez pas aux messages de spam
- Utilisez un filtre anti-spam
- N'ouvrez pas les fichiers joints à des messages d'origine inconnue
- Ne cliquez pas sur les liens contenus dans des messages d'origine inconnue
- Soyez vigilant lors de la transmission d'une adresse courriel sur Internet
- Diffusez votre numéro de téléphone avec précaution
- Créez une adresse dédiée pour chacune de vos activités sur Internet

↳ **Ressource des conseils d'usage** : *Messagerie : faites le tri !* – Surfez intelligent - Disponible sur : <http://surfez-intelligent.dgmic.culture.gouv.fr/spip.php?rubrique8>

→ Vous pouvez compléter en précisant les **conseils d'usage pour l'ordinateur** :

- Mettez régulièrement à jour votre système d'exploitation
- Activez les fonctionnalités de sécurité
- Supprimez les applications qui ne sont pas utilisées
- Conservez vos moyens d'authentification en lieu sûr

↳ **Ressource des conseils d'usage** : *Ordinateur : garder le en forme !* – Surfez intelligent - Disponible sur : <http://surfez-intelligent.dgmic.culture.gouv.fr/spip.php?rubrique6>

→ Vous pouvez terminer cette activité en proposant aux élèves de répondre au quiz du site « Surfez intelligent » pour tester leurs connaissances.

↳ **Ressource utile** : *Le quizz* – Surfez intelligent - Disponible sur : <http://surfez-intelligent.dgmic.culture.gouv.fr/spip.php?article21>

■ **On est suivi à la trace !**→ **Présenter aux élèves les traces qu'ils laissent sur le net sans le savoir !**

On laisse toujours une trace sur le net à découvrir en visionnant la vidéo « *Alerte aux traces sur Internet* » (CNIL) : <http://www.jeunes.cnil.fr/alerte-aux-traces/sur-internet/> et avec un exemple d'informations qui peuvent être collectées quand on surfe : <http://www.anonymat.org/vostraces/index.php>

→ Puis montrer comment on peut **reconstituer toute leur vie par une simple enquête sur le net**. Voir la terrible histoire de « Marc L » dont le journal *Le Tigre* a retracé la vie et donné tous les détails personnels à partir de données récoltées sur le web. Édifiant !

↳ **Ressource utile** : *Marc L. Genèse d'un buzz médiatique* – Le Tigre, 2009 - Disponible sur : <http://www.le-tigre.net/Marc-L.html>

→ **Sur la toile on est donc suivi à la trace ! Mieux vaut savoir les effacer :**

↳ **Ressource utile** : *Vos traces, ce n'est pas du virtuel !* – CNIL - Disponible sur : <http://www.cnil.fr/vos-libertes/vos-traces/>

(SUITE-2) Pistes pédagogiques à l'usage des enseignants

■ Spam, spam, spam...

➔ De l'humour so british ! Un film d'animation , **en anglais**, présente de manière humoristique ce que sont les spams et ce qu'ils feraient dans votre boîte aux lettres classique : <http://youtu.be/nnD50mSvLPk>

■ Rumeur vous avez dit rumeur ?

➔ Proposer aux élèves de réfléchir sur une plaisanterie bien innocente et ses graves conséquences

Exemple : L'avis de recherche d'Ashley Flores, qui en fait n'avait jamais disparu : http://www.hoaxkiller.fr/hoax/2007/disparition_ashley_flores.htm

↳ Ressource utile : HERBIET, Aurélie - **Information/ Rumeur : comment savoir ?** (Une séquence de 3 séances en lycée professionnel) – E-profsDocs, 2009 - Disponible sur : <http://eprofsdocs.crdp-aix-marseille.fr/Information-Rumeur-comment-savoir.html>

■ S'exposer sur la toile comporte des risques...

① Moqueries, railleries, humiliations, insultes, menaces peuvent être des actions répétées plusieurs fois sans que la personne concernée puisse y mettre fin alors on peut commencer à parler de harcèlement. La **communauté** du web et les **nouvelles technologies** (telles que la vidéo d'une agression sur le téléphone portable appelée « **Happy-slapping** » ou vidéolynchage) permettent d'atteindre plus facilement la victime dans son **intimité** par son côté intrusif dans la vie privée (« passe la porte du foyer »), sous couvert d'anonymat ou d'absence de contrôle d'identité, renforcé par une supériorité technique et une forme de « loi du silence » pour une victime qui a honte et n'ose pas en parler. Le harcèlement en ligne ou **cyberharcèlement** ou **cyberbullying** facilité par les outils virtuels fait de plus en plus parler de lui.

↳ Ressource utile : **Fiche pédagogique n°6 : Le cyberbullying ou cyberharcèlement** – CNIL - Disponible sur : <http://www.jeunes.cnil.fr/fileadmin/documents/Jeunes/cnilpedago6.pdf>

➔ Visionner avec les élèves le clip de la commission européenne contre le harcèlement : Halte au harcèlement en ligne ! - Disponible sur : <http://eprofsdocs.crdp-aix-marseille.fr/Information-Rumeur-comment-savoir.html>

➔ Sensibiliser les élèves à ce problème en tant que potentiel « victime », « harceleur » ou « témoin »

➔ **Que faire en cas de problèmes ?** En parler à un adulte, demander au responsable du site d'effacer les contenus, si cela ne fonctionne pas contacter la CNIL pour se faire aider pour la suppression de contenus, signaler les abus pour des incidents potentiellement illégaux, aller sur le site : www.pointdecontact.net, conserver les messages, bloquer l'expéditeur, changer de pseudo ou d'adresse mail,... ou utiliser la ligne d'écoute anonyme et gratuite pour les enfants et leurs parents **Net Ecoute** : 0 820 200 000 - Disponible sur : www.netecoute.fr

↳ Ressource utile : **Le cyberharcèlement : que peut faire l'école** – ClickSafe.be - Disponible sur : <http://www.clicksafe.be/leerkrachten/fr/cyber-harcelement/>

À retenir

DONNÉES PERSONNELLES
CYBER HARCELEMENT
POURRIEL
PUBLICITÉ CIBLÉE
CYBERCRIMINALITÉ
VIRUS
SPAM
MESSAGERIE ÉLECTRONIQUE
TEEN MARKETING
COOKIES
POLLUPOSTAGE
TRACES
HOAX
HAMEÇONNAGE