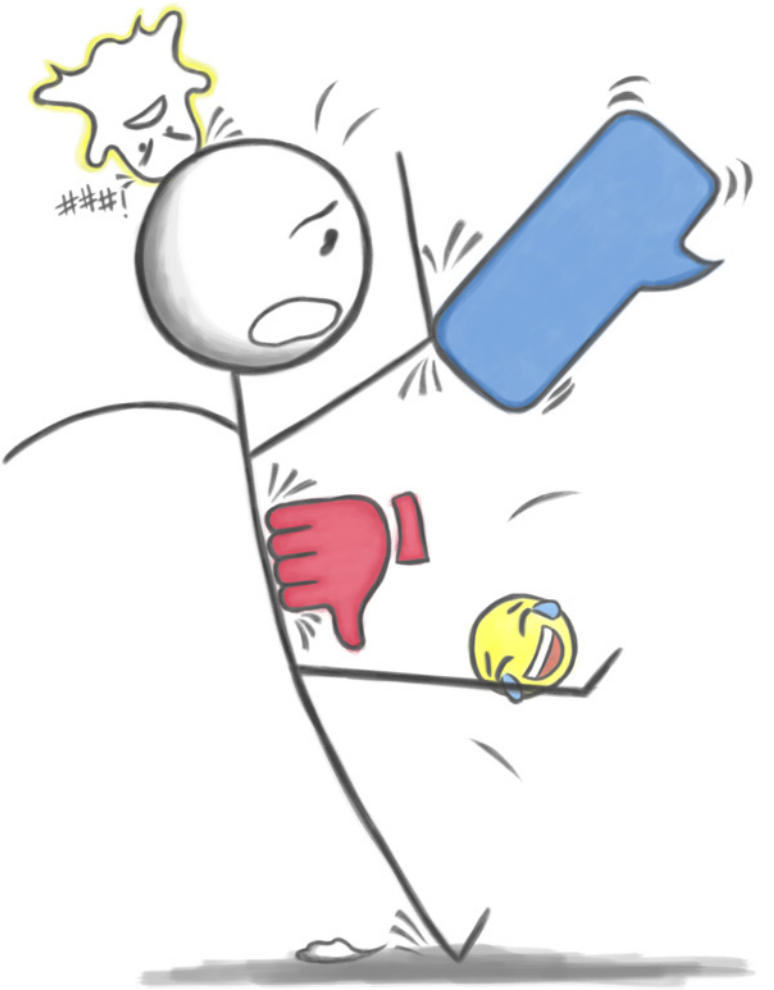
CONSEIL DÉPARTEMENTAL
DES JEUNES



Les dangers et bons usages d'Internet

Agis !

Les réseaux sociaux n'oublient jamais rien !
Profil et publications uniquement visibles pour tes amis !
Les infos restent **privée**s !
Protège tes données !
Réfléchis avant de publier !
Respecte les autres !
Ne dis pas tout !
Sécurise tes comptes !
Utilise un **pseudonyme** !
Crée-toi **plusieurs** adresses mail !
Attention aux photos et aux vidéos !
Attention aux mots de passe !
Vérifie tes traces !
Fais le ménage dans tes **historiques** !

Sommaire

Internet est un formidable outil d'information et de communication permettant d'échanger des idées, des contenus et des fichiers, d'appartenir à un réseau et de créer des liens. Face à cet outil, tu dois rester méfiant et prudent en vérifiant les sources d'informations. L'Internet et les réseaux sociaux sont la cause de nombreux dangers. Il est facile d'être victime de vol d'identité, de cyber-harcèlement ou de cyberdépendance.

Le Web n'a rien de virtuel. Réfléchis avant de cliquer !

I. Internet

1. Réseaux sociaux, forums et blogs

Conseils

Efface tes traces et contrôle ce que l'on enregistre sur toi

- N'oublie pas de te déconnecter des sites sur lesquels tu as navigué.
- Verrouille ton ordinateur et pense à effacer régulièrement ton historique de navigation.
- Utilise le mode de navigation privé et clôture manuellement tes sessions ouvertes.
- Vérifie tes traces : recherche régulièrement ton nom dans un moteur de recherche et abonne-toi à une alerte à ton nom.
- Installe un module bloqueur de publicités sur ton navigateur.
- N'hésite pas à refuser les cookies (préférences / sécurité du navigateur).
- Contrôle et supprime les anciens contenus.

Choisis un pseudo et change tes mots de passe

- Ne dévoile pas ton identité, utilise des pseudos.
- Un mot de passe efficace : plus de 8 caractères, sans lien avec son détenteur + majuscules + ponctuation + chiffres.
- Créé toi plusieurs adresses mail selon tes activités en ligne.
- Protège tes données personnelles et ta vie privée
- Ne remplis que les champs obligatoires sur les formulaires.
- Ne communique pas tes informations personnelles (numéros de téléphone, adresses, photos, vidéos, renseignements financiers) car elles sont archivées par les gestionnaires des sites et pourront être

exploitées et détournées par des personnes mal intentionnées.

- Désactive la géolocalisation sur ton smartphone quand tu ne t'en sers pas.

- Utilise un cache-webcam.

Protège ton image, tes idées et celles des autres

- Rappelle-toi que tu ne peux pas publier une photo ou une vidéo sans demander au préalable l'autorisation des personnes qui sont représentées. Pars du principe que tout ce que tu mets en ligne devient public.

- Partage des idées et des créations en respectant le droit d'auteur.

Liberté d'expression et vie privée

- N'oublie pas que tes propos ne doivent nuire à autrui ou être diffamatoires à l'égard d'une personne ou d'une communauté. Tu es responsable de ce que tu dis.

- Évite de donner des informations trop personnelles sur toi, ta famille et tes amis.

Paramètre ton réseau social (options de confidentialité)

- Limite la diffusion de tes données personnelles : te demander qui peut voir tes contenus, qui peut te contacter, ce qui peut être diffusé sur Internet et être vu à partir d'un moteur de recherche.

- Il ne faut ajouter que tes vrais amis, ceux que tu connais vraiment. L'ami de ton ami n'est pas forcément ton ami. Paramètre une audience par défaut plutôt stricte pour que seulement tes amis puissent voir tes contenus.

- Pense à désactiver la « reconnaissance faciale » sur les photos publiées sur Facebook.

- Renseigne-toi : il est possible de contrôler, rectifier, supprimer les informations qui te concernent sur d'autres comptes aussi.
- Utilise les fonctionnalités anti-piratage proposées par les réseaux sociaux que tu utilises.
- Attention à la diffusion de photos, vidéos et écrits intimes.
- Sur Snapchat : capture d'écran du destinataire qui conserve la photo sur son téléphone et la rediffuse.
- Sur Facebook : on peut taguer ton nom sur une photo gênante.
- Ne crois pas tout ce que tu vois sur les réseaux sociaux. La personne qui se cache derrière l'écran n'est pas forcément celle que tu crois être.

Dangers

La violence physique : apologie de la violence physique par la captation de vidéos ou d'images mettant en valeur ces comportements.

La violence psychologique : harcèlement moral et sexuel (insulter, menacer par des mots, images et gestes, de manière répétitive, afin de nuire à une personne).

- Certains sites incitent leurs contacts aux suicides, à l'anorexie, à certains comportements les mettant en danger. Il s'agit souvent d'individus mal intentionnés recherchant une forme de « plaisir » en manipulant leurs victimes.

Racisme et antisémitisme

- Attention aux discours et aux idées propagées sur le Net. Le but des auteurs de ces sites est de te manipuler, de chercher de nouveaux adhérents, adeptes qui serviront leurs causes, qui seront actifs à leur place.

Radicalité religieuse : embrigadement de personnes en souffrance ou faibles pour devenir des adeptes de ces idées dangereuses avec pour seul but de les utiliser.

Conséquences : poursuites pénales, danger pour la santé psychologique de la victime, troubles, voire traumatismes.

- Pense à la victime : le harcèlement peut mener à une perte de confiance, des troubles psychologiques, de l'anxiété, dépression et même à des conduites suicidaires.

- Les propos tenus à l'égard des autres : diffamation, outrages et menaces sont réprimés par la loi.

- L'usurpation d'identité : le fait de se faire passer pour quelqu'un d'autre est sanctionné par la loi (création d'un profil ou blog au nom d'une tierce personne).

Que faire si toi ou quelqu'un d'autre est victime de harcèlement ?

- Ne pas obéir et ne pas écouter le harceleur.

- Ne surtout pas répondre publiquement.

- En parler à un adulte (parents, CPE, professeurs, surveillants, amis) ou appeler au 0800100 NetEcoute.

- Capture écran des photos et signalement au site pour demander l'effacement sans délais. Demander au moteur de recherche de déréférencer le contenu.

- Porter plainte auprès de la Gendarmerie / Police si le harcèlement est très grave.

- Signaler des comportements d'amis qui se radicalisent auprès de proches, de professeurs, voire de la Police.

2. Jeux vidéo en ligne

Conseils

- Limite ton temps de jeu ou de consultation du web.
- Evite de jouer à des jeux déconseillés pour ton âge.
- Les jeux trop violents peuvent te choquer et déformer ta réalité.
- Cherche à avoir des activités annexes, à rencontrer d'autres personnes (amis, famille) pour rompre l'isolement.

T'en sortir

- Fais une cure de réintégration dans la vie sociale.
- Intègre un groupe de soutien.

Conséquences

- Banalisation de la violence.
- La dépendance qui peut causer isolement et renfermement, troubles du sommeil, mauvais résultats scolaires, agressivité et violences.

3. Sites d'achats

- Vérifie le « s » à la fin de http et / ou le cadenas dans l'adresse url du site
- Les escroqueries sont fréquentes. Ne communique jamais tes données bancaires personnelles, excepté sur les sites sécurisés (avec le cadenas).

4. Téléchargement illégal

- Les œuvres originales sont protégées par le Code de la Propriété Intellectuelle (musiques, vidéos, jeux vidéo). Leur téléchargement sans autorisation présente un délit de contrefaçon de droits d'auteur.

5. Sites d'informations et de documentation

- Vérifie la qualité des informations que tu trouves sur Internet en les comparant et en regardant avec attention leur source pour t'assurer qu'elles sont fiables et précises.
- Wikipédia, l'encyclopédie libre, ne garantit pas le contenu mis en ligne. Les articles peuvent contenir des erreurs étant donné qu'ils sont rédigés par des internautes.

Tu es responsable de ce que tu consultes comme de ce que tu diffuses sur Internet, sur les réseaux sociaux. En tant que mineur, tu engages la responsabilité de tes parents.

Test : Facebook et toi

1. Ton profil est-il visible par tous ?

Oui Non

2. As-tu des informations personnelles sur Facebook ?

Oui Non

3. Y a-t-il des personnes dans ta liste d'amis que tu ne connais pas ?

Oui Non

4. As-tu des photos sur Facebook qui ne devraient pas être copiées ou vues par des étrangers ?

Oui Non

5. Tu as un contrat avec Facebook. Sais-tu ce qui y est écrit ?

Oui Non

6. Sais-tu comment Facebook gagne de l'argent ?

Oui Non

7. Supprimes-tu régulièrement les anciens contenus sur Facebook ?

Oui Non

8. Une semaine sans Facebook, est-ce possible pour toi ?

Oui Non

9. Tes publications indiquent-elles toujours où tu te trouves (localisation) ?

Oui Non

10. Vérifies-tu les notifications / messages avant de les partager ou les « aimer » ?

Oui Non

Réponses :
Question 1, 2, 3, 4, 9 – bonne réponse NON
Question 5, 6, 7, 8, 10 – bonne réponse OUI

Quiz

1. À qui faut-il demander l'autorisation pour publier une photo d'un(e) ami(e) ?

- **A.** Les parents de ton ami(e)
- **B.** Ton ami(e)
- **C.** Personne

2. Que peux-tu faire si tu découvres une photo horrible de toi sur Facebook ?

- **A.** Rien
- **B.** Demander à la personne (webmaster) qui l'a publié de la supprimer

3. Qui peut lire ce que tu écris sur un réseau social si tu n'as pas paramétré correctement ton profil ?

- **A.** Uniquement tes amis
- **B.** Tout le monde
- **C.** Uniquement tes parents

4. Que peux-tu faire si un site te demande de donner ton adresse ?

- **A.** Je suis obligé de donner mon adresse
- **B.** Je donne une fausse adresse

5. Quelle information permet d'identifier chaque ordinateur connecté à Internet ?

A. L'adresse mail

B. L'adresse IP

C. Le numéro de téléphone

6. Les sites sont obligés de te dire ce qu'ils feront des informations que tu donnes (adresse, date de naissance, téléphone, etc.).

A. Vrai

B. Faux

7. Toutes les informations sur Internet sont vraies.

A. Vrai

B. Faux

C. Seulement sur Wikipédia

8. Comment peux-tu vérifier si les informations sur Internet sont vraies ?

A. Utiliser Google pour les recherches

B. Croiser les sources et identifier l'auteur

C. Demander à ses amis

9. Tu ne dois jamais accepter de rencontrer en personne quelqu'un rencontré sur un chat, même s'il te paraît très sympa.

A. Vrai

B. Faux

10. Que dois-tu faire si tu reçois un mail qui te paraît bizarre d'un inconnu ?

A. Le supprimer sans l'ouvrir

B. L'envoyer à tes amis

C. Répondre au mail en demandant d'arrêter de te déranger

11. Dans un questionnaire a-t-on droit de te demander ta religion ou ta couleur de peau ?

A. Vrai

B. Faux

12. Sur Internet je suis à l'abri en utilisant un bon pseudo

A. Vrai

B. Faux

13. Sur Internet, je ne risque pas d'avoir des sanctions légales car je suis mineur

A. Vrai

B. Faux

C. Sur Internet, je ne risque rien même si je suis majeur

Réponses: 1 – B, 2 – B, 3 – B, 4 – B, 5 – B, 6 – A, 7 – B, 8 – B, 9 – A, 10 – A, 11 – B, 12 – B, 13 - B

Quelques sites et numéros utiles

- www.internet-signalement.gouv.fr : pour signaler tous sites et tous comportements suspects
- www.InternetSansCrainte.fr : des conseils, des infos, des dessins animés et des jeux
- www.Pointdecontact.net : pour signaler des sites ou contenus choquants ou illégaux
- www.Jeunes.cnil.fr : pour faire respecter ta vie privée
- www.2025exmachina.net : tu es un net détective, on t'appelle à l'aide. A toi de jouer !

http://eduscol.education.fr/internet -responsable/ : le site info du ministère de l'Éducation

- 0800 200 00 – numéro gratuit, anonyme et confidentiel de NetEcoute
- www.netecoute.fr
- www.bee-secure.lu
- www.passe-ton-permis-web.com
- www.educnum.fr
- www.e-enfance.org
- www.actioninnocence.org


RUMORS
teasing
gossiping
insults
threats
CYBER BULLYING
LIES
name-calling
harassment
mean words

Les lois

Sanctions légales :

- Harceler autrui par agissements répétés ayant pour objet ou pour effet une dégradation des conditions de travail susceptible de porter atteinte à tes droits et à ta dignité, d'altérer ta santé physique ou mentale (articles 222-33-2 du Code pénal condamne de deux ans d'emprisonnement et de 30 000 euros d'amende).

- Porter atteinte à l'intimité de la vie privée d'autrui en captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ou l'image d'une personne se trouvant dans un lieu privé (article 226-15 du Code pénal punit d'un an d'emprisonnement et à 45 000 euros d'amende).

- Porter atteinte au secret des correspondances, comme par exemple le fait de prendre frauduleusement connaissance de l'e-mail d'un tiers et/ou de le divulguer (article 226-15 du Code pénal punit d'un an d'emprisonnement et à 45 000 euros d'amende).

- Diffuser des messages à caractères violents ou pornographiques portant atteinte à autrui (article 227-24 du Code pénal, condamnant à trois ans d'emprisonnement et à 75 000 euros d'amende, lorsque ce message est susceptible d'être vu par un mineur).

- Usurper l'identité : le fait de se faire passer pour quelqu'un d'autre. Il existe une gradation dans ces sanctions en fonction des conséquences pour les victimes (article 434-23 du Code pénal condamne à cinq ans d'emprisonnement et 75 000 euros d'amende, et article 222-16-1 du Code pénal condamne à un an d'emprisonnement et 15 000 euros d'amende).

Lexique

Porter atteinte
Action, fait de causer à quelqu'un un dommage, un préjudice matériel ou moral.

Code pénal
Ensemble de textes qui définissent les crimes, délits et contraventions ainsi que les peines qui leur sont applicables.

Réintégration
Retrouver sa place dans la vie sociale.

Cure
Traitement conduit selon les principes de la psychanalyse.

Cyber-harcèlement : un acte agressif, intentionnel perpétré par un individu ou un groupe d'individus au moyen de formes de communication électroniques, de façon répétée à l'encontre d'une victime qui ne peut facilement se défendre seule. Le cyber-harcèlement se pratique via les téléphones portables, messageries instantanés, forums, chats, jeux en ligne, mails, réseaux sociaux, etc.

Donnée personnelle : permet d'identifier une personne précise (adresse IP, nom, numéro d'immatriculation, numéro de téléphone) mais aussi un like, une photo de toi, un commentaire. L'article 38 de la loi Informatique et libertés reconnaît à toute personne physique le droit de « s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement ».

Droit à l'image : permet à toute personne de s'opposer – quelle que soit la nature du support utilisé – à la reproduction et à la diffusion, sans son autorisation expresse, de son image.

Diffamation : imputation d'un fait non avéré qui porte atteinte à l'honneur et à la considération d'une personne. Elle relève d'une procédure spécifique permettant de protéger la liberté d'expression.

Usurpation d'identité : prendre contrôle de l'identité virtuelle d'une personne en soutirant son mot de passe et son identifiant et à se faire passer pour elle pour utiliser son compte à différentes fins, souvent frauduleuses.

Cookies : Les *cookies* sont les marques de ton passage sur Internet qui sont conservées : mots de passe, logins, préférences de connexion, références de facturation (adresse, téléphone, mail…).

Cybercriminalité

C'est l'ensemble des crimes et délits commis en utilisant les nouvelles technologies (tentatives d'escroquerie, harcèlement en ligne, etc.). En France, ce sont les autorités de police regroupées dans l'OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication) qui traitent les signalements de ces crimes et délits : www.internet-signalement.gouv.fr

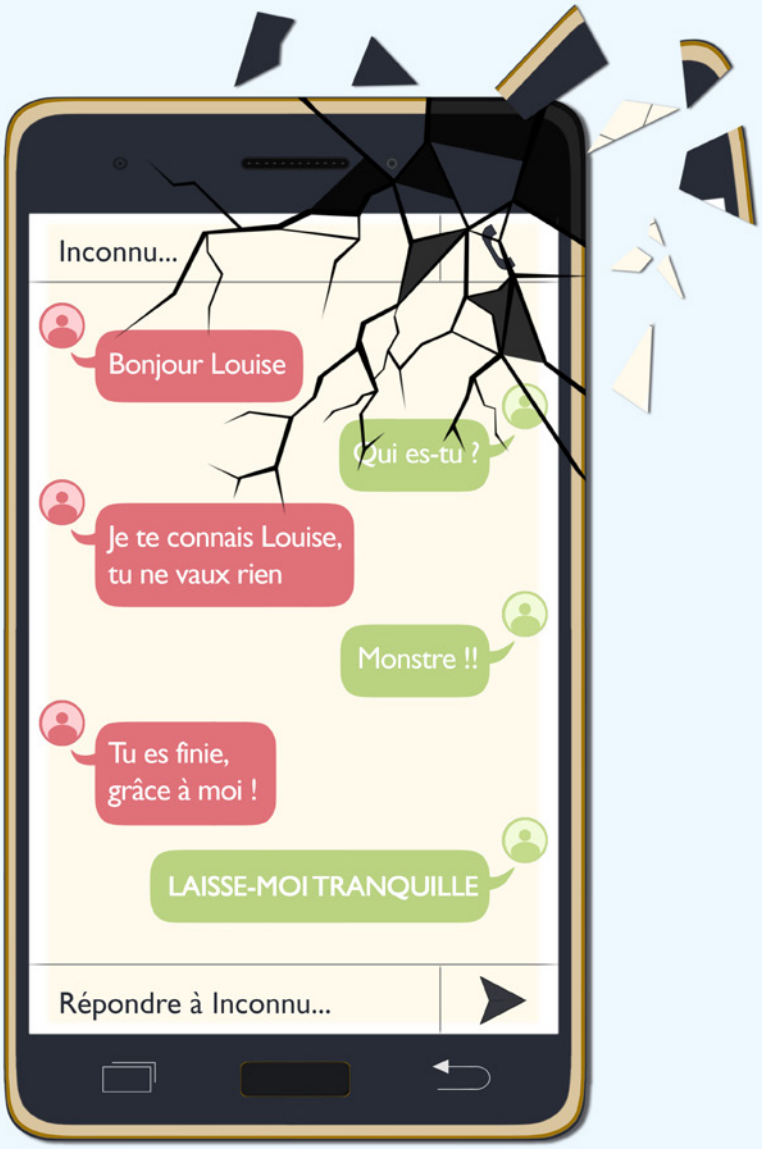
Phishing

Le terme « phishing » est une contraction des mots anglais *password* (mot de passe), *harvesting* (moisson) et *fishing* (pêche). Il s'agit d'une technique d'escroquerie, aussi appelée hameçonnage, utilisée pour se procurer les données confidentielles d'internautes (mots de passe, numéros de carte

de crédit, etc.). L'attaque peut se produire par courriel, par un site web, par un service de téléphonie sur Internet (VoIP) ou par SMS.

Webcam hacking

Webcam hacking ou espionnage par webcam. Un pirate pénètre un ordinateur afin d'y installer un RAT (Remote Access Tool), outil permettant de commander un ordinateur à distance. Après cette manipulation, il est possible d'activer la webcam à distance sans que la victime ne puisse s'en apercevoir.



RÉFLÉCHISSEZ AVANT DE DÉTRUIRE UNE VIE