

Les comportements dangereux sur internet. **Script de l'émission le mercredi 31 mars 2010 à Radio Pulsar**

Fichier MP3 : 1_droit_a_l_image_sanela.mp3 (7mn 4 s) 6,5 Mo

*Hey Toute le monde ! Bienvenue sur Radio Pulsar !
Nous sommes sept élèves du collège Prosper Mérimée de Saint Savin.
On est ensemble pendant une heure pour parler des comportements dangereux sur internet.
Au programme : des reportages, des invités et de la musique.
Dans cette émission on passera en revue la cyber-intimidation, le hackage, et la diffusion de
votre image à votre insu.
En bref, on vous dira tout sur les façons de se protéger des risques sur le net.*

JINGLE

On commence avec ce micro trottoir réalisé au collège de St Savin.

MICRO TROTTOIR

*Tout au long de cette émission, pour répondre à nos questions, on accueille Bernard Usé.
Bonjour !*

Vous travaillez sur les TIC : technologies de l'information et de la communication pour l'académie de Poitiers. Pouvez-vous nous dire un peu plus précisément en quoi consiste votre travail ?

Mon travail consiste à promouvoir les pratiques pédagogiques des technologies de l'information et de la communication à l'école, au collège et au lycée. En effet le numérique peut faciliter les apprentissages des jeunes, et rendre l'école plus intéressante. Mais bien sûr il faut aussi apprendre à se comporter sur les réseaux de manière responsable.

J'ai également à mes côtés Sanéla. Tu vas nous parler de la diffusion de notre image à notre insu sur internet.

1^{ère} partie : La diffusion d'image à notre insu (Sanéla)

Eh oui Léo, ça n'arrive pas qu'aux stars, les photos ou les films volés. A nous aussi ça peut nous arriver de se retrouver dans un album ou sur des blogs alors qu'on ne le souhaitait pas.

Quand on diffuse une photo sur internet à l'insu de la personne concernée, quelle peine risque-t-on ?

Les infractions au droit à l'image sont punies par les tribunaux :

- Photos d'élèves ou de professeurs sans autorisation de publication : 1 an de prison et 45.000 Euros d'amende*
- Montage (caché) de paroles et d'images : 15 000 euros et 1 an de prison*

Pourquoi les ados prennent-ils en vidéo ou en photo sans la permission de la personne ?

Pour jouer ? Parce qu'ils ne se rendent pas compte que cela peut être grave ? Parce qu'ils ne savent pas comment demander ?

Par exemple, l'an dernier au collège, deux de mes camarades de classe ont pris en vidéo ma professeur de math et l'ont montré à plusieurs élèves. Que faut-il faire pour éviter cela ?

Peut-être déjà se mettre à la place de la prof de math : aimeriez-vous que des photos où vous n'êtes pas à votre avantage circulent sur les blogs ou les téléphones portables des autres, pour se moquer de vous ?

Et puis, éviter de relayer ce genre d'images. Si les autres voient que ça n'intéresse personne, ils arrêteront peut-être... En tous cas il est raisonnable de ne pas céder à la surenchère du trash.

Un autre exemple : à mon anniversaire, j'ai pris plein de photos de mes copines. Elles m'ont donné un simple accord oral pour les mettre en ligne. Est-ce que je peux les mettre sur mon blog ?

Il vaut mieux que tu leur demandes par courriel, et que tu archives leur réponse. De plus, si plus tard elles ne veulent plus apparaître sur ton blog, elles peuvent toujours exiger que tu retires les photos : c'est le droit de retrait – on a le droit de changer d'avis, on a le droit d'être « oublié ».

Sur Facebook, quelles précautions doit-on prendre avant de diffuser une photo ?

C'est comme sur un blog. Même si tes informations sont a priori mieux protégées sur Facebook que sur ton blog, qui te dit que des « amis d'amis » ne vont pas les rendre publiques à leur tour ?

Toujours sur Facebook, qu'est-ce qu'on peut faire pour supprimer une photo de nous lorsqu'une personne l'a diffusée ?

Si la photo est marquée (« taggée »), il suffit de la démarquer pour qu'elle ne soit plus dans « mes photos ». En revanche la photo existe toujours sur le compte de celui qui l'y a placée. Facebook dit : « Si vous souhaitez que la photo ne soit plus diffusée, discutez-en avec la personne qui l'a publiée. Elle devrait se montrer suffisamment respectueuse pour supprimer une photo inconvenante. Facebook ne peut malheureusement PAS contraindre des utilisateurs à supprimer des photos qui ne constituent pas une infraction à nos Conditions d'utilisation. »

Comment faire pour éviter que plusieurs personnes diffusent des images de nous sans notre permission ?

Sur Facebook, surveille le mur de tes amis. Tu peux régler tes paramètres de notification de façon à toujours savoir quand une personne t'identifie dans une photo ou identifie quelqu'un d'autre dans une de tes photos.

Va voir le blog de tes amis de temps en temps. Fais une recherche sur leur nom et sur le tien avec un moteur de recherche.

Certains lancent une entreprise de « nettoyage de réputation » pour éliminer du web toutes les traces que tu y as laissées et que tu n'arrive plus à faire disparaître (pour chercher un emploi, par exemple, il vaut mieux ne pas apparaître trop souvent sur des blogs dans des situations gênantes...)

Les sites pour créer des montages-photo sont-ils autorisés par la loi ?

Pourquoi les interdire ? Tout dépend de ce que tu fais avec. Si tu causes du tort à quelqu'un en trafiquant des images non légales, c'est toi qui es fautif, pas le site.

Voilà Léo !

LEO : *Merci Sanéla ! Tu restes avec nous car tu es notre DJ pendant cette émission. Alors, tu nous a préparé quoi ?*

SANELA *Salut Léo ! tout-de-suite on va écouter Robby Williams. Il va vous donner envie de bouger, avec son titre « Bodies »*

1^{ère} PAUSE MUSICALE

FICHIER MP3 : 2_CYBER_INTIMIDATION_LEO.MP3 (3MN59s) 3,7 Mo

JINGLE

2^{ème} partie : La cyber-intimidation (LEO)

LEO : *Je vous propose maintenant d'écouter le témoignage de cette enseignante, qui a été harcelée sur internet.....*

Témoignage Madame B.

Eh bien, pour cette 2^{ème} partie, c'est moi qui vais poser les questions sur la cyber-intimidation.

Bernard Usé, est-ce qu'on peut dire que cette enseignante a été victime de cyber-intimidation ?

Oui, pour plusieurs raisons :

- L'intention est clairement de nuire à la personne en la dominant, en lui faisant peur et en tentant de l'humilier
- L'auteur se réfugie derrière l'anonymat d'internet
- Il harcèle sa victime (c'est un acte répété)
- La victime ne peut pas s'échapper
- L'agression utilise internet comme une arme ; Internet garde les traces, même après qu'elles ont été effacées

La cyber-intimidation peut-elle prendre la forme d'insultes ?

L'insulte, l'injure, la diffamation, font partie de la cyber-intimidation.

Le chantage fait-il partie de la cyber-intimidation ?

Le chantage, mais aussi les menaces, l'humiliation...

Si je trouve le mot de passe d'une personne sur mon msn par exemple, et que j'insulte toutes les personnes en contact avec elle. Cela fait-il partie de la cyber-intimidation ?

Oui, mais il s'agit surtout d'une usurpation d'identité, ce qui peut être très grave.

Avez-vous d'autres exemples de cyber-intimidation ?

On constate de fréquents abus de Facebook par des élèves qui se liguent contre un prof. Ce n'est pas parce que votre profil Facebook est privé que vous êtes à l'abri de poursuites : les amis de vos amis ont aussi des amis, etc. et tous ne protègent pas leurs données sur Facebook.

Et vous, avez-vous déjà été victime de la cyber-intimidation ?

Non, jamais. Ni victime, ni coupable.

Si je suis moi-même un cyber-intimidateur, qu'est-ce que je risque ?

Voilà un aperçu des « tarifs » :

- Happy slapping (violence physique filmée) : 75 000 euros et – ou 5 ans de prison
- Commentaires sur un camarade ou un professeur du style « c'est un voleur » (diffamation) : 12.000 Euros
- Commentaires du style « la prof de (matière) est une » (injure) : 12.000 euros
- « N... ta mère ! » (propos indécents) : 750 euros

LEO : *Merci Bernard Usé, vous restez avec nous. Je passe la parole à Sanéla, qui nous fait bouger en musique !*

SANELA : *On écoute maintenant Helmut Fritz, le plus franco-allemand des chanteurs... Il va vous faire disjoncter avec son titre « Ça m'énerve »*

2^{ème} PAUSE MUSICALE

FICHER MP3 : 3_PIRATAGE_DONOVAN_VICTOR.MP3 (4MN45S) 4,4 Mo

JINGLE

LEO : Vous êtes toujours sur Radio Pulsar, dans une émission spéciale consacrée aux pirates du net.

On écoute d'abord un extrait de notre micro trottoir.

Une assistante d'éducation nous explique comment elle s'est fait prendre son compte.

Témoignage Sophie

Qu'est ce que le hackage de jeux en réseaux ?

Moi je ne sais pas, mais si je parcours les forums de jeux vidéo en ligne (les jeux de plateforme multi joueurs), il me semble bien que la plupart des ados le savent très bien, non ?

Est-ce que vous vous êtes déjà fait hacker votre session ?

N'étant pas joueur, c'est un risque que je ne cours pas...

Quant à mes mots de passe, je les protège assez bien, je crois.

Comment peut-on éviter de se faire hacker sa session ?

J'imagine qu'il faut d'abord protéger son identité : le mot de passe associé à son identifiant ne doit être connu que de toi.

Avez-vous déjà piraté quelqu'un ?

Non, jamais. Comme je te l'ai dit, je ne joue pas, ni sur internet ni ailleurs.

En revanche il est assez courant de se voir usurper son identité sur Facebook : quelqu'un essaie de se faire passer pour vous. Le bouton « signaler cette personne > faux profil > usurpation de mon identité » permet de demander la suppression d'un faux profil.

Si oui comment avez vous fait ?

Peut-on avoir une amende pour avoir hacké un compte de jeux ?

Je suppose que si la victime porte plainte et qu'elle peut justifier d'un dommage qu'elle a subi, il doit y avoir une loi pour punir ça. En réalité je n'en sais rien, je ne suis pas juriste et le monde du jeu en réseau ne m'est pas familier.

Le piratage en général est un délit, mais la gravité dépend du préjudice que la victime a subi.

Qu'est que le hameçonnage ?

C'est une arnaque particulière : il s'agit de vol de données (généralement bancaires : n° de carte de crédit) par des sites qui prennent l'apparence d'un autre site : tu crois être sur le site

de ta banque, alors qu'en fait tu es sur le site d'un pirate, qui te vole ton numéro de carte de crédit.
Souvent l'internaute est dirigé vers ces sites frauduleux par des liens contenus dans des courriers électroniques.

Comment savoir si je suis sur le bon site, et pas sur un site pirate ?

Si tu utilises un navigateur à jour et qu'il affiche le cadenas des sites sécurisés en https, il y a peu de risques, mais c'est une bonne habitude de se méfier : il faut faire attention à l'adresse URL de la page où tu es : observe l'URL de la page et des éléments qui la composent (clic droit : examine la source).

LEO. *On rappellera ces infos pratiques à la fin de l'émission, mais pour l'instant, une petite pause en musique !*

SANELA : *Et maintenant, vous allez écouter un chanteur. Il est guadeloupéen, il fait du surf. Vous savez très bien de qui je parle : Tom Frager, avec son titre « Give me that love »*

3^{ème} PAUSE MUSICALE

FICHER MP3 : 4_IMPACT_PSYCHOLOGIQUE_CYBERINTIMIDATION_OCEANE.MP3 (6MN57S) 6,4 Mo

JINGLE

4^{ème} partie : Aspect psychologique de la cyber-intimidation (Océane)

LEO : *Pour préparer cette émission sur les comportements dangereux sur le net, on a rencontré Mathieu.*

Il travaille dans une radio et utilise beaucoup internet pour son travail et ses loisirs. On lui a demandé son avis : D'après lui, pourquoi des gens s'amuse-t-ils à harceler les autres sur internet ?

Témoignage Mathieu

Est-ce que beaucoup de gens envoient des chaînes, des canulars ou des harcèlements sur internet ? Pourquoi font-ils ça ?

Il y a deux choses bien différentes dans ta question :

- Pour les canulars : il y a toujours des gens pervers pour faire circuler des rumeurs, et des gens naïfs prêts à les croire. Internet ne fait qu'accentuer les choses. Je ne sais pas pourquoi les gens font ça : j'imagine par méchanceté, ou par désœuvrement, pour le plaisir un peu vicieux de faire circuler des fausses informations...
- Pour le harcèlement, c'est clairement la volonté de nuire, d'embêter quelqu'un.

Comment internet peut modifier le comportement des gens ? Par exemple : des gens qui sont timides dans la vie deviennent insultant sur internet ?

Tu mets le doigt sur un aspect important de la nature humaine : beaucoup de gens aiment faire du mal aux autres et profitent d'une certaine impunité pour se livrer à des actes blessants. Les coupables sont d'ailleurs bien naïfs : ils ignorent à quel point personne n'est anonyme sur le net...

Pourquoi continuent-ils à faire cela, sachant que cela peut blesser ceux qui en sont victimes ?

Depuis toujours certains se comportent en tyrans. Il faut juste les empêcher de nuire.

Après avoir reçu un message blessant, est-ce que les gens osent en parler ?

Pas toujours, mais c'est important pour une victime de savoir se défendre, et d'abord d'en parler à quelqu'un de confiance, un autre adolescent mais surtout un adulte.

Quand on se fait harceler sur internet, à qui doit-on en parler ?

Ça dépend des gens : toi, à qui te confierais-tu ? En général on se confie à ses meilleurs amis, parfois à ses parents, mais ça dépend du climat de confiance dans la famille. Parfois certains adultes au collège écoutent bien les problèmes des élèves (le CPE, l'infirmière, le prof principal...)

Quelles sont les stratégies pour éviter de recevoir des messages de ce genre ?

Première chose : ne pas répondre (sinon tu relances les provocations)

Si tu es victime, les règles de comportement sont simples :

- Il faut d'abord faire une copie de sauvegarde des contenus offensants (pour avoir une preuve)
- Ensuite il faut couper la connexion par laquelle passe la menace (le chat, le mobile...)
- Enfin il faut signaler l'incident à un adulte de confiance.

Qu'est-ce que cela peut entraîner chez les personnes fragiles ?

La victime se sent menacée, persécutée. Les victimes isolées peuvent se fermer encore plus aux autres, se sentir isolées, dévalorisées. Elles perdent confiance en elles. Elles peuvent devenir agressives ou dépressives.

A l'école, ces comportements peuvent « pourrir » l'ambiance : il faut clairement montrer aux coupables qu'ils seront partout montrés du doigt s'ils ne cessent pas leurs intimidations.

LEO : *Merci pour toutes tes questions, Océane ! c'est l'heure de notre 4^{ème} morceau ! Sanéla, qu'est-ce que tu as dans ton juke box ?*

SANELA : *Il s'appelle David Guetta, il a mixé tout l'été à Ibiza. Il va vous faire décoller avec son titre « Mémoires »*

4^{ème} PAUSE MUSICALE

FICHIER MP3 : 5_PIRATAGE_IDENTITE_LOGAN.MP3 (7MN56S) 7,3 Mo

JINGLE

5^{ème} partie : Comment se protéger des risques de piraterie (LOGAN)

LEO : *On écoute la suite de l'interview de Mathieu. Il nous donne ses trucs et astuces pour éviter d'avoir des problèmes de virus ou de harcèlement sur le net.*

Interview Mathieu. Suite

LEO : *Logan, c'est à toi de jouer !*

Salut Léo ! Monsieur Usé, vous allez nous expliquer comment se protéger des risques de piraterie sur internet.

Tout d'abord, qu'est ce que le piratage ?

Le piratage informatique est l'accès non autorisé aux données contenues dans un ordinateur.

Quel est le but de ceux qui piratent ?

Certains piratent des systèmes pour le sport, pour devenir célèbres dans le milieu des pirates, d'autres pour voler des informations ou de l'argent, d'autres pour nuire à une personne ou une organisation (voler des données ou les détruire, empêcher le fonctionnement d'un site...)

Comment se protéger de leurs attaques ?

C'est difficile. Le meilleur système a toujours des failles. Mais on peut déjà tenir son ordinateur à jour : pare-feu, anti-virus, mises à jour du système d'exploitation et des logiciels...

Méfie-toi particulièrement :

- des logiciels Peer-to-peer : ils transportent souvent des logiciels espions ;
- des courriers électroniques douteux, qui peuvent installer des « bots » (robots) qui transforment ton ordinateur en machine-zombi qui envoie des spams à ton insu ;
- des sites louches (ceux qui donnent des clés de logiciels par exemple) : ils peuvent installer des logiciels qui téléphonent à des sites surtaxés.

On peut aussi conseiller de faire le ménage régulièrement dans son navigateur internet, par où passent beaucoup de virus. Utiliser un programme de nettoyage est une bonne précaution. Savoir régler son navigateur internet aussi.

Régler son logiciel de messagerie pour envoyer ses messages en texte brut plutôt qu'en html : c'est moins joli mais beaucoup plus sûr.

Utiliser Linux plutôt que Windows réduit aussi beaucoup les risques : Linux est beaucoup moins vulnérable aux attaques.

Pourquoi faut-il protéger son ordinateur ?

Parce que les logiciels malveillants (les malware : virus et vers, logiciels espions, etc.) peuvent nuire à ton ordinateur, et aux données qu'il contient.

Il ne devrait rien y avoir de sensible dans un ordinateur : un ordinateur n'est pas une bonne cachette, surtout s'il est connecté à internet ! Et si tu tiens au contenu de ton ordinateur, fais-en des copies de sauvegarde que tu rangeras ailleurs.

Est-ce qu'un antivirus gratuit est moins efficace qu'un anti virus payant ?

Non, il n'y a aucun lien entre le prix et l'efficacité. C'est comme pour tous les logiciels : la plupart des logiciels libres sont gratuits, et pourtant ils sont aussi efficaces que les payants. Si tu utilises Windows, la suite Microsoft Security Essentials offre un bon niveau de protection, gratuitement.

A quoi sert un mot de passe ?

C'est la clé qui ouvre la serrure. Attention : comme dans les maisons, si tu laisses ta porte ouverte et qu'un cambrioleur entre chez toi, c'est quand même lui le coupable.

Sur internet, si tu entres par erreur dans un endroit où tu n'as pas le droit d'aller (le site de la CIA !), il ne faut pas y rester, même si la porte était ouverte !

Comment trouver un bon mot de passe ?

Il faut qu'il soit assez long (7 ou 8 caractères minimum), qu'il mélange des lettres majuscules et des minuscules, des chiffres et d'autres caractères.

Il ne faut pas qu'il soit un mot du dictionnaire ni un nom de ton entourage.

Il faut éviter d'avoir le même mot de passe pour tous les services que tu utilises. Mais bien sûr il faut alors se souvenir de tous tes mots de passe : un bon moyen mnémotechnique peut être de prendre l'initiale des tous les mots d'une phrase connue (chanson, proverbe...)

Mais un bon mot de passe c'est d'abord un mot de passe que tu es le SEUL à connaître. Ne l'écris jamais nulle part. Si tu as trop de mots de passe mémoriser, enregistre-les dans un logiciel crypté de gestion de mots de passe (il en existe des gratuits).

Si tu penses que quelqu'un a peut-être réussi à te voler un mot de passe, change-le aussitôt.

Y a t il des moyens de savoir si un mot de passe est fort ou faible ?

Parfois quand tu choisis un mot de passe, l'application (par exemple hotmail) te signale s'il est fort ou faible en affichant un curseur vert ou rouge. Mais c'est toi qui juge de la fiabilité du

mot de passe. Attention aussi à ce que ta question secrète pour retrouver ton mot de passe soit bien secrète...

Pouvez-vous nous parler de l'identité numérique ?

Combien as-tu de boîtes mels ? Combien de services utilises-tu qui nécessitent un mot de passe ? A chaque fois que tu t'identifies sur un service (Facebook, le chat, Gibii, le courrier électronique, le serveur pédagogique du collège, un blog que tu tiens à jour, un jeu en réseau...), tu es reconnu par le système qui connaît ton identité et te donne les droits qui vont avec. Tu peux avoir des identités différentes selon les systèmes.

Souvent pour chaque identité tu utilises un nom différent, voire un avatar censé te représenter (un symbole).

Comment faire pour protéger son identité numérique ?

Ne pas la laisser traîner partout ! Evite de donner trop d'informations sur toi dans ton blog, sur ton compte Facebook, sur tes albums photos en ligne...

A toi Léo !

LEO : *Merci Logan ! Avant de conclure cette émission, une avant-dernière pause musicale, avec notre super DJ : Sanéla !*

Sanéla : *Et maintenant, voici notre coup de cœur, un groupe américain. Ils ont cartonné aux derniers NRJ Music Awards. Voici le groupe Black Eyed Peas, avec le titre « Meet me Alfay »*

5^{ème} PAUSE MUSICALE

FICHER MP3 : 6_CONCLUSION_LIENS.MP3 (4MN37S) 4,2 Mo

JINGLE

Léo : *Les comportements dangereux sur internet : dernière ligne droite de cette émission ! J'espère qu'elle vous a été utile.*

Bernard Usé, avez vous des adresses utiles à conseiller à nos auditeurs pour compléter toutes ces informations ?

- Le site « protegetonordi.com » donne de bons conseils.
- Le « [forum des droits sur l'internet](#) » aussi.
- Hoaxbuster est une bonne ressource pour savoir si un message est une info ou une intox.
- Et j'aime bien certaines vidéos du site « [Internet sans crainte](#) », qui expliquent avec humour comment bien se comporter sur internet.
- Enfin, restez curieux, en éveil : lisez les « [petites lignes](#) », les paramètres de confidentialité dans Facebook, les conditions d'utilisation des blogs, etc.

L'émission touche à sa fin, merci beaucoup d'avoir accepté de répondre à toutes nos questions, Bernard Usé !

Je rappelle que vous êtes spécialiste des TIC pour l'académie de Poitiers.

Cette émission a été préparée et présentée par Océane, Sanéla, Donovan, Victor et Logan.

Une petite pensée pour Nicolas, qui nous a accompagnés pendant tout l'atelier.

On remercie également Evelyne Vincent et Gaël Beaumard, du collège Prosper Mérimée, et l'équipe de Pulsar.

Vous pourrez très prochainement télécharger cette émission sur les sites du collège de Saint-Savin et de Radio Pulsar.

Sanéla, à toi de jouer pour ce décollage en musique !

Sanéla : *Merci à toi aussi, Léo. Pour terminer l'émission, j'ai décidé de rendre hommage au roi de la pop. Vous devez tous savoir de qui je parle. C'est notre très cher Mickael Jackson avec son titre «Beat it ».*