

Le cyberharcèlement

Adrien RAMELET



MonAssistant
Numerique.com
Strasbourg

Qu'est-ce que le cyberharcèlement ? Quelles sont ses formes ?



Quelques chiffres

Etude IPSOS pour Meetic fin 2021 :

“59% des Français, sans différence selon le genre, ont déjà été victimes de cyberharcèlement”

<https://www.ipsos.com/fr-fr/le-harcelement-en-ligne-est-un-probleme-tres-grave-selon-68-des-francais>

-Etude E-enfance Caisse d'épargne : 20% des jeunes français ont déjà été victimes de cyberharcèlement

<https://newsroom.groupebpce.fr/actualites/etude-caisse-depargne-association-e-enfance-sur-le-cyber-harcelement-des-jeunes-20-des-jeunes-francais-ont-deja-ete-confrontes-a-une-situation-de-cyber-harcelement-8f13-7b707.html>

Étude IPSOS pour Meetic - Chiffres clés

- “Le harcèlement en ligne est un problème très grave selon 68% des Français
- 1 Français sur 2 estime que l’on n’en parle pas assez, et près de 8 sur 10 que les actions mises en œuvres pour prévenir et lutter contre ne suffisent pas (79%)
- 78% des Français pensent que les femmes sont plus souvent victimes que les hommes, or...
- 59% des Français, sans différence selon le genre, ont déjà été victimes de cyberharcèlement”

Source:

:

<https://www.ipsos.com/fr-fr/le-harcelement-en-ligne-est-un-probleme-tres-grave-selon-68-des-francais>

Définition du cyberharcèlement

Définition du Ministère de l'Éducation Nationale :

“Le cyber-harcèlement est défini comme "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".

-Agression

-Intentionnel

-Un ou plusieurs auteurs

-En ligne

-Répété

Une agression

Propos insultants, dégradants, menaçants : via des commentaires, des messages privés, mails, des faux comptes sur les réseaux sociaux

But : atteindre la santé mentale de la victime, affecter ses conditions de vie, pour la “manipuler”

Exemples : moqueries, insultes, menaces, rumeurs etc.-> EN LIGNE

Le cyberharceleur veut vous déstabiliser, vous atteindre psychologiquement !

Intentionnel

Les cyberharceleurs connaissent leur but et les risques de leur action

L'acte ou les actes peuvent être prémédités, réfléchis, avec un “plan d'action”

Volonté de nuire à la victime, de la blesser, de la faire culpabiliser, de la rendre vulnérable pour obtenir quelque chose en retour

Qui sont les cyberharceleurs ?

Un ou plusieurs individus

-Troll

-Entourage de la victime



Le troll

Un inconnu sur le net

Anonyme, “caché” derrière un pseudo

Souvent en matière politique, religieuse, débat d'idées

Troll 100% : inonde les réseaux de commentaires, stratégie du pourrissement

Troll 50% : inonde de commentaires + hack ou fake news

Troll militant

Pourquoi “troller” ? Jouer, attirer l'attention, déverser sa haine, plaisir d'ennuyer les autres/leur faire perdre leur temps

Anonymat + dissémination + diffusion + large = fort pouvoir de nuisance



Entourage de la victime

Amis, proches, famille, connaissances de connaissances, collègues de fac, d'entreprise etc.

Force : connaissance plus ou moins élevée de la victime, de ses habitudes, de ses passions, de ses opinions (et parfois de ses mots de passe...)

Attaque peut être très forte

Désir de vengeance, de nuire, de détruire, de culpabiliser, pour obtenir une ou plusieurs choses

Atteinte à la réputation, à l'honneur, à son intégrité

Atteintes morales, psychologiques, voire physiques

Reconnaître un cyberharceleur

Attitude agressive, provocante

Encouragement de ce type de comportement ou non condamnation, négation des impacts négatifs de leurs actes

Utilisation de plusieurs (parfois beaucoup) comptes en ligne sur le même réseau social, plusieurs identités digitales (M. X sur Facebook, M.Y sur Instagram etc.)

Cercle d'amis agressifs, participant parfois à ce type d'action



Formes du cyberharcèlement

Happy slapping

https://www.bfmtv.com/police-justice/agression-filmee-d-une-adolescente-a-reims-qu-est-ce-que-le-happy-slapping_AV-202009100029.html

Formes du cyberharcèlement

Rumeurs propagées en ligne, ou par téléphone, par mail

Intention de nuire, d'atteindre la réputation de la personne, sa personne en elle-même

Fausse identité en ligne d'une personne : faux profil sur les réseaux sociaux, faux groupe, fausse page pour se moquer d'une personne

Se faire passer pour vous, usurpation de votre identité digitale

Intimidations/insultes, menaces en ligne

Piratage de vos comptes en ligne : se faire passer pour vous, obtenir des avantages en faisant croire à votre cercle de connaissances en usurpant votre identité

Diffusion d'images sensibles : photos/vidéos pornographiques, humiliantes, dégradantes

Formes du cyberharcèlement

Slut shaming : femmes jugées sur leur sexualité ou leur tenue vestimentaire

Grossophobie

Body shaming : en fonction du physique de la personne

Handicap

Sexisme

Racisme, antisémitisme, islamophobie

Propos/chantage sur les personnes homosexuelles, transgenres

Amplification du cyberharcèlement : reprise/repartage des publications par d'autres comptes

Le cyberharcèlement tue...



Cyberharcèlement : comment réagir ?



1. Identifier une personne cyberharcelée

Repli sur soi

Absence au travail, de son milieu scolaire/universitaire / Phobie

Stress / Agressivité

Déprime/dépression

Automutilation



1. Identifier une personne cyberharcelée

Refus de montrer ses comptes en ligne

Sommeil perturbé

Maux de ventre/de tête

Résultats scolaires, réussite professionnelle en baisse

Diminution voire fin des interactions sociales

Comportement agressif, menaçant, insultes

2. Se protéger en amont

- Ne pas donner de détails sur sa vie privée en ligne
- Ne pas confier ses mots de passe
- Ne pas poster de contenus personnels ou sensibles
- Ne pas partager ses informations personnelles, sécuriser ses mots de passe

Exemples : éviter de donner sa localisation précise, de partager des photos de tous les lieux dans lesquels on se rend, de partager une photo/vidéo intime etc.

Moins on donne de détails sur soi, plus on se protège

Mettre le moins d'informations possibles dans sa biographie, sa présentation, les informations publiques et demandées par un réseau social

Masquer le plus d'informations possibles sur son profil (âge, situation, lieu de résidence, opinions politiques et religieuses), prendre un pseudo ou ne pas mettre son vrai nom de famille

2. Se protéger en amont

-Respecter sa vie privée et celle des autres : droit à l'image + droit à la vie privée = demander à une personne son autorisation avant de publier une photo/vidéo d'elle sur un réseau social

-Verrouiller la confidentialité de ses profils

Instagram : Paramètres > Confidentialité > Compte privé

Facebook : Comment modifier vos paramètres de sécurité sur Facebook

<https://www.avast.com/fr-fr/c-change-facebook-privacy-settings>

Ne partagez pas tout avec n'importe qui ! Vous ne donneriez pas les clés de votre maison à un(e) inconnu(e) rencontré dans la rue. En ligne c'est pareil !

2. Se protéger en amont

Bien paramétrer ses réseaux sociaux :

-Utiliser un pseudo, verrouiller son compte en privé, limiter l'audience de ses publications

Et SURTOUT : un mot de passe FORT !!!

<https://www.internetsanscrainte.fr/dossiers/cyberharcèlement-2/conseils/prevenir-le-cyberharcèlement-comment-paramétrer-ses-réseaux-sociaux>

3. Se constituer des preuves

Faire des captures d'écran

Sur PC : touche imp écran, ouvrir un document et enregistrer la capture

Sur Mac : cmd+majuscule+4

Sur votre téléphone Android : appuyez simultanément sur le bouton marche/arrêt et sur le bouton volume -

S'envoyer les captures d'écran par mail

Capture d'écran horodatée : logiciel Screengrab ou Pagesaver (extension via le navigateur)

4. En parler

Se confier à ses proches, à une personne de confiance : besoin de soutien

Se confier à un tiers



Etre accompagné

Le 3018

Numéro unique gratuit et confidentiel pour soutenir et accompagner les parents et leurs enfants victimes de cyberviolences

Disponible depuis peu via une application

<https://www.youtube.com/watch?v=-HfLEnnsJpA>



30 18

Violences numériques
Prévenir – Intervenir

Pour joindre le 30 18 :

    

gratuit - anonyme - confidentiel
du lundi au samedi de 9h00 à 20h00


e-Enfance
Coordination nationale des services numériques
www.monassistantnumerique.com



Signaler !



Signaler

SE RENSEIGNER

Questions et Réponses

Conseils

Conseils aux Jeunes

Conseils aux Parents

Internet Prudent

Protéger son ordinateur

Liens Utiles

Internet est un espace de liberté où chacun peut communiquer et s'épanouir. Les droits de tous doivent y être respectés, pour que la « toile » reste un espace d'échanges et de respect. C'est pourquoi les pouvoirs publics mettent ce portail à votre disposition. En cliquant sur le bouton « SIGNALER », vous pouvez transmettre des signalements de contenus ou de comportements illicites auxquels vous vous seriez retrouvés confrontés au cours de votre utilisation d'Internet.

Signaler >>

Vous trouverez également sur ce site des pages d'information, ainsi que des conseils de spécialistes pour mieux vous protéger et protéger vos proches dans leur utilisation de l'Internet.

ACTUALITÉS

Formulaire de signalement

1.Contenu 2.Quand/Où 3.Description 4.Informations 5.Validation

Quel type de contenu souhaitez-vous signaler ?

Choisissez le type de contenu dans la liste ci-dessous* : [?]

- Pédophilie ou corruption de mineur sur Internet
- Provocation à la discrimination ou à la haine de personnes en raison de leur origine, de leur appartenance ou non à une ethnie, une nation, une race ou une religion, de leur sexe, de leur orientation ou identité sexuelle ou de leur handicap
- Menaces ou incitation à la violence
- Trafic illicite (stupéfiants, armes, etc.)
- Mise en danger des personnes
- Incitation à commettre des infractions
- Spam
- Injure ou diffamation
- Escroquerie
- Terrorisme : menace ou apologie

Abandonner

Etape suivante >

* : indication obligatoire

Etre accompagné, s'informer



 ESPACE PRESTATAIRE

 MON ESPACE



ASSISTANCE ET PRÉVENTION DU RISQUE NUMÉRIQUE AU SERVICE DES PUBLICS

LES MENACES ET BONNES PRATIQUES

L'ACTUALITÉ DE LA
CYBERMALVEILLANCE

NOUS DÉCOUVRIR

VICTIME D'UN ACTE DE
CYBERMALVEILLANCE ?

<https://www.cybermalveillance.gouv.fr>



Nouvelle campagne Cybermalveillance



Demander le retrait du contenu

- Demander à la personne de retirer le contenu
- Bloquer la personne sur les plateformes, signaler son profil
- Signaler aux plateformes : droit d'opposition, demande de déréférencement du contenu

Plus d'informations sur le site de la CNIL :

<https://www.cnil.fr/fr/cnil-direct/question/reseaux-sociaux-comment-faire-supprimer-des-informations-publiees-sans-mon>

Signaler un profil Facebook

Publications À propos Amis Photos Vidéos Lieux Plus ▾



- Appel vocal
- Appel vidéo
- Rechercher dans le profil
- Voir les liens d'amitié
- Trouver de l'aide ou signaler le profil
- Bloquer

Signaler

Veillez sélectionner une raison

Si une personne est en danger immédiat, demandez de l'aide sans attendre avant de le signaler à Facebook.

- Usurpation d'identité >
- Faux compte >
- Faux nom >
- Publication de contenus inappropriés >
- Harcèlement ou intimidation >
- Je veux aider >
- Autre >



COMMENT UTILISER LES RESEAUX SOCIAUX EN TOUTE SECURITE ?



CONSO MAG vous conseille pour sécuriser
l'utilisation de vos réseaux sociaux.

Déposer plainte



Sanctions du cyberharcèlement :

- Si la victime a plus de 15 ans, l'auteur des propos risque 2 ans de prison et 30.000€ d'amende.
- Si la victime a moins de 15 ans, la peine maximale encourue est portée à 3 ans de prison et 45.000€ d'amende.

Pour aller plus loin...

Réagir en cas de harcèlement en ligne

<https://www.cnil.fr/fr/reagir-en-cas-de-harcelement-en-ligne>

www.cybermalveillance.gouv.fr

www.cnil.fr

Non au harcèlement

<https://www.education.gouv.fr/non-au-harcelement>



Cyberharcèlement : “tous concernés, tous responsables !”

Merci pour votre attention !