

*Le Conseil de quartier Pigalle-Martyrs
vous invite à une réunion publique sur*

LA CYBERMALVEILLANCE

AVEC SAMUEL COMBLEZ, DIRECTEUR GÉNÉRAL ADJOINT
DE L'ASSOCIATION E-ENFANCE

SE PROTÉGER CONTRE
LES ARNAQUES EN LIGNE

LES DANGERS MENAÇANT LES
ENFANTS ET LES ADOLESCENTS



JEUDI 13 NOVEMBRE À 18 H 30
à l'école 5 rue Milton



MAIRIE DU NEUVIÈME
ARRONDISSEMENT DE PARIS
6 rue Drouot 75009 Paris
01 71 37 75 09
www.mairie09.paris.fr
mairie9paris

Mairie du
NEUF
PARIS

Le bureau du Conseil de quartier Pigalle-Martyrs a souhaité organiser une réunion publique sur la Cybermalveillance à destination des riverains. Celle-ci s'est tenue le jeudi 13 novembre 2025 à l'école du 5 rue Milton.

La réunion publique était purement informative, conformément aux règles liées à la période de réserve électorale.

I. SE PROTEGER DES ARNAQUES EN LIGNE

Sont intervenus, pour la Préfecture de police (DSPAP) :

- Le Major DUSUEL
- La Cheffe de division BERDEIL LOUIS.

Contexte :

- Environ 400 milliards de mails sont envoyés et reçus chaque jour dans le monde. Les infections se propagent très vite. Il faut avoir le réflexe de se protéger et rester vigilant.
- La prolifération des arnaques en ligne est due en partie à la facilité d'accès aux outils malveillants par une cyberdélinquance sans compétence particulière.

A – Les bonnes pratiques pour assurer sa cybersécurité

1. Protéger ses accès avec des mots de passe solides

- Le mot de passe doit comporter au moins 10 caractères, mêlant minuscules, majuscules, chiffres et caractères spéciaux.
- Il convient de diversifier et de ne pas réutiliser ses mots de passe.
- En cas de doute sur sa cybersécurité, immédiatement changer ses mots de passe.

2. Sauvegarder ses données régulièrement

- Essayer de sauvegarder tous les 15 jours ses données, sur disque dur externe plutôt que sur un cloud.
- Bien débrancher le support de l'ordinateur, une fois la sauvegarde effectuée.

3. Utiliser un antivirus et faire des scans réguliers.

4. Appliquer les mises à jour de sécurité sur tous les appareils dès qu'elles sont proposées.

5. Se méfier des messages inattendus ou alarmistes.

- Faire toujours attention à l'adresse mail de l'expéditeur. Si celle-ci est inconnu, ne jamais cliquer sur le lien proposé et supprimer le mail.
- Avant de cliquer sur un lien douteux, positionner le curseur de la souris sur celui-ci sans cliquer afin de vérifier l'adresse vers laquelle il pointe réellement.
- En cas d'alerte par pop-up, ne jamais appeler le numéro d'assistance qui s'affiche et simplement éteindre ou redémarrer son ordinateur.
- Une banque ou une administration ne demande jamais des informations sur des comptes par téléphone ou par mail, et envoie encore moins un coursier en urgence pour remplacer une carte bancaire.

6. Eviter les réseaux Wifi publics ou inconnus.

7. Eviter de dévoiler des données personnelles sur ses réseaux sociaux.

- 8. En cas de rançongiciel, ne jamais payer pour récupérer ses données.**
- En effet, vous n'êtes pas certain de récupérer vos données (notamment parce qu'une clé de chiffrement a pu être achetée sur le dark web sans la clé de déchiffrement) et vous encourageriez les cybercriminels à surenchérir.
 - Débranchez votre ordinateur.

B – Assistance en ligne, depuis un ordinateur non infecté :

- Faire un diagnostic et bénéficier d'une assistance sur 17cyber.gouv.fr. Il s'agit du guichet unique d'assistance en France.
- Si le problème est déjà identifié, suivre le parcours de signalement sur cybermalveillance.gouv.fr.
- Alerter la plateforme ou le service où a eu lieu l'attaque et changer immédiatement son mot de passe.

C – Signalements

- Pour signaler les ARNAQUES sur Internet (faux sites de vente, piratage de compte, rançongiciel...) : déposer plainte sur le téléservice THESEE.
- Pour signaler TOUT CONTENU ILLICITE sur Internet (violence, injure, apologie du terrorisme, discrimination, atteintes aux mineures...) : faire un signalement à PHAROS
- Pour signaler un SPAM par SMS : le transférer au 33700 sans commentaire.

II. LA LUTTE CONTRE LE HARCELEMENT EN LIGNE DES ENFANTS ET DES ADOLESCENTS

Est intervenu pour l'association e-enfance le Directeur général adjoint, M. Samuel COMBLEZ, psychologue de l'enfant et de l'adolescent.

A – Présentation d'e-Enfance

Il s'agit d'une association française de protection des mineurs sur Internet, créée en 2005.

Sa mission : prévenir et sensibiliser aux risques liés aux usages d'internet des jeunes et aux risques de harcèlement (à l'école, dans le sport...).

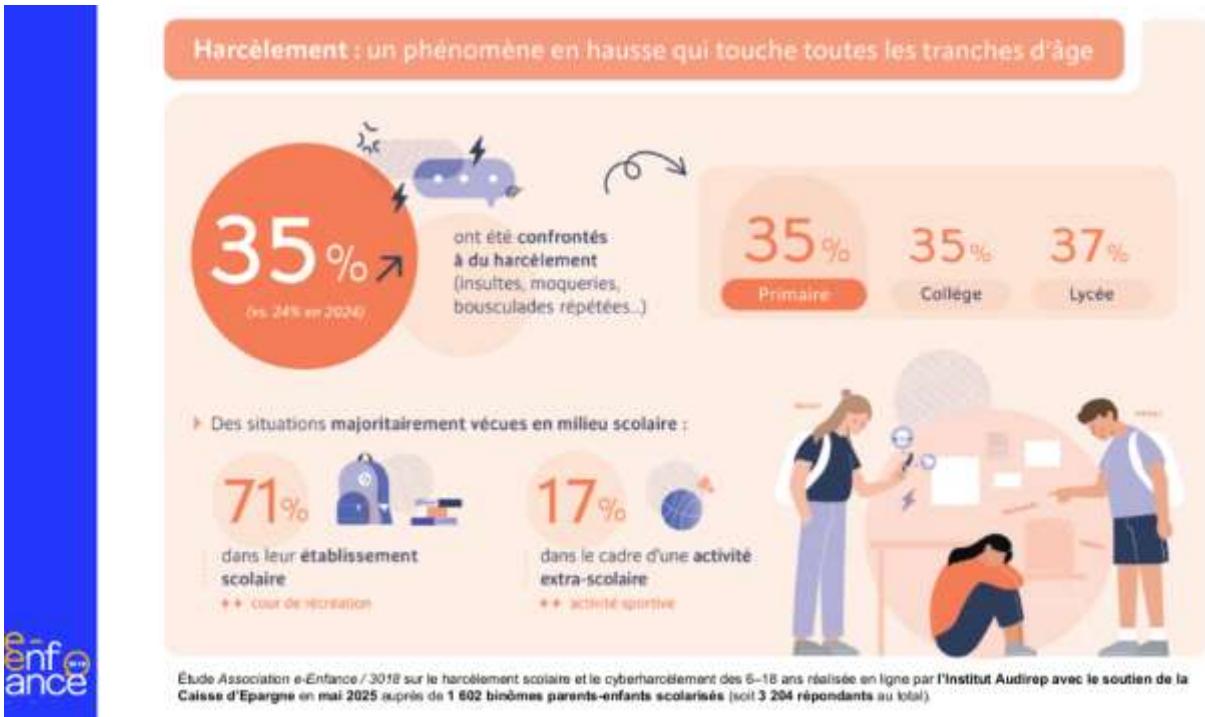
E-Enfance réalise ainsi des actions de prévention dans les écoles primaires, les collèges et les lycées, soit du CP à la Terminale.

B – Quelques chiffres

- Le harcèlement commence très tôt, dès le début des interactions sociales. 35% des mineurs (entre 6 et 18 ans) disent être ou avoir été confrontés à du harcèlement.

En France, on compte 12 millions de mineurs scolarisés en France. 35% de 12 millions = 5 millions, soit à peu près l'équivalent de la population de la Norvège.

Ce chiffre de 35% est valable dès l'école primaire (entre 6 et 10 ans).



- 65% des enfants entre 6 et 10 ans disent être inscrits sur un réseau social. Normalement, les inscriptions ne sont possibles :
 - qu'à partir de 13 ans, avec l'accord des parents
 - à partir de 15 ans sans l'accord des parents (c'est l'âge de la majorité numérique).



13-15-16-17

A CHAQUE ÂGE SON UTILISATION ET SON ACCOMPAGNEMENT

Il est intéressant de pouvoir créer cet outil avec l'adolescent seul et/ou avec ses parents

**e-
enfance**

Association e-Enfance / 3018



- 53% des enfants victimes de cyberharcèlement évaluent leur douleur, sur une échelle de 0 à 10, à un chiffre entre 9 et 10.

C – L’importance de sensibiliser les enfants

Le cyberharcèlement commence très tôt parce que la vie numérique commence très tôt. En moyenne en France on commence à utiliser Internet à partir de 5 ans et 10 mois avec ses parents, et à partir de 6 ans et 10 mois sans les parents.

Sur Internet, on peut acheter des dispositifs de berceau avec tablette comprise ou un kit de la petite influenceuse dès l’âge de 3 ans.

Il est conseillé de fixer des règles pour limiter les temps de connexion, avec ou sans logiciel de contrôle parental (sur le temps et sur le contenu).

La règle des 4 PAS

4 temps sans écrans

4 pas pour mieux avancer



○ Pas le matin

○ Pas durant les repas

○ Pas dans la chambre

○ Pas avant de s'endormir

○ Pas ?

Des règles qui évoluent avec l’âge, le plus important étant de construire une relation de confiance !

Le cyber-Harcèlement

Définition:

**Comportements intentionnellement agressifs
d'une ou plusieurs personnes
visant à porter préjudice à un internaute, le blesser, le
mettre en difficulté et établir une relation
dominant-dominé de manière répétée et à long terme
en utilisant les outils numériques**

enfance

Les processus

Violence et micro-violence conjointes

C'est un rapport de force, d'intimidation et de domination

Répétition

Agressions qui se répètent régulièrement

Intention de nuire et dégradation des conditions de vie

Le but est de blesser, d'intimider, de mettre en difficulté, de ridiculiser

enfance

Isolement de la victime

La victime est souvent isolée, plus petite, plus faible

Le Grooming

Fait pour un adulte de se faire passer pour un mineur devant un écran pour obtenir des faveurs sexuelles de la part de mineurs.



Si cela arrive, dire aux mineurs de :

- FAIRE DES SCREENS -

- SIGNALER – BLOQUER -

En PARLER à des adultes de confiance

enfance

Le cyberharcèlement ne s'interrompt pas entre la sortie scolaire et le lendemain matin, il ne s'arrête jamais.

Les profils types

Il n'existe pas de profil type de victime, ni de harceleur !

La discrimination comme source d'exclusion

Le harcèlement est fondé sur le **rejet de la différence** et sa stigmatisation :
couleur de peau, sexe, origine, religion, sexualité ou goûts culturels

Développer l'esprit critique par l'expérience :



Profil des victimes



E – Les sanctions

Loi du 4 août 2014 sur le cyberharcèlement

Propos ou comportements répétés ayant pour effet une dégradation des conditions de vie :

1 an de prison + 15 000 euros d'amende



Sur un mineur :
2 ans de prison
30 000 euros d'amende

Sur un mineur et via les technologies de communication :

3 ans de prison
45 000 euros d'amende



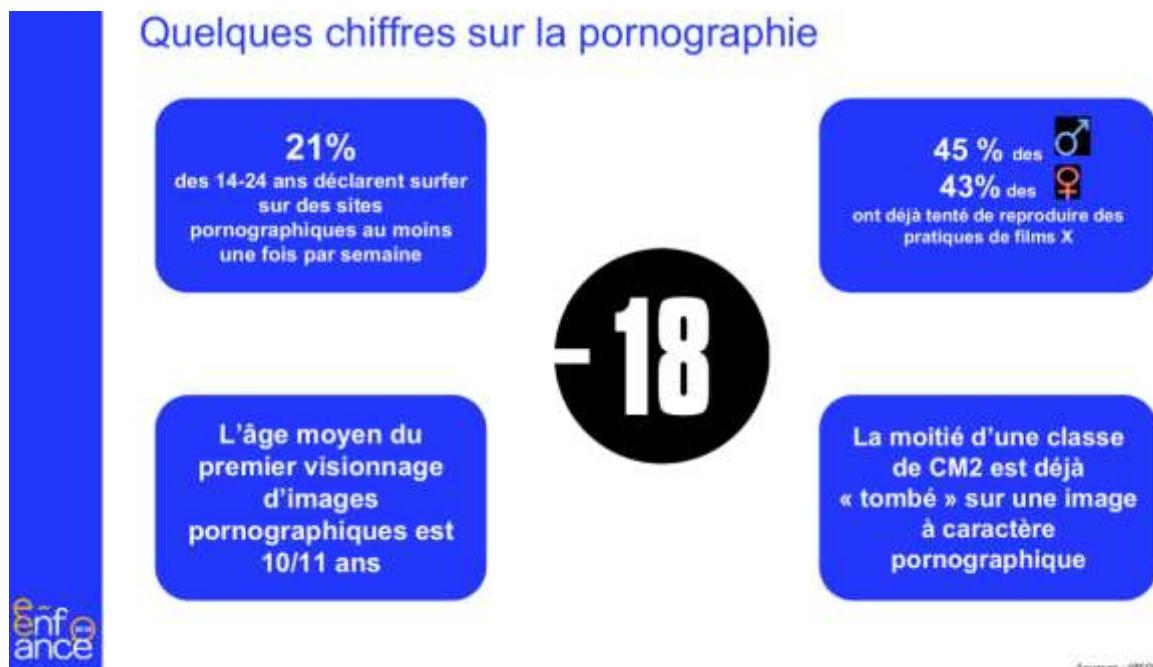
F – L’accompagnement des enfants dans leurs débuts sur les réseaux sociaux

Il faut leur apprendre que l’écran ne protège pas, que l’on soit auteur ou victime.

On peut les accompagner au début :

- « avant de publier, tu peux me montrer ? »
- « tu le dirais en face ? » (effet cockpit)

G – La pornographie



H – La plateforme 3018



L'application anti-harcèlement

- Mise en relation directe par tchat ou téléphone avec un professionnel du 3018 pour une prise en charge rapide et personnalisée
- Stockage des preuves du harcèlement vécu (captures d'écran, photos, liens url, etc.) dans un coffre-fort numérique et sécurisé, ainsi que la possibilité de transférer tout ou partie de ces preuves aux équipes 3018
- Auto-évaluation de sa situation à l'aide du quiz "Suis-je harcelé?", pour encourager la victime à demander de l'aide
- Accès rapide à des fiches conseil sur le cyberharcèlement pour s'informer sur ses droits et savoir comment réagir



ECOUTE, ACCOMPAGNEMENT ET CONSEILS PERSONNALISÉS

ACCOMPAGNEMENT PSYCHOLOGIQUE

- Orientation vers les Maisons des adolescents
- Orientation vers le 3114

3114



ACCOMPAGNEMENT JURIDIQUE

- Aide au dépôt de plainte
- Aide à la protection des données
- Aide juridique

Défenseurs des droits
CNIL.

CONSEILS

- Conseils personnalisés aux jeunes, parents et professionnels selon leur situation

500 SOLICITATIONS PAR JOUR

RELATIONS A L'EUROPE

- Membre actif du réseau européen Insafe qui regroupe les 27 lignes d'écoute en Europe
- Plier du programme européen Better Internet For Kids pour la protection des mineurs en ligne
- Échange de bonnes pratiques à l'échelle européenne

OBSERVATOIRE

- Analysé les données du 3018
- Anticiper les nouvelles menaces numériques
- Renforcer les politiques publiques, en lien avec les partenaires nationaux et internationaux



LIGNE D'ECOUTE ET D'ACTION

VIOLENCES NUMÉRIQUES

HARCÈLEMENT

7j/7 de 9h à 23h

GRATUIT, ANONYME, CONFIDENTIEL

Pour les jeunes de moins de 25 ans, les parents, les professionnels

Accessible aux personnes sourdes et malentendantes

Disponible en 180 langues

Écoutants salariés : psychologues, juristes, sociologues et éducateurs spécialisés

TELÉPHONE TCHAT WHATSAPP MAIL



SIGNALEMENTS

SIGNALEMENTS AUX PLATEFORMES NUMÉRIQUES

- 1^{er} signaleur de confiance en France désigné par l'Arcom au titre du DSA
- Suppression prioritaire de contenus illicites

Arcom

SIGNALEMENTS EN MILIEU SCOLAIRE

- Signalement aux Académies et signalements directs au ministère de l'Education nationale
- Signalement au référent harcèlement

MINISTÈRE DE L'ÉDUCATION NATIONALE, DE LA RECHERCHE ET DU NUMÉRIQUE
MINISTÈRE DE LA JEUNESSE, DES SPORTS ET DE LA COHÉSION SOCIALE

SIGNALEMENTS EN MILIEU SPORTIF

- Signalements au ministère des Sports via « Signal-sports »
- Signalements aux Fédérations partenaires

MINISTÈRE DES SPORTS, DE LA JEUNESSE ET DE LA COHÉSION SOCIALE
FFVolley
Fédération Française de l'Automobile

EN CAS DE DANGER IMMÉDIAT

- Orientation immédiate vers les services de secours (17-18-112)
- Signalement au procureur de la République
- Signalement à la plateforme Phareos
- Transmission d'informations préoccupantes aux cellules départementales de protection de l'enfance (CRIP)
- Signalement au 119 pour les cas de maltraitance



OCRETEH OFMIN

En partenariat avec l'Union européenne

Remontée des signalements

SIGNALEMENTS

15 000
SIGNALEMENTS
AUX
PLATEFORMES

SIGNALEMENTS
AUX PLATEFORMES
NUMÉRIQUES

- 1^{er} signaleur de confiance en France désigné par l'ARCOM au titre du DSA
- Suppression prioritaire de contenus illicites

Arcom

SIGNALEMENTS
EN MILIEU SCOLAIRE

- Signalement aux Académies et signalements directs au ministère de l'Education nationale
- Signalement au référent harcèlement



SIGNALEMENTS
EN MILIEU SPORTIF

- Signalements au ministère des Sports via « Signal-sports »
- Signalements aux Fédérations partenaires



EN CAS DE
DANGER IMMÉDIAT

- Orientation immédiate vers les services de secours (17-18-112)
- Signalement au procureur de la République
- Signalement à la plateforme Pharos
- Transmission d'informations préoccupantes aux cellules départementales de protection de l'enfance (CRIP)
- Signalement au 119 pour les cas de maltraitance

PIABOS

Gendarmerie

OCREH OFMIN

119



Premier signaleur de confiance français

Dans le cadre du Digital Service Act (DSA)

Statistiques 2024

160 000 sollicitations par an

15 000 contenus et comptes supprimés



25 écoutants, psychologues, juristes, spécialistes des outils numériques