RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

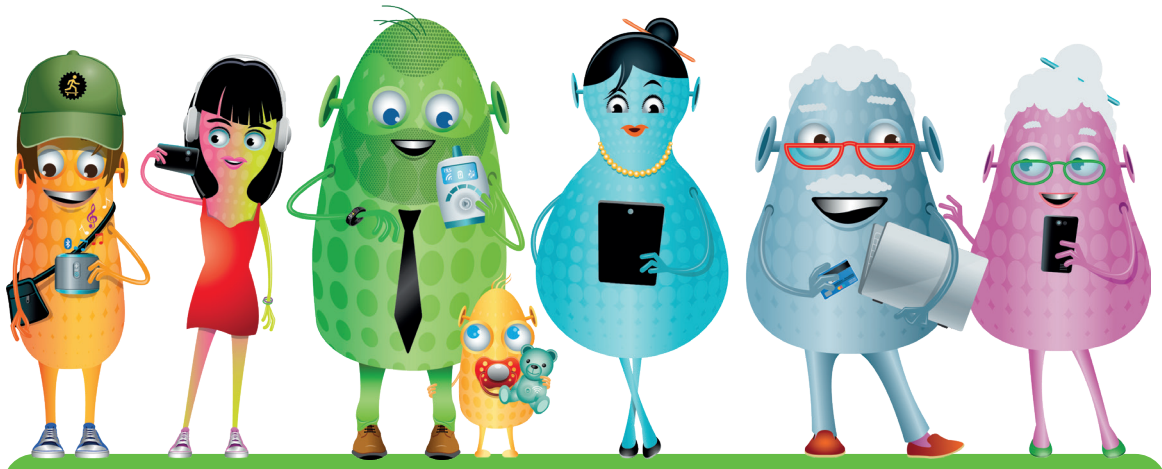
CYBER GUIDE FAMILLE

10 BONNES PRATIQUES ESSENTIELLES

pour protéger les usages numériques de la famille

WWW.CYBERMALVEILLANCE.GOUV.FR

SOMMAIRE



ÉDITO

Depuis une quinzaine d'années, avec l'arrivée des offres des opérateurs télécom attractives et celle du smartphone, Internet s'est fortement développé en France. Avec plus de 6 écrans par foyer et 2 h 30 passées en moyenne sur le web, les Français ont multiplié par 5 leur consommation d'Internet en 10 ans*.

Une situation qui a été bien sûr fortement exacerbée par la pandémie, où, plus que jamais, Internet a joué un rôle clé pour s'imposer dans nos vies comme une réponse évidente au maintien de toutes nos activités et à la continuité du lien social avec nos proches, et ce, en modifiant encore un peu plus notre façon de consommer.

De nouveaux usages sont ainsi apparus, constituant autant d'opportunités pour les cybercriminels de toucher un public rarement conscient des risques encourus. Ainsi en 2021, Cybermalveillance.gouv.fr connaissait une progression de près de 70 % des demandes d'assistance en ligne, concernant à 90 % le grand public.

« Comme le rappelle cette campagne, la prévention et la lutte contre toutes les formes de harcèlement sont l'affaire de tous. À ce titre, l'Ecole, aux côtés des familles, joue un rôle important pour renforcer l'engagement collectif et travailler globalement dans le cadre de la politique d'éducation à la citoyenneté numérique et le programme pHARe à l'instauration d'un climat scolaire serein et épanouissant. »

Pap **NDIAYE**
Ministre de l'Éducation nationale
et de la Jeunesse

© Philippe Devernay / MENJ

Fort de ce constat, nous avons décidé avec nos membres d'apporter des réponses concrètes à la nécessité de sensibiliser le grand public et notamment les familles. C'est précisément la raison pour laquelle Cybermalveillance.gouv.fr propose aujourd'hui un contenu pédagogique, à travers ce guide de bonnes pratiques.

La Cybersécurité est l'affaire de tous et cette initiative s'inscrit pleinement dans la mission d'intérêt public de Cybermalveillance.gouv.fr. Notre objectif est non seulement de rendre la cyber plus accessible et plus compréhensible à tous mais également de responsabiliser et de mieux préparer ces cibles vulnérables et particulièrement exposées que sont les familles aux enjeux de sécurité.

Jérôme **NOTIN**
Directeur général de
Cybermalveillance.gouv.fr

* Source Médiamétrie
https://www.mediametrie.fr/fr/lannee-internet-2021

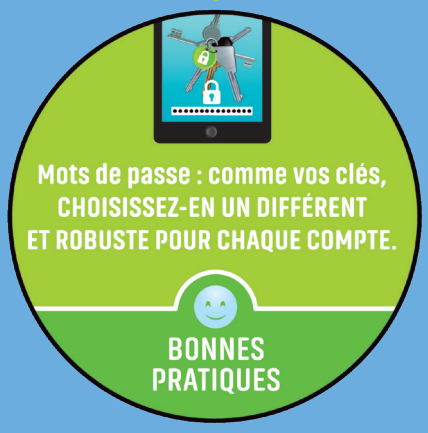
1 PROTÉGEZ VOS COMPTES AVEC DES MOTS DE PASSE ROBUSTES

En tant que parents, nous disposons tous de nombreux accès à des services que nous utilisons au quotidien : messagerie (mail), comptes bancaires, espace famille (cantine, périscolaire…), rendez-vous médicaux ou autres services administratifs (CAF, Assurance Maladie, Impôts…), réseaux sociaux… Par conséquent, la tentation est forte de n'utiliser qu'un ou deux mots de passe souvent faciles à retenir (et donc à deviner) pour l'ensemble de nos comptes.

MAIS DE TELLES PRATIQUES SONT TRÈS DANGEREUSES !

LES RISQUES

En cas de vol d'un de vos mots de passe, tous les services pour lesquels vous l'utilisez pourraient être piratés. En d'autres termes, vous vous exposeriez alors à une **prise de contrôle de l'ensemble de vos comptes** par un individu malveillant qui pourrait vous dérober des informations personnelles pour en faire un usage frauduleux : **usurpation d'identité, achats ou virements en votre nom, revente de vos données…**



LES CONSEILS

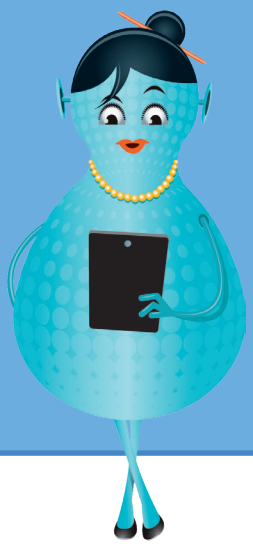
Pour réduire les risques et éviter un piratage de vos différents comptes en ligne, nous vous recommandons d'utiliser des mots de passe suffisamment longs, **complexes et différents** pour accéder à chacun de vos équipements et services. Au moindre doute, ou même par prévention, n'hésitez pas à **en changer et à activer la double authentification** chaque fois que possible pour renforcer votre sécurité. Enfin, utilisez un **gestionnaire de mots de passe** pour les stocker de manière sécurisée.

POUR ALLER PLUS LOIN

Les 10 bonnes pratiques à adopter pour gérer ses mots de passe :
www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe

Tutoriel, utiliser « Keepass » pour gérer ses mots de passe :
www.youtube.com/watch?v=XTnDKJl1zOQ

Source : CNIL – https://www.cnil.fr 19/09/2022



2 SAUVEGARDEZ VOS DONNÉES RÉGULIÈREMENT

Nous utilisons de nombreux appareils numériques pour créer et stocker des données importantes : photos, vidéos, contacts téléphoniques, documents juridiques et administratifs (bulletins de salaire, avis d'imposition, factures…) que nous n'aimerions pas perdre.

ET POURTANT, NOUS OUBLIONS SOUVENT DE LES SAUVEGARDER.

LES RISQUES

Les appareils numériques (ordinateur, téléphone portable, tablette…) sont soumis à des risques qui peuvent entraîner une perte, parfois irréversible, de vos données. Ces situations sont plus nombreuses que vous ne l'imaginez : il peut s'agir **d'un piratage, d'une panne, d'un vol ou d'une perte, voire de la destruction de votre appareil**… La sauvegarde est alors souvent le seul moyen de retrouver vos données.

LES CONSEILS

Afin de prévenir de tels risques, Cybermalveillance.gouv.fr vous recommande fortement de réaliser des **sauvegardes régulières** de l'ensemble de vos appareils en ayant au préalable identifié les données que vous estimez importantes. Pensez à en conserver une **copie sur un support externe** (clé USB, DVD ou disque dur externe), que vous débranchez une fois la sauvegarde effectuée, pour éviter qu'elle ne soit détruite également en cas de piratage ou d'infection de votre appareil par un virus. Il existe par ailleurs des **services en ligne, appelés « Cloud »**, qui offrent des fonctionnalités de sauvegarde de données. Ces solutions peuvent être gratuites ou payantes en fonction de la capacité de stockage dont vous avez besoin.

POUR ALLER PLUS LOIN

Les 10 bonnes pratiques à adopter pour gérer ses sauvegardes :
www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes

3 FAITES SANS TARDER LES MISES À JOUR DE SÉCURITÉ SUR TOUS VOS APPAREILS

Nous recevons régulièrement des notifications de mise à jour sur nos appareils numériques et il nous arrive de les différer, voire de les supprimer, par facilité, manque de temps, d'intérêt ou tout simplement parce que nous sommes occupés à une autre activité.

SI CETTE OPÉRATION DE MISE À JOUR EST SOUVENT RESSENTIE COMME UNE CONTRAINTE, IL S'AGIT POURTANT D'UN ACTE ESSENTIEL POUR SE PROTÉGER.

LES RISQUES

Les appareils numériques et les logiciels que nous utilisons au quotidien sont **exposés à des failles de sécurité.** Ces failles peuvent être utilisées par des cybercriminels comme une **porte d'entrée pour s'introduire dans nos équipements, pour en prendre le contrôle ou bien encore dérober des informations personnelles ou confidentielles** afin d'en faire un usage frauduleux (usurpation d'identité, espionnage, fraude bancaire...). Face à ces risques, les éditeurs et les fabricants proposent régulièrement des mises à jour de sécurité (*patch* en anglais) qui corrigent ces failles.

LES CONSEILS

Cybermalveillance.gouv.fr vous recommande d'**accepter les mises à jour de sécurité sur tous vos appareils** (ordinateurs, tablettes, téléphones mobiles, objets connectés...) dès qu'elles sont proposées pour corriger ces failles et ainsi vous protéger. Nous vous conseillons également de **vérifier régulièrement dans les paramètres de vos équipements et logiciels que les mises à jour sont bien appliquées** et d'activer l'option de téléchargement et d'installation automatique des mises à jour, si le logiciel le permet. Enfin, veillez à **ne télécharger les mises à jour uniquement depuis les sites officiels**, sinon, vous risqueriez de télécharger également un virus.

POUR ALLER PLUS LOIN

Comment bien gérer ses mises à jour:
www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mises-a-jour

4 UTILISEZ UN ANTIVIRUS

Certains considèrent les antivirus comme une dépense inutile au moment de l'acquisition d'un nouvel ordinateur. D'autres achètent une licence mais ne l'activent pas forcément.
Il s'agit pourtant d'un élément aussi utile qu'une alarme dans notre foyer.
En effet, nos appareils peuvent être infectés par un virus en naviguant sur Internet, en branchant une clef USB, en cliquant sur un lien ou en ouvrant une pièce jointe d'un message.

IL EST ESSENTIEL D'UTILISER UN ANTIVIRUS, GRATUIT OU PAYANT, POUR SE PROTÉGER.

LES RISQUES

Sans antivirus, vous exposez les équipements numériques de votre foyer à des virus informatiques cherchant à **porter atteinte à vos données ou à perturber le fonctionnement normal de vos appareils, à votre insu.** Les antivirus contribuent à vous protéger contre **le vol ou la destruction d'informations, l'espionnage ou le chantage**, voire à éviter de détourner vos appareils pour en attaquer d'autres.

LES CONSEILS

Nous vous recommandons d'**utiliser un antivirus sur tous vos équipements** (ordinateur, tablette, téléphone mobile...). Il existe de **nombreuses solutions gratuites ou payantes** selon vos usages et le niveau de protection recherché. **N'hésitez pas à vérifier régulièrement que les antivirus de vos équipements sont bien à jour** et à procéder à des analyses approfondies (scans) pour vérifier que vous n'avez pas été infecté.

POUR ALLER PLUS LOIN

Réponses aux 10 questions les plus fréquentes sur les antivirus :
www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/antivirus

Une vidéo sur les virus informatiques :
www.dailymotion.com/video/x7wys3a

5 SOYEZ PRUDENTS LORS DE VOS ACHATS EN LIGNE

Internet a révolutionné notre façon de consommer, qu'il s'agisse de courses alimentaires, d'achat de vêtements, de vacances ou tout simplement de petits cadeaux pour nos proches. Hier marginaux, ces nouveaux usages en ligne sont aujourd'hui banalisés dans tous les secteurs d'activité avec une offre aussi large qu'attractive, accessibles d'un clic.

POURTANT, PARMI LES NOMBREUX SITES DE COMMERCE EN LIGNE ET DERRIÈRE LES BONNES AFFAIRES, SE DISSIMULENT PARFOIS DES ESCROCS.

LES RISQUES

Les criminels redoublent d'imagination et de savoir-faire pour essayer de vous abuser : messages hameçonnage (*phishing*) par SMS, mail ou téléphone, fausses annonces promotionnelles (bon de réduction, cadeaux…), faux sites de commerce en ligne ou créés pour les circonstances (fête des mères ou des pères…), faux sites « officiels », faux transporteurs, fausses confirmations de commandes… L'objectif : **vous voler vos données personnelles ou bancaires**, vous inciter à acheter un bien que vous ne recevrez jamais, à rappeler des numéros surtaxés ou à vous abonner à des services payants à votre insu.

LES CONSEILS

Choisissez de préférence un site d'achat français ou de l'Union Européenne : la réglementation européenne qui s'applique à tous ces sites en cas de litige vous protégera. Nous vous invitons également à **vérifier la notoriété et l'adresse des sites sur lesquels vous allez faire vos achats** : si c'est votre premier achat sur un site Internet, n'hésitez pas à taper son nom sur un moteur de recherche et à consulter les avis pour vous éviter des déconvenues. De plus, vérifiez bien l'adresse car un seul caractère dans le nom du site peut différer du site officiel. Et lorsque les offres sont trop alléchantes, nous vous conseillons de comparer le prix du produit recherché sur différents sites Internet pour vous assurer du caractère crédible de la vente. Enfin, **privilégiez les moyens de paiement les plus sécurisés** (Paylib, e-Carte Bleue…).

POUR ALLER PLUS LOIN

Comment faire ses achats en ligne en toute sécurité ?
www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/zoom-sur-les-achats-en-ligne

6 MÉFIEZ-VOUS DES MESSAGES SUSPECTS

Qui n'a jamais reçu un message (mail ou SMS) ou un appel de la part d'individus se faisant passer pour une banque, une administration (impôts, assurance maladie…), une entreprise de livraison ou encore un site marchand ? Ces escrocs cherchent à nous tromper et vont nous inciter à communiquer des informations personnelles, à ouvrir une pièce jointe susceptible de contenir un virus ou à cliquer sur un lien malveillant pour nous rediriger vers un site frauduleux.

POUR NOUS PIÉGER, LES CYBERCRIMINELS UTILISENT DIFFÉRENTS RESSORTS TELS QUE LA PEUR, L'APPÂT DU GAIN, LA CRÉDULITÉ, L'URGENCE OU LA COÏNCIDENCE AVEC UNE SITUATION DE LA VIE QUOTIDIENNE.

Ex. : arnaque à la livraison de colis, à la mise à jour de notre carte Vitale, remboursement d'impôts…

LES RISQUES

Les informations dérobées (mots de passe, informations d'identité ou bancaires) seront ensuite **directement utilisées par les escrocs ou bien revendues** à d'autres cybercriminels pour mener diverses actions frauduleuses : piratage de compte en ligne, fraude à la carte bancaire, usurpation d'identité, hameçonnage ciblé sur la victime ou ses proches…

LES CONSEILS

Premier réflexe : **ne pas cliquer sur le lien qui vous est proposé**. **Au moindre doute**, lors de la réception d'un message inattendu ou alarmiste, **nous vous recommandons de contacter directement l'organisme concerné par un autre moyen** (exemple : par téléphone ou en se connectant par soi-même à son compte en ligne). Il peut en effet s'agir d'un message d'hameçonnage (phishing) visant à vous piéger.

POUR ALLER PLUS LOIN

Comment se prémunir et faire face au phishing ?
www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing

Retrouvez toutes nos ressources dédiées au phishing :
www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/dossier-phishing

7 APPRENEZ À MAÎTRISER VOS RÉSEAUX SOCIAUX

Facebook, Instagram, LinkedIn, Snapchat, TikTok, Twitter, WhatsApp… Les réseaux sociaux sont omniprésents dans notre quotidien et celui de nos adolescents. Il ne se passe rarement un jour sans consulter ou publier des photos, vidéos, messages…

CES RÉSEAUX CONTIENNENT DE NOMBREUSES INFORMATIONS PERSONNELLES ET FAMILIALES SENSIBLES, QUI NE DOIVENT PAS TOMBER DANS DE MAUVAISES MAINS
(identité, adresse postale ou de messagerie, numéro de téléphone, date de naissance, etc.).

LES RISQUES

Les réseaux sociaux n'échappent pas aux activités malveillantes : escroquerie, usurpation d'identité, chantage, vol d'informations, cyberharcèlement, désinformation, diffamation… Les techniques frauduleuses ne manquent pas. **Certaines malveillances ciblent expressément les enfants et les adolescents sur les réseaux sociaux** : les jeux morbides ou dangereux déguisés en challenges, jeu-concours frauduleux, messages privés à caractère pornographique ou incitant à la prostitution…

LES CONSEILS

Pour utiliser les réseaux sociaux en toute sécurité et protéger l'accès à vos comptes, nous vous recommandons d'utiliser à la fois **des mots de passe robustes et systématiquement différents pour chaque service** mais aussi d'**activer la double authentification** lorsque cela est possible. Par ailleurs, nous vous recommandons de **vérifier régulièrement les paramètres de confidentialité de vos comptes** pour définir les options de visibilité de vos publications. Enfin, ne diffusez pas d'informations personnelles ou sensibles qui pourraient être utilisées pour vous nuire et bien sûr, **faites attention à qui vous parlez sur les réseaux.**

LE SAVIEZ-VOUS ?

- **28 %*** des enfants (9-11 ans) ont déjà un compte sur les réseaux sociaux, **alors que l'âge légal pour créer un profil sur la plupart des plateformes est de 13 ans et que l'autorisation des parents est obligatoire jusqu'à 15 ans.**
- **78 %* des parents** ne savent pas ce que leurs enfants font sur Internet et les réseaux sociaux

* Source : e-Enfance.org

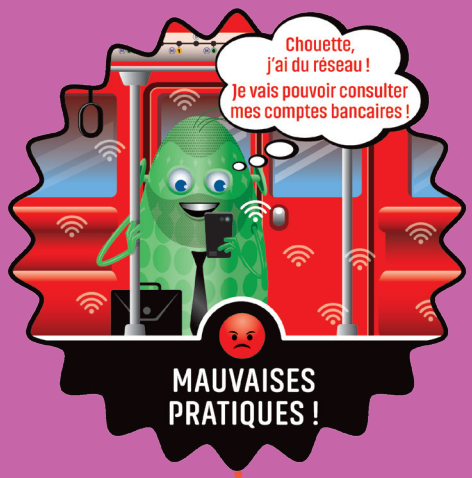
POUR ALLER PLUS LOIN

La sécurité sur les réseaux sociaux :
www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/reseaux-sociaux

8 ÉVITEZ LES WI-FI PUBLICS OU INCONNUS

Aujourd'hui, chacun souhaite pouvoir accéder partout et à tout moment à Internet, et ce, y compris dans ses déplacements.

S'ILS SONT PRATIQUES ET FACILES D'ACCÈS, LES RÉSEAUX WI-FI PUBLICS PEUVENT SE RÉVÉLER DANGEREUX ET CONSTITUER UNE VÉRITABLE AUBAINE POUR LES PIRATES INFORMATIQUES.



LES RISQUES

En effet, **les réseaux Wi-Fi publics ne sont pas toujours sécurisés et peuvent être contrôlés ou usurpés par des cybercriminels**. Des pirates pourraient ainsi capturer vos informations personnelles : mots de passe, numéro de carte bancaire par exemple, pour les utiliser à des fins frauduleuses.

LES CONSEILS

En dehors de votre domicile, **nous vous suggérons de privilégier la connexion de votre abonnement téléphonique** (3G, 4G ou 5G) aux réseaux Wi-Fi publics. Si vous ne pouvez faire autrement, nous vous conseillons de vérifier scrupuleusement le nom du réseau proposé et celui affiché sur votre appareil et de **ne jamais y réaliser d'opérations sensibles** (paiement par CB, consultation de compte bancaire, renseignement d'informations confidentielles…).

POUR ALLER PLUS LOIN

Comment naviguer sur les Wi-Fi publics en toute sécurité ?

Vidéo : Comment empêcher le vol de données sur les Wi-Fi publics ?
www.dailymotion.com/video/x7nwhg7
Article : 4 précautions à prendre avec les réseaux WiFi publics
www.cnil.fr/fr/utiliser-un-wi-fi-public-voici-4-precautions-prendre

Source : CNIL – https://www.cnil.fr 19/09/2022

9 SÉCURISEZ VOS OBJETS CONNECTÉS

Contrôler son rythme cardiaque sur sa montre, suivre ses performances sportives sur son téléphone, régler à distance le thermostat de notre domicile ou le surveiller avec une caméra, offrir un jouet connecté à un enfant ou utiliser un babyphone… Les objets connectés ont littéralement envahi notre quotidien.

CETTE « CONNECTIVITÉ » DÉCUPLE NOTRE EXPOSITION AUX RISQUES NUMÉRIQUES.

LES RISQUES

Parce qu'ils ne sont pas toujours correctement sécurisés ou bien paramétrés, **ces objets représentent de véritables menaces de piratage ou de vol d'informations personnelles.** Ils peuvent donc constituer le « maillon faible » de notre environnement numérique.

LES CONSEILS

Dès la première utilisation de votre objet connecté, **changez le mot de passe par défaut** et utilisez un mot de passe suffisamment long et complexe pour sécuriser chacun de vos équipements. Nous vous conseillons également de réaliser les mises à jour de sécurité et celles de leurs applications dès qu'elles vous sont proposées.
Veillez aussi à **vérifier leurs paramètres de sécurité en fonction de vos usages** et à désactiver les fonctionnalités que vous n'utilisez pas.
Enfin, nous vous conseillons d'**éteindre systématiquement vos objets connectés lorsque vous ne les utilisez pas**.

POUR ALLER PLUS LOIN

10 conseils pour sécuriser vos objets connectés
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-objets-connectes-iot

Zoom sur la Tv et les assistants vocaux connectés :

- https://www.cnil.fr/fr/televiseurs-connectes-les-conseils-de-la-cnil
- https://www.cnil.fr/fr/les-conseils-pour-configurer-et-utiliser-son-assistant-vocal

Source : CNIL – https://www.cnil.fr 19/09/2022

10 CYBERHARCÈLEMENT, PARLEZ-EN !

Le harcèlement peut revêtir différentes formes et se reconnaît par son caractère répétitif et sa durée. Il peut être le fait d'une ou plusieurs personnes et toucher aussi bien les adultes que les plus jeunes. Avec l'avènement des nouvelles technologies et des réseaux sociaux, le harcèlement s'est également développé en ligne : intimidations, insultes, rumeurs, publication de photos ou vidéos compromettantes…

SI CERTAINS HARCELEURS L'ASSIMILENT À UN JEU, LES VICTIMES QUANT À ELLES, EN SOUFFRENT ET SOUVENT N'OSENT PAS EN PARLER, SE RETROUVANT SEULES FACE À CES VIOLENCES.

LES RISQUES

Les conséquences du cyberharcèlement sur la santé physique ou morale de ceux qui en sont victimes ne doivent pas être minimisées. Elles **peuvent s'avérer importantes voire dramatiques** : sentiment d'insécurité, dépression, décrochage scolaire ou professionnel, troubles psychologiques ou émotionnels, violence en tout genre… Et peuvent même parfois conduire au suicide.

LES CONSEILS

Il est important de ne pas rester seul face au cyberharcèlement et de libérer la parole dans un cadre apaisé. Aussi **nous vous conseillons d'aborder le sujet du cyberharcèlement en famille avec vos enfants pour expliquer de quoi il peut s'agir et de les encourager à vous en parler s'ils sont témoins, victimes ou susceptibles d'être contributeurs**.

Voici un exemple de questions pour engager la discussion : *Tu sais ce que c'est que le cyberharcèlement ? As-tu déjà vu des situations de cyberharcèlement ? Que ferais-tu si tu voyais ou subissais un cyberharcèlement ?*

Si un cyberharcèlement se produit dans le cadre scolaire, informez-en la direction de l'établissement pour qu'elle puisse prendre les mesures nécessaires.

POUR ALLER PLUS LOIN

Que faire en cas de cyberharcèlement ?
www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/que-faire-en-cas-de-cyberharcelement-ou-harcelement-en-ligne

Pour être conseillé et accompagné :
- 3018 : Violences numériques
- 116 006 : France Victimes
- 3020 : Non au harcèlement

LE SAVIEZ-VOUS ?

12 % des 8/18 ans ont déjà été confrontés à une situation de cyberharcèlement.

(Source : Audirep/Association e-Enfance, Juin 2021)

Le cyberharcèlement est puni par la loi et les sanctions infligées sont considérablement aggravées quand l'acte vise un mineur de moins de 15 ans.

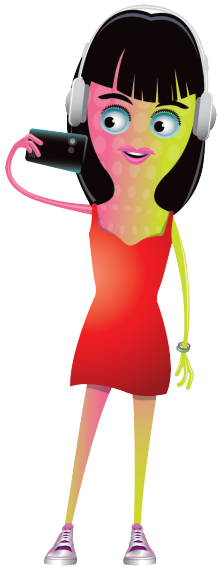
POUR ALLER PLUS LOIN

COMMENT PARLER DE CYBERSÉCURITÉ AVEC SES ENFANTS ?

Quotidiennement exposés aux outils numériques, mais souvent peu conscients des risques encourus dans leurs pratiques, les jeunes représentent des cibles faciles (cyberharcèlement, vol de données personnelles, piratage de comptes en ligne…). D'où l'importance de les sensibiliser et de les aider à acquérir des « réflexes » avec les bonnes pratiques, et ce, dès le plus jeune âge.

QUE FAIRE FACE AUX CONTENUS ILLICITES SUR INTERNET ?

DES MINEURS VICTIMES…



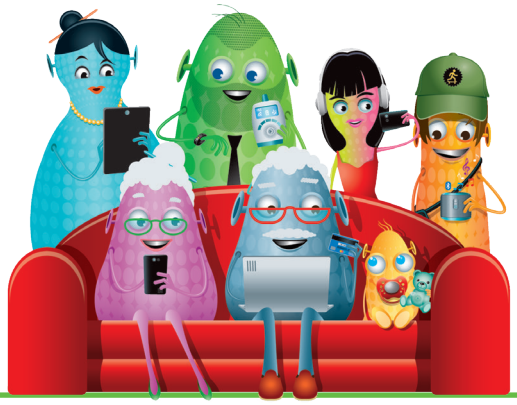
Au même titre que les adultes, les enfants peuvent être confrontés à des contenus choquants, parfois illicites : incitation à la haine, propagande terroriste, pédopornographie, etc. L'encadrement des mineurs dans leur navigation sur Internet reste donc un enjeu majeur. Cyberharcèlement, injure, diffamation, corruption de mineur, incitation à commettre un crime ou un délit… Pour signaler un contenu illicite sur Internet, rendez-vous sur le site du ministère de l'Intérieur www.internet-signalement.gouv.fr. Le 3018 propose également des informations sur ces dangers.

…OU AUTEURS DE CONTENUS ET DE COMPORTEMENTS ILLICITES

Il arrive également que les jeunes soient tentés de se rendre visibles sur les réseaux sociaux ou Internet, avec un fort sentiment d'impunité. Or, Internet n'est pas un espace de non-droit et contrairement à certaines légendes, l'anonymat absolu n'y existe pas. Sur le web, tout comme le monde « réel », des lois existent dont les mineurs et les familles ne sont pas toujours conscients. Selon la nature des infractions, les auteurs de propos illicites tenus sur Internet encourent des peines qui peuvent aller jusqu'à plusieurs milliers d'euros d'amende et même dans certains cas des peines d'emprisonnement.

ET LE CONTRÔLE PARENTAL ?

Vous pouvez installer un contrôle parental pour vos enfants afin de créer un espace sécurisé pour les accompagner dans leur apprentissage du numérique.



Plus que jamais il est essentiel de sensibiliser nos enfants sur le sujet de la cybersécurité. Pour ce faire, Cybermalveillance.gouv.fr vous recommande différents supports gratuits pour les accompagner selon leur âge.

DE 7 À 11 ANS

LES INCOLLABLES « DEVIENS UN SUPER-HÉROS DU NET »

Jeu avec des questions/réponses ludiques sur les usages numériques, accessibles aux petits et grands, pour apprendre à naviguer en toute sécurité.

PRUDENCE SUR INTERNET !

Quiz, jeu de cartes, poster, vidéos ou encore livret pratique : dès le 18 octobre 2022, découvrez les nouvelles ressources de la CNIL pour apprendre de façon ludique à protéger sa vie privée en ligne (8-10 ans) !

LE CAHIER DE VACANCES POUR LA SÉCURITÉ NUMÉRIQUE

Cahier de vacances composé de 6 thématiques afin de sensibiliser les plus jeunes sur les dangers d'internet et permettre aux parents d'accompagner leurs enfants dans le monde numérique.

11 ANS ET PLUS

TÉLÉ-CROCHET FICTIF : « LA HACK ACADEMY »

Télé-crochet fictif où des personnages hauts en couleur présentent, par le contre-exemple et avec dérision, les risques auxquels chacun peut être exposé sur Internet.

LE KIT PÉDAGOGIQUE « LA CYBERSÉCURITÉ, MON FUTUR MÉTIER »

Des ressources et des activités pour animer des ateliers de cybersécurité destinés à des jeunes âgés de 15 à 21 ans.

INTERNET IS A BICHE

Des vidéos pour une réponse pédagogique et créative à un vrai problème de société.

TOUS LES CONTENUS

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/dossier-accompagnement-sensibilisation-des-jeunes

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR

Assistance et prévention en sécurité numérique

PREMIÈRE MINISTRE

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE

MINISTÈRE DE L'INTÉRIEUR ET DES OUTRE-MER

MINISTÈRE DE LA JUSTICE

MINISTÈRE DES ARMÉES

MINISTÈRE DE L'ÉDUCATION NATIONALE ET DE LA JEUNESSE

REMERCIEMENTS

Ce guide a été réalisé en collaboration avec
les membres du GIP, notamment ceux du Groupe de Travail « Famille »
auxquels nous adressons nos sincères remerciements :
Aéma GROUPE, Bouygues Telecom, CLCV, CLUSIF, COVEA, e-Enfance/3018, Eset,
Google France, INC, Kaspersky, La Poste, MAIF, Microsoft France
Ministère de l'Éducation nationale et de la Jeunesse, Ministère de l'Intérieur et des Outre-mer,
Ministère de la Justice, Palo Alto Networks, SNCF.

WWW.CYBERMALVEILLANCE.GOUV.FR