Utiliser **Internet** en toute **sécurité**

Mgéfi
groupe matmut

PRÉVENTION

La cybersécurité est l'affaire de tous !

Selon une étude conduite par Opinion Way pour **www.cybermalveillance.gouv.fr**, le dispositif national d'assistance aux victimes d'actes de cybermalveillance, près de 9 Français sur 10 déclarent avoir déjà été confrontés à une situation de malveillance informatique. Face à ces cybermenaces, 1 Français sur 4 se sent encore insuffisamment informé. Plus surprenant encore, ce sentiment est encore plus présent chez les 24-35 ans, pourtant ultra-connectés et dont les usages numériques sont supérieurs à la moyenne en raison de leur présence sur les réseaux sociaux, notamment.

C'est pourquoi nous avons voulu vous proposer ce guide cybersécurité afin de vous accompagner vers un usage plus sûr d'Internet et de ses outils. Vous y trouverez l'essentiel à savoir sur les données personnelles, les tentatives de piratages et d'arnaques, mais aussi des conseils pour encadrer l'usage du web pour les enfants et les adolescents à l'ère du smartphone et du « tout connecté ». Bonne lecture !

**source : CNIL et cybermalveillance.gouv.fr*

> *Près de 9 Français sur 10 déclarent avoir déjà été confrontés à une situation de malveillance informatique.*

SOMMAIRE

Sécuriser la transmission de ses données personnelles en ligne

Une donnée personnelle est un élément d'information permettant de vous identifier directement ou indirectement. Par exemple, votre nom, votre adresse postale ou électronique, votre historique de navigation, vos identifiants en ligne (adresse IP, cookies conservés dans votre navigateur Internet, etc.) Ces données représentent un vrai danger pour vous si elles tombent entre de mauvaises mains et pourraient être utilisées pour usurper votre identité. Il est donc primordial aujourd'hui d'apprendre à protéger ses données personnelles en adoptant les bons réflexes. Nous vous proposons quelques bonnes pratiques à mettre en place :

- Limitez le nombre de données que vous partagez. Demandez-vous toujours si l'envoi d'un document est indispensable.
- Envoyez des documents à des organismes de préférence via les messageries des espaces adhérents / clients s'ils sont soumis à authentification.
- Verrouillez les documents envoyés par mail ou par sms grâce à un mot de passe connu uniquement par le destinataire.
- Ajoutez un filigrane sur vos documents. Le gouvernement a lancé le site filigrane.beta.gouv.fr pour vous permettre de protéger vos documents avant de les partager.
- Obervez la barre de navigation des sites des organismes. Il doit être indiqué HTTPS en premier et vous devez voir l'icône d'un petit cadenas.
- Soyez vigilant en utilisant des services en ligne, en particulier pour stocker des documents. Pour les documents les plus sensibles, peut-être est-il plus sage de les conserver sur un disque dur externe...

Toutes ces pratiques constituent un premier niveau de sécurisation des données personnelles et peuvent leur éviter d'être récupérées à des fins frauduleuses.

Vos données personnelles ont fuité ?

Si vous êtes informé d'une possible violation de vos données personnelles, le site **www.cybermalveillance.gouv.fr** vous indique la marche à suivre pour limiter au maximum les éventuels problèmes.
Qui prévenir ? Faut-il déposer plainte ? Que risquez-vous ? Quid de la CNIL ? Vous y trouverez toutes les réponses aux questions que vous vous posez.

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Mots de passe et double authentification : sécurisez au maximum vos connexions

Sans spécialement nous en rendre compte, au quotidien, nous utilisons beaucoup de services en ligne tels que les messageries, les réseaux sociaux, les banques, les achats en ligne... Et la sécurité de l'accès à tous ces services dépend aujourd'hui principalement des mots de passe. Ils nous sont tellement demandés qu'il est plus facile d'en utiliser un, voire deux, simples à retenir. Mais ne pas prêter attention à leur complexité est dangereux. En effet, selon cybermalveillance.gouv.fr, cela augmenterait considérablement les risques de compromettre la sécurité de nos accès. Voici de bonnes pratiques à adopter pour gérer efficacement vos mots de passe.

La double authentification pour renforcer la sécurité de vos accès

Également appelée « authentification forte », « vérification en deux étapes », « authentification à deux facteurs »... De plus en plus de services proposent cette option. En complément de votre identifiant et de votre mot de passe, ces services vous demandent une confirmation que vous pouvez recevoir, par exemple, sous forme de code provisoire reçu par SMS ou par email, via une application ou une clé spécifique que vous contrôlez, ou encore par reconnaissance grâce à votre empreinte digitale. Ainsi, grâce à cette confirmation, vous seul pourrez autoriser un nouvel appareil à se connecter aux comptes protégés.

- N'utilisez pas le même mot de passe pour vos différents services : ainsi, en cas de piratage, seul le service auquel il est rattaché est fragilisé.
- Votre mot de passe doit être long et complexe : au moins 12 caractères mélangeant des majuscules, des minuscules des chiffres et des caractères spéciaux. Choisissez-en un particulièrement robuste pour votre messagerie, car un cybercriminel pourrait facilement utiliser la fonction « mot de passe oublié » des différents services auxquels vous pouvez accéder, comme votre compte bancaire, pour en prendre le contrôle. Votre mot de passe de messagerie est donc l'un des plus importants à protéger.
- Changez de mot de passe au moindre doute avant qu'il ne tombe dans de mauvaises mains.
- Ne donnez jamais votre mot de passe à un tiers : aucune société ou organisation sérieuse ne vous demandera jamais de lui communiquer votre mot de passe par messagerie ou téléphone.
- N'utilisez pas de mot de passe sur un ordinateur partagé : si vous devez utiliser un ordinateur qui n'est pas le vôtre, activez le mode de « navigation privée » du navigateur qui permet d'éviter de laisser trop de traces informatiques.

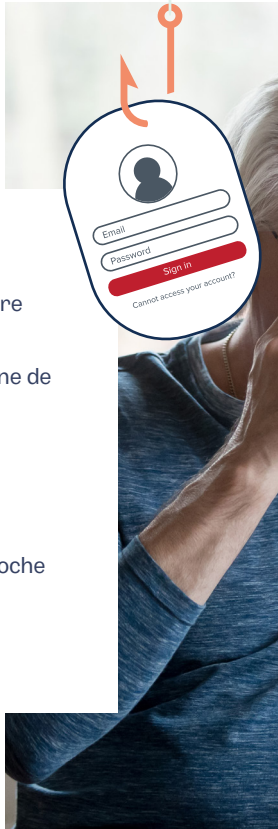
Hameçonnage, arnaques… Savoir les détecter pour mieux agir

Avez-vous déjà reçu, par email ou par téléphone, des messages non sollicités ? Ou été invité à communiquer vos coordonnées et références bancaires pour retirer un gain sorti de nulle part ? Pire encore, reçu des menaces de poursuites liées à une grave infraction qui vous aurait été attribuée par les forces de l'ordre ? L'objectif de ces messages parfois alarmants est de récupérer un maximum de données personnelles ou professionnelles pour en faire un usage frauduleux. Ils peuvent venir de votre banque, de votre opérateur téléphonique, de l'administration, de sites e-commerce… Face à ces fléaux numériques, des plateformes de signalement ont été mises en place par les pouvoirs publics et les professionnels. Mais pour pouvoir les signaler, encore faut-il les reconnaître. Nous vous donnons quelques clés sur ces pratiques pour ne pas en être victime.

Soyez attentifs aux messages qui vous paraîtraient étranges : vous sont-ils directement destinés, sont-ils personnalisés ? Si le sujet abordé ne vous parle pas, il peut s'agir d'un acte malveillant. Le texte est-il correctement rédigé ? Si ce n'est pas le cas, surtout dans le cadre d'un message de votre banque ou d'une administration, méfiez-vous !

Ne cliquez sur aucun lien avant d'avoir la certitude que le message est sûr.

Vérifiez l'adresse email de l'expéditeur : si elle vous semble suspecte et ne fait pas partie de vos contacts, soyez vigilant !



Le type de messages qui doivent vous alerter :

- ☒ Problème de facturation ou défaut de paiement afin de vous faire parvenir un colis.
- ☒ Demande de mise à jour de coordonnées personnelles sous peine de sanctions.
- ☒ Demande d'information contre l'envoi d'un lot ou pour un remboursement inattendu.
- ☒ Appel aux dons frauduleux
- ☒ Appel à l'aide : le cybercriminel peut se faire passer pour un proche afin d'obtenir une aide financière. Contactez ce proche par vos propres moyens pour vous en assurer.
- ☒ Chaîne d'emails type porte-bonheur.

Comment réagir face à une suspicion de hameçonnage ?

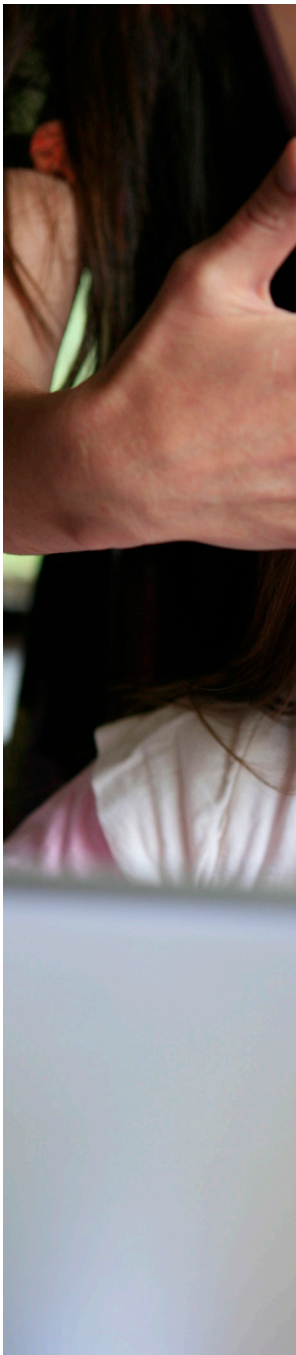
- Signalez tout mail de hameçonnage sur **www.signal-spam.fr**, un organisme composé d'experts en cybersécurité et associé à la CNIL.
- Vous pouvez signaler un mail frauduleux ou un site au contenu illicite sur la plateforme PHAROS à l'adresse suivante : **www.internet-signalement.gouv.fr**. Cette plateforme de signalements du ministère de l'Intérieur offre la possibilité de signaler certains types de phishing comme l'escroquerie à la livraison de colis ou l'escroquerie à la loterie.

Que faire si vous pensez avoir été victime d'une escroquerie ?

Dans le cas où vous auriez répondu à l'un de ces messages, rendez-vous sur **www.cybermalveillance.gouv.fr**, la plateforme nationale d'assistance aux victimes d'actes de malveillance. Vous pouvez aussi contacter l'association France Victimes au 116 006 (appel et service gratuits). Si vous constatez des mouvements bancaires suspects ou une usurpation d'identité, rendez-vous au commissariat le plus proche de chez vous pour déposer plainte. Enfin, vous pouvez contacter le service Info Escroqueries du ministère de l'Intérieur au 0 805 805 817 (appel et service gratuits de 9h à 18h30 du lundi au vendredi). Ce service de la police nationale est chargé d'informer, de conseiller et d'orienter les personnes victimes d'une escroquerie, que vous soyez un particulier ou une entreprise.

Protéger les adolescents sur les réseaux sociaux

Facebook, Instagram, TikTok, Snapchat, Whatsapp… Les réseaux sociaux font partie intégrante de notre quotidien. Au-delà du divertissement, les réseaux sociaux peuvent être dangereux, en particulier pour les plus vulnérables. Contenus indésirables, arnaques, mauvaises rencontres ou encore harcèlement… Comment protéger les adolescents ? Comment les mettre en garde ?



Règle d'or : les accompagner !

N'en faites pas un sujet tabou. Renseignez-vous sur les différentes plateformes et connaissez-en les grandes lignes afin d'avoir des échanges éclairés avec eux.

Proposez-leur de participer au paramétrage de leurs profils. L'occasion de les alerter sur la sécurité de leurs données, les dangers d'un profil public ou les contenus et informations qu'ils pourraient publier.

N'hésitez pas à installer un contrôle parental. Il vous permettra de recevoir une notification en cas d'utilisation à risque ou de contenu inapproprié (violence, haine, pornographie, propagande…).

Expliquez-leur qu'il s'agit bien de les protéger et non de les espionner.

Cyberharcèlement : la CNIL dispense quelques conseils pour ne pas devenir harcelé ou harceleur…

Utiliser des pseudonymes et des avatars.

Réfléchir avant d'agir en ligne : ce que l'on écrit, partage, « aime » peut avoir des conséquences réelles pour les personnes concernées.

Ne pas tout dire de soi : pour se protéger, donner le minimum d'informations.

Éviter de communiquer ses opinions, son numéro de téléphone, sa religion ou son état de santé.

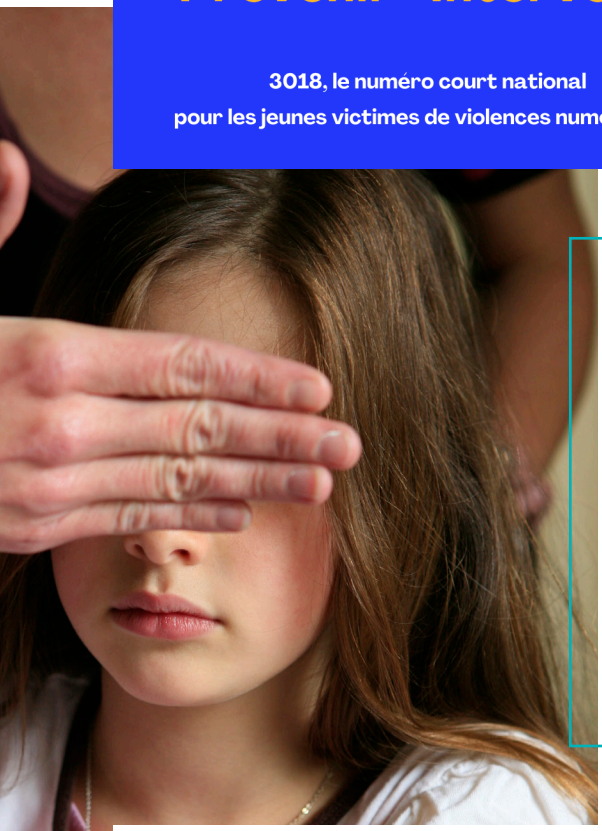
Même si vous n'êtes pas directement concerné, rester vigilant et signaler les faits, comportements et contenus illicites.

En cas de cyberharcèlement, surtout en parler à des personnes de confiance et signaler les comportements abusifs.

Violences numériques
Prévenir – Intervenir

3018, le numéro court national pour les jeunes victimes de violences numériques.

3018



Numéro national pour les victimes de violences numériques : 3018

Par téléphone, tchat ou via l'application 3018, pour obtenir de l'aide de spécialistes du droit et de psychologues.

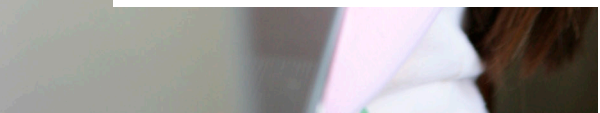
Ce service est joignable gratuitement
➡ **7 jours sur 7 de 9 h à 23 h.**

Signaleur de confiance, le 3018 peut intervenir auprès des plateformes pour faire supprimer des contenus en moins d'une heure.

Protéger ses enfants dès le plus jeune âge

Les enfants ont accès à Internet de plus en plus tôt. Quand ils ne possèdent pas déjà une tablette numérique ou un smartphone, ce sont ceux de leurs parents qu'ils utilisent avant d'aller à l'école. Du simple dessin animé aux contenus les moins appropriés, les enfants aussi doivent être accompagnés dans l'apprentissage des nouvelles technologies.

Pour les accompagner du CE2 au CM2 dans le monde du numérique, la CNIL propose des fiches pratiques, des jeux et des vidéos clairs et simples. Parmi ces différents supports, on retrouve aussi un jeu de cartes en ligne, un quiz et des livrets à destination des enseignants et des parents. Tous ces contenus sont accessibles gratuitement sur **www. cnil.fr** rubrique éducation.



Besoin de conseils ?

09 69 39 69 29
(Appel gratuit)
Du lundi au vendredi
de 8h30 à 17h

mgefi.fr

Mgéfi
6, rue Bouchardon – CS 50070
75481 Paris Cedex 10

Retrouvez-nous sur

Pour en savoir plus, rendez-vous sur
www.cnil.fret sur www.cybermalveillance.gouv.fr

Mgéfi
groupe matmut

MGEFI204 - 02/2024 – Crédit photos: Getty Images - Document publicitaire n'ayant pas de valeur contractuelle.