Bercy infos Particuliers

Bercy infos évolue pour mieux vous informer. Vous pouvez rencontrer des difficultés de navigation temporaires à compter du vendredi 18 juillet 2025. Nous vous remercions de votre compréhension.

Arnaques et cybermenaces sur les réseaux sociaux : comment s'en protéger ?

Écrit le 17/07/2025

LECTURE : 9 MINUTES

Utilisés quotidiennement par des millions d'utilisateurs, les réseaux sociaux sont devenus des outils de communication incontournables. Ils sont aussi la cible privilégiée de tentatives d'arnaques et de cybermalveillance. Quels sont les principaux risques liés aux réseaux sociaux ? Comment se protéger efficacement et réagir en cas d'attaque ? Voici les bons réflexes à adopter.

Arnaques, faux liens, escroqueries : mieux les repérer pour mieux s'en protéger

Les réseaux, comme tout autre espace numérique, ne sont pas exempt de tromperie ou de manipulation. Faux concours, messages d'amis piratés, arnaque à la crypto-monnaie, offres trop belles pour être vraies… Les menaces sont nombreuses et variées, mais quelques réflexes peuvent vous permettre de les éviter.

Pour vous protéger

- **ne cliquez jamais sur un lien suspect**, même s'il vient d'un proche. Cliquer dessus vous expose par exemple à : un vol d'identifiants ou de données personnelles (***phishing***), une installation de maliciels/**ransomwares** sur votre appareil, une compromission ou un vol de vos comptes,
- **vérifiez toujours l'URL** du site avant de saisir des informations personnelles,
- **méfiez-vous des offres** trop belles pour être vraies,
- **ne donnez jamais d'informations sensibles** par message privé (mots de passe, codes, données bancaires…),
- en cas de doute, **demandez un deuxième avis** ou signalez le contenu.

Influenceurs : attention aux produits « miracles »

Les influenceurs bénéficient d'une forte visibilité sur les réseaux sociaux, notamment auprès des jeunes. Certaines marques les rémunèrent pour promouvoir des produits auprès de leur audience, mais certaines collaborations masquent des pratiques trompeuses, voire **dangereuses** : contrefaçons, compléments alimentaires non autorisés, produits non conformes, arnaques financières, etc.

Face à ces abus, **la législation française a évolué. La** loi du 9 juin 2023 encadre strictement l'activité des influenceurs sur les réseaux sociaux et leur impose, sous peine de sanctions, de rendre explicite tout contenu à but commercial, d'interdire la promotion de certains produits (placements à risque, actes médicaux, produits illicites…) et de respecter la **réglementation** sur la publicité.

Pour vous protéger

- **vérifiez toujours la fiabilité du produit ou service recommandé avant d'acheter** et ce, même si la personne est populaire,
- **soyez attentif aux mentions légales** : tout contenu sponsorisé doit être signalé clairement,
- **méfiez-vous des offres « exclusives » ou des codes promo « limités »**,
- **signalez tout contenu suspect ou trompeur** sur la plateforme **SignalConso** .

En savoir plus

Fake news et manipulation de l'information : bien s'informer, un enjeu majeur

Les réseaux sociaux sont devenus **la première source d'information** pour de nombreux utilisateurs, notamment les jeunes. Cependant, ces informations sont parfois fausses (*fake news*) ou manipulées.

Quelles sont les conséquences ?

- **polarisation** de l'opinion publique,
- **défiance** envers les institutions et les médias traditionnels,
- **influence** sur les processus démocratiques (élections, référendums),
- **propagation de théories du complot**,
- impact sur la santé publique (désinformation médicale).

Comment se protéger et lutter contre les fake news ?

Avant de partager une information :

- **vérifiez la source** : qui a publié l'information ? Est-ce un média reconnu ?
- **croisez les sources** : l'information est-elle reprise par plusieurs médias fiables ?
- **regardez les commentaires** : que disent-ils ?
- **méfiez-vous des titres trop sensationnels ou des images sorties de leur contexte**,
- **vérifiez la date de publication** : s'agit-il d'une information récente ou ancienne ?

Si l'information sur laquelle vous êtes tombé est fausse :

- **signalez le contenu suspect** sur la plateforme,
- **signalez le contenu sur la plateforme Pharos** .

En savoir plus

Protéger sa vie privée : vos données valent de l'or

Sur les réseaux sociaux, chaque photo, lieu visité, « j'aime » ou commentaire génère des données. Ces informations sont collectées par les plateformes pour alimenter leurs algorithmes publicitaires et, de plus en plus, pour entraîner leurs intelligences artificielles. Sans paramètres de confidentialité adaptés, vos données peuvent être exploitées bien au-delà de ce que vous imaginez.

Quels sont les risques ?

- **utilisation de vos photo**s pour créer de faux profils (*deepfakes*),
- **chantage** par l'utilisation de photos à caractères sensibles (*nudes* par exemple) avec la menace que celles-ci soient révélées

si vous ne versez pas une certaine somme d'argent (***sextorsion***),
- **harcèlement**,
- **utilisation de votre géolocalisation** à votre insu,
- **utilisation de vos données** pour entrainer des IA,
- **revente de vos données personnelles** à des courtiers,

- **détournement de vos profils** pour des **arnaques sentimentales** .

Pour vous protéger

- **passez votre profil en privé** pour mieux contrôler sa visibilité,
- **limitez les informations visibles publiquement** (numéro de téléphone, adresse, etc.) et privilégiez les pseudonymes,
- **désactivez la géolocalisation automatique** de vos publications,
- **vérifiez régulièrement vos paramètres de confidentialité** (ceux-ci changent régulièrement),
- **évitez la publication publique de photos de mineurs.**

Bon à savoir : vous pouvez **demander l'effacement de vos données aux plateformes** et **limiter l'utilisation de celles-ci pour entraîner leurs IA** .

En savoir plus

Mon compte a été compromis : comment réagir ?

Un compte piraté n'est pas rare, et cela peut arriver à tout le monde. L'essentiel est d'agir rapidement pour limiter les conséquences.

Pour vous protéger

- **utilisez des mots de passe forts et différents** pour chaque réseau,
- **limitez les applications tierces** connectées à vos comptes,
- **vérifiez régulièrement les connexions à votre compte** et déconnectez les appareils inconnus,
- **évitez de vous connecter via des réseaux Wi-Fi publics**,
- **supprimez tout contenu compromettant**,
- **activez la double authentification** si ce n'est pas encore fait.

Que faire si votre compte de réseau social est piraté ?

- **modifiez** immédiatement **votre mot de passe**,
- **prévenez vos contacts** en cas de compromission de votre profil afin qu'ils ne soient pas à leur tour victimes d'arnaques,
- **signalez l'incident** à la plateforme concernée et sur le portail officiel de signalement des contenus illicites de l'Internet, Pharos ,
- **consultez la plateforme** cybermalveillance.gouv.fr pour être accompagné et orienté vers les services adaptés,
- **déposez plainte** auprès des forces de l'ordre si nécessaire (post de contenu sensible ou préjudiciable par exemple).

Le service en ligne 17Cyber peut également vous orienter rapidement en cas d'urgence.

En savoir plus

Mineurs sur les réseaux sociaux : quelle vigilance ?

Même si l'âge légal pour créer un compte seul sur les réseaux sociaux est de **15 ans**, dans la pratique, de nombreux enfants plus jeunes y accèdent. Les risques pour les mineurs sont particulièrement importants (cyberharcèlement, prédateur sexuel, exposition aux écrans et à des contenus inadaptés à leur âge, pression sociale liée à l'image et aux « *likes* », isolement, etc.).

Quelques conseils pour les parents

- **accompagnez vos enfants** dans leurs premiers pas sur les réseaux. Rien ne sert de les diaboliser, mieux vaut instaurer un climat de confiance avec votre enfant sur ces sujets afin que celui-ci puisse par la suite vous parler librement de son expérience en ligne,
- **paramétrez ensemble les options de confidentialité** afin de protéger ces informations personnelles,
- **expliquez a votre enfant** les risques des réseaux sociaux sans dramatiser.

En cas de cyberviolence : conservez les preuves et signalez rapidement.
Pour obtenir de l'aide, le 3018 (anonyme et gratuit, 7j/7) peut intervenir même pour faire supprimer des contenus en moins d'une heure. **En savoir plus**.

Une plateforme d'information et d'accompagnement dédiée à la parentalité numérique existe également pour accompagner les parents sur ces questions : **jeprotegemonenfant.gouv.fr**.

> **A savoir**
>
> Depuis la **loi du 6 février 2024**, le droit à l'image et à la vie privée des enfants est inscrit dans le code civil. Les parents doivent veiller à respecter la vie privée de leurs enfants lorsqu'ils publient des contenus les concernant sur les réseaux sociaux et retirez ces publications si leur enfant en fait la demande.

Cyberharcèlement : ne restez pas seul

Les réseaux sociaux peuvent être des lieux d'expression, mais aussi d'agressions. Le **cyberharcèlement** se manifeste par des insultes, des moqueries répétées, de l'humiliation publique, la diffusion de rumeurs ou de messages privés violents.
Les conséquences sont lourdes : angoisse, isolement social, perte d'estime de soi… Chez les plus jeunes, cela peut entraîner **décrochage scolaire** ou **mise en danger psychologique**.

Que faire en cas de cyberharcèlement ?

- **sauvegardez les preuves** (captures d'écran, horodatage des messages),
- **ne répondez pas**, **bloquez** l'auteur et signalez les contenus sur la plateforme,
- **déposez plainte**. Le harcèlement **scolaire, moral** ou **sexuel** en ligne est puni par le Code pénal,
- **consultez le site cybermalveillance.gouv.fr** pour une prise en charge,
- **signalez votre ca***s via* **PHAROS** ou **17Cyber** .

En savoir plus

FAQ : Vos questions fréquentes

Comment savoir si mes données ont déjà été compromises lors d'une fuite ou d'un piratage ?

Vous avez entendu parler d'une fuite de donnée et vous vous voulez savoir si vous êtes concerné ? Pour cela, **utilisez des services de vérification reconnus** comme **"Have I Been Pwned"** et consultez les alertes de sécurité envoyées par vos plateformes. Changez les mots de passe dès la moindre alerte.

Que faire si un proche se fait piéger sur un réseau social ?

Aidez-le sans le juger. Changez les mots de passe, activez la double authentification, signalez l'incident à la plateforme concernée et documentez les preuves avec des captures d'écran. Vous pouvez aussi l'orienter vers des ressources publiques d'accompagnement comme **Cybermalveillance.gouv.fr** , le service téléphonique d'information de la police nationale Info-escroqueries **0 805 805 817** ou **porter plainte** si nécessaire.

Est-ce risqué d'utiliser la même photo de profil sur plusieurs réseaux ?

Oui, cela facilite l'usurpation d'identité et le profilage par les escrocs. L'utilisation d'une même photo sur plusieurs plateformes permet aux cybercriminels de créer facilement de faux profils en récupérant votre image. Pour vous protéger, il est recommandé d'utiliser des photos distinctes ou des avatars spécifiques à chaque réseau et d'éviter de partager des photos personnelles trop reconnaissables. En effet, **partager des photos de vous n'est pas anodin** et peux se retourner contre vous.

Les groupes privés ou fermés sont-ils vraiment sûrs ?

Non, la confidentialité n'est jamais totale. Même dans des groupes privés, les membres peuvent partager, capturer ou divulguer des contenus. Les paramètres de confidentialité offrent une protection limitée et ne garantissent pas l'absence totale de risques. Pour vous protéger, **restez sélectif sur ce que vous publiez, même en privé** .

Les applications tierces (« booster », « nettoyer » un compte) sont-elles fiables ?

Rarement. Beaucoup collectent des données sensibles, exposent à des piratages ou à de la publicité intrusive. Pour vous protégez, limitez-vous aux outils officiels proposés par les plateformes, évitez les applications promettant des fonctionnalités « magiques », vérifiez toujours les permissions demandées avant installation et lisez les avis sur l'application.

Que faire si les algorithmes me recommandent sans cesse des contenus dérangeants ou douteux ?

Agissez sur vos paramètres et votre historique. Les algorithmes se basent sur votre comportement passé pour faire des recommandations. Pour vous protégez : signalez les contenus inappropriés, nettoyez votre historique de navigation et vos préférences, désabonnez-vous des pages et comptes problématiques et utilisez les options « Ne plus voir ce type de contenu ». Si cela persiste vous pouvez créer un nouveau compte avec un historique vierge.

Peut-on concilier usage professionnel et usage personnel sans risque ?

La séparation stricte des profils et des informations (e-mail, mot de passe, paramètres) est **hautement recommandée** . Mélanger vie professionnelle et personnelle sur les réseaux sociaux présente des risques importants. Pour éviter cela, créez des comptes séparés avec des adresses e-mail différentes et utilisez des mots de passe distincts et robustes pour chacun des comptes.

Comment gérer son e-réputation et nettoyer ses traces numériques ?

Surveillez régulièrement votre présence en ligne. Votre réputation numérique peut avoir des conséquences sur votre vie professionnelle et personnelle. Pour vous protégez : recherchez régulièrement votre nom sur les moteurs de recherche, configurez des alertes pour votre nom, révisez et supprimez les anciens posts problématiques, **demandez la suppression de contenus inappropriés** et **exercez votre droit à l'oubli** si nécessaire.

Quelle sont les ressources en cas de cyberharcèlement ?

En cas de cyberharcèlement, **ne restez pas isolé et contactez immédiatement les services spécialisés.** Le cyberharcèlement est un délit puni par la loi français et de nombreuses ressources existent pour vous aider. Contacter le **3018**, le numéro national contre les violences numérique. Il existe aussi le **116 006** pour vous accompagner gratuitement dans vos démarches pour déposer plainte. **En cas d'urgence ou de danger, appelez le 17** (fixe ou mobile) ou le **112** (téléphone mobile).

Ressources complémentaires

Ces contenus peuvent aussi vous intéresser

- **Comment assurer votre sécurité numérique ?**
- **Usurpation d'identité, comment s'en protéger ?**
- **Dix règles pour vous prémunir contre le piratage de vos données personnelles**
- **Attention aux faux courriels et appels qui se font passer pour l'administration**

En savoir plus sur les risques d'arnaque sur les réseaux sociaux

- **La sécurité sur les réseaux sociaux** *sur le site cybermalveillance.gouv.fr*
- **Particuliers : quelles sont les cybermalveillances les plus fréquentes en 2024 ?** *sur le site cybermalveillance.gouv.fr*
- **Appliquer les dix règles d'or préventives** *sur le site cyber.gouv.fr*
- **Intelligence Artificielle : les travaux de l'ANSSI** *sur le site cyber.gouv.fr*
- **Cybersécurité** *sur le site de la Commission Nationale de l'Informatique et des Libertés (Cnil)*

- **Guide du bon usage des réseaux sociaux** *publié par le ministère des armées*
- **Cyberharcèlement (harcèlement sur internet)** *sur le site service-public.fr*
- **Lutter contre les « fake news »** *sur le site info.gouv.fr*

Ce que dit la loi

- **Article 226-4-1 du code pénal** sur l'usurpation d'identité numérique
- **Articles 313-1 à 313-3 du code pénal** sur l'escroquerie
- **Articles 222-32 et 222-33 du code pénal** sur les peines encourues en cas de harcèlement sexuel sur internet
- **Articles 222-33-2 à 222-33-2-3 du code pénal** sur les peines encourues en cas de harcèlement moral et harcèlement scolaire sur internet
- **Loi n° 2021-643 (loi Naegelen)** visant à encadrer le démarchage téléphonique et à lutter contre les appels frauduleux
- **Loi n° 2004-575 (LCEN)** sur la confiance dans l'économie numérique, notamment la responsabilité des plateformes en ligne
- **Règlement général sur la protection des données (RGPD)** sur la protection des données personnelles en ligne
- **Loi n° 2018-1202 du 22 décembre 2018** relative à la lutte contre la manipulation de l'information
- **Loi n° 2023-566 du 7 juillet 2023** visant à instaurer une majorité numérique et à lutter contre la haine en ligne

Souhaitez-vous ajouter un commentaire pour nous aider à continuer à améliorer l'accès aux informations ?

De quel continent fait partie la France ? *

Soumettre

Merci de votre participation.

A propos de Bercy infos | Retrouvez toutes nos fiches pratiques