Cyber 4 *good*, **votre guide pour** *vivre le numérique* **au quotidien, en toute sécurité.**

Capgemini

Bienvenue dans ce livret de sensibilisation à la cybersécurité.

À mesure que le numérique prend une place grandissante dans nos vies, il est essentiel de savoir naviguer en ligne en toute sécurité.

Que ce soit pour communiquer avec vos proches, gérer vos finances ou simplement explorer Internet, il existe des **risques**, mais aussi des solutions simples pour vous **protéger**. Ce guide vous accompagnera pas à pas pour **renforcer votre sécurité** et votre sérénité dans le monde numérique.

Sommaire

1

Apprendre à sécuriser **ses** *données personnelles*

“Je n’ai rien à cacher”… Mais est-ce cela l’important ?

Les informations bancaires ne sont pas les seules cibles des attaques internet, il est important de vous protéger en protégeant vos informations personnelles.
Beaucoup pensent que la sécurité de leurs appareils numériques et de leurs activités en ligne ne les impactent pas, car ils n’ont rien à cacher ou que les informations ne sont pas importantes.

Il y a deux types d’informations :

Les directes, comme le prénom ou le nom de famille.

Les indirectes, comme le numéro de téléphone, votre adresse postale, une plaque d’immatriculation ou encore la voix et l’image.

Or, vos informations valent beaucoup d’argent !

Nom, prénom, email = 2€

CB britannique avec code CCV = 18€

Carte de crédit avec solde >4600€ = 100€

Passeport français = 2740€

Compte gmail piraté = 55€

Leur vol peut engendrer des situations compliquées.
L’usurpation d’identité peut vous amener à devoir rembourser un crédit contracté en votre nom ou même être fiché banque de France.

Perdre l’accès à votre boîte mail, c’est bien plus qu’un simple désagrément :
ce sont des années d’échanges, de souvenirs et de photos envolés, comme si quelqu’un avait fouillé votre maison et emporté vos biens les plus précieux.

2

Choisir des *mots de passe* faciles à retenir et sécurisés

Pourquoi utiliser un mot de passe fort et unique pour chaque compte en ligne que vous possédez ?

Les pirates informatiques utilisent souvent des attaques automatisées pour tenter de deviner les mots de passe des utilisateurs. Ces logiciels passent en revue des millions de combinaisons, y compris tous les mots du dictionnaire.

C'est pourquoi il est essentiel d'utiliser un mot de passe complexe : un mot de passe qui n'a aucun sens logique, qui n'est lié ni à un mot réel ni à une information personnelle.

Les mots de passe courts, simples ou faciles à retenir sont les premières cibles de ces attaques.

Comment faire ?

Changer votre mot de passe tous les 3 à 6 mois, ou immédiatement en cas d'activité suspecte.

Ajouter des caractères spéciaux, comme par exemple : **-, /, !, ?**

Mettre des majuscules et minuscules et pas uniquement au début des mots. Par exemple : sOlEIl

Ne pas mettre de mot de passe étant relié à une information personnelle. Comme par exemple, une date d'anniversaire, ou le nom de vos enfants.

Activer la double authentification, c'est à dire, ajoutez votre numéro de téléphone ou email pour qu'un code sécurisé vous soit envoyé comme sur AMELI afin de vérifier votre identité.

Utilisez une phrase plutôt qu'un mot

Vous pouvez choisir une phrase que vous aimez, comme :

J'adore Les glaces à La vanille quand il Fait Chaud ! *

Vous la transformez en un mot de passe en utilisant les initiales de chaque mot, ainsi que des symboles et des chiffres.

Dans cet exemple, votre mot de passe pourrait être :

JLgàLvqiFC!*

Cette méthode vous permet de créer un mot de passe complexe, tout en étant facile à retenir.

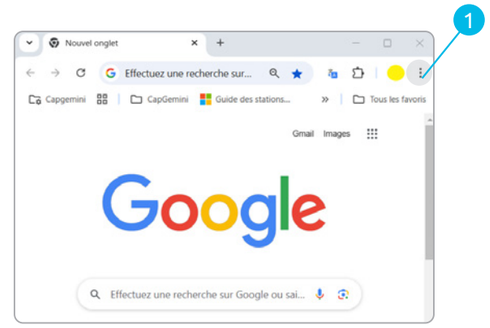
Utilisez un gestionnaire de mots de passe

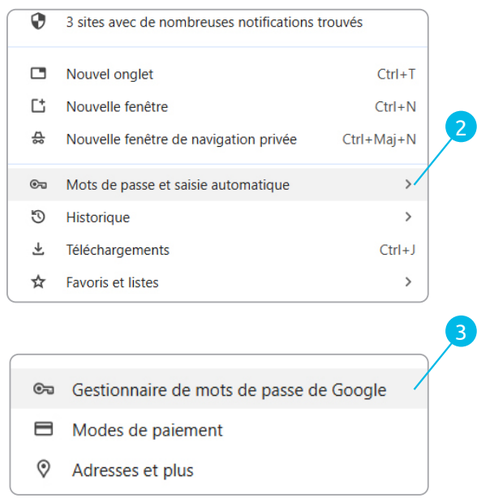
Avec cet outil, vous pourrez générer et stocker des mots de passe forts et uniques pour tous vos comptes en ligne.

Ces outils peuvent vous faciliter la tâche en vous permettant de créer des mots de passe complexes sans avoir à les retenir tous.

Google Chrome

Il est gratuit et inclus dans votre navigateur !





En appliquant ces conseils, vous renforcez la sécurité de vos comptes et protégez vos informations personnelles contre les cyberattaques.

3

Reconnaître et éviter *les arnaques*

Régulièrement, vous recevez des mails, appels ou messages provenant de comptes ou de personnes malveillantes, imitant des sources fiables.

Les arnaques en ligne, aussi appelées « phishing », sont des tentatives de fraude sur Internet. Les escrocs envoient de faux e-mails, SMS ou messages qui ressemblent à ceux d'organismes de confiance, comme une banque, un service public ou un livreur. Parfois, ils peuvent aussi téléphoner.

Leur but est de tromper la personne et de lui faire donner des informations personnelles, comme ses mots de passe ou ses coordonnées bancaires. Il est donc important de rester vigilant et de ne jamais communiquer ces informations sans vérifier l'identité de son correspondant.

Voici quelques exemples :

exemple 1

Bonjour, c'est le livreur votre colis ne rentrait pas dans la boite aux lettres merci de choisir un point relais sur : https://livraisons-dossiers-france.info/

exemple 2

Assurance maladie : Dernière relance pour le renouvellement de votre carte vitale veuillez-vous réactualiser. https://secur-sociale.com

exemple 3

Coucou papi, c'est moi, je n'ai plus de téléphone. J'ai pris celui d'un ami, est-ce que tu peux m'envoyer de l'argent via ce lien (www.banquep0pulaire.com) afin de me permettre de rentrer ?

Comment se protéger du phishing

Vérifiez l'adresse e-mail de l'expéditeur. Méfiez vous des adresses suspectes ou mal orthographiées. Exemple :

inf0banquep0stal@gmail.com

Attention aux numéros personnels. Un SMS venant d'une institution commençant par 06 ou 07 est souvent frauduleux. *Cf : exemple 1*

Évitez les urgences suspectes : les tentatives de phishing créent un sentiment de panique pour vous pousser à agir vite, par exemple : *"nous venons d'arrêter un virement suspect en direction d'un pays étranger, communiquez nous votre code afin d'annuler le virement"*.

Lorsqu'une institution vous contacte et que l'interlocuteur vous demande des informations personnelles, raccrochez et rappelez le numéro officiel que vous connaissez de l'institution. Vous pouvez le trouver sur internet et demandez-leur si c'était bien eux. *Cf : exemple 2*

Ne cliquez pas sur les liens suspects. Tapez le nom du service/entreprise directement dans votre navigateur.

Ne partagez jamais d'informations sensibles. Les banques et entreprises ne demandent pas de données par e-mail ou par téléphone.

Ne désactivez jamais les sécurités, même si on vous le demande au téléphone.

Attention à votre numéro de téléphone : le spoofing est une arnaque dans laquelle quelqu'un utilise votre numéro sans votre accord pour tromper d'autres personnes. Vous pouvez le remarquer si des proches vous disent avoir reçu des appels ou messages étranges de votre part, alors que vous ne les avez jamais contactés. Si cela vous arrive, informez votre entourage, puis signalez-le à votre opérateur, au **33700** (numéro gratuit), ou sur le site "J'alerte l'Arcep".

Prenez garde aux appels et messages de numéros étrangers inconnus, ils cachent souvent des arnaques pour vous soutirer de l'argent ou des informations personnelles.

Assurez-vous toujours que les informations sont vraies en parlant avec une personne de confiance. Des personnes malintentionnées peuvent se faire passer pour vos enfants ou vos proches et inventer une situation urgente pour vous tromper. *Cf : exemple 3*

Les arnaques sentimentales sont de plus en plus fréquentes et visent particulièrement les personnes seules ou en quête de compagnie. Les escrocs se font passer pour quelqu'un de bienveillant et attentionné afin de gagner la confiance de leur victime. Ils entretiennent une relation à distance pendant des semaines ou des mois, puis inventent un problème grave (maladie, accident, problème financier) pour demander de l'argent. Ces manipulations peuvent être très convaincantes et causer de lourdes pertes financières et émotionnelles.

Il n'est jamais trop tard !

Si vous pensez que vous avez donné vos informations de connexion à une personne illégitime, **changez rapidement votre mot de passe sur le site original** ou appelez votre banque pour bloquer votre compte !

4

Utilisation et dangers des *clés USB*

Les clés USB : pratiques mais risquées

Les clés USB peuvent propager des logiciels malveillants en contaminant plusieurs appareils.
Leur petite taille les rend faciles à perdre ou à voler, exposant ainsi les données sensibles. Même protégées par un mot de passe, elles ne sont pas totalement sécurisées.

Comment limiter les risques ?

Ne pas la brancher sur un ordinateur inconnu
Le risque est que cet ordinateur soit contaminé par un virus et que la clé USB le soit aussi en se branchant.

Faire attention à ne pas la perdre
Les informations contenues dans la clé pourraient être récupérées par quelqu'un de malveillant.

Limiter les documents importants ou sensibles
Si la clé venait à être perdue ou volée, vos informations ne seraient plus sécurisées.

Ne pas utiliser de clés USB trouvées ou données
Elles peuvent contenir des virus informatiques qui vont se déplacer sur votre PC.

Alternative : Utiliser Google Drive

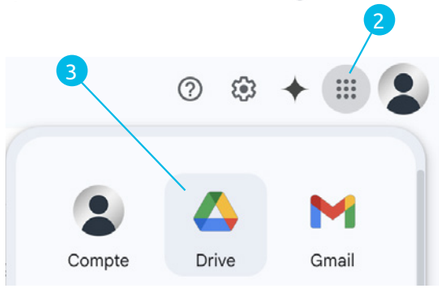
Google Drive est un espace de stockage en ligne gratuit qui permet de sauvegarder, organiser et partager des fichiers (photos, documents, vidéos…).
Il fonctionne comme un disque dur, mais accessible depuis n'importe quel appareil connecté à Internet (ordinateur, tablette, smartphone).

Recherchez "Gmail" 1 dans votre navigateur : si vous avez déjà un compte, connectez-vous, sinon, créez-en un.

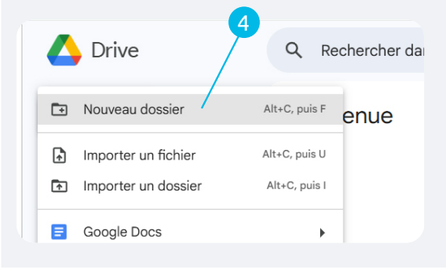
Pour créer un compte

Vous allez avoir plusieurs étapes où vous allez devoir remplir votre date de naissance, le mode de connexion souhaité, un mot de passe et une adresse mail de récupération de compte. Une fois ces étapes faites, votre compte Gmail est opérationnel.

Pour accéder à Google Drive, cliquez sur « Applications Google » 2 situé en haut à droite de la page d'accueil, puis sélectionner Drive 3.

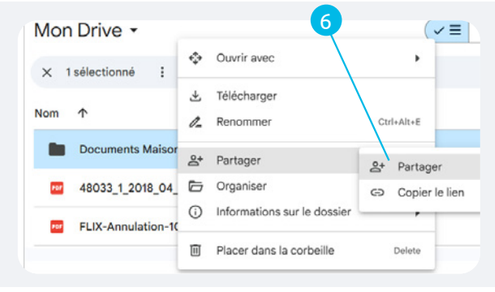


Pour créer un dossier, saisissez son titre, cliquez sur « Nouveau dossier » 4, et il apparaîtra dans votre Drive. Vous pouvez importer facilement des fichiers en les faisant glisser directement depuis votre ordinateur.



En cliquant sur « Nouveau » 5, vous pouvez créer un dossier, importer un fichier ou utiliser Google Docs pour rédiger un document automatiquement enregistré dans Google Drive.

Le dossier se partage 6 ou s'envoie à un ou plusieurs utilisateurs. Vous pouvez aussi le partager par adresse e-mail.



5

Comment le *RGPD* **protège** *vos informations personnelles*

Que deviennent vraiment vos données une fois publiées sur Internet ?

“Internet n’oublie jamais”

Le RGPD (Règlement Général sur la Protection des Données), créé par l’Union européenne en 2018, vous aide à contrôler et à protéger vos informations personnelles en ligne. Il s’applique à toutes les entreprises opérant en Europe, même si elles sont basées ailleurs.

Quels sont ses avantages ?

1. Le droit de savoir quelles données sont collectées vous concernant et comment elles sont utilisées par l’organisation.
2. Le droit de demander aux entreprises l’accès à vos propres données personnelles.
3. Le droit de modifier vos données à tout moment dans les bases de données de l’entreprise.
4. Le droit de demander la suppression de vos données aux entreprises les collectant.
5. Le droit de demander à limiter l’utilisation de vos données au strict nécessaire.
6. Le droit de demander et recevoir vos données personnelles dans un format lisible et de les transférer à une autre organisation.
7. Le droit de vous opposer au traitement de vos données dans certaines situations.

Bon à savoir !

Si des informations personnelles ou une photo de vous ou de vos proches se retrouvent sur un site internet sans votre consentement vous avez le droit de demander leur suppression.

Comment exercer votre droit à l’oubli ?

Le droit à l’oubli permet de demander la suppression de ses données personnelles dans certains cas. Voici des exemples et la démarche à suivre :

Les données ne sont plus utiles

Vous vous désabonnez d’une newsletter, l’entreprise ne doit plus garder votre adresse e-mail.
Démarche : demandez la suppression par e-mail ou via un formulaire. En cas de refus, contactez la CNIL.

Vous retirez votre consentement

Vous aviez accepté qu’une photo de vous soit sur un site, mais vous changez d’avis.
Démarche : contactez l’entreprise et demandez la suppression. Si elle ne répond pas, saisissez la CNIL.

Les données ont été utilisées illégalement

Un site vend vos informations sans votre accord.
Démarche : exigez la suppression et signalez le site à la CNIL ou aux autorités compétentes.

Obligation légale de suppression

Une entreprise doit effacer les informations de ses anciens clients après un certain délai.
Démarche : rappelez-lui son obligation. Si elle ne s’exécute pas, contactez la CNIL.

Bon à savoir !

Pour exercer votre droit à l’effacement, il est conseillé de contacter directement l’organisme concerné en utilisant les informations disponibles sur leur site. L’organisme a un mois pour répondre à votre demande, mais ce délai peut être prolongé de deux mois si la demande est complexe.
Si votre demande est refusée sans raison valable ou si l’organisme ne répond pas, vous pouvez porter plainte auprès de la CNIL pour défendre vos droits.

En application de l’article 17.1 du Règlement général sur la protection des données (RGPD), je vous prie d’effacer de vos fichiers les données personnelles suivantes me concernant:

[infos_a_supprimer]

Je demande que ces informations soient supprimées car :

[motif_de_la_suppression]

Vous voudrez bien également notifier cette demande d’effacement de mes données aux organismes auxquels vous les auriez communiquées (article 19 du RGPD).

Enfin, je vous prie de m'informer de ces éléments dans les meilleurs délais et au plus tard dans un délai d’un mois à compter de la réception de ce courrier (article 12.3 du RGPD).

A défaut de réponse de votre part dans les délais impartis ou en cas de réponse incomplète, je saisirai la Commission nationale de l’informatique et des libertés (CNIL) d’une réclamation.

Je vous prie d'agréer, Madame, Monsieur, l'expression de mes salutations distinguées.

6

Protéger votre vie privée *sur les réseaux sociaux*

Limiter sa visibilité sur les réseaux sociaux, c'est comme fermer les rideaux de sa maison pour que les voisins ne voient pas ce que l'on fait à l'intérieur.

Pourquoi protéger votre compte ?

En protégeant votre compte, vous gardez vos informations personnelles en sécurité et évitez que des personnes non souhaitées ne les voient. En contrôlant qui peut voir vos publications et vos photos, vous évitez aussi les problèmes comme le harcèlement ou le vol d'identité en ligne.

Pour vos proches mineurs

Restez le plus privé possible afin d'éviter que des photos des enfants de votre entourage ne se retrouvent sur des sites dangereux.

Plus de 50% du contenu présent sur les sites pédopornographiques provient de comptes personnels publics de familles.

Pour protéger votre vie privée et celle de vos proches, il est essentiel de bien réfléchir avant de partager des photos, de restreindre autant que possible le partage d'images personnelles et de prendre soin de paramétrer les options de confidentialité sur les réseaux sociaux.

Il est important de se rappeler que toutes les photos, qu'elles soient prises en maillot de bain ou dans des vêtements ordinaires, peuvent être utilisées de manière détournée par des personnes malveillantes, y compris les pédocriminels. Même les images qui semblent innocentes peuvent être exploitées de manière néfaste.

Protéger sa vie privée

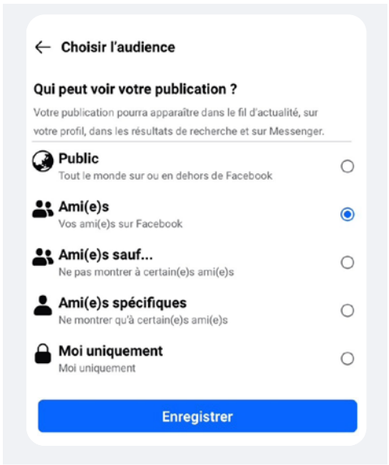
Vérifiez souvent les applications qui ont accès à votre compte et retirez celles que vous n'utilisez plus ou qui vous paraissent étranges.

Contrôlez qui voit quoi
Utilisez les paramètres pour modifier qui peut voir vos messages et photos. Vous pouvez créer des groupes d'amis pour partager seulement avec certains.

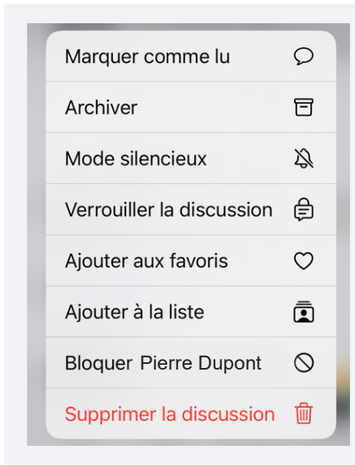
N'acceptez que les personnes que vous connaissez
Supprimez de votre liste d'amis ceux que vous ne connaissez pas.

N'hésitez pas à bloquer les personnes que vous ne connaissez pas.
Dans les paramètres de confidentialité de whatsApp, vous pouvez bloquer les contacts indésirables.

sur Facebook



Sur Whatsapp



7

L'intelligence artificielle vous aide au quotidien

L'intelligence artificielle (IA) est une technologie qui permet aux machines d'accomplir des tâches quotidiennes

Elle peut par exemple, comprendre la parole, traduire des textes ou rappeler des rendez-vous. Elle apprend en analysant de grandes quantités de données fournies par les utilisateurs, ce qui lui permet de s'adapter et de s'améliorer avec le temps.

L'IA facilite notre quotidien, mais elle présente aussi des risques. Certaines arnaques l'exploitent pour imiter des voix, créer de faux messages ou usurper des identités, rendant les fraudes plus convaincantes. Il est donc essentiel de rester vigilant : toujours vérifier les informations et ne jamais partager de données personnelles. L'IA est un outil très utile, mais elle doit être utilisée avec précaution.

Quelques exemples de bonne utilisation.

"Indique-moi 3 superbes destinations européennes accessibles en train."

"Il me reste 3 œufs, 2 poivrons, du poulet et j'ai un four, quelle recette puis-je faire ?"

"Écris-moi une lettre pour résilier mon abonnement à mon journal quotidien."

Bonnes pratiques de l'IA

Robots conversationnels
Des sites comme **ChatGPT** ou **Mistral.ai.fr** peuvent aussi discuter avec vous et fournir des informations.

Ne donnez jamais vos résultats médicaux
ou d'autres informations personnelles, sur ChatGPT.

Attention à vos données personnelles
l'IA collecte et stocke des données personnelles, ce qui peut exposer votre vie privée à des risques. Faites attention aux informations que vous partagez, car elles peuvent être utilisées à des fins commerciales.

8

Comment se prémunir du **cyber-harcèlement**

Comment pouvez-vous vous protéger du cyber-harcèlement et éviter de devenir un harceleur involontaire en ligne ?

Le cyber-harcèlement : un danger en ligne

Le cyber-harcèlement se produit en ligne, souvent sur les réseaux sociaux ou par e-mail. Il inclut des insultes, des menaces, des rumeurs ou le partage de photos sans consentement. Cela peut avoir de graves conséquences sur la vie des gens.

Attention à vos actions en ligne

Parfois, sans le vouloir, nos actions en ligne peuvent être mal interprétées. Par exemple, en partageant des informations ou des photos sans consentement, ou en participant à des discussions qui peuvent blesser autrui. N'oubliez jamais que ce sont des vraies personnes qui sont derrières et qui reçoivent ces commentaires comme si vous leur parliez en face.

Nos conseils

Respectez la vie privée des autres
Assurez-vous d'avoir l'autorisation avant de partager des informations ou des photos concernant quelqu'un d'autre.

Soyez conscient de l'impact de vos mots
Ce que vous dites en ligne peut avoir des conséquences réelles. Essayez d'éviter les commentaires qui pourraient être perçus comme blessants.

Informez-vous et sensibilisez-vous
Comprendre ce qu'est le cyber-harcèlement et ses conséquences peuvent aider à éviter des comportements involontaires qui pourraient être nuisibles.

Se protéger du cyber-harcèlement

Ne répondez pas aux provocations
Réagir aux messages de harcèlement peut parfois aggraver la situation.

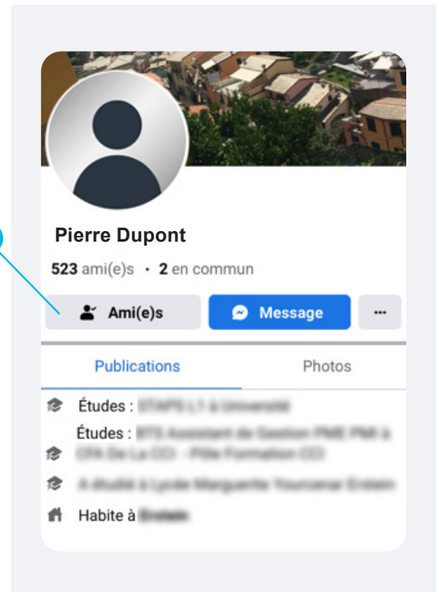
Bloquez et signalez les harceleurs
Les réseaux sociaux et les plateformes de messagerie offrent des outils pour bloquer et signaler les personnes qui vous harcèlent et les empêcher de vous contacter.

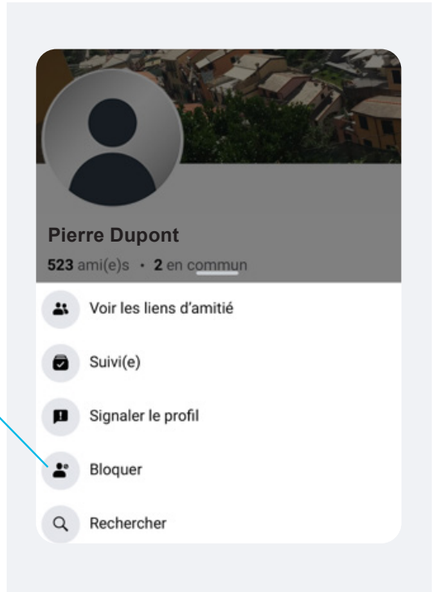
Conservez des preuves
Faites des captures d'écran des messages et publications offensants pour garder une trace des actes de harcèlement. Cela pourra être utile si vous décidez de signaler ou de porter plainte.

Parlez-en !

Si vous êtes victime de cyber-harcèlement, il est important d'en parler à des proches ou des professionnels qui peuvent vous soutenir et vous conseiller.

Bloquer quelqu'un sur Facebook





9

Distinguer les *vraies informations* et se protéger **des fausses**

Les fake news, ou fausses informations, sont des contenus mensongers diffusés dans le but de tromper, manipuler l'opinion publique ou parfois escroquer les internautes.

Elles apparaissent sous la forme d'articles, vidéos ou images avec des titres accrocheurs et des faits souvent exagérés pour capter l'attention.

Ces informations se basent fréquemment sur des éléments qui semblent possibles ou crédibles, ce qui les rend encore plus difficiles à détecter.

Elles peuvent être créées par des individus malintentionnés, des sites peu fiables ou partagées sans vérification préalable. Leur objectif peut être de semer la confusion, d'influencer les comportements ou de soutirer de l'argent, comme dans les arnaques en ligne.

Les fake news peuvent être dangereuses, surtout sur des sujets sensibles comme la santé.

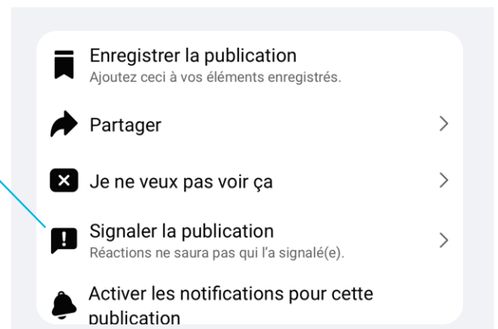
Par exemple, un article affirmant qu'une plante guérit le cancer doit être vérifié avant d'être cru et partagé. Les fake news peuvent aussi concerner des théories du complot ou des arnaques financières.

Nos conseils pour les repérer

1. **Vérifiez toujours la source**
   Par exemple, si l'information est relayée par plusieurs sources.
2. **Méfiez-vous des informations trop incroyables**
   Exemple : En Italie, une loi interdit de mettre de l'ananas sur une pizza sous peine d'amende.
1. **Utilisez des sites de vérification** comme "Les Décodeurs" ou "Hoaxbuster". Ce sont des sites dit de " fack checker" c'est-à-dire que leur métier est de vérifier la fiabilité des informations partagées sur internet. N'oubliez pas d'avoir toujours un esprit critique.
2. **Ne pas repartager des fausses informations**, car les cybercriminels utilisent cette technique pour repérer les personnes qui pourront plus facilement croire à leur arnaque.
3. **Signalez les fausses informations** que vous rencontrez en utilisant les outils intégrés pour limiter leur propagation et protéger les autres utilisateurs.

Exemple d'une publication générée par une IA.
Les personnes malveillantes vont dans les commentaires et choisissent les personnes qui semblent penser que la publication est réelle afin de les approcher dans le but de les arnaquer.

Signaler une fausse publication



10

Liens et **numéros utiles**

3020

Numéro gratuit pour signaler les cas de harcèlement scolaire et obtenir de l'aide.

3018

Numéro gratuit dédié à l'assistance en cas de cyber-harcèlement, géré par l'association e-Enfance. 3018.fr

33700

Numéro gratuit pour signaler les appels et SMS frauduleux, comme les arnaques et le spoofing.

J'alerte l'Arcep

Service permettant de signaler les numéros de téléphone suspectés de pratiques frauduleuses comme le harcèlement ou le spoofing, afin d'aider à lutter contre ces abus.

e-Enfance

Organisation spécialisée dans la protection des enfants et des adolescents en ligne, qui propose également des conseils pour les parents et les adultes concernés.

internetsanscrainte.fr

Plateforme dédiée à la sensibilisation des jeunes aux bons usages du numérique.

Cybermalveillance.gouv.fr

Site officiel d'accompagnement des victimes d'actes de cybermalveillance (hameçonnage, piratage, arnaques en ligne, etc.).

17 CYBER

Plateforme de signalement des cybercrimes et assistance aux victimes, accessible via : www.cybermalveillance.gouv.fr/17cyber

CNIL

Pour supprimer des données personnelles. https://www.cnil.fr/fr/modele/courrier/supprimer-des-donnees-personnelles

La cybersécurité concerne tout le monde et évolue constamment.

Nous espérons que ce livret vous a apporté des informations précieuses et des conseils pratiques pour naviguer en toute sécurité dans le monde numérique.

Restez informés, adoptez de bonnes pratiques et n'hésitez pas à solliciter votre entourage en cas de doute.

Pour toutes questions supplémentaires relatives au risque numérique ou en cas de doute, rendez-vous sur la page www.cybermalveillance.gouv.fr

A propos de Capgemini

Capgemini, partenaire de la transformation business et technologique de ses clients, les accompagne dans leur transition vers un monde plus digital et durable, tout en créant un impact positif pour la société. Le Groupe, responsable et multiculturel, rassemble 340 000 collaborateurs dans plus de 50 pays. Depuis plus de 55 ans, ses clients lui font confiance pour répondre à l'ensemble de leurs besoins grâce à la technologie. Capgemini propose des services et solutions de bout en bout, allant de la stratégie et du design jusqu'à l'ingénierie, en tirant parti de ses compétences de pointe en intelligence artificielle et IA générative, en cloud, et en data, ainsi que de son expertise sectorielle et de son écosystème de partenaires. Le Groupe a réalisé un chiffre d'affaires de 22,1 milliards d'euros en 2024.

www.capgemini.com

Capgemini