N°8 - JUILLET/SEPTEMBRE 2026

CYBER-IT MAGAZINE

LA CYBER EST UN MARATHON PAS UN SPRINT !

Cyber Sensibilisation

En partenariat avec

Guiddy & AXBX CyberSecurity Solutions

Une question ? Un besoin ?
cyberit.magazine@gmail.com

EDITO

Chères lectrices, chers lecteurs,

L'été est enfin là une parenthèse bienvenue pour ralentir, décrocher et laisser derrière soi le rythme soutenu du quotidien, du travail, les notifications incessantes et les boîtes mail saturées.

Mais pendant que nous levons le pied, les cybercriminels, eux, restent pleinement actifs. Mieux encore : ils profitent de cette période où la vigilance diminue pour intensifier leurs arnaques. Et elles sont nombreuses, bien trop nombreuses pour être toutes abordées en un seul numéro.

Nous avons donc fait le choix de nous concentrer sur les menaces qui nous semblent aujourd'hui les plus critiques. D'autres, comme les faux QR codes, les arnaques sentimentales ou encore les fausses locations de vacances, mériteraient également toute votre attention et feront sans doute l'objet de prochaines éditions.

Ce numéro a été pensé comme un guide accessible et visuel, conçu pour être compris par tous : des plus jeunes aux moins initiés, sans oublier celles et ceux qui souhaitent simplement mieux appréhender les risques numériques du quotidien.

Car au fond, le véritable enjeu n'est pas l'utilisateur lui-même, mais la manière dont il perçoit les situations et se positionne face aux menaces. Nous vous invitons à partager largement ce numéro autour de vous, afin de contribuer, ensemble, à des usages numériques plus sûrs et plus éclairés.

Excellente lecture, et à très bientôt.

ARNAUD LEROY

Nos partenaires

AXBX CyberSecurity Solutions

AxBx lance une offre de solution de cybersécurité pour les PME

AxBx est une société Française d'édition de logiciels de cybersécurité.

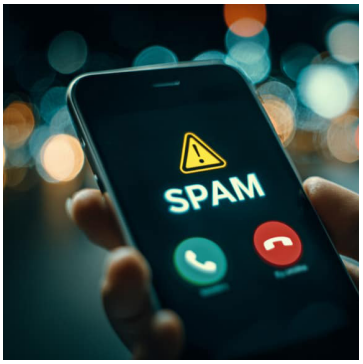
Depuis plus de 20 ans, AxBx conçoit, développe et commercialise des solutions decybersécurité innovantes : antivirus nouvelle génération, pare-feu intelligent, coffre-fort à mots de passe...

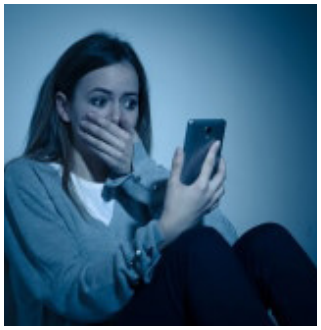
Guiddy

Guiddy est une ESN française spécialisée en cybersécurité, créée en 2022 et basée en Île-de-France. Elle accompagne les TPE, PME et ETI avec des services d'audit, de conseil et de sensibilisation.

Guiddy se distingue par ses supports pédagogiques innovants et ludiques, rendant la cybersécurité accessible et transformant les collaborateurs en acteurs efficaces de la protection informatique au quotidien pour clients.

SOMMAIRE





SENSIBILISATION CYBER

Information - Bonnes pratiques - Risques

La sensibilisation cyber ne vise pas à culpabiliser les utilisateurs mais à leur donner les moyens de mieux se proteger.

Les difficultés apparaissent lorsque les repères manquent, que les bons réflexes ne sont pas suffisamment intégrés, ou que la sécurité est perçue comme une contrainte abstraite plutôt que comme une pratique du quotidien.

Sensibiliser, ce n'est donc pas pointer du doigt les comportements, mais donner les moyens d'agir avec plus de discernement et de cohérence, dans des situations concrètes et souvent banales.

L'enjeu n'est pas de faire peur, ni de culpabiliser, mais de permettre à chacun de comprendre ce qu'il fait, pourquoi il le fait, et quelles conséquences peuvent découler d'un geste apparemment anodin.

Les risques numériques s'invitent partout, y compris dans des usages très ordinaires. Les réseaux sociaux, par exemple, exposent des informations parfois trop personnelles, souvent partagées sans mesurer leur portée ni leur durée de circulation.

Les appareils mobiles occupent aujourd'hui une place centrale dans la vie privée comme dans la vie professionnelle, ce qui en fait des cibles privilégiées, mais aussi des outils que l'on utilise sans toujours prendre le temps de les sécuriser correctement. Un téléphone perdu, un verrouillage trop faible, une application installée sans vérification ou une connexion sur un réseau public peuvent ouvrir la porte à des usages non souhaités.

Les sauvegardes, les mises à jour, ou encore la séparation entre usages professionnels et personnels sont autant de sujets simples en apparence, mais déterminants pour limiter les incidents et réduire l'impact d'une erreur ou d'une attaque. L'intérêt de la cyber sensibilisation est justement de rappeler que ces gestes ne relèvent pas d'une expertise réservée à quelques spécialistes. Ils font partie d'une hygiène numérique de base, au même titre que fermer une porte à clé ou vérifier une information avant de la diffuser.

Trop souvent, les consignes de sécurité sont connues en théorie mais peu appliquées en pratique, soit par manque de temps, soit par habitude, soit parce qu'elles semblent moins urgentes que l'activité elle-même. Pourtant, une sauvegarde régulière, une mise à jour effectuée à temps ou une séparation claire entre usages personnels et professionnels peuvent éviter des conséquences lourdes.

Les attaques les plus fréquentes s'appuient rarement sur des techniques spectaculaires. L'hameçonnage exploite la confiance, la curiosité ou l'urgence. Il suffit parfois d'un message bien rédigé, d'une pièce jointe trompeuse ou d'un lien crédible pour provoquer une action inadaptée. Les rançongiciels profitent d'une faille, d'un clic trop rapide ou d'un accès mal protégé, puis transforment un incident technique en blocage majeur. L'arnaque au faux support technique, elle, mise sur la peur et la précipitation, en donnant l'impression qu'il faut intervenir immédiatement pour éviter un danger supposé.

La sécurité ne dépend pas seulement des outils en place, mais aussi de la capacité des utilisateurs à reconnaître les signaux d'alerte et à adopter les bons réflexes au bon moment.

LE PLUS GRAND RISQUE EN MATIÈRE DE CYBERSÉCURITÉ EST L'IGNORANCE

Kevin Mitnick
Légende de la cybersecurité

Quelles ont été les principales demandes d'assistance cyber en 2025 ?

D'après les données récoltées auprès de cybermalveillance.gouv.fr

Hameçonnage, piratage de comptes, violations de données… Ces menaces comptent parmi les plus couramment rencontrées par les particuliers. Décryptage des principales tendances et évolutions observées.

Cybermalveillance.gouv.fr tire la sonnette d'alarme. Dans son rapport d'activité 2025, la plateforme nationale d'assistance aux victimes de cyberattaques constate une nette accélération des cybermalveillances

L'année 2025 a marqué un nouveau cap pour le dispositif public. Grâce notamment au lancement de 17Cyber fin 2024, plus de **500 000 victimes** ont pu être accompagnées sur l'ensemble de l'année, soit une hausse de 20 % par rapport à 2024, confirmant le rôle structurant et désormais incontournable du dispositif dans l'écosystème national de lutte contre la cybercriminalité.

La plateforme a également franchi un seuil symbolique en dépassant les 5 millions de visiteurs annuels, ce qui témoigne d'une prise de conscience de plus en plus marquée des risques numériques au sein de la population française, tant chez les particuliers que chez les professionnels, ainsi que d'une meilleure identification des bons réflexes de signalement.

Chez les particuliers, **l'hameçonnage** demeure la menace dominante. Il représente près d'un tiers des demandes d'assistance adressées à Cybermalveillance.gouv.fr, avec une **hausse de 71 % sur un an**. Cette progression s'explique notamment par la sophistication croissante des campagnes de phishing, qui exploitent de manière systématique les données personnelles issues des récentes fuites ayant touché de nombreux secteurs économiques et administrations, rendant les attaques plus ciblées et plus crédibles.

Le piratage de compte constitue toujours la deuxième menace la plus fréquemment signalée, malgré une légère baisse des signalements observée sur la période. Ce recul relatif ne doit cependant pas masquer la persistance du risque, les compromissions de comptes

restant une porte d'entrée majeure pour des attaques plus larges, notamment via la réutilisation d'identifiants ou l'absence d'authentification forte.

Mais c'est surtout la progression des **violations de données** qui retient l'attention des autorités et des acteurs de la cybersécurité. Désormais troisième menace la plus signalée, elles enregistrent une **hausse de 107 %**, traduisant une intensification significative des compromissions à grande échelle ainsi qu'une industrialisation des attaques visant les bases de données.

Les secteurs du commerce, des télécommunications, de la santé, de l'assurance ainsi que de l'emploi figurent parmi les plus touchés par ces fuites massives d'informations personnelles, confirmant la vulnérabilité persistante des environnements traitant de grands volumes de données sensibles et leur exposition structurelle aux attaques opportunistes comme ciblées.

PARTICULIERS		
Plus de 20000 assistances	**Entre 10000 et 20000 assistances**	**Moins de 10000 assistances**
• Hameçonnage (+71%) • Piratage de compte (+11,6%) • Violations de données (+107%)	• Faux support informatique (+39%) • Cyberharcèlement (+134%) • Faux conseiller bancaire (+159%) • Virus (+8%) • Fraude au virement (+196%)	• Fraude à la carte bancaire (+96%) • Usurpation de numéro de téléphone (+517%)

Chiffres en % des demandes d'assistance

En recul relatif, l'arnaque au **faux support technique** se positionne désormais en quatrième place, représentant 5,9% des demandes d'assistance.

Après un net ralentissement consécutif à des actions judiciaires menées en 2024, les acteurs malveillants ont repris leurs activités début 2025, entraînant une nouvelle hausse des signalements (+39% sur un an).

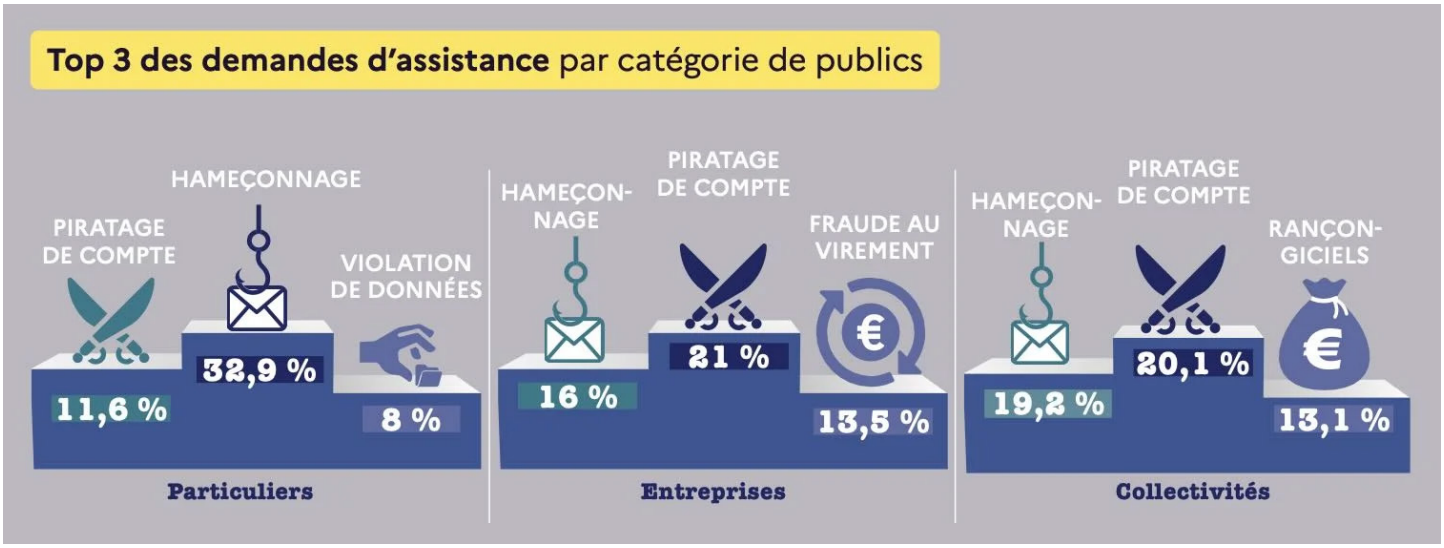
Parallèlement, les situations de **cyberharcèlement** connaissent une progression marquée.

Principalement liées à des menaces, des campagnes de dénigrement sur les réseaux sociaux ou encore des appels anonymes, elles atteignent désormais près de 18 000 demandes d'assistance annuelles, soit une **hausse de 134%**.

La fraude au **faux conseiller bancaire** s'inscrit également dans cette dynamique, avec une augmentation significative de 159%, pour un total d'environ 15 000 sollicitations sur l'année.

Dans un registre plus technique, les demandes liées aux virus informatiques progressent légèrement en volume (+8%), mais reculent dans le classement, passant de la cinquième à la septième position.

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



Source : https://www.cybermalveillance.gouv.fr

L'invité

Jérôme NOTIN

Directeur général du GIP ACYMA cybermalveillance, 17Cyber

" Cela n'arrive pas qu'aux autres "

Il y a quelques années encore, beaucoup de victimes de cyberattaque ne savaient pas vraiment vers qui se tourner. Un compte piraté, un faux SMS de livraison, une fraude au virement, une fuite de données… autant de situations malheureusement devenues trop fréquentes, mais qui laissent encore trop souvent particuliers et organisations seules face à l'urgence.

Créé en 2017 par l'ANSSI et le ministère de l'Intérieur, le dispositif accompagne les victimes d'actes de cybermalveillance, tout en les guidant pour mieux comprendre la menace et faire de la sensibilisation un véritable levier de protection. En 2025, la plateforme a enregistré environ 500 000 demandes d'assistance, ce qui confirme l'ampleur de la menace, mais aussi le besoin d'un accompagnement adapté aux besoins de chaque victime.

Pour mieux comprendre le rôle de la plateforme, son évolution et les bons réflexes à adopter face aux cybermenaces, nous avons rencontré Jérôme Notin, directeur général de Cybermalveillance.gouv.fr.

Pouvez-vous nous présenter le dispositif Cybermalveillance ?

Cybermalveillance.gouv.fr a été créé pour assister les victimes.

Nous proposons des solutions et un accompagnement à celles et ceux qui se retrouvent confrontés à un acte de cybermalveillance, sans savoir immédiatement quoi faire ni à qui s'adresser. Le dispositif s'adresse aux particuliers, aux entreprises, aux associations, aux collectivités et aux administrations qui ne relèvent pas directement du périmètre d'intervention de l'ANSSI.

Lorsqu'un utilisateur arrive sur la plateforme, il suit un parcours intitulé 17Cyber (également disponible sur 17Cyber.gouv.fr) qui lui permet de qualifier la menace. Il peut s'agir d'un piratage de compte, d'une tentative d'hameçonnage, d'une fraude au faux conseiller bancaire, d'une fraude au virement, d'un rançongiciel ou d'un autre type d'attaque.

Une fois la situation identifiée, la victime reçoit des conseils adaptés. Si l'incident le nécessite, elle peut aussi être orientée vers un prestataire de proximité, un professionnel référencé ou labellisé ExpertCyber, un CSIRT (Computer Security Incident Response Team), ou encore vers un policier ou un gendarme.

Lancé en 2024, 17Cyber permet aux victimes d'être guidées dans leur recherche d'assistance et, si besoin, d'être mises en relation avec les bons interlocuteurs. Le rôle du dispositif est d'éviter que la victime reste seule face à une situation qu'elle ne comprend pas toujours et ne sait pas gérer.

Quelles sont les origines du dispositif et sa vision ?

Lorsqu'une attaque survient, beaucoup de victimes se retrouvent démunies. Elles ne savent pas toujours si elles doivent appeler la police, la gendarmerie, prévenir leur banque, contacter leur prestataire informatique, conserver des éléments de preuve ou déposer plainte. Cybermalveillance.gouv.fr a été pensé pour leur apporter une première orientation au moment où chaque décision compte.
Cependant, Cybermalveillance.gouv.fr ne se limite pas à l'assistance. Le GIP ACYMA, qui porte le dispositif, agit aussi sur la prévention et l'observation de la menace.

Les parcours réalisés sur la plateforme permettent de mieux comprendre les attaques réellement rencontrées par les particuliers, les entreprises et les collectivités. Ces informations servent ensuite à adapter les messages de prévention et les campagnes de sensibilisation, à l'échelle nationale et européenne, notamment dans le cadre du Cybermois.

Cette année, nous avons présenté notre stratégie 2026-2030. Cette feuille de route doit accompagner la montée en puissance du dispositif face à des menaces numériques de plus en plus présentes et sophistiquées. L'objectif est que le 17Cyber devienne un réflexe pour les victimes, avec une réponse nationale capable de s'appuyer, lorsque c'est nécessaire, sur un accompagnement local grâce aux CSIRT territoriaux déployés sur l'ensemble du territoire national, hexagonal et ultramarin.

Travaillez-vous en coordination directe avec l'ANSSI ou les forces de l'ordre en cas d'attaque majeure ?

Cybermalveillance.gouv.fr intervient aux côtés d'autres acteurs de la cybersécurité.

L'ANSSI accompagne les structures les plus sensibles ou réglementées, comme les ministères, les opérateurs d'importance vitale et les opérateurs de services essentiels.
Cybermalveillance.gouv.fr s'adresse, de son côté, aux particuliers, TPE-PME, associations, collectivités et administrations qui ne relèvent pas directement de ce périmètre.

Avec le 17Cyber, le lien avec les forces de l'ordre est intégré au parcours. Lorsque la situation le nécessite, une victime peut être mise en relation avec un policier ou un gendarme. Pour les incidents techniques, elle peut aussi être dirigée vers des prestataires de proximité, des professionnels labellisés ExpertCyber ou des CSIRT territoriaux.

L'objectif est que chaque victime puisse obtenir rapidement une première réponse claire pour comprendre les démarches à engager et être orientée vers l'assistance la plus adaptée à sa situation.

Selon vous, qu'est-ce qui freine l'adoption des bonnes pratiques cyber ?

Le premier frein reste la perception du risque.

Beaucoup de petites structures pensent encore qu'elles ne sont pas des cibles, parce qu'elles n'ont pas beaucoup de budget, peu de visibilité ou des moyens limités. Mais les attaquants ne cherchent pas toujours une cible prestigieuse. Ils cherchent surtout une opportunité. Un compte mal protégé, une messagerie compromise ou un collaborateur qui clique trop vite peuvent suffire.

Toutes les attaques ne sont pas ultra-ciblées dès le départ. Beaucoup reposent sur une logique de volume, avec des campagnes massives qui finissent par trouver une faille exploitable. C'est ce qui rend le discours "cela n'arrive qu'aux autres" particulièrement dangereux.

En 2026, les fragilités restent importantes. Chez les TPE-PME, six entreprises sur dix semblent encore ne pas savoir évaluer les conséquences d'une cyberattaque, et beaucoup estiment ne pas être suffisamment préparées.
L'autre difficulté, c'est l'apprentissage des bons réflexes. Nous utilisons chaque jour des outils puissants à travers nos smartphones, les réseaux sociaux, les applications bancaires, sans avoir toujours appris les règles de base pour les utiliser de manière sécurisée.

La sensibilisation ne peut pas se résumer à quelques rappels ponctuels. Pour être utile, elle doit s'inscrire dans les habitudes, prendre différentes formes et s'appuyer sur des exemples dans lesquels chacun peut se reconnaître. C'est ainsi que les réflexes s'installent peu à peu pour mieux repérer un message suspect, mieux protéger ses accès, signaler une tentative d'arnaque ou demander de l'aide avant que la situation devienne préoccupante.

Quels sont les premiers réflexes à adopter lorsqu'on est touché par une cyberattaque ?

Dans les premières heures, il faut surtout éviter d'aggraver la situation car une attaque provoque souvent un moment de sidération.

Certaines situations comme un écran bloqué, un compte inaccessible, une demande de rançon, un virement suspect ou une messagerie compromise peuvent pousser à agir trop vite. C'est précisément dans ces moments qu'il faut garder son calme et avancer avec méthode.

Le premier réflexe est de qualifier la menace, car toutes les attaques ne se traitent pas de la même manière. Dans ces premières heures, il faut conserver ce qui peut aider à comprendre l'attaque et se faire accompagner pour remettre les systèmes en état. Selon la nature de l'incident, une entreprise par exemple, pourra être orientée vers un prestataire spécialisé, un professionnel labellisé ExpertCyber, un CSIRT territorial ou les forces de l'ordre.

Protégez-vous du phishing !

Le phishing, ou hameçonnage, désigne une technique de fraude visant à tromper un internaute pour l'amener à divulguer des informations sensibles, telles que ses identifiants de connexion, ses mots de passe ou encore ses données bancaires, en se faisant passer pour un tiers de confiance.

Cette pratique peut prendre différentes formes, comme l'envoi de faux emails, de SMS ou encore des appels téléphoniques usurpant l'identité d'organismes légitimes : banque, réseau social, opérateur téléphonique, fournisseur d'énergie, site de e-commerce ou administration.

56% **des attaques de phishing passent par un lien malveillant classique**

25% **via QR code**

19% **via pièces jointes malveillantes**

Selon le rapport Proofpoint, The Human Factor 2025 Vol. 2

Comment reconnaître un mail de phishing ?

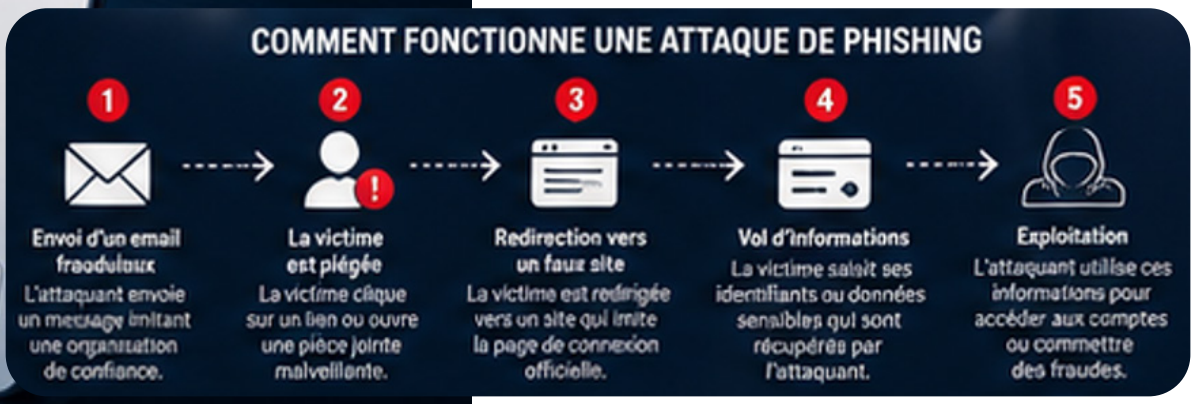
Si les tentatives d'hameçonnage sont aujourd'hui de mieux en mieux réalisées, un mail frauduleux présente souvent des signes d'alerte qu'il est possible de déceler : offre trop alléchante, apparence suspecte, pièce jointe inattendue, adresse d'expédition fantaisiste…

Témoignage d'une victime d'hameçonnage

« Quand j'étais en arrêt maladie, j'ai reçu un mail de la sécurité sociale qui m'annonçait un remboursement de plus de 200 euros de frais de santé que j'attendais. J'ai cliqué sur le lien et je suis arrivé sur un site qui avait l'air officiel.

Ce site me proposait d'être remboursé immédiatement si je donnais mon numéro de carte bancaire. Je ne me suis pas méfié et je l'ai fait mais le remboursement n'est jamais arrivé. J'ai contacté la sécurité sociale pour me renseigner et le conseiller m'a annoncé que je m'étais fait arnaquer. J'ai immédiatement prévenu ma banque pour bloquer ma carte, mais plusieurs prélèvements avaient déjà été faits sur mon compte.»

Boulanger anonyme dans la région Bourgogne
via Cybermalveillance.gouv.fr



Les 8 arnaques les plus courantes en France

Victime de phishing, que faire ?

Au moindre doute, contactez l'organisme concerné
Ne répondez pas au message, contactez directement l'organisme via ses canaux officiels.

Faites opposition immédiatement
En cas de fuite d'informations bancaires ou de débit frauduleux, contactez votre banque sans attendre.

Conservez les preuves
Gardez le message, les pièces jointes et toute information utile.

Déposez plainte
Au commissariat ou à la gendarmerie, ou par courrier au procureur de la République.

Changez immédiatement vos mots de passe
Sur le site concerné et partout où vous utilisez le même mot de passe.

Signalez tout message ou site douteux à Signal Spam
Ne cliquez pas sur les liens suspects. Vérifiez l'adresse du site. Signalez sur www.signal-spam.fr

Signalez les SMS suspects au 33 700
Transférez le SMS ou signalez-le sur la plateforme 33 700 (service gratuit).

Signalez les sites d'hameçonnage à Phishing Initiative
Vérifiez l'adresse du site et signalez-le sur www.phishing-initiative.fr pour faire bloquer le site.

Exemple de mail de phishing

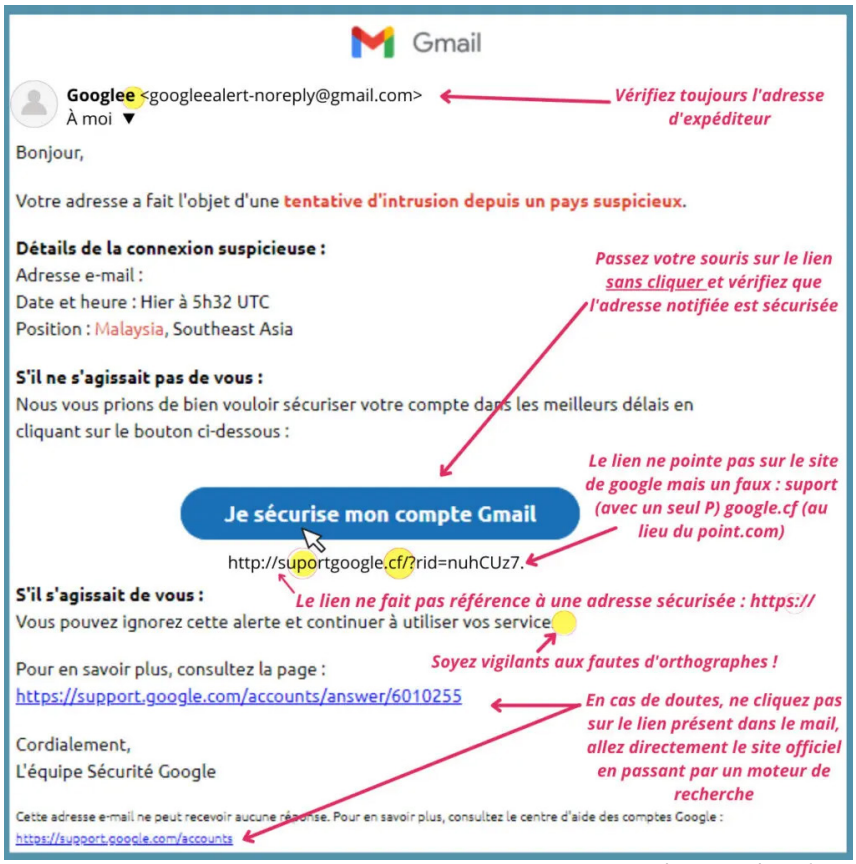


image : gplexpert.com

Cette fausse alerte Gmail est un bon exemple de phishing : le message imite une notification officielle pour créer un sentiment d'urgence et pousser la victime à **cliquer rapidement**, sans prendre le temps de **vérifier l'adresse de l'expéditeur** ni la véritable destination du lien.

Le but est de **faire croire à une compromission du compte** afin d'inciter l'utilisateur à "sécuriser" son accès sur un faux site conçu **pour voler ses identifiants**.

CONSEIL NATIONAL DES BARREAUX

LES AVOCATS

PRÉSENTE

20.000 EUROS SOUS LES MERS

Phishing, arnaque en ligne, mordre à l'hameçon peut coûter cher.
Protégez-vous, faites appel à un avocat dès les premiers signes.

RENDEZ-VOUS SUR AVOCAT.FR

Piratage de compte

quand vos données ne vous appartiennent plus !

Le piratage de compte correspond à la prise de contrôle d'un compte en ligne par un cybercriminel, sans l'autorisation de son propriétaire. Tous les types de comptes peuvent être concernés : messagerie électronique, réseaux sociaux, services administratifs, plateformes d'e-commerce, espaces bancaires ou encore applications professionnelles.

Cette compromission peut résulter de plusieurs facteurs. Dans de nombreux cas, le mot de passe est trop faible ou a déjà été divulgué lors d'une fuite de données. L'utilisateur peut également avoir été victime d'une campagne de phishing et avoir communiqué ses identifiants sur un faux site sans s'en apercevoir.

La réutilisation d'un même mot de passe sur plusieurs services constitue également un risque majeur : si l'un de ces services est compromis, les cybercriminels peuvent tenter d'accéder à tous les autres comptes utilisant les mêmes identifiants. Enfin, certains logiciels malveillants, appelés stealers, sont capables de dérober automatiquement les mots de passe enregistrés sur les appareils infectés.

Le but de l'attaquant

Dérober des informations personnelles, professionnelles ou bancaires afin de les exploiter à des fins malveillantes.

Les chiffres clès

Un rapport publié récemment par la société Surfshark révèle qu'environ **425,7 millions de comptes auraient été compromis sur l'année écoulée.** Cela représente un rythme proche d'un compte piraté chaque seconde, ce qui illustre de manière frappante l'intensité des compromissions dans l'environnement numérique actuel.

Les fuites d'identifiants se comptent désormais en milliards, avec une gigantesque base de 16 milliards d'identifiants découverte en 2025

Comment le piratage arrive ?

Hameçonnage : un message pousse la victime à saisir ses identifiants sur un faux site.

Réutilisation de mots de passe : si un service est compromis, les autres comptes utilisant le même mot de passe deviennent vulnérables.

Fuite de données : des identifiants circulent ensuite sur les réseaux malvaillants.

Appareil infecté : un logiciel malveillant peut voler des mots de passe ou des sessions déjà ouvertes.

Le scénario le plus fréquent commence par un mot de passe compromis : mot de passe trop faible, réutilisé sur plusieurs services, ou récupéré après une fuite de données publiée ailleurs.

L'attaquant peut aussi tromper la victime avec un faux e-mail, un faux SMS ou une fausse page de connexion qui ressemble au service officiel, ce qui lui permet de récupérer les identifiants.

comment éviter de se faire pirater son compte ?

LES 11 RÉFLEXES INDISPENSABLES POUR PROTÉGER SON IDENTITÉ NUMÉRIQUE

La grande majorité des compromissions de comptes pourraient être évitées en adoptant quelques bonnes pratiques de cybersécurité. Si aucune protection n'est infaillible, des gestes simples et des habitudes adaptées permettent de réduire considérablement les risques de piratage et limiter les conséquences d'une attaque.

1 UN MOT DE PASSE UNIQUE POUR CHAQUE COMPTE

Réutiliser le même mot de passe sur plusieurs sites constitue l'une des erreurs les plus fréquentes. Lorsqu'un service est victime d'une fuite de données, les cybercriminels testent automatiquement les identifiants récupérés sur d'autres plateformes : messagerie, réseaux sociaux, banques, boutiques en ligne ...
La meilleure protection consiste à créer un mot de apsse différent pour chaque service, couplé à un gestionnaire de mot de passe. Plus il est long, complexe et aléatoire, plus il sera difficile à deviner ou à pirater.

2 ACTIVER LA DOUBLE AUTHENTIFICATION

Aujourd'hui proposée par la majorité des services en ligne, la double authentification ajoute une couche de sécurité supplémentaire.
Même si un pirate découvre votre mot de passe, il lui faudra également valider une seconde étape 'application mobile, code SMS, clé de sécurité...) avant d'accéder à votre compte.
Cette protection est particulièrement recommandée pour les comptes de messagerie, les services bancaires, les réseaux sociaux et les espaces pro.

3 NE PAS COMMUNIQUER D'INFORMATIONS SENSIBLES

Aucune administration, banque ou entreprise sérieuse ne demandera votre mot de passe par téléphone, SMS ou mail. Les cybercriminels exploitent régulièrement des scénarios de faux support technique, de faux conseillers bancaires ou de faux services administratofs pour récupérer vos identifiants.

RÈGLES D'OR

° Ne jamais communiquer ses mots de passe

° Ne pas transmettre de codes de validation

° Ne pas partager de données bancaires

4 INSTALLER TOUTES LES MISES À JOUR DE SÉCURITÉ

Les mises à jour ne servent pas uniquement à ajouter de nouvelles fonctionnalités. Elles corrigent surtout des failles pouvant être exploitées par des pirates pour prendre le contrôle d'un ordinateur. Le système d'exploitation, le navigateur ou encore les applications mobiles doivent être maintenus à jour.

5 MAINTENIR SON ANTIVIRUS ET SON PARE-FEU ACTIFS

Un antivirus correctement mis à jour détecte de nombreuses menaces avant qu'elles n'infectent l'appareil. Associé à un pare-feu configuré correctement, il permet de limiter les connexions malvaillantes et les tentatives d'intrusion.

6 SE MEFIER DES MAILS INATTENDUS

Un simple clic sur une pièce jointe infectée ou sur un faux lien peut conduire au vol de données personnelles ou à l'installation d'un logiciel malvaillant.
Redoublez de vigilance lorsque le mail :
° provient d'un expéditeur inconnu
° semble inhabituel
° contient des fautes
° demande une action urgente
° comporte des pièces jointes inattendues

7 EVITER LES SITES INTERNET DOUTEUX

Les plateformes proposant gratuitement des contenus normalement payants (films, logiciels, musiques ...) ou certains site illégaux sont fréquemment utilisés pour diffuser des virus. Les cybercriminels y cachent des logiciels capables d'espionner l'utilisateur, de voler ses mots de passe ou de chiffrer ses données.

8 VÉRIFIER SYSTÉMATIQUEMENT L'ADRESSE DU SITE

Les faux sites internet imitent parfois parfaitement les plateformes légitimes. La seule différence peut être une lettre remplacée, un tiret ajouté ou une extension inhabituelle (.info, .xyz ...)
Avant de saisir vos identifiants ou vos coordonnées bancaires, prenez quelques secondes pour vérifier l'adresse affichée dans le navigateur.

9 CONTRÔLER LES DERNIÈRES CONNEXIONS

De nombreux services proposent un historique des dernières connexions. Cette fonctionnalité permet de détecter rapidement une activité inhabituelle: connexion depuis un pays étranger, appareil inconnu ou horaire suspect.
En cas de doute, changez immédiatement votre mot de passe et déconnectez toutes les sessions ouvertes.

10 SE MÉFIER DES RÉSEAUX WIFI PUBLICS

Les réseaux WIFI gratuits proposés dans certains lieux publics (gares, hôtels, restaurants, aéroports ...) peuvent être compromis. Un pirate connecté au même réseau peut parfois intercepter certaines communications.
Lorsque cela est possible : privilégiez votre connexion mobile (4G ou 5G), utilisez un VPN reconnu et évitez toute opération sensible sur un réseau public.

11 TOUJOURS SE DÉCONNECTER APRÈS UTILISATION

Sur un ordinateur partagé ou un appareil accessible à d'autres personnes, rester connecté à un compte représente un risque important. Fermer simplement la fenêtre du navigateur ne suffit pas toujours. Il est recommandé de se déconnecter manuellement, fermer complètement le navigateur, ne JAMAIS enregistrer ses mots de passe sur un ordinateur public.

Spam téléphonique

l'industrie de l'arnaque ne prend pas de repos

Le spam téléphonique désigne une communication non sollicitée à des fins publicitaires, commerciales ou malveillantes. Il peut prendre différentes formes, SMS, MMS ou bien appel téléphonique.

Dans bien des cas, il s'agit de messages publicitaires adressés à des fins de prospection commerciale. Mais le spam téléphonique peut également revêtir un caractère malveillant : incitation à rappeler un numéro surtaxé, envoyer un SMS à un numéro payant ou encore tentatives de phishing pour récupérer des données personnelles et/ou confidentielles.

« Il est interdit de démarcher par téléphone [...] un consommateur qui n'a pas exprimé préalablement son consentement à faire l'objet de prospections commerciales par ce moyen. »

Article L223-1 du Code de la consommation

Appels et messages non sollicités ou abusifs sont en forte croissance de 113% par rapport à 2024

ARCEP - Autorité de régulation des communications électroniques, des postes et de la distribution de la presse

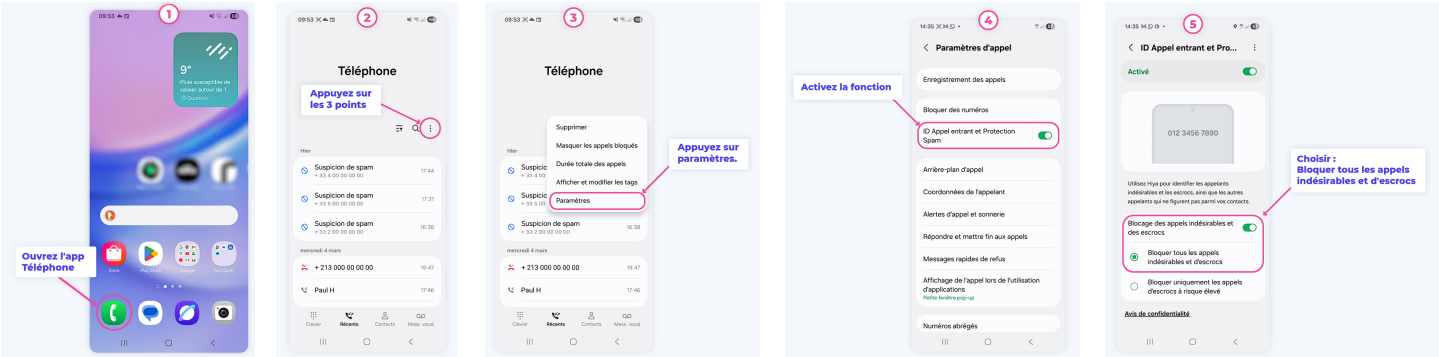
Exemple de SMS frauduleux

Selon le baromètre ARCEP édition 2026, 94 % des consommateurs ont reçu au moins un appel ou un SMS indésirable au cours des trois derniers mois, et 57 % reçoivent près d'un appel non sollicité par jour. Sur l'usurpation de numéro, le phénomène où un fraudeur affiche à votre écran un faux numéro français pour gagner votre confiance, 43 % des utilisateurs déclarent en être victimes au moins une fois par mois, et 13 % au moins une fois par jour.

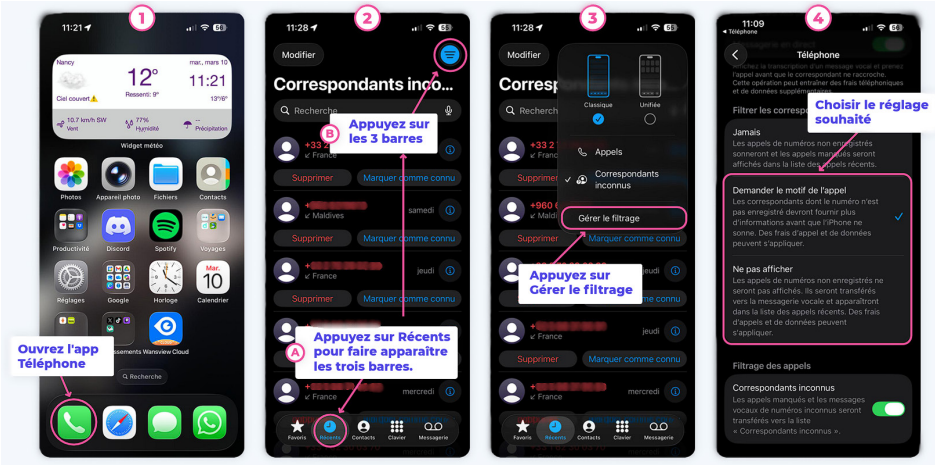
Spam téléphonique
les bons réflexes pour s'en protéger

TUTORIEL : BLOQUER LES APPELS INDÉSIRABLES SUR SMARTPHONE

Android (samsung etc ...)



iOS (iphone)



Source : https://lesbases.anct.gouv.fr

CONSEILS

- N'hésitez pas à installer une application de filtrage des appels indésirables ou à configurer votre téléphone afin de limiter au maximum les sollicitations.

- Voici la liste officielle des indicatifs réservés au démarchage téléphonique en France *(à ajouter à vos listes noires des appels téléphoniques)* :

0162, 0163, 0270, 0271, 0377, 0378, 0424, 0425 0568, 0569, 0948 et 0949


CONSEIL NATIONAL
DES BARREAUX
LES AVOCATS
PRÉSENTE
LA REINE DES PIÈGES
En ligne, les pièges pour obtenir vos données sont réels.
Protégez-vous, faites appel à un avocat dès les premiers signes.
RENDEZ-VOUS SUR AVOCAT.FR

Usurpation d'identité quand les fraudeurs prennent le contrôle

Le but de l'attaquant

Utilisation de données personnelles et/ou professionnelles permettant d'identifier une personne sans son accord et se faire passer pour elle pour réaliser des actions frauduleuses.

Dans les faits, ces informations peuvent être obtenues de différentes manières : perte ou vol de documents d'identité, campagnes d'hameçonnage, piratage de comptes en ligne ou d'appareils, compromission de sites web contenant des données personnelles, voire récupération de documents jetés.

Une fois en possession de ces éléments, les fraudeurs peuvent multiplier les usages malveillants : création de faux profils sur les réseaux sociaux, escroqueries visant l'entourage, publication de fausses annonces, actes de diffamation ou de cyberharcèlement, chantage, extorsion, ou encore ouverture de lignes téléphoniques, de comptes bancaires, souscription de crédits ou location de véhicules.

Au-delà de l'impact psychologique, les conséquences peuvent être particulièrement lourdes pour les victimes, qui peuvent se retrouver impliquées dans des procédures judiciaires et contraintes de démontrer qu'elles ne sont pas à l'origine des faits reprochés.

Protéger son identité c'est protéger sa liberté

Chaque jour, des centaines de personnes voient leur identité être utilisée à leur insu. Un justificatif envoyé à la hâte, un mot de passe faible, une information partagée sans y penser ...

LES BONS RÉFLEXES AU QUOTIDIEN

Ne communiquez jamais d'informations personnelles sensibles

par messagerie, par téléphone ou sur Internet, ni de documents d'identité (pièce d'identité, fiche de paie, avis d'imposition, RIB…) à des personnes ou organismes que vous n'avez pas authentifiés avec certitude.

Marquez les copies des documents d'identité que vous transmettez

inscrivez par-dessus le motif de l'envoi, la date et le destinataire pour éviter que vos documents ne soient réutilisés à des fins frauduleuses. Pour vos documents numérisés, le service **filigrane.beta.gouv.fr** permet d'ajouter un marquage personnalisé.

Ne donnez que le minimum d'informations personnelles

sur un site ou un service en ligne sur lequel vous vous enregistrez. Lorsque cela est possible, utilisez des pseudonymes au lieu de vos nom et prénom.

Vérifiez les paramètres de confidentialité de vos informations personnelles

(numéro de téléphone, adresse de messagerie…) et de vos publications sur les réseaux sociaux pour éviter qu'elles ne soient visibles publiquement.

Détruisez les documents qui contiennent des informations personnelles avant de les jeter.

ils pourraient être récupérés et utilisés par des criminels à vos dépens.

N'ouvrez pas les messages suspects et ne cliquez jamais sur les liens

provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu mais dont le contenu est inhabituel ou vide. Vous risqueriez d'être infecté par un virus qui pourrait donner l'accès à vos informations personnelles.

Ne communiquez jamais d'informations personnelles sensibles

par messagerie, par téléphone ou sur Internet, ni de documents d'identité (pièce d'identité, fiche de paie, avis d'imposition, RIB…) à des personnes ou organismes que vous n'avez pas authentifiés avec certitude.

Activez la double authentification

lorsque le site ou le service le permettent, pour renforcer le niveau de sécurité d'accès à vos comptes et en limiter les risques de piratage.

Mettez régulièrement à jour vos appareils et leurs logiciels ou applications

afin de corriger les failles de sécurité qui pourraient permettre à un cybercriminel de prendre le contrôle de vos équipements et accéder à vos informations personnelles.

Que faire en cas d'usurpation d'identité ?

Réagir rapidement est essentiel pour limiter les dommages et rétablir votre identité.

> L'usurpation d'identité peut arriver à chacun. L'important c'est de savoir comment réagir !

COMMENT SAVOIR SI L'ON EST VICTIME D'USURPATION D'IDENTITÉ ?

Soyez attentif aux signaux d'alerte suivants :

- Courriers ou mails de créanciers inconnus
- Comptes ouverts sans votre accord
- Refus de crédit inexpliqué
- Activité inhabituelle sur vos comptes
- Réception de documents officiels qui ne vous concernent pas

Si un doute persiste, agissez rapidement. Plus tôt vous réagissez, moins les impacts peuvent être graves.

1 SÉCURISER VOS COMPTES IMMÉDIATEMENT

Changez tous vos mots de passe en commençant par vos mails, vos accès bancaires et les compte sensibles. Activez la double authentification pour où cela est possible. Vérifiez vos appareils connectés et déconnectez ceux que vous ne connaissez pas.

2 INFORMEZ VOTRE BANQUE ET VOS PRESTATAIRES

Contactez votre banque pour vérifier les opérations en cours et faire opposition si nécessaire. Prévenez également vos opérateurs, assureurs et autre services concernés.

3 SIGNALEZ L'USURPATION

Rendez-vous sur la plateforme officielle : www.cybermalveillance.gouv.fr pour effectuer un signalement. Vous serez guidé dans les démarches à suivre.

4 DÉPOSEZ PLAINTE

Rendez-vous au commissariat ou à la gendarmerie avec toutes les preuves en votre possession (mails, relevés, captures d'écran ...). La plainte est essentielle !

5 SURVEILLEZ VOS COMPTES

Dans les semaines à venir, restez vigilant. Vérifiez régulièrement vos relevés bancaires, votre boite mail et vos compte en ligne pour détecter tout activité suspecte.

PRÉCAUTIONS FINANCIÈRES

L'usurpation d'identité peut avoir des conséquences financières importantes.

- Demandez l'opposition sur vos moyens de paiement (cartes, chèques). Surveillez vos comptes quotidiennement.
- Vérifiez votre solvabilité auprès de la Banque de France (service FICP et FCC).
- En cas de crédit frauduleux, contestez par écrit auprès des organismes et joignez votre plainte.
- Activez les alertes SMS/e-mail de votre banque pour être informé de toute opération.

BESOIN D'AIDE ?

Vous n'êtes pas seul. Des professionnels sont à votre disposition

FRANCE VICTIMES

Réseau national d'aide aux victimes présent partout en France

Numéro d'aide 7j/7j :
116 006 (appel gratuit)

france-victimes.fr

CYBERMALVEILLANCE.GOUV.FR

Information, assistance et dépôt de signalement en ligne.

Numéro (Lun - Ven 9h -18h) :
01 8970 80 90

cybermalveillance.gouv.fr

Cyber Harcelement
la violence invisible qui détruit en silence

Le but de l'attaquant

Utiliser les outils numériques pour cibler une personne de manière répétée dans le but de lui nuire. L'objectif est l'atteinte et la dégradation des conditions de vie de la personne qui en est victime.

Le cyberharcèlement désigne l'ensemble des comportements malveillants répétés exercés par le biais des outils numériques. Il peut prendre de nombreuses formes : insultes, menaces, intimidations, diffusion de rumeurs, usurpation d'identité, publication de contenus humiliants ou encore partage de photos et de vidéos sans le consentement de la victime. Ces agissements peuvent être le fait d'une seule personne ou d'un groupe, et se dérouler sur les réseaux sociaux, les messageries instantanées, les forums, les plateformes de jeux en ligne ou tout autre espace numérique.

Les conséquences pour les victimes sont souvent profondes et durables. Le cyberharcèlement peut entraîner une perte de confiance en soi, de l'anxiété, des troubles du sommeil, une dépression, un isolement social, un décrochage scolaire ou professionnel et, dans les situations les plus graves, conduire à des actes d'automutilation ou à des pensées suicidaires.

Reflexe à avoir

NE PAS RÉPONDRE AUX MESSAGES

Ne pas répondre aux messages blessants ou provocants. Cela évite d'envenimer la situation.

EN PARLER À UNE PERSONNE DE CONFIANCE

Parlez-en à un ami, un adulte, un enseignant ou un membre de votre famille. Rompre le silence, c'est aussi se libérer.

CONSERVER DES PREUVES

Faites des captures d'écran des messages, des profils et des publications. Ces preuves peuvent être utiles.

VERROUILLER VOS COMPTES

Passez vos profils en privé et vérifiez vos paramètres de confidentialité.

SIGNALER SUR LES PLATEFORMES

Utilisez les outils de signalement intégrés (bouton "Signaler') sur les réseaux sociaux, jeux en ligne ...

SIGNALER AUPRÉS DES MOTEURS DE RECHERCHE

Demandez le déréférencement de contenus nuisibles via les formulaires de signalement (Google, Bing etc ...)

CONTACTER LA POLICE

Déposez plainte dans un commissariat ou à la gendarmerie ou signalez en ligne sur : www.pre-plainte-en-ligne.gouv.fr

COMMENT AIDER UNE VICTIME

° Ne likez pas, ne commentez pas, ne partagez pas les contenus abusifs

° Signalez les contenus et les comptes

° Soutenez la victime avec bienveillance

° Encouragez-la à en parler à une personne de confiance ou un professionnel

COMMENT RÉAGIR EN TANT QUE PARENT

(Dans le cas d'un enfant subissant du harcelement)

° Ecoutez sans minimiser

° Rassurez votre enfant

° Aidez-le à faire les bons signalements

° Accompagnez-le dans ses démarches

° Dialoguez réguliérement sur sa vie numérique

La prise de conscience de la réalité de ces atteintes est primordiale et permet la libération de la parole et la révélation des faits.

Pour t'aider, une grille d'évaluation du danger face au harcèlement entre jeunes est à ta disposition afin de mieux évaluer la situation et pouvoir l'anticiper.

Évaluer sa situation face au harcelement

POUR LES ENFANTS (9+) ET ADOS

Je m'appelle :		Tes réponses		
		Jamais	De temps en temps	Très souvent
Au cours de la journée	Je n'ai pas envie d'aller à l'école			
	On m'insulte/se moque de moi, on me tape			
	Mes notes ont baissé			
À la cantine	Je mange seul			
	On me jette de la nourriture			
	On ne me laisse pas manger tranquillement			
Dans mes loisirs	On m'isole, me met à l'écart			
	On se moque de moi			
	On me cache mes affaires			
À la maison	J'ai du mal à m'endormir, je me réveille, je fais des cauchemars...			
	J'ai mal à la tête/au ventre			
	J'ai du mal à faire mes devoirs quand je rentre à la maison			
Sur internet	Je reçois des messages menaçants			
	Je sais que des photos/messages circulent sur moi sans mon accord			
	Des photos intimes de moi sont diffusées sur les réseaux sociaux sans mon consentement			
	Je suis victime d'insultes à caractère sexuel			
Dans la rue	J'ai peur d'être seul dans la rue			
	On me vole mes affaires/mon argent de poche			
	On me suit en ricanant			
Comment je me sens ?	Je me sens triste			
	Je me sens seul			
	J'aimerais bien qu'on m'aide			
Sous-total			Nombre de cases cochées x 3	Nombre de cases cochées x 4
TOTAL			Additionner le résultat des deux cases jaunes	

Source : www.masecurite.interieur.gouv.fr

0 à 6 : Tu sembles ne pas être victime de harcèlement. Si tu connais un ami qui a besoin d'aide, n'hésite pas à lui donner le numéro du **3018** pour lutter contre les cyberviolences, le **119** contre les maltraitances, ou le **3020** en cas de harcèlement à l'école.

7 à 13 : Tu sembles vivre des situations parfois difficiles dont tu pourrais parler à un adulte de confiance de ton entourage pour être aidé. Si tu ne sais pas à qui en parler ou si c'est difficile de le faire, appelle le 3018 en cas de cyberviolences, le 119 si tu es victime de maltraitances ou le 3020 si les problèmes ont lieu à l'école. Un personnel de ton école ou de ton collège peut t'aider.

14 à 20 : Tu évoques des situations de harcèlement dont tu es victime et qui doivent cesser. Pour t'aider, appelle le 3018 en cas de cyberviolences, le 119 si tu es victime de maltraitance ou le 3020 si les problèmes ont lieu à l'école. Il faut le signaler rapidement à un adulte de ton école ou de ton collège et envisager avec les parents d'en parler à la police ou à la gendarmerie.

21 à 27 : Tu es manifestement victime de harcèlement. Tu as besoin d'aide pour faire rapidement cesser ces situations. Le harcèlement est puni par la loi. Pour t'aider, appelle le 3018 en cas de cyberviolences, le 119 si tu es victime de malt raitance ou le **3020** si les problèmes ont lieu à l'école. Il faut immédiatement le signaler à un adulte de ton école ou de ton collège et envisager avec les parents d'en parler à la police ou à la gendarmerie.

28 à 33 : Ce que tu subis est inacceptable. Pour t'aider, appelle le numéro du 3018 pour lutter contre les cyberviolences, le 119 contre les maltraitances ou le 3020 si le harcèlement a lieu à l'école. Parles-en à des adultes de confiance autour de toi, le harcèlement est puni par la loi, et tu es en droit de porter plainte pour que celles ou ceux qui te font du mal soient sanctionnés. Il faut immédiatement le signaler à un adulte de ton école ou de ton collège.

Plus de 34 : Tu as bien fait de remplir ce questionnaire car ta situation est grave ! Ce que tu subis est inacceptable. Pour t'aider, appelle le numéro du 3018 pour lutter contre les cyberviolences, le 119 contre les maltraitances ou le 3020 si le harcèlement a lieu à l'école. Parles-en a des adultes de confiance autour de toi, le harcèlement est puni par la loi et tu es en droit de porter plainte pour que celles ou ceux qui te font du mal soient sanctionnés. Il faut immédiatement le signaler à un adulte de ton école ou de ton collège

CONSEIL NATIONAL DES BARREAUX

LES AVOCATS

PRÉSENTE

Alice au Pays du Cyberharcèlement

En ligne, le harcèlement devient un cauchemar.
Protégez-vous, faites appel à un avocat dès les premiers signes.

RENDEZ-VOUS SUR AVOCAT.FR

Campagne “citoyen numérique”

Tout au long de ce magazine, vous avez pu découvrir plusieurs visuels réalisés par le Conseil national des barreaux. Cette campagne de sensibilisation nous a particulièrement marqués, tant par son impact visuel que par la pertinence des messages qu’elle véhicule.

À cette occasion, nous avons échangé avec Catherine Gazzeri, avocate, membre élue et présidente de la commission Communication du Conseil national des barreaux.

Catherine Gazzeri
AVOCATE MEMBRE ÉLUE ET PRÉSIDENTE DE LA COMMISSION COMMUNICATION DU CONSEIL NATIONAL DES BARREAUX

Qu’est-ce qui vous a conduit à lancer la campagne “Citoyen numérique” ?

Cette campagne est née d’un constat très clair : nos usages numériques explosent, mais la connaissance des droits qui les accompagnent reste encore insuffisante. Aujourd’hui, les citoyens réalisent leurs démarches administratives en ligne, échangent sur les réseaux sociaux, utilisent des outils d’intelligence artificielle, effectuent des achats à distance ou stockent des données personnelles sur de nombreuses plateformes. Pourtant, beaucoup ignorent encore les risques juridiques liés à ces usages.

Le Conseil national des barreaux suit ces évolutions de près grâce au Baromètre de l’accès au droit réalisé chaque année avec l’institut indépendant Odoxa. Les résultats montrent un décalage important entre l’intensité des usages numériques et le niveau d’information des citoyens sur des sujets comme le cyberharcèlement, l’usurpation d’identité ou encore la protection des données personnelles.
L’objectif de la campagne “Citoyen numérique” est donc double : rappeler que le droit s’applique pleinement dans l’espace numérique et donner aux citoyens des repères simples pour mieux comprendre leurs droits et adopter les bons réflexes.

Dans quels types de situations faut-il envisager de consulter un avocat spécialisé en droit du numérique ?

Le réflexe avocat doit intervenir beaucoup plus tôt qu’on ne le pense. Qu’il s’agisse de cyberharcèlement, d’usurpation d’identité, de piratage de comptes, d’atteinte à l’e-réputation, de diffusion non autorisée de contenus, de fraude bancaire en ligne, de litiges liés aux plateformes ou aux données personnelles, l’avocat ne sert pas uniquement à engager une procédure judiciaire. Il peut intervenir très en amont pour : analyser la situation, qualifier juridiquement les faits, sécuriser les preuves, orienter les démarches ou encore faire retirer rapidement des contenus.Dans l’univers numérique, la rapidité de réaction est essentielle. Plus une situation est prise en charge tôt, plus il est possible d’en limiter les conséquences.

Quels sont les premiers réflexes à adopter en cas de fraude, de harcèlement ou d’atteinte à sa réputation en ligne ?

Le premier réflexe est de conserver son sang-froid et de préserver les preuves.
Très souvent, les victimes ont le réflexe de supprimer immédiatement les contenus ou de fermer leurs comptes. Pourtant, en matière numérique, les captures d’écran, les URL, les échanges, les mails ou les historiques de connexion peuvent constituer des éléments déterminants.

Il faut également sécuriser rapidement ses accès (mots de passe, double authentification), signaler les contenus ou comptes concernés auprès des plateformes, prévenir sa banque en cas de fraude financière et déposer plainte lorsque cela est nécessaire.
Enfin, il ne faut pas rester isolé face à ces situations. L’accompagnement juridique permet souvent de reprendre le contrôle plus rapidement.

Pourquoi est-il important de conserver des preuves avant toute suppression ou signalement ?

Parce qu’en matière numérique, la preuve est souvent fragile et volatile. Un contenu peut disparaître très rapidement : un compte peut être supprimé, une story peut expirer, un message peut être effacé ou un contenu peut être modifié.
Sans preuve, il devient beaucoup plus difficile d’identifier les auteurs, d’établir les faits ou de démontrer la répétition dans les cas de cyberharcèlement.
Le numérique laisse des traces, mais encore faut-il les conserver correctement pour qu’elles puissent être exploitées juridiquement.

Quels retours avez-vous reçus depuis le lancement de la campagne ? A-t-elle permis de mieux faire comprendre le rôle des avocats face aux risques numériques ?

Nous avons eu des retours très positifs depuis le lancement de la campagne. Ce qui est encourageant, c’est que nous avons réussi à capter l’attention du grand public et à ouvrir un véritable questionnement autour des usages numériques et des droits qui y sont associés.

La campagne semble avoir trouvé un écho important. En seulement trois semaines, les contenus “Citoyen numérique” ont généré près de 3 millions d’impressions sur TikTok, ce qui montre que ces sujets suscitent un réel intérêt et concernent très largement le public.

Au-delà des chiffres, l’objectif était surtout de provoquer une prise de conscience : rappeler que le droit ne s’arrête pas aux écrans et que les citoyens ne doivent pas rester seuls face aux difficultés rencontrées en ligne.
La campagne permet aussi de mieux faire comprendre que l’avocat peut intervenir très en amont, dans une logique de prévention, de conseil et d’accompagnement, et pas uniquement lorsqu’un contentieux est déjà engagé.

Guiddy AKADEMY

HTTPS://GUIDDY.FR

95%

des cyberattaques réussies exploitent une erreur humaine.

FAITES DE VOS COLLABORATEURS VOTRE PREMIER REMPART

FORMATION CYBERSÉCURITÉ POUR LES COLLABORATEURS

La meilleure protection reste l'humain. GUIDDY Akademy aide vos collaborateurs à adopter les bons réflexes face aux cybermenaces grâce à des cas réels, des conseils pratiques et une approche accessible à tous.

ATELIER "LES BONS RÉFLEXES CYBER"

- **Situations du quotidien :** Analyse d'e-mails frauduleux, arnaques courantes et erreurs à éviter.
- **Conseils immédiatement applicables :** Des réflexes simples à mettre en œuvre dès le retour au bureau.
- **Accessible à tous :** Sans jargon technique, pour tous les collaborateurs.
- **Exemples concrets :** Basés sur des cyberattaques réelles et des situations vécues.

DURÉE	FORMAT	MÉTHODE
3H30	En direct sur Teams	Classe Virtuelle

INTERVENANT EXPERT

Arnaud Leroy

Formateur Cybersécurité - Guiddy Akademy

AGENDA DES SESSIONS

Petits groupes pour favoriser les échanges.

16 SEPT. 26	13H30 - 17H00
06 OCT. 26	13H30 - 17H00
04 NOV. 26	13H30 - 17H00
16 DÉC. 26	13H30 - 17H00

Besoin d'un format Intra ?

Sessions sur-mesure adaptées à vos contraintes métiers et outils.

CENTRE CERTIFIÉ

PRISE EN CHARGE À 100% POSSIBLE

Qualiopi processus certifié RÉPUBLIQUE FRANÇAISE

Organisme certifié Qualiopi. Nos formations sont éligibles aux financements via vos budgets de formation **OPCO**. Notre équipe vous accompagne dans l'ensemble des démarches de prise en charge administrative.

INSCRIPTIONS OUVERTES

Scannez le QR Code pour accéder à tous nos dates choisir votre session Cyber ou et compléter votre inscription.

UN CADEAU OFFERT
POUR LES 10 PREMIERS INSCRITS

Inspiré de l'univers pédagogique SENTINELLE by GUIDDY

FAIRE DE CHAQUE ACTEUR UN BOUCLIER CYBER

CREDITS

Rédacteurs : Arnaud LEROY
Design Graphique : Arnaud LEROY
Traduction Anglaise : Maëva ASTORGA
Parrain du magazine : Guillaume POUPARD

Nous remercions toutes les personnes ayant pris part à ce numéro

Juillet/Septembre 2026

www.cyberit-magazine.com