RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR

Assistance et prévention en sécurité numérique

RAPPORT D'ACTIVITÉ 2022

Dispositif national d'assistance aux victimes d'actes de cybermalveillance, de sensibilisation des publics aux risques numériques et d'observation de la menace.

www.cybermalveillance.gouv.fr

SOMMAIRE

Directeur de la publication : Jérôme Notin
Coordination éditoriale : Béatrice Hervieu, Clémentine Lemal, Stella Azzoli et Maïlys Derville
Conception graphique : Elsa Godet
Crédits photos :
p. 3 : @ Patrick Gaillardin
p. 3 : @ Pierre Morel
p. 8 : @ GIP ACYMA
pp. 9, 14 : @ Aurore Lejeune

www.cybermalveillance.gouv.fr
contact@cybermalveillance.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

ÉDITOS

2022 ANNÉE DES 5 ANS


© Patrick Gaillardin

« À l'heure où les outils et les services numériques sont devenus indispensables à nos vies quotidiennes et professionnelles, l'activité cybercriminelle continue de se maintenir à un niveau trop élevé. L'ANSSI a en effet constaté un regain d'activité cybercriminelle fin 2022, en particulier à l'encontre des collectivités territoriales et des établissements de santé. Chaque jour, les données sensibles de nos concitoyens et de nos organisations sont convoitées pour être revendues à prix d'or sur le *darknet*. Et les arnaques que mettent en œuvre ces attaquants 3.0 ont un véritable impact dans la vie de leurs victimes.

Dans ce contexte, le GIP ACYMA continue d'apporter une réponse essentielle et de qualité pour lutter contre la cybermalveillance à travers des actions d'assistance, de prévention et d'observation de la menace. Depuis son lancement fin 2017, la fréquentation de la plateforme d'assistance cybermalveillance.gouv.fr n'a cessé de croître pour atteindre plus de 8,3 millions de visiteurs en 5 ans. C'est la preuve que le GIP gagne chaque année en notoriété.

Face à une menace qui se professionnalise, le GIP ACYMA est à un tournant de son histoire. L'année 2022 a vu naître plusieurs actions structurantes en partenariat avec l'ANSSI telles que le Cybermoi/s ou le projet de filtre anti-arnaque qui répondent au besoin croissant d'accompagnement des victimes. Les petites et moyennes entreprises, les collectivités territoriales, avec des niveaux de protection moindre, sont particulièrement ciblées par les cyberattaques. Le GIP, fort de son positionnement à la croisée des enjeux d'assistance et de prévention, s'est engagé à les protéger.

Le passage à l'échelle est un enjeu clé pour Cybermalveillance.gouv.fr. L'implication de ses membres, la détermination de ses partenaires et l'engagement des agents du GIP font la force du dispositif. Merci à tous ceux qui œuvrent au quotidien pour relever le défi de notre sécurité numérique. »

Vincent STRUBEL
*Président Directeur Général du GIP ACYMA**
*et Directeur Général de l'ANSSI***

« 2022 a été une année particulièrement singulière pour Cybermalveillance.gouv.fr.


© Pierre Morel

Une année *charnière*, car, 5 ans après son avènement, la plateforme vient de passer un cap, avec près de 3,8 millions de visiteurs uniques et 280 000 demandes d'assistance, soit presque autant que les 4 années précédentes réunies pour un total de plus de 8 millions de VU et 600 000 parcours d'assistance.

Une année *prolifique* : parce qu'après 2 années de pandémie durant laquelle la menace a été exacerbée, les attaques n'ont cessé de croître et de se contextualiser, ainsi qu'en témoignent les 51 cybermalveillances identifiées et traitées par le dispositif. *Prolifique* également, avec plus de 200 contenus en ligne, enrichis cette année de nouvelles publications spécialement dédiées aux familles ainsi qu'aux collectivités avec le guide juridique édité avec la CNIL et la *Méthode clé en main* de sensibilisation cyber, réalisée avec l'AMF.

Une année placée sous le signe de l'*innovation* avec le lancement d'*Assistance Cyber en ligne* pour accéder, à tout moment, à un diagnostic cyber, un service déjà adopté par plus d'une centaine d'organisations. Et le développement de projets structurants, dans les lesquels Cybermalveillance.gouv.fr jouera ces prochains mois un rôle déterminant, tels que la future solution de filtre anti-arnaque ou la mise en place de l'équivalent numérique du 17Cyber, qui permettra d'assister encore mieux les victimes de cybermalveillance.

Autant de projets qui, avec le concours de ses membres, l'engagement des professionnels référencés et labellisés et la mobilisation des agents du GIP*, renforceront l'empreinte du dispositif auprès de l'ensemble de ses parties prenantes pour s'inscrire pleinement dans sa démarche d'intérêt public, *au cœur de l'action cyber*. »

Jérôme NOTIN
*Directeur Général du GIP ACYMA**

**GIP ACYMA : Groupement d'intérêt Public Actions contre la cybermalveillance*
*** ANSSI : Agence nationale de la sécurité des systèmes d'information*

QUI SOMMES-NOUS ?

Issu de la Stratégie numérique du Gouvernement présentée le 18 juin 2015, le Groupement d'Intérêt Public Action contre la cybermalveillance (GIP ACYMA) a été créé en 2017 et vient de fêter ses cinq ans.

Quel champ d'action ? Le GIP ACYMA agit contre la cybermalveillance au sens large, sous toutes ses formes et manifestations, quels que soient les supports (ordinateurs, téléphones, réseaux sociaux, systèmes d'information professionnels…) et le public (particuliers, entreprises, associations, administrations), tant qu'il y a une victime, et hors du périmètre d'intervention de l'ANSSI (administrations, opérateurs d'importance vitale, opérateurs de services essentiels, fournisseurs de services numériques).

Quels publics ?

Extrait de l'arrêté du 3 mars 2017 portant approbation de la convention constitutive du groupement d'intérêt public pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance, modifié le 24 décembre 2020.

La dénomination du Groupement est : « Groupement d'intérêt public pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance ». Son sigle est « GIP ACYMA ». Le Groupement a pour objet d'assurer :

- *Une mission d'intérêt général de lutte contre les cybermenaces, portant en particulier sur la prévention, l'accompagnement et l'assistance aux particuliers, aux entreprises, aux associations et aux administrations victimes d'actes de cybermalveillance par la mise en place d'un « guichet unique ». Plus particulièrement, le groupement s'attachera d'une part, à permettre la mise en relation avec des acteurs de proximité capables de procéder à la sécurisation et à la reprise d'activité des victimes et d'autre part, à fournir l'aide aux démarches administratives requises pour le dépôt de plainte ;*
- *la sensibilisation du public sur les enjeux de la sécurité et de la protection de la vie privée numérique en lien avec les autorités compétentes et le développement de campagnes de prévention en la matière ;*
- *la fourniture d'éléments statistiques offrant une vue réelle et consolidée de la menace cyber afin de mieux l'anticiper à travers la création d'un observatoire dédié.*

Quelles sont les missions du GIP ?

Pour lutter contre les actes de cybermalveillance, le GIP ACYMA mise sur une stratégie d'action articulée autour de trois axes clés :

1. ASSISTER LES VICTIMES D'ACTES DE CYBERMALVEILLANCE

grâce à la plateforme Cybermalveillance.gouv.fr, qui assure un service d'assistance en ligne aux victimes de cybermalveillance et une mise en relation avec des professionnels en cybersécurité référencés sur l'ensemble du territoire.

2. PRÉVENIR LES RISQUES ET SENSIBILISER SUR LA CYBERSÉCURITÉ

avec la réalisation de publications et de campagnes de sensibilisation et de prévention contre les cybermenaces, grâce à des contenus sous différents formats (vidéos, fiches, kit de sensibilisation, affiches, stickers, mémos…) et à travers l'accompagnement à la sécurisation des systèmes d'information des publics professionnels (entreprises, collectivités et associations) par des prestataires labellisés ExpertCyber.

3. OBSERVER ET ANTICIPER LE RISQUE NUMÉRIQUE

grâce à la remontée et l'analyse de données d'utilisation, qui permet d'accroître la connaissance de la menace numérique et ainsi d'adapter les actions d'assistance et de sensibilisation du dispositif Cybermalveillance.gouv.fr.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

GOUVERNANCE ET ORGANISATION DU GIP

Gouvernance

Le GIP ACYMA est composé de 56 membres, d'un Président du Conseil d'administration et d'un Directeur Général. Les membres sont répartis en 4 collèges représentant l'ensemble de l'écosystème :

- **Les étatiques :** ministères ;
- **Les utilisateurs :** associations de consommateurs, d'aide aux victimes, clubs d'utilisateurs et organisations professionnelles ;
- **Les prestataires :** syndicats et fédérations professionnelles ;
- **Les offreurs de solutions et de services :** constructeurs, éditeurs, opérateurs, sociétés de services, etc.

Le GIP est organisé autour d'une Assemblée générale et d'un Conseil d'administration qui déterminent les orientations du Groupement.

Organisation

17
agents en 2022

dont 8 mis à disposition par des membres du GIP :

- ministère de l'Intérieur et des Outre-mer ;
- ANSSI,
- ministère de la Justice ;
- ministère des Armées ;
- ministère de l'Éducation Nationale et de la Jeunesse.

Subvention exceptionnelle de France Relance de

400 000 €

+

2,3 millions €

de budget en 2022

NOS MEMBRES

PREMIÈRE MINISTRE
MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE
MINISTÈRE DE L'INTÉRIEUR ET DES OUTRE-MER
MINISTÈRE DE LA JUSTICE
MINISTÈRE DES ARMÉES
MINISTÈRE DE L'ÉDUCATION NATIONALE ET DE LA JEUNESSE

Nouveaux membres en 2022

Collège utilisateurs :

Collège offreurs de solutions et services :

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

PAROLES DE MEMBRES

« Un accompagnement rapide d'une grande utilité »

Cybermalveillance.gouv.fr est très actif depuis sa création. Son action d'accompagnement rapide en cas d'attaque ou suspectée est d'une grande utilité. Malheureusement les cyberattaques ne sont pas près de disparaître. Aussi, au vu des réalisations de ces dernières années, je leur souhaite de continuer sur ce même rythme et avec ce même engagement pour la sécurité numérique de tous.

Antoine TRILLARD
Président du CoTer Numérique, DSI de la Ville de Chelles

« Une écoute et une proximité »

Cybermalveillance.gouv.fr c'est d'abord une écoute pour les publics TPE, particuliers et collectivités. C'est aussi des conseils, comme le guide que nous avons coédité à ses côtés cette année, et une proximité pour répondre au mieux aux besoins de ses 3 publics. Nous lui souhaitons de continuer à grandir et à développer ses services et son efficacité face à la cyber.

Bertrand PAILHÈS
Directeur des technologies et de l'innovation de la CNIL

« Une action essentielle »

L'action de Cybermalveillance.gouv.fr est essentielle notamment pour apporter une réponse aux profils les plus vulnérables, face à la menace, et le label ExpertCyber créé en 2021 permet, quant à lui, d'apporter une vraie réponse sur le terrain aux victimes. Je félicite les équipes pour le chemin parcouru en 5 ans et leur donne rendez-vous pour les 10 ans, avec toujours plus de partenaires de confiance pour les aider dans cette mission.

Pierre-Yves HENTZEN
Président de Stormshield

« Une contribution extrêmement importante »

Cybermalveillance.gouv.fr, c'est une contribution extrêmement importante au développement de la culture de gestion du risque, qui fait beaucoup défaut en France. Ce que nous lui souhaitons, ce n'est pas seulement de la pérennité, mais surtout du développement, une plus grande visibilité, une plus grande notoriété, avec des moyens renforcés pour tenir une place centrale dans la société du numérique.

Alain BAZOT
Président d'UFC–Que Choisir

« Faire progresser la cyber au sein des organisations »

Le CLUSIF soutient Cybermalveillance.gouv.fr depuis ses débuts avec un double objectif : faire progresser la cybersécurité au sein des organisations et sensibiliser le public aux enjeux cyber. Comme le CLUSIF, Cybermalveillance.gouv.fr regroupe à la fois des acteurs du secteur privé et public pour partager des contenus synthétiques, faciles à diffuser surtout dans un contexte de surinformation. Pour les années à venir, nous souhaitons à Cybermalveillance.gouv.fr plus de visibilité et de partages pour continuer à porter des projets pertinents et ambitieux.

Benoît FUZEAU
Président du CLUSIF

« Une action essentielle dans la transformation numérique »

L'action de Cybermalveillance.gouv.fr est devenue essentielle dans la transformation numérique en mettant à la disposition de tous, des outils pragmatiques et pédagogiques. Son label ExpertCyber permet notamment de valoriser les prestataires informatiques, d'attester d'une vraie expertise et d'instaurer un environnement de confiance pour ses publics. C'est une belle réussite d'être parvenu à réunir à la fois des partenaires publics et privés pour contribuer à cette mission d'intérêt général. Pour les 5 années à venir, je souhaite à Cybermalveillance.gouv.fr d'asseoir sa notoriété et de poursuivre son développement avec le même dynamisme et l'implication de ses membres.

Delphine CUYNET
Directrice Générale de la Fédération EBEN

« Rassurer les entreprises et les accompagner au mieux dans leur dynamique de numérisation »

Nous ne pouvons que féliciter les équipes pour le chemin parcouru : en 5 ans, Cybermalveillance.gouv.fr a trouvé sa place, est parvenu à se faire connaître et à faire croître son audience de manière significative. Nous lui souhaitons 5 ans de plus avec une croissance toujours aussi forte pour continuer de rassurer les entreprises et pouvoir les accompagner au mieux dans cette dynamique de numérisation importante pour notre économie. Le ministère est prêt à les accompagner et à renforcer les synergies avec ses dispositifs, notamment France Num. Nous lui souhaitons longue vie !

Aurélien PALIX
Sous-Directeur Réseaux et Usages Numériques, Ministère de l'Économie et des Finances et de la Souveraineté industrielle et numérique

LES FAITS MARQUANTS

Janvier

1er janvier L'ANCT[1] et l'U2P[2] rejoignent Cybermalveillance.gouv.fr

18 janvier Diffusion d'une Alerte Cyber pour correction d'une faille de sécurité critique Microsoft Windows et Windows Server

27 janvier Conférence en ligne *Cybersécurité, toutes les collectivités sont concernées !*, coorganisée par Cybermalveillance.gouv.fr, l'ANCT, la Gendarmerie nationale et l'AMF[3]

[1] *ANCT : Agence nationale de la cohésion des territoires*
[2] *U2P : Union des entreprises de proximité*
[3] *AMF : Association des Maires de France*

Avril

1er avril Participation au SecNumEco de Belfort

14 avril Webinaire bonnes pratiques pour l'AMRF[8]

15 avril Diffusion d'une Alerte Cyber pour correction d'une faille de sécurité critique Microsoft Windows et Windows Server

[8] *AMRF : Association des maires ruraux de France*

Richard Héral, fondateur de SWALI, reçoit son attestation de Julien Nizri, Directeur Général d'AFNOR Certification (Groupe AFNOR), et Jérôme Notin, Directeur Général de Cybermalveillance.gouv.fr

Février

10 février Intervention à la Préfecture de Région Normandie

10 février Participation à la 15e Université de l'AFCDP[4] à Paris

15 février Cybermalveillance.gouv.fr rejoint le Campus Cyber

16 février Intervention à l'École de Gendarmerie de Chaumont – 1re e-compagnie

17 février Diffusion d'une Alerte Cyber pour correction d'une faille de sécurité critique Apple iOS, iPadOS, macOS, Safari

21 février Campagne nationale France Télévisions *Cybersécurité : de vraies solutions existent*

[4] *AFCDP : Association Française des Correspondants à la protection des Données à caractère Personnel*

Mai

11 mai Conférence en ligne *Spam, phishing : comment les détecter et protéger votre boîte mail ?* co-organisée par Cybermalveillance.gouv.fr, Signal Spam et l'AFCDP

17 mai Publication de l'étude sur la cybersécurité dans les collectivités de moins de 3 500 habitants

17 mai Webinaire pour les Agences de l'eau

17 mai Intervention au séminaire du Sisse[9] pour les 20 Délégués auprès des Préfets de Région

18 mai Intervention à l'Agence de l'eau à Orléans et en webinaire

[9] *Sisse : Service de l'information stratégique et de la sécurité économiques*

Mars

1er mars Intervention lors du stage de prévention et gestion de crise de niveau 3 à l'IHEEF[5] de Poitiers

3 mars L'AMF, l'Institut des actuaires et la CNIL[6] rejoignent Cybermalveillance.gouv.fr

3 mars Webinaire pour l'AMRF[7]

9 mars Conflit en Ukraine : diffusion de mesures de vigilance en cybersécurité

[5] *IHEEF : Institut des hautes études de l'éducation et de la formation*
[6] *CNIL : Commission nationale de l'informatique et des libertés*
[7] *AMRF : Association des maires ruraux de France*

Juin

Cybermalveillance.gouv.fr : plus de 50 Cybermenaces traitées par l'assistant de diagnostic

1er juin Campagne de sensibilisation *Les freins des collectivités en matière de cybersécurité*

7/9 juin Participation au FIC[10] à Lille (14 000 visiteurs) : Cybermalveillance.gouv.fr remet le 200e label ExpertCyber et lance le module *Assistance Cyber en Ligne*

14 juin Participation au salon CoTer Numérique à Saint-Malo

14 juin Signature de la convention avec l'ANCT

15/16 juin Participation au salon IT Partners à Marne-la-Vallée (5 600 visiteurs)

17 juin Animation d'ateliers lors du stage prévention et gestion de crise de niveau 3 à l'EOGN[11] de Melun

21 juin Diffusion d'une Alerte Cyber pour correction d'une faille de sécurité critique Microsoft Windows et Windows Server (Follina)

29 juin Webinaire pour l'Agence de l'eau à Lyon

[10] *FIC : Forum International de la Cybersécurité*
[11] *EOGN : École des officiers de la Gendarmerie nationale*

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

Juillet

1er juillet Webinaire pour les acteurs de la médiation numérique de la Creuse

4 juillet Publication du guide juridique sur les obligations et les responsabilités des collectivités locales en matière de cybersécurité avec la CNIL

Août

23 août Diffusion d'une Alerte Cyber pour correction de failles de sécurité critiques Zimbra

Septembre

15 septembre Webinaire pour l'Agence de l'eau à Toulouse

16 septembre Podcast pour *lesbonclics.fr*

21 septembre Intervention à l'ENSP[12] auprès des référents sécurité économique du ministère de l'Intérieur

27 septembre Intervention lors de la journée des CNFS[13] à Lens

27 septembre Participation au NEC[14] à Lens

[12] *ENSP : École Nationale Supérieure de la Police*
[13] *CNFS : Conseiller numérique France Services*
[14] *NEC : Numérique En Commun[s]*

Octobre

Copilotage du Cybermoi/s
Lancement du Cyber Guide
et du Cyber Quiz Famille

4 octobre Participation au SecNumEco de Dijon

11 octobre Intervention à l'ENSP auprès des référents sécurité économique du ministère de l'Intérieur

12/15 octobre Participation aux Assises de la Cybersécurité à Monaco (3000 participants)

12 octobre Annonce de la création d'un Référentiel de compétences pour les prestataires de services en cybersécurité

13 octobre Journée de formation à la cybersécurité pour les enseignants de NSI[15] franciliens au cybercampus

17 octobre Cybermalveillance.gouv.fr a 5 ans

18 octobre Webinaire pour les médiateurs numériques de Guyane

20 octobre Participation au SecNumEco de Lons-le-Saunier

20 octobre Webinaire lesbonclics.fr/ Wetechcare.org pour les médiateurs numériques

24 octobre Diffusion de la campagne de sensibilisation TV Consomag réalisée en partenariat avec l'INC[16] sur les chaînes du groupe France Télévisions

25 octobre Webinaire organisé par HUBIK pour les médiateurs numériques

26 octobre Sensibilisation des députés à l'Assemblée nationale aux enjeux de la cybersécurité

[15] *NSI : Numérique et sciences informatiques*
[16] *INC : Institut national de la consommation*

Novembre

10/17 novembre Participation au Cisco Tour 2022 à Strasbourg et Marseille

16/17 novembre Participation au Cloud & Cyber Security Expo à Paris (9000 visiteurs)

22 novembre Diffusion de la *Méthode Cyber clé en main* pour les agents des collectivités avec l'AMF

22 novembre Participation au salon CBC[17] à Toulouse (1000 visiteurs)

23 novembre Intervention à l'ENSP auprès des référents sécurité économique du ministère de l'Intérieur

24 novembre Participation au Congrès de l'AMF et des Présidents d'Intercommunalité de France à Paris

24 novembre Participation aux Rencontres AGIR[18] à Paris

[17] *CBC : Cybersecurity business convention*
[18] *AGIR : Accompagnement par la Gendarmerie de l'Innovation de l'Industrie et de la Recherche*

Décembre

1er décembre Célébration du 5e anniversaire de Cybermalveillance.gouv.fr aux côtés de ses membres

6 décembre Webinaire organisé par CLCV[19] sur les principales menaces pour les particuliers sur Internet

14 décembre Intervention à l'ENSP auprès des référents sécurité économique du ministère de l'Intérieur

15 décembre Intervention à l'Agence de l'eau à Douai et en webinaire

[19] *CLCV : Association nationale de consommateurs et usagers*

Célébration du 5e anniversaire de Cybermalveillance.gouv.fr au Cercle National des Armées, aux côtés de ses membres.

NOS PRINCIPALES RÉALISATIONS

TOUS PUBLICS

Contenus de prévention et d'assistance publiés sur la plateforme

Au-delà des parcours permettant d'établir des diagnostics de la menace aux victimes et de les mettre en relation avec des prestataires référencés, Cybermalveillance.gouv.fr publie et enrichit régulièrement sa plateforme avec divers contenus thématiques de sensibilisation et de remédiation aux dangers du numérique pour informer tous ses publics à travers des fiches et articles de référence et d'actualité.

Au total, Cybermalveillance.gouv.fr a créé en 2022 :

- **3 FICHES PRATIQUES :** Que faire en cas de cyberattaque ? (2 versions dirigeants et collectivités), Mon site Internet est-il sécurisé ?
- **3 FICHES RÉFLEXES :** La fuite ou violation de données personnelles, Le cyberharcèlement, Le piratage d'un système informatique de particulier ;
- **3 CAMPAGNES DE COMMUNICATION** (France Télévisions, INC et Fables) ;
- **3 GUIDES** (Juridique coédité avec la CNIL, Cyber Guide Famille, Méthode de sensibilisation copubliée avec l'AMF) ;
- **UNE DIZAINE D'ARTICLES :** les 10 cybermalveillances les plus fréquentes, le piratage d'une boîte mail, le piratage de compte sur les réseaux sociaux, l'hameçonnage à la vignette Crit'Air…

Campagne nationale France Télévisions

Cybersécurité : de vraies solutions existent

Face à la recrudescence des cyberattaques liée à l'augmentation des usages numériques et en réponse à sa mission d'intérêt général, Cybermalveillance.gouv.fr a mené avec le groupe France Télévisions une campagne de sensibilisation de 3 spots destinée à tous les publics, diffusée sur les chaînes du groupe en février. En jouant sur l'humour et le décalage, elle invite les publics à s'intéresser au sujet de la cybersécurité et les interpelle sur le fait que de vraies solutions existent face aux risques numériques, notamment au travers des réponses qu'apporte la plateforme Cybermalveillance.gouv.fr.

Lancement du module *Assistance Cyber en Ligne*

Afin de rendre accessible au plus grand nombre son service de diagnostic et d'assistance aux victimes, Cybermalveillance.gouv.fr a lancé en juin 2022 *Assistance Cyber en Ligne*. Grâce à un module dynamique intégrable dans n'importe quelle page d'un site Internet, tout utilisateur victime d'une cybermalveillance peut accéder à un diagnostic en ligne directement depuis le site ayant intégré le service. Il peut alors accéder à des conseils personnalisés sur Cybermalveillance.gouv.fr et, s'il le souhaite, se mettre en relation avec un professionnel en cybersécurité référencé sur la plateforme. À ce jour, plus de 100 modules ont été intégrés sur des sites français.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

PARTICULIERS

90 % des sollicitations sur Cybermalveillance.gouv.fr proviennent du grand public. Afin d'accompagner les particuliers, le dispositif met en place des actions variées tout au long de l'année.

Conférence en ligne :
Spam, phishing : comment les détecter et protéger votre boîte mail ?
avec Signal Spam et l'AFCDP

Le 11 mai 2022 s'est tenue en direct une conférence en ligne sur les thèmes du spam et de l'hameçonnage, coorganisée par Cybermalveillance.gouv.fr, Signal Spam et l'AFCDP. La table ronde avait pour vocation d'expliquer aux internautes comment identifier et signaler ces menaces, les risques et conséquences possibles de ce type de messages et les bonnes pratiques à adopter pour s'en protéger.

Cybermoi/s

Dans le cadre du Cybermoi/s 2022, copiloté par l'ANSSI et Cybermalveillance.gouv.fr, le dispositif a produit 2 contenus spécifiques :

Campagne nationale 2022 TV-médias de sensibilisation à la cybersécurité

Afin de sensibiliser les particuliers aux risques numériques de la cybersécurité, Cybermalveillance.gouv.fr a renouvelé son partenariat avec l'INC pour réaliser une série d'émissions *Consomag* diffusées sur les chaînes du groupe France Télévisions du 24 octobre au 5 novembre 2022, ainsi que des capsules *La Minute Info*. Ces vidéos abordent les cybermenaces qui touchent les consommateurs et les bonnes pratiques à adopter pour s'en prémunir.

Lancement du *Cyber Guide Famille* et du *Cyber Quiz Famille*

Alors que la plateforme est majoritairement fréquentée par les particuliers, Cybermalveillance.gouv.fr et ses membres ont décidé de lancer un guide pédagogique spécialement dédié aux parents et aux enfants pour les sensibiliser aux risques numériques et aux bonnes pratiques et les accompagner dans leurs gestes quotidiens. Pour compléter ce guide pédagogique paru en septembre, Cybermalveillance.gouv.fr a également lancé en octobre le *Cyber Quiz Famille* : un jeu-concours destiné à faciliter le dialogue autour de la cybersécurité au sein du foyer.

NOS PRINCIPALES RÉALISATIONS

PROFESSIONNELS

Tout au long de l'année, Cybermalveillance.gouv.fr prend la parole régulièrement lors de nombreux événements. Au total, ce sont 130 interventions qui ont été données lors de temps forts tels que le FIC, IT Partners, les Assises de la Cybersécurité, AGIR ou encore Cloud & Cybersecurity Expo et au travers de conférences ou tables rondes sur l'ensemble du territoire.

200
labellisés ExpertCyber

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

Lancé en 2021, le label ExpertCyber a franchi le cap des 200 labellisés. Ainsi, lors du FIC 2022, Cybermalveillance.gouv.fr a remis le 200e label ExpertCyber à Richard Héral, fondateur de SWALI. Celui-ci a reçu son attestation de Julien Nizri, Directeur Général d'AFNOR Certification (Groupe AFNOR), et de Jérôme Notin, Directeur Général de Cybermalveillance.gouv.fr.

En complément du label ExpertCyber et afin de répondre à la demande en ressources qualifiées et de spécialistes en cybersécurité, Cybermalveillance.gouv.fr a annoncé à l'occasion de la 22e édition des Assises de la Cybersécurité, en collaboration avec le groupe AFNOR, le Campus régional de Cybersécurité et de Confiance numérique Nouvelle-Aquitaine (C3NA) et le Centre de formation de l'ANSSI (CFSSI), la création d'un Référentiel de compétences intégrant tous les aspects essentiels du métier de prestataire cyber de premier niveau (sécurisation, maintien en conditions opérationnelles et de sécurité, ainsi que remédiation). L'objectif est d'accompagner la montée en compétences des prestataires informatiques dans les domaines de la cybersécurité.

Parce que les collectivités sont particulièrement vulnérables face aux menaces, Cybermalveillance.gouv.fr a développé de nombreuses initiatives pour les sensibiliser et les responsabiliser à la cybersécurité.

Conférence en ligne *Cybersécurité, toutes les collectivités sont concernées !* **avec l'ANCT**

Le 27 janvier 2022, un webinaire d'information, de prévention et de solutions intitulé *Cybersécurité, toutes les collectivités sont concernées !* a été organisé par l'ANCT, en association avec Cybermalveillance.gouv.fr, la Gendarmerie nationale et l'AMF. Quelle que soit leur taille, les collectivités deviennent des cibles privilégiées des cybercriminels. Ainsi, la question n'est plus de savoir si elles seront victimes de cyberattaques mais quand et donc comment s'en prémunir. La conférence en ligne a permis aux experts présents de détailler les enjeux et les bons réflexes à adopter pour renforcer leur cybersécurité.

Étude sur la cybersécurité dans les collectivités de moins de 3 500 habitants

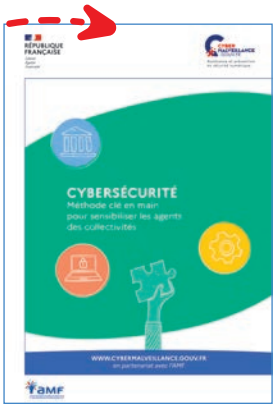
Pour mieux comprendre leurs usages numériques, identifier leurs besoins et ainsi leur apporter des réponses utiles et concrètes, Cybermalveillance.gouv.fr a mené une étude auprès des collectivités de moins de 3 500 habitants, qui représentent 91 % des communes en France. Publiés en mai 2022, les résultats de l'étude indiquent que ces publics sont peu informés et qu'ils sous-estiment l'importance du risque cyber. Par ailleurs, l'étude met en lumière de véritables freins à la sécurité numérique. Fort de ce constat et afin d'accompagner les collectivités dans leur appréhension de la cybersécurité, Cybermalveillance.gouv.fr a réalisé une campagne de sensibilisation sous forme de vidéos inspirées des fables de Jean de La Fontaine pour s'affranchir de ces barrières, un guide juridique en collaboration avec la CNIL et une *Méthode clé en main* de sensibilisation à la cyber à destination des agents des collectivités coéditée avec l'AMF.

Campagne de sensibilisation *Les freins des collectivités en matière de cybersécurité*

À travers cette étude, les collectivités ont exprimé plusieurs freins en matière de cybersécurité. Pour les sensibiliser à la sécurité numérique, lever ces obstacles et déconstruire les préjugés des élus et des directeurs généraux des services (DGS), Cybermalveillance.gouv.fr a réalisé une série de 4 films, illustrant les objections sous forme de parodies des fables de La Fontaine, pour interpeller ces derniers aux conséquences d'une cyberattaque. Chacune des vidéos se conclut par une morale de fable unique.

Guide sur les obligations et les responsabilités des collectivités locales en matière de cybersécurité avec la CNIL

Suite aux résultats de l'enquête, Cybermalveillance.gouv.fr a rédigé, en collaboration avec la CNIL, un guide relatif à leurs obligations et à leurs responsabilités en matière de cybersécurité. Publié en juillet 2022, ce guide a pour objectif d'informer les élus locaux et les agents territoriaux quant aux obligations liées à la protection des données personnelles, à la mise en œuvre des téléservices locaux et à l'hébergement des données de santé. Il rappelle également les différents types de responsabilités juridiques auxquels sont exposés les collectivités locales et leurs établissements publics en cas de cyberattaques ou de dommages liés à la responsabilité administrative, à la responsabilité civile et à la responsabilité pénale.



Diffusion de la *Méthode Cyber clé en main* pour sensibiliser les agents des collectivités avec l'AMF

L'étude menée par Cybermalveillance.gouv.fr auprès des collectivités de moins de 3 500 habitants met en exergue leur faible préparation vis-à-vis de l'enjeu cyber. C'est pourquoi Cybermalveillance.gouv.fr a souhaité, en partenariat avec l'AMF, membre du dispositif, proposer à chaque collectivité une méthodologie clé en main pour sensibiliser l'ensemble des agents, avec une approche à la fois théorique et pragmatique et une proposition de plan d'action concret et facilement réalisable, ainsi qu'un ensemble d'outils et de contenus pédagogiques dédiés. L'objectif de cette prévention ? Responsabiliser, préparer et former les agents pour être plus fort face au risque cyber.

Congrès des Maires

Le 23 novembre 2022, à Paris, Cybermalveillance.gouv.fr participait au 104e Congrès des maires et présidents d'intercommunalité de France pour y dévoiler sa méthodologie réalisée avec l'AMF. L'opportunité également d'intervenir lors d'une table ronde aux côtés du Commandement de la gendarmerie dans le Cyberespace (COMCyberGEND) et de la Police nationale sur le sujet de la sécurité numérique des communes et des EPCI*. Par ailleurs, Cybermalveillance.gouv.fr a pris part à un atelier sur les outils d'information et d'accompagnement à destination des maires et des EPCI aux côtés de CyberGEND, la Police nationale et l'ANSSI.

*Établissement public de coopération intercommunale

LES 5 ANS

Il y a 5 ans, Cybermalveillance.gouv.fr voyait le jour, en réponse à la Stratégie nationale pour la sécurité du numérique qui prévoyait la mise en place d'un dispositif national « destiné à porter assistance aux victimes d'actes de cybermalveillance ».
Le 1er décembre dernier, l'équipe du GIP a tenu à rassembler autour d'elle ses membres et ceux qui soutiennent le dispositif depuis ses débuts. Retour sur les moments clés.

« Nous sommes partis d'une page relativement blanche avec les 11 propositions du GT* interministériel [...] pour créer le dispositif d'assistance qui devait également apporter des messages de sensibilisation et permettre d'observer la menace. La première version de la plateforme [...] nous a permis de massivement diffuser du contenu, sous différentes formes : vidéos, kits de sensibilisation, flyers, mais aussi différents guides mis à disposition pour l'ensemble de nos publics. [...]

Les 1 250 prestataires de proximité, qui interviennent au quotidien pour aider les victimes sont l'ADN du dispositif. Il nous fallait des bras armés pour aider ces victimes, qu'il s'agisse d'entreprises frappées par des rançongiciels, de collectivités dont le site web a été défiguré ou de particuliers frappés par une fraude à la réparation informatique. [...]

En 5 ans, nous sommes passés de 200 000 à 3,8 millions de visiteurs. Et face à la menace qui augmente, nous pouvons considérer que le travail fait collectivement, par les membres et par l'ensemble des agents, a permis d'atteindre ces chiffres. »

Jérôme NOTIN
Directeur Général du GIP ACYMA

« L'idée initiale était de répondre aux besoins en termes d'assistance aux victimes [...] notamment grâce à une structure qui n'était pas forcément l'ANSSI. [...]

Le GIP ACYMA est né de cette intuition. Il s'est imposé car il découle d'une œuvre collective, avec une structure de GIP permettant justement de garder l'équilibre entre l'État, qui joue un rôle majeur, et nos partenaires, dans toutes leurs diversités, pour qu'ils soient membres et acteurs du GIP. [...]

Depuis sa création, le GIP s'est étoffé, a pris une place considérable et a acquis une notoriété [...] de manière extrêmement rapide. [...]

Je suis admiratif du travail, de l'énergie qui a été ainsi portée, de toutes ces idées, de toute cette innovation et surtout du fait que tout cela est concret et pratique. [...]

Les menaces vont continuer à se développer, les victimes vont continuer à être de plus en plus nombreuses et le GIP va continuer à être capable de s'adapter aux besoins de ces victimes. »

Guillaume POUPARD
Président Directeur Général du GIP ACYMA et Directeur Général de l'ANSSI

La soirée des 5 ans du dispositif Cybermalveillance.gouv.fr au Cercle National des Armées, le 1er décembre 2022.
Jérôme Notin, Jean-Noël Barrot et Guillaume Poupard

« Il fallait évidemment une brique, un guichet unique, quelque chose qui fasse rentrer la cybersécurité dans le quotidien de nos concitoyens, de nos petites entreprises et de nos petites collectivités qui, elles aussi, sont désormais la cible des assaillants. [...]

Cybermalveillance.gouv.fr s'est désormais installé dans le paysage comme guichet unique et point de repère pour la cybersécurité. Et 5 ans plus tard, on s'aperçoit, en regardant les chiffres, du succès de cette initiative. C'est 8 millions de visites cumulées sur le site avec près de 3,8 millions cette année contre 2,5 millions l'année dernière. C'est à la fois la manifestation de la menace qui augmente mais à n'en pas douter, c'est aussi une reconnaissance pour le travail du GIP, sous la direction de Jérôme et de ses équipes, pour faire connaître cette plateforme, qui est à disposition de chaque citoyen français lorsqu'il a des doutes, en prévention et lorsqu'il est victime, en remédiation avec un certain nombre d'outils. [...]

Parmi les chantiers qui sont devant nous et auxquels je souhaite que le GIP soit associé de la manière la plus étroite qui soit, il y a, entre autres, le filtre anti-arnaque dont le GIP est chef de file et qui nous permettra, à l'été 2024 – c'est-à-dire au moment des JO** – d'offrir à nos concitoyens un outil gratuit, facultatif, simple, qui les avertira par avance qu'ils se dirigent vers un site malveillant. [...]

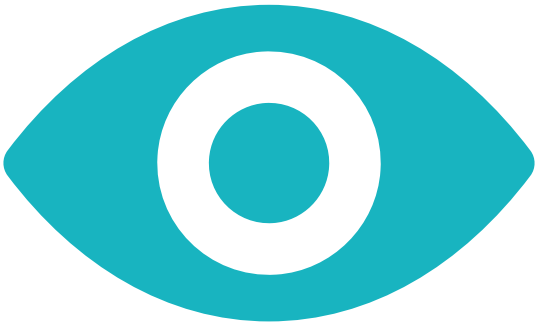
Merci à l'équipe d'ACYMA, à toute l'équipe de Cybermalveillance.gouv.fr pour le travail accompli, pour son rôle d'animation et d'éveil des consciences sur le sujet de la cybersécurité. »

Jean-Noël BARROT
Ministre délégué chargé de la Transition numérique et des Télécommunications

* Groupe de travail
** Jeux Olympiques

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique



ÉTAT DE LA MENACE

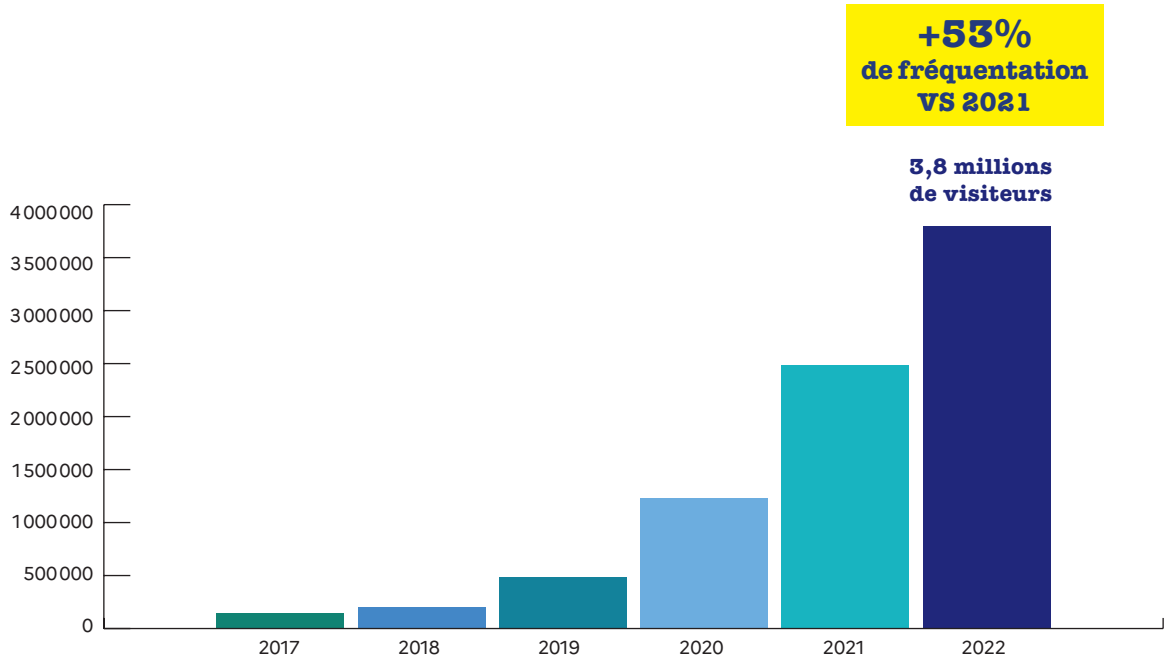
ÉTAT DE LA MENACE

L'ASSISTANCE AUX VICTIMES

2022 : un nouveau cap de fréquentation

Depuis son lancement fin 2017, la fréquentation de la plateforme Cybermalveillance.gouv.fr n'a cessé de croître pour atteindre plus de 8,3 millions de visiteurs en 5 ans. En cette seule année 2022, elle a réuni près de 3,8 millions de visiteurs uniques (3 799 282), soit quasiment la moitié de son audience depuis 5 ans.
Ce nouveau record d'audience est dû en partie au développement croissant de la notoriété du dispositif auprès de ses publics, notamment du fait d'une présence accrue dans les médias, pour lesquels **le dispositif est devenu en 5 ans une référence sur les sujets de cybersécurité**. Cette progression est également liée à un travail continu d'amélioration du référencement naturel des publications de prévention et d'assistance, afin de les rendre toujours plus facilement accessibles via les moteurs de recherche, premier canal de recherche d'information des victimes. Enfin, ces chiffres témoignent de l'intérêt grandissant de tous les publics – tant particuliers que professionnels – pour l'information et les services offerts par la plateforme et sont révélateurs du besoin des populations face à une cybercriminalité toujours en forte expansion.

En 2022, la fréquentation de la plateforme Cybermalveillance.gouv.fr affiche **une hausse de 53 %** pour atteindre **près de 3,8 millions de visiteurs sur l'année** (3 799 282). Soit plus de 8,3 millions de visiteurs depuis la création du dispositif en 2017.



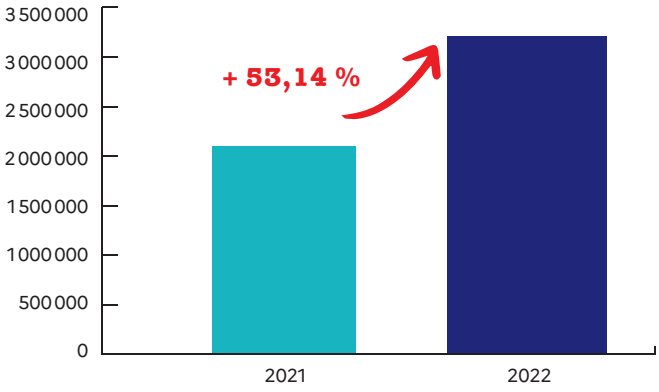
Fréquentation annuelle de la plateforme de Cybermalveillance.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

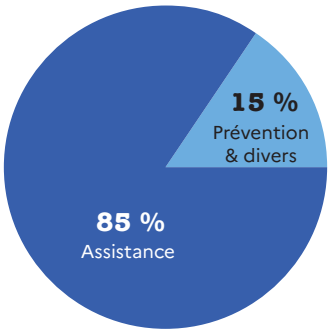
Une fréquentation majoritairement centrée sur l'assistance

Cybermalveillance.gouv.fr dispose sur sa plateforme de plus de 200 contenus thématiques de prévention et de remédiation aux dangers du numérique.
Sur l'année écoulée, les articles sur les menaces ont fait l'objet de plus de 2,9 millions de consultations, auxquelles s'ajoutent près de 280 000 recherches d'assistance en ligne. Au total, **plus de 3,2 millions de personnes ont pu trouver une assistance sur Cybermalveillance.gouv.fr en 2022, une augmentation de 53 % par rapport à l'année précédente.**



Évolution de l'assistance aux victimes

La plateforme Cybermalveillance.gouv.fr trouve toujours l'essentiel de son public dans sa **mission première d'assistance qui représente près de 85 % de son trafic.**

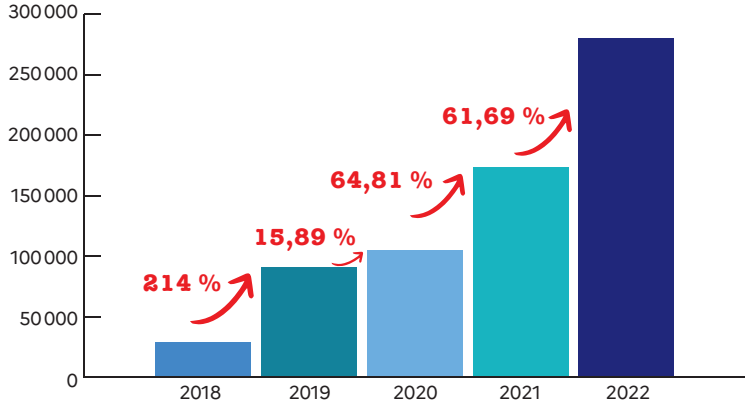


LES CHIFFRES DE LA CYBERMALVEILLANCE EN 2022

L'assistance en ligne en 2022

Cybermalveillance.gouv.fr propose un outil de diagnostic et d'assistance en ligne qui permet, en répondant à quelques questions, d'obtenir un diagnostic du problème rencontré et de disposer des conseils pour y faire face. Ces conseils peuvent être d'ordre technique et/ou administratif. Ce service offre également la possibilité d'être mis en relation avec plus de 1 250 prestataires référencés sur l'ensemble du territoire national, pour apporter une assistance technique de proximité aux victimes.

Sur l'année écoulée, **près de 280 000 demandes d'assistance en ligne ont été enregistrées sur Cybermalveillance.gouv.fr, en augmentation de plus de 61 %** par rapport à l'année précédente.



Évolution des demandes d'assistance en ligne

Cybermalveillance.gouv.fr enregistre un taux de satisfaction de 92,8 % sur son assistance en ligne, soit 7 points de plus par rapport à 2021. Cette progression est le fruit d'une amélioration continue de cet outil pour correspondre au mieux aux attentes des publics du dispositif et leur délivrer l'information la plus pertinente selon la situation qu'ils rencontrent.

85 % des demandes d'assistance de la part des entreprises et des collectivités reçoivent une réponse d'un prestataire référencé en moins d'une heure.

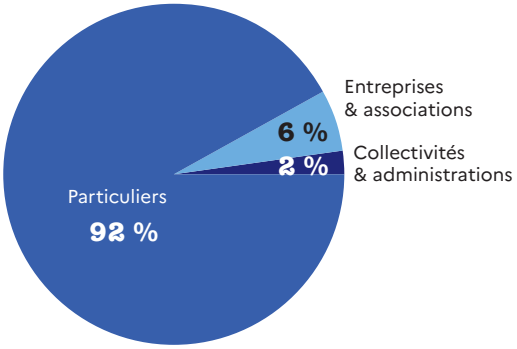
ÉTAT DE LA MENACE

La répartition des recherches d'assistance par publics

La répartition des publics de la plateforme Cybermalveillance.gouv.fr en 2022 se révèle quasiment stable par rapport aux années antérieures avec 92 % de particuliers, 6 % d'entreprises et associations et 2 % de collectivités et administrations.

Cet indicateur quantitatif fait apparaître que Cybermalveillance.gouv.fr est majoritairement utilisé par des particuliers (en volume).

Cette réalité est toutefois à rapprocher de la taille respective des populations cibles, soit 68 millions de particuliers, 5,6 millions d'entreprises et associations, et 36 000 collectivités et EPCI.



Ainsi, rapporté à la proportion de ces populations, **pour 1 particulier assisté en 2022, Cybermalveillance.gouv.fr a assisté 1 entreprise et 34 collectivités.**

En 2022, **plus de 16 000 professionnels** (12 658 entreprises et associations et 3 510 collectivités et administrations) **sont venus chercher une assistance en ligne sur Cybermalveillance.gouv.fr, ce qui représente une augmentation de 30 % par rapport à l'année précédente** (+23 % pour les entreprises/associations et +67 % pour les collectivités). Cette tendance démontre que **la pression de la cybermalveillance sur les publics professionnels continue de s'accroître, notamment sur les collectivités.**

En fin d'année 2022, l'outil de diagnostic et d'assistance en ligne de Cybermalveillance.gouv.fr traite **51 cybermenaces** et délivre **plus de 500 conseils personnalisés.** Durant l'année, **4 nouvelles menaces** ont été ajoutées à cet outil afin de répondre aux besoins des victimes et leur donner les conseils nécessaires pour y faire face : l'escroquerie à l'infraction pédopornographique, l'escroquerie au placement financier, l'escroquerie au virement (faux RIB) et la fraude au faux conseiller bancaire.

LES PRINCIPALES MENACES PAR CATÉGORIE DE PUBLICS EN 2022

Sur les 51 formes de cybermalveillance traitées par l'outil d'assistance en ligne en 2022, l'analyse des principales recherches par catégorie de publics est un indicateur fort des grandes tendances de la cybermalveillance.
Les 10 principales cybermenaces par catégorie de publics décrites ci-après représentent à elles seules plus de 90 % des recherches d'assistance en ligne sur la plateforme.

Principales recherches d'assistance pour les particuliers

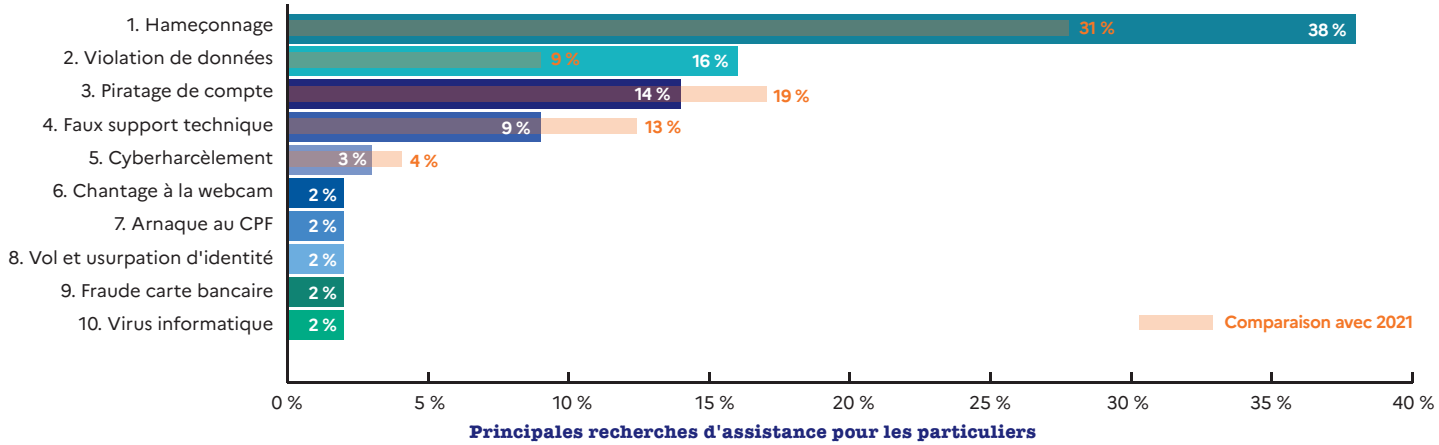
À l'instar des années précédentes, **l'hameçonnage (*phishing*) continue de progresser (+7 points) et reste, de loin, avec 38 % des demandes, la première cybermalveillance** pour laquelle les victimes viennent chercher de l'aide en 2022 (voir page 22).

Avec une année marquée par de nombreux incidents et fuites de données qui ont touché le secteur de la santé, **les violations de données personnelles passent de la quatrième à la deuxième place**, avec 16 % des demandes (+7 points).

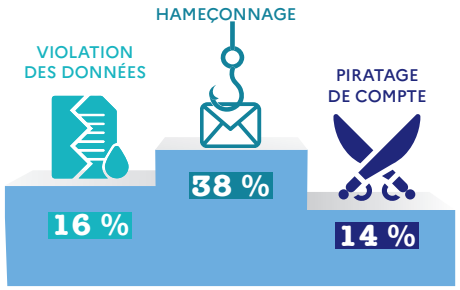
Le **piratage de compte en ligne**, en léger retrait par rapport à l'année précédente (-5 points), devient la **troisième menace** avec 14 % des recherches d'assistance.

Aux rangs suivants, si leur poids a légèrement baissé, on retrouve respectivement les **fraudes au faux support technique** (de 13 à 9 %) et le **cyberharcèlement** (de 4 à 3 %), qui atteint la cinquième place du classement des principales cybermalveillances et représente une préoccupation toujours forte des victimes qui y sont confrontées.

Les demandes d'assistance de victimes en matière d'**escroquerie au placement financier** ou d'**escroquerie sentimentale** restent relativement faibles en volume et ne figurent donc pas dans ce classement. Toutefois, les montants de préjudices financiers subis par les victimes peuvent être très importants (de plusieurs dizaines à plusieurs centaines de milliers d'euros).



Principales recherches d'assistance pour les particuliers



ÉTAT DE LA MENACE

Principales recherches d'assistance pour les entreprises et associations

Cette année pour les entreprises, **c'est l'hameçonnage qui constitue de nouveau la menace majeure.** Les recherches d'assistance sur ce phénomène ont en effet plus que doublé, en passant de 13 % en 2021 à 27 %, soit une progression de 14 points.

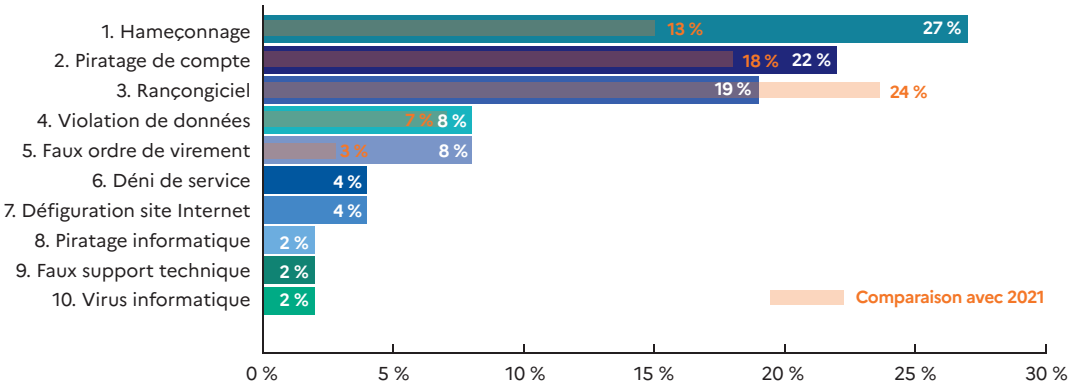
En hausse de 4 points, **le piratage de compte en ligne représente toujours la seconde menace** avec 22 % des demandes d'aide de cette catégorie de public.

Et les demandes d'assistance liées à des attaques par **rançongiciels passent de la première à la troisième place (-5 points)**, tout en restant à un niveau élevé.

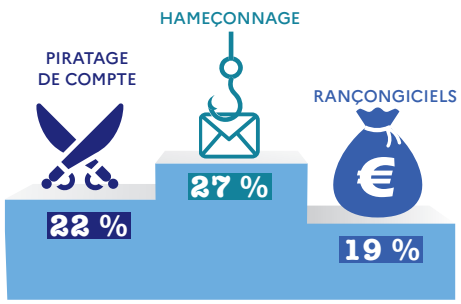
Souvent consécutives à une intrusion, **les violations de données arrivent en quatrième position**, dans une proportion quasiment stable par rapport à 2021.

Les fraudes aux virements, quant à elles, progressent de la sixième à la cinquième place et marquent ainsi une hausse notable des recherches d'aide (+5 points).

Enfin, les attaques visant les sites web des entreprises et associations figurent également dans ce classement des principales menaces qui frappent ces publics, avec **le déni de service** et **la défiguration de site Internet** qui fait son entrée dans le top 10.



Principales recherches d'assistance pour les entreprises et associations



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

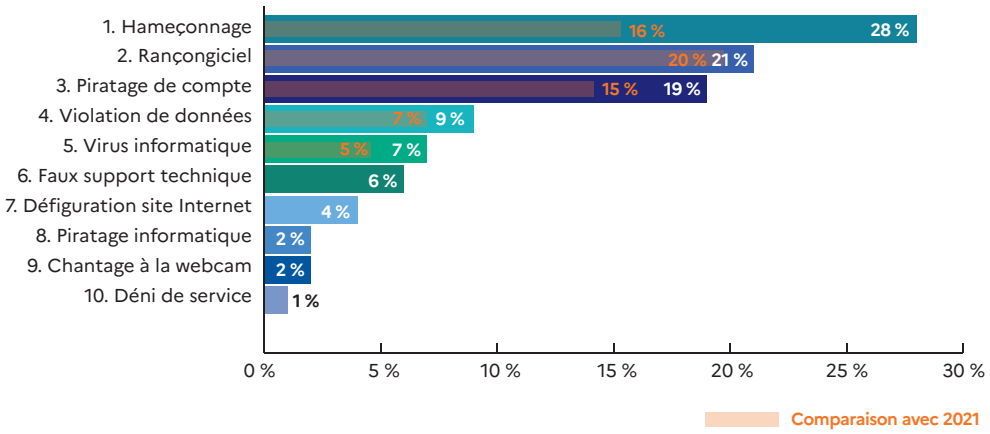
Principales recherches d'assistance pour les collectivités et administrations

À l'instar des entreprises et associations, **l'hameçonnage prend la première place des principales recherches d'assistance en ligne des collectivités et administrations sur Cybermalveillance.gouv.fr avec 28 %**, également en forte hausse par rapport à l'année précédente (+12 points).

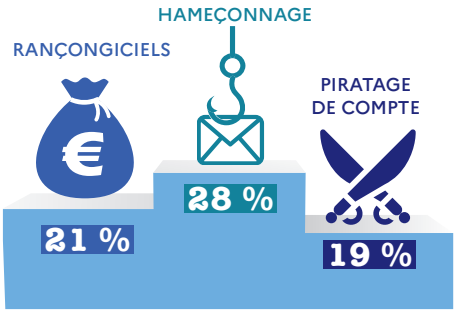
Si elles augmentent d'un point par rapport à 2021, les attaques par **rançongiciels** passent, pour leur part, en deuxième position avec 21 % des demandes d'assistance (312 parcours en 2021 contre 329 en 2022).

Quant au **piratage de compte en ligne**, il reste la troisième cause de recherche d'assistance avec 19 % des recherches (+4 points).

Enfin, comme pour les autres publics professionnels du dispositif, les **violations de données et les attaques sur les sites Internet** des collectivités et administrations font partie des principales menaces pour lesquelles ces publics recherchent une assistance en ligne sur la plateforme.



Principales recherches d'assistance pour les collectivités et administrations



ÉTAT DE LA MENACE

LES GRANDES TENDANCES DE LA MENACE 2022

L'hameçonnage (*phishing*) : menace n°1 tous publics

HAMEÇONNAGE
+54 %
de recherches d'information

L'hameçonnage (*phishing* en anglais) ne cesse de progresser et reste, en 2022, la principale menace à laquelle est confronté l'ensemble des publics du dispositif, tant à titre personnel que professionnel.

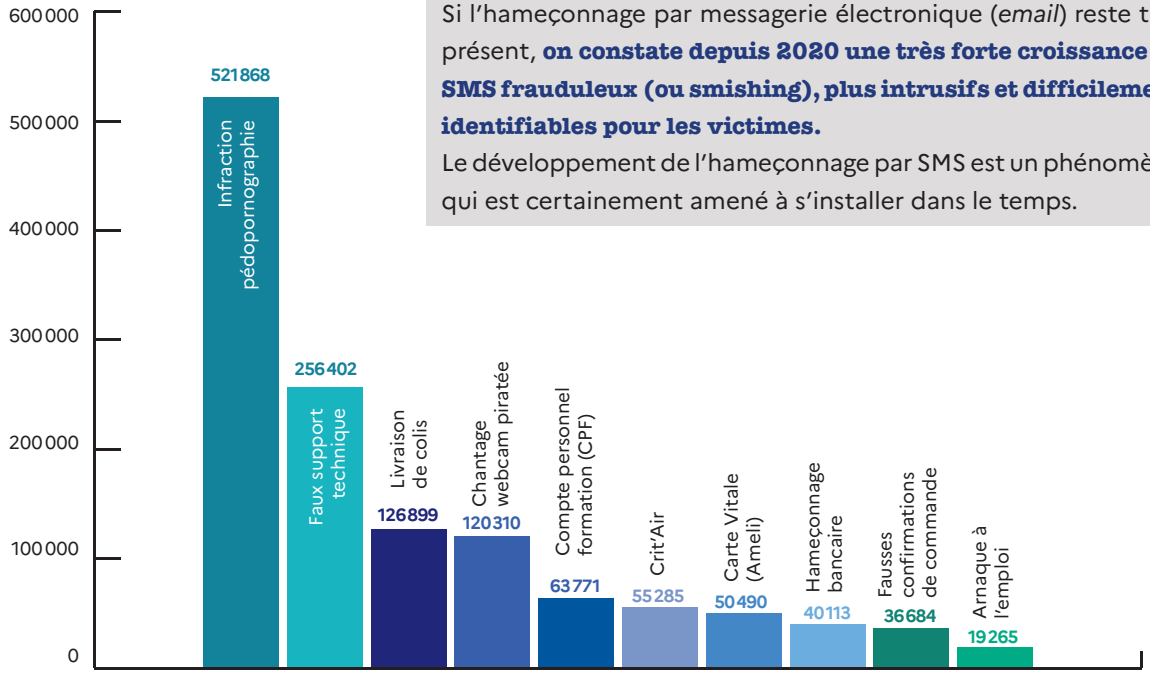
En 2022, l'hameçonnage représente 37 % des recherches d'assistance sur Cybermalveillance.gouv.fr et les articles de la plateforme permettant de faire face à cette menace ont reçu près de 1,9 million de consultations, soit une augmentation de 54 %.

Cette forme d'attaque s'avère particulièrement prisée par les cybercriminels. En effet, sa relative simplicité de mise en œuvre leur permet d'obtenir de leurs victimes des informations personnelles sensibles (identité, numéros de carte bancaire, mot de passe…) ou de leur faire installer un programme malveillant afin de prendre le contrôle de leur équipement dans le but de l'utiliser frauduleusement.

Le développement et l'industrialisation de l'écosystème cybercriminel facilitent l'accessibilité des techniques et outils d'hameçonnage qui continuent de gagner en sophistication.

Une grande majorité de cybermalveillances trouvent ainsi leur origine des suites d'un hameçonnage : piratage de compte, usurpation d'identité, fraude bancaire, faux support technique, rançongiciel…

Hameçonnages les plus fréquents en 2022*



Si l'hameçonnage par messagerie électronique (*email*) reste très présent, **on constate depuis 2020 une très forte croissance de SMS frauduleux (ou smishing), plus intrusifs et difficilement identifiables pour les victimes.**
Le développement de l'hameçonnage par SMS est un phénomène qui est certainement amené à s'installer dans le temps.

*en nombre de consultations des articles menace dédiés

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

Focus sur les principales formes d'hameçonnage en 2022

Déjà prédominant dès 2019, l'hameçonnage s'est fortement généralisé depuis la pandémie avec l'explosion des usages numériques et touche tous les publics. Si la menace apparaît de plus en plus sophistiquée, les cybercriminels sont particulièrement créatifs et n'hésitent plus à s'appuyer sur l'actualité pour adapter ou hyper contextualiser leur approche auprès des victimes.

L'HAMEÇONNAGE À L'INFRACTION PÉDOPORNOGRAPHIQUE

Dans ce type d'hameçonnage, la victime se fait reprocher des faits de pédopornographie par un faux service de police ou de gendarmerie qui lui intime de payer une amende de plusieurs milliers d'euros sous peine de condamnation et de rendre les faits publics. Cette escroquerie reste en tête des hameçonnages les plus fréquents en 2022 avec plus de **21 000 recherches d'assistance et 500 000 consultations de l'article dédié à cette menace**. Elle suscite toujours une forte inquiétude chez de nombreuses personnes qui reçoivent ces messages frauduleux, d'apparence officielle.

L'ARNAQUE AU FAUX SUPPORT TECHNIQUE

Cette catégorie d'escroquerie démarre le plus souvent à la suite de la réception d'un message d'hameçonnage ou lors de la navigation sur Internet. Le message incite la victime à cliquer sur un lien qui déclenche le blocage de son ordinateur avec une *pseudo* alerte de sécurité et la pousse à contacter en urgence un faux support technique dans le but de lui faire payer un dépannage factice à distance. Des pratiques toujours plus agressives des faux supports ont été constatées, les escrocs n'hésitant plus à **pirater les comptes de la victime, voire à saboter les ordinateurs** de celles qui refusent de payer. Durant l'année écoulée, **plus de 12 000 personnes** ont sollicité une assistance sur la plateforme pour ce type d'attaque qui ne faiblit pas. L'article donnant les conseils pour faire face à cette menace a été consulté **plus de 250 000 fois**.

L'HAMEÇONNAGE À LA LIVRAISON DE COLIS

Les **messages d'hameçonnage à la livraison de colis** qui incitent à cliquer sur un lien pour consulter un colis en attente ou régler des frais d'affranchissement **ont connu une forte augmentation au second semestre, en particulier par SMS**. Dans une majorité des cas, l'objectif des cybercriminels reste de dérober les informations personnelles et de carte bancaire des victimes. **Toutefois, de nouvelles campagnes massives ont été détectées à l'été 2022** avec un message invitant à cliquer sur un lien téléchargeant un programme malveillant (virus) pour prendre le contrôle du téléphone de la victime, lui dérober ses mots de passe et l'utiliser pour relayer des SMS frauduleux. **Près de 3 500 personnes** sont venues chercher une assistance sur Cybermalveillance.gouv.fr en 2022 pour ces phénomènes et **125 000 consultations** de l'article dédié à cette menace ont été enregistrées.

L'ESCROQUERIE AU CHANTAGE À LA WEBCAM PRÉTENDUE PIRATÉE

Dans ce type d'escroquerie, les victimes reçoivent un message d'un *prétendu* pirate qui affirme avoir pris le contrôle de leur appareil et les avoir filmées avec leur webcam durant des consultations de sites pornographiques. Pour ne pas divulguer les images obtenues, il demande une rançon, généralement en cryptomonnaie. **Détectée par Cybermalveillance.gouv.fr en 2019**, cette forme d'escroquerie revient très régulièrement et continue d'interpeller les publics, avec **une forte recrudescence au second semestre**. En 2022, près de **3 500 personnes** ont demandé de l'assistance sur cette menace et les articles consacrés à ce phénomène ont reçu **plus de 120 000 consultations**.

LES ESCROQUERIES AU COMPTE PERSONNEL FORMATION (CPF)

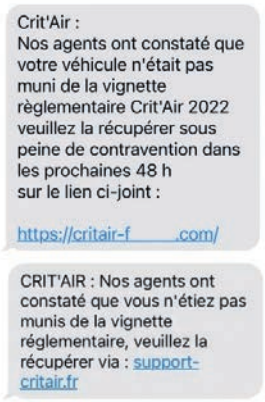
Les escroqueries au CPF ont quasi systématiquement pour origine un hameçonnage, que ce soit par messagerie (mail), SMS ou appel téléphonique. L'objectif des escrocs est principalement de faire souscrire aux victimes une formation factice ou de récupérer leur mot de passe pour pirater les avoirs de leur compte formation. Toujours très massives au premier semestre, **ces campagnes d'hameçonnage se sont considérablement taries à l'automne, après la mise en place de dispositifs de sécurité renforcés** sur les comptes des ayants droit, qui ont drastiquement limité

ÉTAT DE LA MENACE

les possibilités de piratage. En 2022, **plus de 2 100 personnes** ont demandé une assistance sur la plateforme pour des escroqueries et hameçonnage relatifs au CPF et l'article consacré à cette menace a suscité **plus de 63 000 recherches d'informations**.

L'HAMEÇONNAGE À LA VIGNETTE CRIT'AIR

Cette nouvelle forme d'hameçonnage a été **détectée à l'automne de manière concomitante aux annonces dans les médias de l'extension des zones à faibles émissions mobilité (ZFE)** aux grandes métropoles nationales. Les victimes reçoivent un message, principalement par SMS, les incitant à commander rapidement leur vignette Crit'Air sous peine d'amende. Le lien contenu dans ce message les amène sur un site frauduleux d'apparence officielle, où leur seront demandées leurs informations personnelles et de carte bancaire pour les leur dérober.
Dès sa détection, Cybermalveillance.gouv.fr a émis plusieurs alertes sur ce phénomène et l'article consacré à cette menace a reçu **plus de 55 000 consultations en moins de 2 mois**. Il est fortement probable que cette forme d'hameçonnage continue de proliférer dans les prochains mois.



L'HAMEÇONNAGE À LA CARTE VITALE (AMELI)

Épisodique les années antérieures, **l'hameçonnage au renouvellement ou à la mise à jour de la carte Vitale a connu une forte recrudescence inédite et constante depuis fin 2021, particulièrement par SMS**. Les victimes qui y donnent suite se voient dérober leurs informations personnelles et de carte bancaire. Et nombre d'entre elles disent avoir été appelées peu de temps après par un faux conseiller bancaire qui leur a fait subir d'importants dommages financiers (voir focus page 25). En 2022, l'article qui décrit cette menace et les moyens d'y faire face a fait l'objet de **plus de 50 000 consultations**.

L'HAMEÇONNAGE BANCAIRE

Avec la mise en place de l'authentification renforcée sur l'accès aux comptes bancaires en ligne dans le cadre de la directive européenne sur les services de paiement (DSP2), une forte baisse de l'hameçonnage bancaire aurait pu être attendue. Or, cela n'a pas été le cas. **Ces hameçonnages ont même gagné en sophistication** en recherchant de plus en plus souvent à obtenir de la victime, outre son mot de passe, le code de double authentification reçu par SMS pour se connecter à leur compte, voire, dans certains cas, les informations d'identification de sa ligne de téléphone mobile (code RIO), en vue de la dupliquer (technique dite de *SIM swapping*) pour leur permettre de recevoir les codes connexion, de confirmation d'achats ou de virements. L'article dédié à l'hameçonnage bancaire de Cybermalveillance.gouv.fr, qui présente cette menace et les conseils pour y réagir, a été consulté **plus de 40 000** fois en 2022.

ET BIEN D'AUTRES ENCORE AVEC DES ABONNEMENTS MASQUÉS À LA CLÉ…

Outre les principales formes d'hameçonnage développées précédemment, l'année 2022 a vu bien d'autres formes et prétextes utilisés pour escroquer les victimes. Ont ainsi pu être observés **de nombreux faux jeux concours pour gagner une carte carburant, des bons d'achats pour la grande distribution, des billets d'avion, des téléphones haut de gamme ou encore un barbecue pour la fête des pères**…
Dans ces campagnes d'hameçonnage qui circulent principalement sur les réseaux sociaux et messageries instantanées, en donnant leur numéro de carte bancaire pour des prétendus frais d'envoi, les victimes se voient souscrire à des pseudos services ou programmes en ligne peu lisibles pour plusieurs dizaines d'euros par mois et dont elles peuvent avoir toutes les peines de se défaire. Tout au long de l'année, Cybermalveillance.gouv.fr a émis de nombreuses alertes sur ces campagnes d'hameçonnage sur ses réseaux sociaux et lors d'interventions dans les médias.

FOCUS NOUVELLES MENACES 2022

La mise en œuvre en 2021 de la directive européenne sur les services de paiement (DSP2) oblige les banques à demander un code de confirmation reçu par téléphone ou dans son application bancaire pour certaines opérations réalisées en ligne par leurs clients telles qu'une authentification au compte, un virement ou certaines dépenses importantes par carte bancaire... Pour contourner cette contrainte, les cybercriminels se sont adaptés et de nouvelles menaces sont en forte expansion.

LES FAUX CONSEILLERS BANCAIRES

Dans cette forme d'escroquerie, les victimes sont appelées par un faux conseiller bancaire ou d'un service *anti fraude* ou encore sont invitées à le rappeler après avoir reçu un message inquiétant. Avec un discours rodé et crédible, le faux conseiller leur indique avoir détecté des opérations suspectes sur leur compte. L'escroc propose alors à la victime de bloquer ses opérations en lui communiquant des codes de confirmation qu'elle reçoit sur son téléphone. En réalité, ces codes vont permettre à l'escroc de confirmer des transactions frauduleuses sur le compte de la victime (paiements en ligne par carte bancaire, virements vers des comptes de l'escroc). Dans de nombreux cas rapportés, les victimes étaient contactées après avoir reçu un message d'hameçonnage auquel elles avaient répondu (carte Vitale, Netflix, Crit'Air, bancaire...). Ce type d'arnaque s'est considérablement développé en 2022 et les montants des préjudices sont souvent importants allant de quelques milliers à plusieurs dizaines de milliers d'euros. À l'été, Cybermalveillance.gouv.fr a ajouté cette menace dans son outil d'assistance en ligne. En 6 mois, **près de 1 500 personnes** se sont rendues sur la plateforme afin d'obtenir une assistance en ligne sur cette menace.

LA FRAUDE AU VIREMENT OU « FAUX RIB »

La fraude au RIB était jusqu'alors un phénomène principalement observé chez les publics professionnels. Depuis 2022, il touche aussi en nombre des particuliers. Dans ce type d'arnaque, la victime reçoit par message (mail) une facture en attente de paiement de l'un de ses créanciers : artisan, notaire, avocat, bailleur, propriétaire, fournisseur... Le créancier demande le règlement sur un RIB joint au message qui s'avère, en fait, être celui d'un compte de l'escroc. Ce type de fraude est généralement consécutif au piratage de la messagerie, principalement du créancier, mais parfois aussi de la victime. Le cybercriminel, qui a accès à la messagerie, observe les factures en instance de règlement, les détourne et les modifie à son profit. Les montants de préjudice peuvent aller de plusieurs milliers à dizaines de milliers d'euros pour les particuliers, voire jusqu'à plusieurs centaines de milliers d'euros pour les publics professionnels trompés.
En 2022, l'article de Cybermalveillance.gouv.fr qui décrit comment faire face à cette menace a été consulté **plus de 41 000 fois**, une augmentation de 37 % par rapport à l'année 2021.

CONFLIT RUSSIE-UKRAINE

Le conflit entre la Russie et l'Ukraine aura incontestablement marqué l'actualité 2022. Si de nombreuses cyberattaques et opérations de cyberinfluence entre les deux belligérants ont pu être relevées, force est de constater que ce conflit n'a eu jusqu'alors qu'une incidence cyber visible marginale en France sur le périmètre observé par le dispositif. Dès le début du conflit, de nombreux commentateurs, relayés par les médias, annonçaient qu'une cyberguerre pouvait toucher notre pays. Cette situation a généré une forte inquiétude de la population. Pour y répondre, Cybermalveillance.gouv.fr a publié début mars un article décrivant factuellement sa perception de la menace et en relativisait la portée, en préconisant des mesures, à l'attention de ses publics, pour faire face à toute évolution possible de la situation. Un an plus tard, cette analyse et ces recommandations demeurent d'actualité.

ÉTAT DE LA MENACE

Le piratage de compte en ligne : toujours en seconde place et toujours en croissance

Le piratage de compte en ligne reste en 2022 à la seconde place des principales menaces qui touchent l'ensemble des publics de Cybermalveillance.gouv.fr.

Messageries, réseaux sociaux, banques, services administratifs ou sites de e-commerce : tous les comptes de services en ligne sont ciblés par les cybercriminels.

PIRATAGE DE COMPTE

+97,5 %

de recherches d'information et d'assistance

Avec plus de 20 000 demandes d'aide en ligne et 296 000 consultations des articles permettant de faire face à cette menace, ce sont plus de **316 000 personnes qui sont venues chercher une information et une assistance sur ce phénomène, en hausse de 97,5 %** par rapport à l'année précédente.

Les **comptes de messagerie en ligne** demeurent une cible de prédilection des cybercriminels car ils regorgent d'échanges, d'informations et de documents à même de leur permettre d'usurper l'identité de la victime à des fins principalement d'escroqueries financières. Par ailleurs, les cybercriminels peuvent prendre le contrôle de ses autres comptes (réseaux sociaux, sites de vente en ligne…), en utilisant leurs fonctions de réinitialisation de mot de passe. Le piratage d'un compte de messagerie est susceptible d'occasionner un préjudice important, d'autant qu'il peut se révéler discret et que la victime risque de mettre du temps à s'en apercevoir.

Les **réseaux sociaux** constituent eux aussi un terrain de prédation, notamment les comptes dont l'utilisation frauduleuse ou la perte représentent un préjudice d'image ou financier important, en particulier pour les **victimes professionnelles** à l'instar de personnalités, d'influenceurs ou des entreprises qui utilisent les réseaux sociaux comme principales vitrines promotionnelles ou même de collectivités pour informer leurs administrés. Généralement, les cybercriminels prennent le contrôle des comptes de réseaux sociaux piratés pour y publier des escroqueries financières ou réclament aux victimes une rançon pour leur restituer leur compte.

Le piratage de compte s'applique aussi aux **comptes bancaires en ligne,** qui restent une cible privilégiée des cybercriminels. En raison des dispositifs d'authentification renforcés qui existent sur ces comptes, ils tenteront d'y accéder dans le cadre de fraude au faux conseiller bancaire (voir focus page 25) ou en infectant les appareils de victimes par des virus destinés à dérober leurs mots de passe, à intercepter les SMS de double authentification ou même à prendre le contrôle de leur application bancaire.

Autre type de comptes en ligne visés : les **sites de commerce en ligne** sur lesquels les escrocs passent des commandes sur le compte des victimes en se faisant livrer à une adresse qu'ils contrôlent.

De même, les **services administratifs en ligne** (assurance maladie, impôts, CAF…) sont de plus en plus la proie des cybercriminels, notamment ceux sur lesquels ils pourront modifier les informations de compte bancaire de la victime pour récupérer des fonds ou des prestations sociales.

De nombreux autres types de comptes sont la cible de piratage, tels que les services de vidéos ou de musique à la demande (*streaming* en anglais), de jeux en ligne, de plateformes d'échange de cryptomonnaies ou encore les comptes Google ou Apple, qui centralisent la gestion d'un ensemble de services et d'appareils des victimes.

Les **principales causes du piratage de compte en ligne** restent l'hameçonnage et la réutilisation de mots de passe entre différents comptes, dont l'un a pu être piraté. On observe toutefois une forte croissance des cas d'infection des victimes par des programmes *voleurs de mots de passe* (*virus stealer* en anglais), notamment sur téléphone mobile. Ces infections se produisent généralement suite à un hameçonnage ou au téléchargement d'une application piégée.

Si elles ne peuvent représenter une protection absolue au regard de l'évolution des moyens déployés par les cybercriminels, l'utilisation de **mots de passe uniques** et suffisamment solides ainsi que la **double authentification** représentent des **mesures de sécurité indispensables** à mettre en place pour renforcer la protection de tous ses comptes en ligne importants (messagerie, réseaux sociaux…) afin de limiter leurs risques de piratage.

La hausse constatée ces dernières années des piratages de compte en ligne est une tendance qui devrait se poursuivre au vu, tant de leur prolifération, que des profits financiers qu'en retirent les cybercriminels.

Le téléphone mobile en tant que cible

Au-delà de l'hameçonnage par SMS (*smishing*) qui s'est fortement développé ces deux dernières années, les téléphones mobiles sont de plus en plus visés par les cybercriminels. En effet, ils sont devenus aujourd'hui l'un des **principaux moyens d'accès à Internet et contiennent de nombreuses informations sensibles. Ils sont aussi souvent faiblement sécurisés** par leurs utilisateurs, peu conscients des risques. Cybermalveillance.gouv.fr a constaté en 2022 le développement de multiples campagnes malveillantes qui ont pour but d'infecter les téléphones mobiles avec des virus voleurs de mots de passe (*infostealer*). Ces virus peuvent également prendre le contrôle de diverses fonctionnalités de l'appareil pour, par exemple, pirater les applications bancaires, intercepter ou envoyer des SMS ou encore passer des appels surtaxés à l'insu de leur propriétaire. Les comptes Google et Apple, dédiés à la gestion des téléphones mobiles, sont aussi convoités par les cybercriminels car, une fois piratés, ils donnent accès à de nombreuses informations et fonctionnalités de l'appareil compromis.

De nouvelles violations de données personnelles médicales

L'année 2022 a de nouveau été marquée par des violations de données personnelles médicales importantes : en mars, avec l'Assurance Maladie (Ameli) qui a touché 510 000 personnes et en août, le Centre Hospitalier Sud Francilien de Corbeil-Essonnes (CHSF) qui a potentiellement concerné 700 000 personnes. Ces violations de données personnelles et confidentielles suscitent toujours une forte inquiétude des populations sur l'usage frauduleux qui pourrait en être fait. Cybermalveillance.gouv.fr s'est efforcé d'accompagner au mieux les victimes en leur dispensant les conseils nécessaires pour faire face aux cybermalveillances qui peuvent être consécutives à ce type d'incident, notamment les risques d'hameçonnage et autres tentatives d'escroqueries ciblées. **Plus de 20 000 personnes sont venues rechercher une assistance en ligne sur Cybermalveillance.gouv.fr** suite à ces deux évènements. Dans le cadre de la violation de données du CHSF, en coopération avec les services du ministère de la Justice et du ministère de l'Intérieur, une lettre plainte numérique a été mise à disposition des victimes sur Cybermalveillance.gouv.fr pour les aider à faire face aux conséquences potentielles susceptibles de conduire à une judiciarisation.

ÉTAT DE LA MENACE

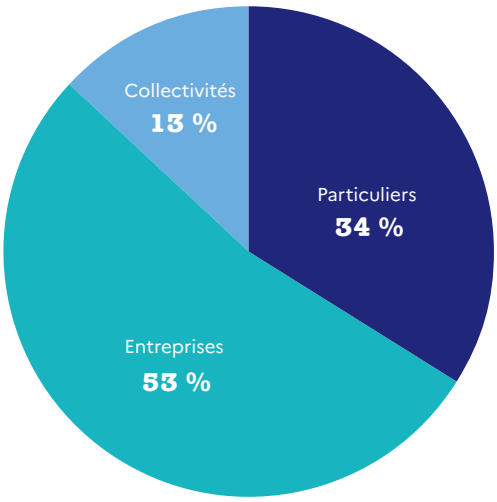
Les rançongiciels : les professionnels toujours les plus ciblés

Avec plus de 74 000 consultations de l'article qui décrit comment faire face à ce type d'attaque et 2 492 recherches d'assistance (en retrait de 7 % vs 2021), les rançongiciels (*ransomwares* en anglais) demeurent, en 2022, l'une des principales menaces traitées par la plateforme. Un type d'attaque qui touche majoritairement les professionnels, à 66 %.

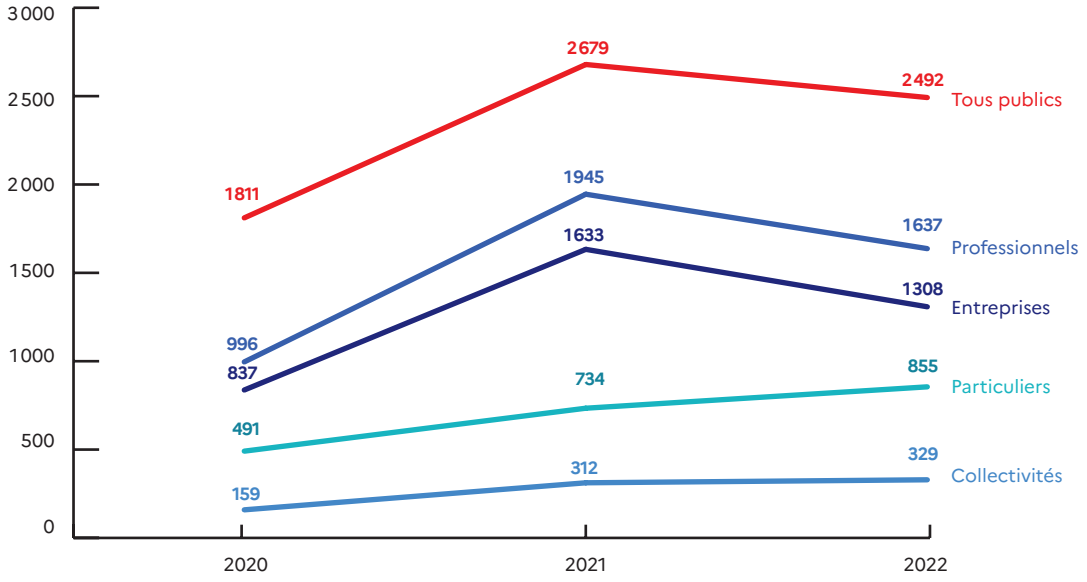
RANÇONGICIELS
2 492
recherches d'assistance tous publics confondus

En ce qui concerne les **particuliers**, les demandes d'assistances sont en augmentation par rapport à l'année précédente (+16 %). Ainsi, avec 855 sollicitations, cette menace se place en 11e position pour cette catégorie de public. Dans une grande partie des cas rapportés, les attaques par rançongiciel semblent essentiellement opportunistes et portent sur des serveurs de fichiers domestiques (NAS), trop faiblement protégés ou font suite à l'installation d'un logiciel piraté ou d'origine douteuse, sur l'ordinateur de la victime. Dans plusieurs dossiers, il a été constaté que les cybercriminels ne perdaient pas de temps à réclamer une rançon lorsqu'ils se rendaient compte qu'ils avaient attaqué un particulier. On peut émettre l'hypothèse qu'il ne s'agit alors que de simples phases « d'entraînement », avant de s'en prendre à des cibles professionnelles, plus solvables, disposant d'équipements similaires.

Pour les **professionnels**, avec 1637 demandes d'assistance (1308 entreprises et 329 collectivités), l'année 2022 affiche un léger recul par rapport à l'année précédente (-16 %), qui avait vu une explosion de cette menace. La population des victimes professionnelles est, en nombre, bien inférieure à celle des particuliers. Toutefois, rapporté aux populations respectives, on peut considérer que pour un particulier touché par un rançongiciel, ce sont 23 victimes professionnelles qui le sont.



Répartition des recherches d'assistance sur les rançongiciels par public



Évolution du nombre de recherches d'assistance sur les attaques par rançongiciel

Si le rançongiciel reste dans le top 3 des menaces rencontrées par les professionnels, on constate une baisse relative des recherches de la part de ces publics, en raison d'une diminution des attaques sur les **entreprises** (-20 %). Elles restent cependant majoritairement ciblées, car elles sont plus susceptibles de payer les rançons, au regard de l'impact financier de ces attaques sur leur activité.

En revanche, pour les **collectivités**, ces attaques sont toujours en légère augmentation (+5 %).

Dans les cas observés, les attaques par rançongiciels sur les victimes professionnelles sont fréquemment dues à une intrusion sur leurs accès externes insuffisamment protégés et surveillés (RDP, VPN, NAS…).

Pour les victimes professionnelles de petite et moyenne taille (TPE, PME, petites collectivités ou associations), on ne déplore pas de chantage associé à la divulgation de données dérobées. Ce type de procédé de **double extorsion** ne semble être utilisé par les cybercriminels que sur des cibles de taille plus importante, pour lesquelles cette divulgation pourrait avoir un impact réputationnel, concurrentiel, financier ou juridique significatif.

Les attaques par rançongiciel sont l'une des activités les plus lucratives de la cybercriminalité qui gagne en permanence en sophistication, structuration et professionnalisme. Cette menace ne devrait pas être appelée à baisser en intensité et il convient de s'y préparer.

FAITS ET CHIFFRES CLÉS

près de
3 800 000
visiteurs uniques sur la plateforme

près de
280 000
demandes d'assistance sur la plateforme

Taux de satisfaction sur les conseils donnés dans les articles sur la cybermalveillance :
97,8 %

Si la plateforme renseigne désormais près de 4 000 000 de personnes à travers des contenus et diagnostics de cybersécurité, Cybermalveillance.gouv.fr veille à répondre aux attentes de ses publics, ainsi qu'en témoigne le taux de satisfaction de la part de ses utilisateurs.

56
membres du dispositif

14 alertes et **5** recommantations cyber notables

plus de
1 250
prestataires
de services référencés

85 %
des demandes d'assistance des entreprises et des collectivités reçoivent une réponse d'un prestataire référencé
en moins d'1 heure

17
agents du GIP ACYMA

106
modules Assistance Cyber en Ligne
intégrés sur des sites tiers

plus de
200
labellisés
ExpertCyber

64 %
des demandes de sécurisation reçoivent une réponse en
moins de 3 heures

130
interventions

une
vingtaine
d'événements

2 260
retombées médias

Près de **100 000** **abonnés** sur LinkedIn

Près de **45 000** **abonnés** sur Twitter

Près de **30 000** **abonnés** sur Facebook

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

REMERCIEMENTS

Cybermalveillance.gouv.fr remercie celles et ceux qui ont apporté leur témoignage dans ce rapport d'activité pour sa cinquième année d'exercice. Il tient également à remercier les membres, partenaires et nombreux relais qui soutiennent et contribuent à ses missions d'intérêt général, au rayonnement du dispositif et à la sensibilisation de tous les publics.

Les ministères membres

- Première Ministre (ANSSI);
- Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique;
- Ministère de l'Intérieur et des Outre-Mer;
- Ministère de la Justice;
- Ministère des Armées;
- Ministère de l'Éducation nationale et de la Jeunesse.

Les autres entités membres

Aéma Groupe, **AFCDP** (Association française des correspondants à la protection des données à caractère personnel), **AFNIC** (Association française pour le nommage Internet en coopération), **ANCT** (Agence Nationale de la cohésion des territoires), **AMF** (Association des maires de France et des présidents d'intercommunalité), **Atempo**, **Avicca** (Association des Villes et Collectivités pour les Communications électroniques et l'Audiovisuel), **Banque des Territoires** (groupe Caisse des Dépôts), **Bouygues Telecom**, **CCR** (Caisse centrale de réassurance), **CCI France** (Chambre de Commerce et d'Industrie), **CDSE** (Club des directeurs de sécurité des entreprises), **CESIN** (Club des Experts de la Sécurité de l'Information et du Numérique), **Cinov Numérique**, **CISCO**, **CLCV** (Association Consommation, Logement et Cadre de Vie), **Club EBIOS**, **CLUSIF** (Club de la sécurité de l'information français), **CNIL** (Commission nationale de l'informatique et des libertés), **CNLL** (Union des entreprises du logiciel libre et du numérique ouvert), **CoTer Numérique**, **Covéa**, **CPME** (Confédération des Petites et Moyennes Entreprises), **e-Enfance/3018**, **ESET**, **Fédération Déclic**, **Fédération EBEN** (Fédération des Entreprises du Bureau et du Numérique), **FEVAD** (Fédération du e-commerce et de la vente à distance), **France Assureurs**, **France Victimes**, **Google France**, **INC** (Institut National de la Consommation), **Institut des Actuaires**, **Kaspersky**, **La Poste Groupe**, **MAIF** (Mutuelle assurance des instituteurs de France), **MEDEF** (Mouvement des entreprises de France), **Microsoft France**, **Neuflize OBC**, **Numeum**, **Orange Cyberdefense**, **Palo Alto Networks**, **Région Pays de la Loire**, **Régions de France**, **Signal Spam**, **SNCF**, **Stormshield**, **U2P** (Union des entreprises de proximité), **UFC-Que Choisir**.

Ses professionnels référencés et labellisés ExpertCyber, qui contribuent, aux côtés du dispositif, à ses missions d'assistance aux victimes ou de sécurisation sur l'ensemble du territoire.

Les **organisateurs et visiteurs des salons et événements** suivants: **AGIR** (Accompagnement par la Gendarmerie de l'Innovation et de la Recherche), les **Assises de la sécurité** (Groupe Comexposium), **CBC - Cybersecurity Business Convention Toulouse**, **Cloud & Cyber Security Expo**, le **Congrès des Maires**, le **Cybercercle**, le **FIC - Forum International de la cybersécurité, GS Days**, **GS Days - Journées Francophones de la sécurité**, **IT Partners** (groupe Reed Exhibition), **Paris Cyber Week** (Garnault et Associés), le **NEC - Numérique En Commun**.

Ses partenaires **média TV**, tels que **France Télévisions** et **TF1** pour la diffusion gracieuse de la campagne *Cybersécurité : de vraies solutions existent*.

Plus généralement, Cybermalveillance.gouv.fr remercie **l'ensemble des acteurs de l'écosystème avec lesquels il interagit** et qui lui permettent d'assurer ses missions au quotidien, dont le **Campus Cyber National**, le **Campus régional de Cybersécurité et de Confiance numérique Nouvelle-Aquitaine** (C3NA), les **Campus Régionaux**, le **Cercle Maritime** et les **CSIRT**.

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

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

GIP ACYMA
6 rue Bouchardon, 75010 Paris
www.cybermalveillance.gouv.fr

Suivez-nous sur :