RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

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

RAPPORT D'ACTIVITÉ 2023

Au cœur
de l'action Cyber

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, Pauline Fabry, Stella Azzoli et Maïlys Derville
Conception graphique : Elsa Godet
Crédits photos :
p. 3 : © Patrick Gaillardin
p. 3, 13 : © Pierre Morel
p. 7 : © Q. Veuillet
p. 9 : © Victor Tonelli
p. 11 : © MDC Leclercq G. COM CYBER GEND
p. 13 : © Régisseur MAIF

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

ÉDITOS

En 2023, la menace cyber a augmenté, s'inscrivant ainsi dans la tendance de ces dernières années. Elle est devenue systémique et s'attaque désormais à tous les pans de la société, de l'État et des grands opérateurs stratégiques jusqu'aux particuliers. Les actes de cybermalveillance affectent la vie courante de nos concitoyens et c'est intolérable.

Dans ce contexte, le GIP ACYMA a plus que jamais un rôle important à jouer au sein de l'écosystème cyber, en sensibilisant la population sur cette menace et en l'accompagnant si elle en est victime. L'État a un objectif majeur, s'assurer que chaque victime d'actes de cybermalveillance identifie un interlocuteur de confiance pour l'assister. Dans cette perspective, ACYMA doit servir d'aiguilleur, en coordination avec les autres acteurs de l'écosystème, CSIRT, Gendarmerie nationale et Police nationale, associations, prestataires privés et l'Agence nationale de la sécurité des systèmes d'information (ANSSI) bien évidemment.

Ce rôle est incarné par les responsabilités nouvelles que le gouvernement lui a confiées en 2023 et qui vont monter en puissance en 2024 : le 17Cyber et le filtre anti-arnaque. Il s'incarne également au travers du Cybermoi/s que le GIP a depuis cette année la responsabilité de coordonner en France.

Ces nouveaux programmes témoignent de la pertinence du modèle du GIP qui lui offre l'agilité nécessaire pour les intégrer et les développer. Une autre force de ce modèle, si ce n'est la principale, est sa capacité à mobiliser une diversité de parties prenantes autour de la lutte contre la cybermalveillance. J'ai eu l'occasion de constater la richesse de cet apport tout au long de cette année, alors que le GIP a initié un vaste chantier de refonte de sa stratégie. Les activités présentées dans ce rapport en sont également une belle illustration. À ce titre, je tiens à remercier l'ensemble des membres du GIP pour leur ouverture et leur engagement dans la structure. Je remercie également son directeur général et son équipe qui conduisent au quotidien un travail remarquable au service de cette cause essentielle.

Vincent Strubel
Président du GIP ACYMA,
Directeur Général de l'ANSSI

Depuis sa création et le lancement du dispositif en 2017, le GIP ACYMA a connu des moments inédits qui ont marqué l'écosystème de la cybersécurité : lancement de sa plateforme Cybermalveillance.gouv.fr et de son outil diagnostic en ligne, de ses premiers programmes de sensibilisation, guides, publications, alertes…

En l'espace de 6 ans, même en période de pandémie, le GIP n'a jamais failli à ses missions : informer ses publics, assister les victimes et ne jamais cesser d'observer la menace pour mieux la cerner et ainsi donner aux particuliers, entreprises et collectivités les moyens de mieux y faire face.

Ainsi, à fin 2023, plus de 12 millions de Français ont déjà consulté la plateforme et 950 000 ont recherché une assistance sur Cybermalveillance.gouv.fr. Si le GIP ACYMA a démontré sa pertinence et sa légitimité face à une menace toujours plus intense et de plus en plus sophistiquée et contextualisée, il reste encore bien évidemment beaucoup à faire.

À l'heure où le dispositif s'engage dans sa 7e année, 2023 aura été une période charnière pour préparer la mise en œuvre de projets gouvernementaux tels que le 17Cyber, qui offrent au dispositif un rôle déterminant pour développer cet enjeu sociétal qu'est la cybersécurité et le positionner comme le premier réflexe de sécurité numérique des Français. De nouveaux défis que le GIP est fier de relever, grâce au soutien de ses 62 membres, des professionnels référencés et labellisés ExpertCyber sans oublier l'investissement de toute son équipe, et qui s'inscrivent pleinement dans sa mission d'intérêt public.

Jérôme Notin
Directeur Général du GIP ACYMA[1]

[2] Groupement d'intérêt Public Actions contre la cybermalveillance

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.

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 d'infraction, et hors du périmètre d'intervention de l'ANSSI* (ministères et structures sous tutelle, 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 24h/24, 7 jours/7 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 (articles, vidéos, fiches, kit de sensibilisation, guides, 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 un travail de veille et d'analyse des 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.

* Agence nationale de la sécurité des systèmes d'information

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

Gouvernance

Le GIP ACYMA est composé de 62 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

19

agents en 2023

dont 9 mis à disposition par des membres du GIP :

- ANSSI (Service du Premier ministre) ;
- Ministère de l'Intérieur et des Outre-mer ;
- Ministère de l'Éducation Nationale et de la Jeunesse ;
- Ministère des Armées ;
- Ministère de la Justice ;
- Groupe SNCF.

Subvention exceptionnelle pour le projet 17Cyber

700 000 €

+

2,5 millions €

de budget en 2023

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

MINISTRE DÉLÉGUÉ CHARGÉ DE LA TRANSITION NUMÉRIQUE
ET DES TÉLÉCOMMUNICATIONS

Nouveaux membres en 2023

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

« PAROLES DE MEMBRES »

ANCT*
Léa Gislais
Directrice adjointe du Programme Société numérique

Si le numérique peut être une source d'émancipation, la cybermalveillance est un risque auquel nos concitoyens sont tous exposés, notamment les 16 millions d'entre eux se trouvant dans une situation d'éloignement du numérique. L'ANCT* s'est appuyée sur Cybermalveillance.gouv.fr en 2023 pour outiller les collectivités locales partenaires et les professionnels de la médiation numérique partout en France d'une mallette cyber composée de supports de sensibilisation aux risques de cybermalveillance.

* Agence nationale de la cohésion des territoires

Orange Cyberdéfense
Hugues Foulon
Directeur Exécutif - CEO

Je crois à l'alliance des acteurs publics et privés pour informer, prévenir et assister les citoyens et les organisations. Nos 3 000 experts sont fiers de partager avec Cybermalveillance.gouv.fr, depuis 2018, le même engagement qui se traduit dans notre mission de construire une société numérique plus sûre pour tous.

CPME*
François Asselin
Président

La CPME* soutient activement Cybermalveillance.gouv.fr dans son action en faveur des TPE–PME, en termes de prévention face aux risques et d'accompagnement des victimes. Depuis 6 ans, Cybermalveillance.gouv.fr apporte une expertise précieuse sur le sujet de la cybercriminalité et contribue à la sécurisation des entreprises.

* Confédération des petites et moyennes entreprises

SGDSN*
Stéphane Bouillon
Secrétaire Général de la défense et de la sécurité nationale

Depuis 6 ans, Cybermalveillance.gouv.fr est un succès et nous pouvons être fiers de deux intuitions : la première était d'offrir un interlocuteur aux victimes de cyberattaques qui ne relevaient pas de dispositifs particuliers ; l'autre était que ministères, administrations et acteurs privés pouvaient travailler au profit de tous. Cette réussite nous montre le chemin pour l'avenir. Toujours ensemble.

* Secrétariat général de la Défense et de la Sécurité nationale

Groupe BNP Paribas
Olivier Nautet
Chief Information Security Officer

La sensibilisation est un champ d'action vaste et complexe qui mérite une réflexion globale et commune. Devenir membre de Cybermalveillance.gouv.fr en 2023, est un moyen pour BNP Paribas, acteur économique majeur, de participer au renforcement du tissu national de Cyberdéfense français.

Unaf*
Marie-Andrée Blanc
Présidente

Dans une société où Internet occupe une place majeure et où la cybermalveillance menace, l'Unaf* s'est engagée au sein de Cybermalveillance.gouv.fr pour contribuer aux actions de sensibilisation et d'accompagnement de nos publics – les familles, nos associations et leurs usagers – à mieux se protéger contre les cybermenaces.

* Union nationale des associations familiales

LES **FAITS MARQUANTS**

JANVIER

1er janvier	L'APVF[1], AWS[2] France, CAMF[3] et NOMIOS rejoignent Cybermalveillance.gouv.fr
12 janvier	Intervention dans le cadre d'une réunion organisée par la CNSJ[4] pour les différentes parties prenantes des JO 2024
14 janvier	Webinaire FFMAS-ESI[5] pour leurs adhérents indépendants
23 janvier	Intervention lors d'une formation proposée par la DGESCO[6] pour les référents académiques
24 janvier	Webinaire coorganisé par l'AFCDP[7], Cybermalveillance.gouv.fr, et l'UFC[8]-Que Choisir sur la fraude bancaire
31 janvier	Webinaire pour l'ANCT[9] dans le cadre du programme Territoires d'Industrie
31 janvier	Webinaire pour l'UNAPL[10] (U2P)

[1] Association des petites villes de France
[2] Amazon Web Services
[3] Commerçants et Artisans des Métropoles de France
[4] Coordination Nationale pour la Sécurité des Jeux Olympiques et Paralympiques
[5] Fédération Française des Métiers de l'Assistanat et du Secrétariat
[6] Direction générale de l'enseignement scolaire
[7] Association Française des Correspondants à la protection des Données à caractère Personnel
[8] Union fédérale des consommateurs
[9] Agence nationale de la cohésion des territoires
[10] Union nationale des professions libérales

FÉVRIER

3 février	Intervention pour Agate[1] Territoires auprès d'élus et DGS[2] de communes de Savoie
9 février	Prise de parole à l'université AFCDP[3] des DPO[4]
16 février	Webinaire de sensibilisation des collectivités pour Microsoft France
21 février	Intervention auprès des acteurs de la médiation numérique du département de la Charente-Maritime
28 février	AlerteCyber pour correction d'une faille de sécurité critique dans Joomla!

[1] Agence alpine des territoires
[2] Directeur général des services
[3] Association Française des Correspondants à la protection des Données à caractère Personnel
[4] Délégué à la protection des données

17 mai 2023. Opération Cyber en Gare.

MARS

15 mars	Présentation du dispositif aux employés de Microsoft France en plénière
10 mars	Intervention auprès du Club RSSI[1] du Clusif
17 mars	Conférence au profit des acteurs de la médiation numérique du réseau national des Pimm's Médiation
21 mars	Prise de parole pour la Banque des territoires dans le cadre de leur programme Territoires d'Innovation
22 mars	Intervention auprès des Hubs territoriaux lors d'un webinaire organisé par la Banque des territoires
23 mars	Présentation de l'état de la menace aux députés de l'Assemblée nationale dans le cadre d'un petit-déjeuner parlementaire
23 mars	Conférence de presse et publication du rapport d'activité et état de la menace 2022
28 mars	Annonce du renforcement du dispositif AlerteCyber et ateliers dans le cadre de la dixième édition de la REF numérique
30 mars	BNP Paribas, Cinov Digital, Mercatel et l'Unaf[2] rejoignent le dispositif Cybermalveillance.gouv.fr

[1] Responsable de la sécurité des systèmes d'information
[2] Union nationale des associations familiales

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

AVRIL

4 avril	Intervention lors de l'AWS SUMMIT
5 avril	Lancement de la campagne *Fraude Fight Club* en partenariat avec Mastercard
13 avril	Webinaire pour les adhérents de la Fevad[1]
13 avril	AlerteCyber pour compromission de l'application 3CX Electron Desktop App
15 avril	Webinaire pour la CLCV[2]
20 avril	Intervention lors des 7e Cyber Days de BNP Paribas

[1] Fédération e-commerce et vente à distance
[2] Consommation Logement Cadre de Vie

MAI

17 mai	Opération *Cyber en Gare* avec le Groupe SNCF et l'Association e-Enfance/3018 en gare de Lyon
25 mai	Webinaire pour Mercatel
23 mai	Participation au premier salon de l'ANCTour
23 mai	Prise de parole lors de l'événement d'OCD[1] *Cybersécurité des collectivités, socle des territoires intelligents et durables*
30 mai	Intervention auprès des demandeurs d'emploi et des entreprises pour Pôle Emploi PACA[2]
31 mai	Participation aux Innodays de Bouygues Telecom

[1] Orange Cyberdéfense
[2] Provence Alpes Côte d'Azur

JUIN

6 juin	Intervention et atelier lors des 2e Rencontres de la Cybersécurité de Plaine Commune au Stade de France
8 juin	Conférence lors d'une formation proposée par la DGESCO[1] pour les référents académiques et animation d'ateliers dans le cadre d'un stage de prévention et de gestion de crise destiné aux personnels de l'Éducation nationale et de la DGESCO
8 juin	Plénière et atelier pour les élus lors d'un évènement organisé par la Métropole Aix-Marseille-Provence
13 juin	Sensibilisation des agents de la Région Île-de-France
16 juin	Prises de parole lors des conférences AWS et SNCF au salon Viva Technology
15 juin	Intervention au bénéfice de l'IGPDE[2]
20 / 21 juin	Participation au congrès du coTer numérique à Deauville. Annonce du lancement de SensCyber en collaboration avec le Ministère de la Transformation et de la Fonction publiques, la DGAFP[3], le CNFPT[4] et l'ANFH[5]
22 juin	Intervention dans le cadre de la journée cybersécurité organisée par Manche Numérique au bénéfice des élus du département
27 juin	Intervention pour la Gendarmerie nationale de la région Normandie
29 juin	Participation à la journée de coordination des Conseillers numériques organisée par le Département de l'Aube

[1] Direction générale de l'enseignement scolaire
[2] Institut de la gestion publique et du développement économique
[3] Direction générale de l'administration et de la fonction publique
[4] Centre national de la fonction publique territoriale
[5] Association nationale pour la formation permanente du personnel hospitalier

JUILLET

6 juillet Webinaire APVF[1] *Face aux risques de cybermalveillances, quelles réponses pour les petites villes ?*

19 juillet Enregistrement de deux cartouches vidéo pour l'Académie des Sciences Techniques Comptables Financières de l'Ordre des experts-comptables

[1] Association des petites villes de France

SEPTEMBRE

11 sept Intervention pour la Coordination des Conseillers numériques Île-de-France

12 sept Matinale de sensibilisation à la cybersécurité pour le CyberCercle à Valence avec la députée Mireille Clapot

19 sept Participation au séminaire annuel des personnels informatiques de la CNAM[1]

19 sept Prise de parole et atelier lors des Université d'Été de la Cybersécurité et du Cloud de Confiance d'Hexatrust à Paris

28 sept Conférence lors du 78e congrès de l'Ordre des experts-comptables

[1] Caisse nationale d'assurance maladie

OCTOBRE

2 oct Événement de lancement du Cybermoi/s organisé par Cybermalveillance.gouv.fr au Campus Cyber

2 oct Cybermalveillance.gouv.fr dévoile la CharteCyber et publie la liste de ses signataires

4 oct Intervention lors d'une journée organisée par la Préfecture de la Meuse pour les Conseillers numériques et les agents France Services

5 oct Participation aux Rencontres Nationales de l'association Déclic

5 oct Conférence au colloque SecNumEco de Vesoul

9 oct Diffusion de la campagne TV *Cybersécurité, de vraies solutions existent* en partenariat avec le groupe France Télévisions

10 oct Sensibilisation de l'ensemble des agents de la Communauté de Communes de Brie-Comte-Robert.

10 oct Intervention lors de la Journée des délégués de région académique au numérique éducatif

10 oct Lancement de la campagne Consomag réalisée en partenariat avec l'INC[1] sur les chaînes du groupe France Télévisions

11 au 14 oct Participation à la 23e édition des Assises de la Cybersécurité à Monaco

11 oct Prise de parole lors des Rencontres de la Sécurité Économique du Ministère de l'Économie et des Finances

17 oct Cybermalveillance.gouv.fr a 6 ans

18 oct Webinaire pour les adhérents de l'Unaf[2]

19 oct Intervention lors de la convention du Réseau Initia à Cannes

19 /20 oct Participation au NEC[3] à Bordeaux et annonce du lancement de la *MalletteCyber* pour favoriser l'inclusion numérique

24 oct Participation et ateliers lors des rencontres Cybersécurité AuRa CyberCercle

24 oct Prise de parole dans le cadre du programme ETIncelles pour la DGE[4]

24 oct Participation aux premières Assises de la Sécurité en Martinique

25 oct Intervention à l'événement de sensibilisation spécial Cybermoi/s organisé pour tous les agents du MIOM[5]

27 oct Conférence lors du colloque régional Bourgogne-Franche-Comté de l'AFCDP[6]

[1] Institut national de la consommation
[2] Union nationale des associations familiales
[3] Numérique En Commun[s]
[4] Direction générale des entreprises
[5] Ministère de l'Intérieur et des Outres-Mer
[6] Association Française des Correspondants à la protection des Données à caractère Personnel

NOVEMBRE

5 nov Participation à la Paris Games Week avec le MIOM

15 nov Webinaire *Comment sécuriser ma vie privée sur le Net ?* avec la CLCV[1]

16 nov Webinaire par WeTechCare et l'APVF *Prévention des risques : un enjeu d'inclusion numérique pour les collectivités et leurs habitants ?*

21 nov Publication de la deuxième étude sur la maturité cyber des collectivités

22 nov Participation au Congrès de l'AMF et des Présidents d'Intercommunalité de France à Paris

24 nov Sensibilisation des représentants territoriaux de l'Unaf à Paris

24 nov Intervention lors du Numérique en Commun[s] de la Réunion

27 nov Conférence lors de la journée Élus et Cyber organisée par le CNFPT[2] région Occitanie

28 nov Participation aux Rencontres AGIR[3] à Paris

30 nov Intervention aux côtés de France Num lors du salon Impact PME

30 nov Animation d'ateliers dans le cadre d'un stage de prévention et de gestion de crise destiné aux personnels de l'Éducation nationale et de la DGESCO[4]

DÉCEMBRE

6 déc Intervention et ateliers lors du salon Open Source Experience à Paris

12 déc Prise de parole lors de la Journée Cybersécurité de la Gazette des Communes

12 déc Participation aux 2e Rencontres judiciaires de la cybercriminalité du ministère de la Justice

13 déc Webinaire de sensibilisation aux sociétaires de la MACIF (Aéma Groupe)

21 déc Participation aux Assises de la cybersécurité du Groupe La Poste et intervention lors de la conférence plénière

2 octobre 2023. Lancement du Cybermoi/s.

[1] Consommation Logement Cadre de Vie
[2] Centre National de la Fonction Publique Territoriale
[3] Accompagnement par la Gendarmerie de l'Innovation, de l'Industrie et de la Recherche
[4] Direction générale de l'enseignement scolaire

CONFÉRENCES

Cette année, l'équipe du dispositif s'est mobilisée au travers de nombreuses conférences et webinaires. Au total, **plus de 160 interventions** ont été dispensées par Cybermalveillance.gouv.fr auprès de ses membres ou partenaires. En voici quelques exemples :

• Conférence en ligne *Fraude bancaire : et si demain, c'était vous la victime ?* avec l'AFCDP

Face à la recrudescence des fraudes bancaires en fin d'année 2022, Cybermalveillance.gouv.fr a organisé une table ronde le 24 janvier 2023 avec l'AFCDP[1] et l'UFC[2]-Que Choisir en partenariat avec l'Internaute.com. Les experts ont répondu à de nombreuses questions suscitées par le risque de fraude bancaire, pour savoir comment faire face lorsque l'on en est victime et surtout comment s'y préparer et éviter de tomber dans le piège.

• Conférence en ligne *La fraude évolue : comment protéger votre entreprise, vos collaborateurs, vos clients contre les cyber-risques et la manipulation ?* avec Mercatel et Kamae

Devant l'avancée des techniques de fraude aux paiements sur Internet, Cybermalveillance.gouv.fr, Kamae et Mercatel ont donné une conférence en ligne aux adhérents de Mercatel, le 25 mai dernier. L'opportunité de dresser un état des lieux des principales menaces mais aussi de présenter des outils et solutions pour s'en prémunir.

• Conférence en ligne *Face aux risques de cybermalveillances, quelles réponses pour les petites villes ?* avec l'APVF

Le 6 juillet s'est tenue une visioconférence co-organisée par l'APVF[3] et Cybermalveillance.gouv.fr pour les communes de moins de 25 000 habitants. L'objectif ? Les informer sur les défis de la cybersécurité et les différentes actions à mettre en place dans leur ville.

• Conférence en ligne à l'occasion du Cybermoi/s avec l'Unaf

Pour sensibiliser le grand public dans le cadre de la onzième édition du Mois européen de la cybersécurité, l'Unaf[4] et Cybermalveillance.gouv.fr ont co-organisé un webinaire le 18 octobre. La conférence a permis de nombreux échanges autour des différentes cybermenaces dont peuvent être victimes les familles et les moyens de s'en protéger.

• Intervention lors de la convention du Réseau Initia

Le 19 octobre, Cybermalveillance.gouv.fr a réalisé une sensibilisation à la cybersécurité lors de la Convention du Réseau Initia, à Cannes. L'occasion de présenter aux près de 500 adhérents Initia les menaces cyber les plus courantes et les pratiques essentielles pour s'en prémunir.

• Conférence en ligne *Comment sécuriser ma vie privée sur le Net* avec la CLCV

Comment mieux assurer sa sécurité en ligne ? Les représentants de Cybermalveillance.gouv.fr et de la CLCV[5], ont fait le point sur les cybermenaces et les conseils pour mieux protéger ses données personnelles lors d'un webinaire organisé le 15 novembre.

• Conférence aux filières RSSI et MSSI de la CNAM

Le 19 décembre, Cybermalveillance.gouv.fr est intervenu à l'occasion du séminaire interne de la CNAM[6] pour présenter le dispositif, ses services et ses ressources de sensibilisation aux RSSI[7] et MSSI[8], ainsi que les temps forts du Cybermoi/s. L'événement rassemblait 300 personnes.

[1] Association Française des Correspondants à la protection des Données à caractère Personnel
[2] Union fédérale des consommateurs
[3] Association des petites villes de France
[4] Union nationale des associations familiales
[5] Consommation Logement Cadre de Vie
[6] Conservatoire national des arts et métiers
[7] Responsable de la Sécurité du Système d'Information
[8] Manager de la Sécurité des Systèmes d'Information

ZOOM

LES **TOURS DE FRANCE**

Google Tour

Le 7 mars, Villes de France, Cybermalveillance.gouv.fr et Google France ont annoncé l'élaboration d'un programme commun de sensibilisation des collectivités locales et formé 600 agents et élus au travers de 12 villes sur l'ensemble du territoire français. Cette formation cyber, qui a débuté par deux ateliers interactifs à Châteauroux, vise à réduire les risques de cyberattaque et élever le niveau de sécurité collectif.

Numérique Éthique Tour

Fédéré par la MAIF[1], le Numérique Éthique Tour sillonne la France pour sensibiliser le plus grand nombre – citoyens, élus, enseignants, entrepreneurs… – aux sujets cyber via des expériences ludiques et immersives. Une tournée nationale débutée en septembre dernier qui aura traversé pas moins de 10 villes dans l'hexagone et à laquelle Cybermalveillance.gouv.fr s'est associé pour permettre à ces publics de s'acculturer et de mieux maîtriser leurs usages numériques au quotidien avec les bons réflexes cyber.

[1] Mutuelle assurance des instituteurs de France

LES INTERVENTIONS DE L'ANNÉE 2023

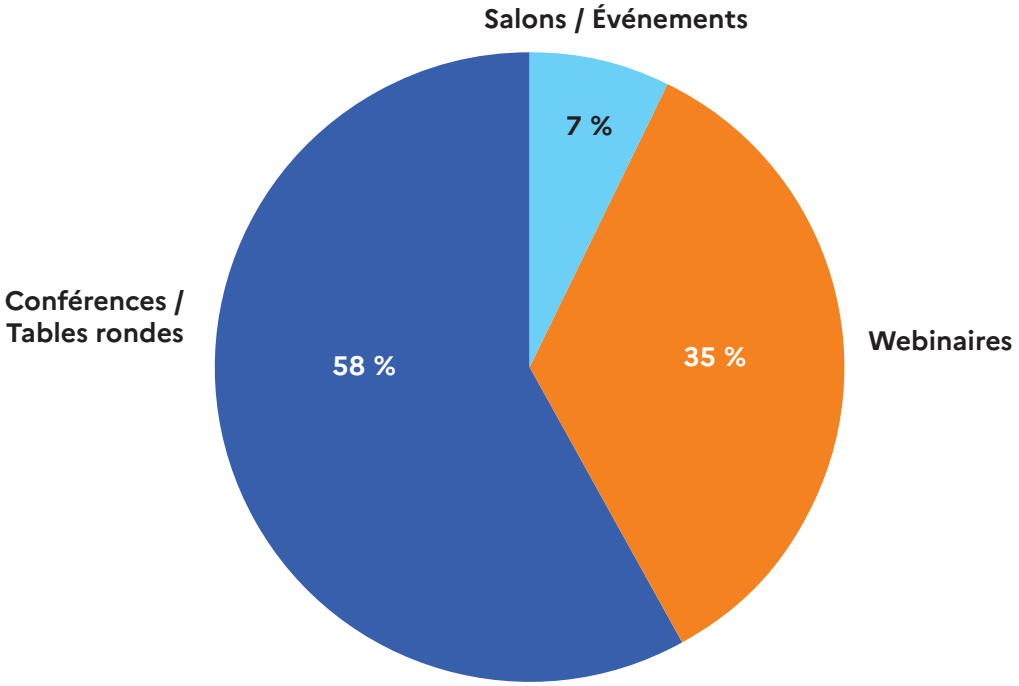
Le pôle sensibilisation de Cybermalveillance.gouv.fr a deux missions principales :

- **Coordonner et mettre en œuvre des interventions de sensibilisation à l'échelle nationale** afin d'optimiser la visibilité de la plateforme et de ses ressources.
- **Concevoir/développer des projets de sensibilisation et de pédagogie** axés sur la cybersécurité tels que SensCyber, la MalletteCyber ou encore une série de podcasts en collaboration avec l'Éducation nationale.

En 2023, le pôle totalise **166 interventions physiques et à distance**. Ainsi, ce sont plus de **22 000 personnes** qui ont bénéficié d'une sensibilisation à la cybersécurité par Cybermalveillance.gouv.fr cette année.

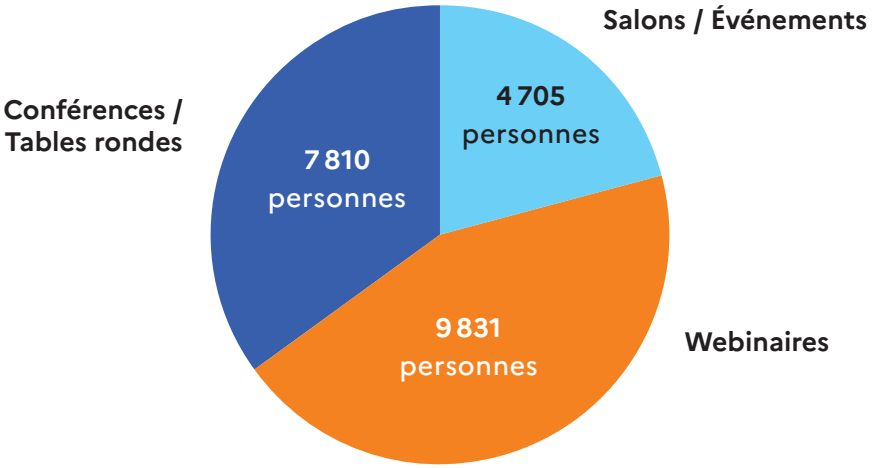
TYPOLOGIE DES INTERVENTIONS

Sur l'année 2023, les deux tiers des interventions ont eu lieu lors d'événements physiques.



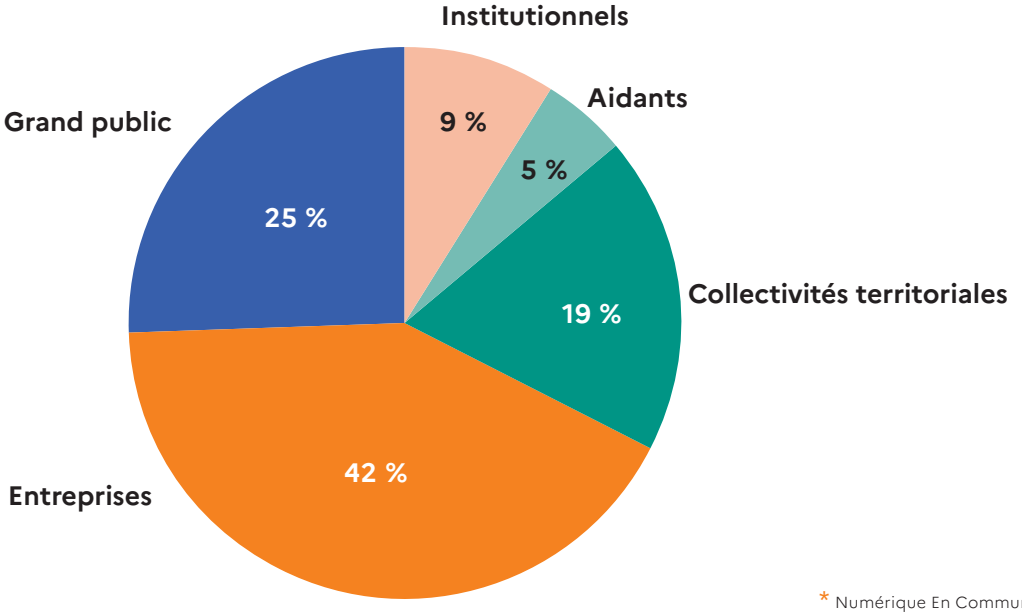
NOMBRE DE PERSONNES SENSIBILISÉES PAR TYPOLOGIE D'ÉVÈNEMENT

Au cours de l'année, **plus de 7 000 personnes ont pu être sensibilisées lors de conférences/tables rondes**, 4 705 personnes lors de salons et **9 831 personnes sensibilisées à l'occasion d'interventions en webinaire**.



TYPOLOGIE DES PUBLICS

En 2023, le **public Entreprises**, englobant les TPE-PME, artisans et professions libérales, constitue **42 % du public total sensibilisé.** Les aidants, représentant 4,99 %, ont été sensibilisés lors du NEC* Bordeaux ou par le biais de la MalletteCyber.



* Numérique En Commun[s]

NOS PRINCIPALES RÉALISATIONS

Guichet unique de la cybersécurité, Cybermalveillance.gouv.fr est également l'un des plus grands producteurs de contenus cyber en France.

En 2023, ses ressources ont été enrichies de **plus de 170 supports** et notamment de :

- **2 fiches pratiques :** Que faire en cas de cyberattaque ? (Consignes pour les collaborateurs) ; Comment piloter sa cybersécurité ? (Dirigeants).

- **2 fiches réflexes :** La fraude au faux conseiller bancaire et La fraude au virement ou au « faux RIB ».

- **2 campagnes de communication :** Groupe France Télévisions et INC[1].

- **5 articles menaces :** Campagne de messages frauduleux réclamant le paiement d'une contravention ; Le « Smishing » ou hameçonnage (*phishing*) par SMS ; Campagnes de messages d'arnaque au tueur à gages ; Coupe du monde de rugby 2023 : 5 conseils de cybersécurité ; Escroquerie à l'enfant qui a un problème avec son téléphone « Coucou maman/papa… ».

- **3 autres réalisations :** un Référentiel de Compétences Cyber pour les Prestataires ; un module de e-sensibilisation SensCyber (mis à disposition des agents de la fonction publique) ; la MalletteCyber.

- **2 AlerteCyber** : *Faille de sécurité critique dans Joomla!* et *Compromission de l'application 3CX Electron Desktop App*.

- **1 CharteCyber** (cf. pages Cybermoi/s).

- **3 campagnes en ligne :** *Cyber for Good* ; *Fraude Fight Club* et *Protection et sécurité* (cf. encadré).

- **3 affiches :** *Les essentiels de la cyber* ; *Cyber réflexes, se protéger sur Internet* (avec la CNIL[2]) et *Numérique Éthique Tour* (avec MAIF[3]).

- **1 lettre d'information mensuelle** pour le grand public, les membres et les prestataires du dispositif.

- **1 Sélection Presse hebdomadaire :** revue de presse pour les membres et les prestataires du dispositif.

[1] Institut national de la consommation
[2] Commission nationale de l'informatique et des libertés
[3] Mutuelle assurance des instituteurs de France

CRÉATION D'UN RÉFÉRENTIEL DE COMPÉTENCES CYBER POUR LES PRESTATAIRES

Dans la continuité du Label ExpertCyber, Cybermalveillance.gouv.fr a dévoilé le 15 mars un Référentiel de Compétences Cyber pour les Prestataires, en collaboration avec le groupe AFNOR, le C3NA[1] et le CFSSI[2] de l'ANSSI. Ce référentiel en libre accès constitue un état de l'art en matière de cybersécurité pour les prestataires s'adressant aux TPE-PME et a pour objectif de contribuer à l'émergence de formations dédiées pour la profession.

[1] Campus Régional de Cybersécurité et de Confiance Numérique de Nouvelle Aquitaine
[2] Centre de formation à la sécurité des systèmes d'information

ORGANISATION DE L'OPÉRATION *CYBER EN GARE*

À l'occasion du pont de l'Ascension, moment de forte affluence, Cybermalveillance.gouv.fr, le Groupe SNCF et l'Association e-Enfance/ 3018 ont organisé le 17 mai une action de sensibilisation à la cybersécurité en gare de Lyon à Paris. L'objectif de cette opération *Cyber en gare ?* Instaurer un dialogue avec les usagers et leur transmettre les bons réflexes à adopter en matière de sécurité numérique. Aux côtés de Christophe Fanichet, Directeur Général Adjoint Numérique Groupe SNCF, Jean-Noël Barrot, ministre délégué, chargé de la Transition numérique et des Télécommunications, s'est associé à la démarche et a participé à l'initiative en échangeant avec les voyageurs sur les enjeux cyber dans la gare parisienne.

COLLABORATION AVEC LE GROUPE ORANGE POUR PROMOUVOIR UNE ATTITUDE #CyberResponsable

Cela fait 6 ans qu'Orange Cyberdefense lutte contre la menace cyber aux côtés de Cybermalveillance .gouv.fr dont il est membre historique. À l'occasion du Cybermoi/s, ce partenariat a pris une nouvelle dimension avec le Groupe Orange. Une collaboration qui vise à informer, sensibiliser et accompagner les Français au quotidien via la diffusion des réflexes cyber dans 500 boutiques Orange et sur les réseaux sociaux, la publication d'articles pédagogiques sur le site bienvivreledigital.orange.fr et l'organisation d'ateliers de sensibilisation à la cyber gratuits, partout sur le territoire, tout au long de l'année, dont l'atelier *Sécuriser son smartphone* co-construit avec Cybermalveillance.gouv.fr.

PROGRAMME DE E-SENSIBILISATION SENSCYBER

SENSCYBER
E-sensibilisation à la cybersécurité pour tous

Avec plus de 5 millions d'agents en France, les services publics, administrations et collectivités représentent une part non négligeable de la population active et sont la cible quotidienne de cyberattaques. Fort de ce constat, Cybermalveillance.gouv.fr a annoncé le 20 juin le lancement de SensCyber, un programme de e-sensibilisation à la cybersécurité destiné aux agents de la fonction publique. Développé dans le cadre du volet cyber du Plan France Relance et proposé à ces publics en partenariat ave le CNFPT[1] et le ministère de la Transformation et de la Fonction Publiques dans le cadre du plan France Relance, SensCyber répond à 3 objectifs pédagogiques : connaître les risques, savoir comment se protéger et transmettre les bonnes pratiques.

[1] Centre national de la fonction publique territoriale

LANCEMENT DE LA MALLETTECYBER POUR FAVORISER L'INCLUSION NUMÉRIQUE

Selon un rapport de l'ANCT[1] publié en 2023, 16 millions de Français restent encore « éloignés du numérique », soit 31,5 % de la population. Afin de protéger ces publics plus vulnérables et de les rapprocher du numérique, Cybermalveillance.gouv.fr et l'ANCT ont annoncé le 18 octobre la sortie de la MalletteCyber : des contenus de sensibilisation et des outils pédagogiques mis gratuitement à la disposition des acteurs de la médiation numérique. L'objectif ? Leur permettre de s'acculturer à la cybersécurité et transmettre à leurs publics, des conseils pratiques et accessibles clé en main.

[1] Agence nationale de la cohésion des territoires

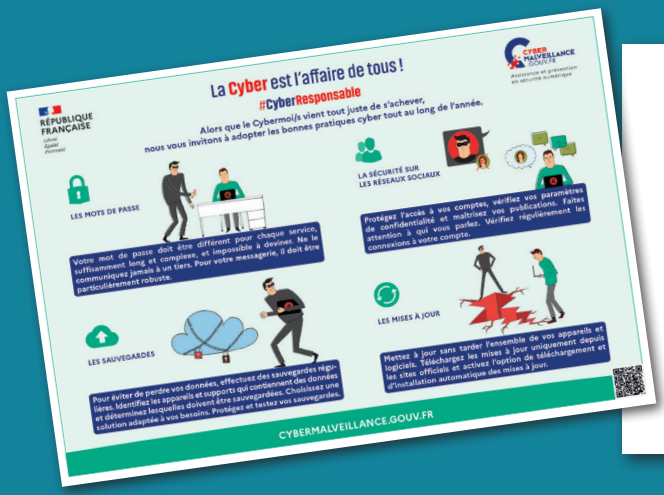
PUBLICATION D'UNE ÉTUDE SUR LA MATURITÉ CYBER DES COLLECTIVITÉS DE MOINS DE 25 000 HABITANTS

Dans la continuité de ses actions de sensibilisation auprès des collectivités, Cybermalveillance.gouv.fr a mené une étude pour évaluer la maturité des collectivités de moins de 25 000 habitants en matière de cybersécurité. Les résultats de l'enquête, dévoilés mi-novembre, ont notamment révélé que si les collectivités sont davantage sensibilisées, 53 % d'entre elles ne se sentent pas préparées. 75 % d'entre elles allouent moins de 2 000 € à la cyber et seules 12 % comptent faire évoluer ce budget à la hausse. Et en termes d'attentes, c'est la sensibilisation qu'elles plébiscitent à 64 %.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

LES **CAMPAGNES PRESSE ET EN LIGNE**

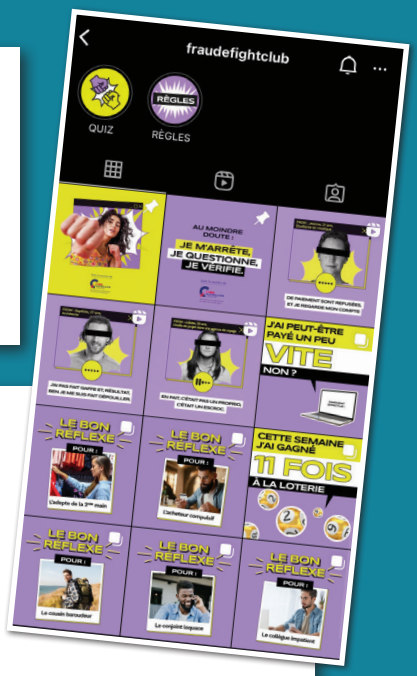


Campagne de sensibilisation presse avec l'ANCT

En octobre, un focus sur les bonnes pratiques cyber à adopter a été réalisé dans la presse dans le cadre d'une communication sur l'offre de service des Conseillers numériques auprès du grand public. Fruit d'une collaboration entre Cybermalveillance.gouv.fr et l'ANCT, cet encart a été distribué dans 16 supports de presse quotidienne régionale et décliné dans leurs éditions respectives.

Lancement de la campagne *Cyber for good* pour les professionnels

En février, Cybermalveillance.gouv.fr a pris part à la campagne portée par Numeum pour souligner l'importance de la cyber dans le développement des entreprises. La démarche visait notamment à mettre en avant les métiers de la cybersécurité à travers la diffusion d'une série de 3 vidéos disponibles sur Tech Talk.



Réalisation de deux capsules vidéo *Protection et sécurité* pour les 6e

Dans le cadre de la sensibilisation des élèves de 6e aux enjeux cyber, une collection de 6 capsules vidéo a été réalisée en partenariat avec la CNIL[1], Cybermalveillance.gouv.fr, l'Association e-Enfance/3018 et Pix. Accessibles sur Pix et les sites des partenaires, ces vidéos détaillent les bons usages à adopter sur Internet et les réseaux sociaux ainsi que les dérives et risques liés à ces outils.

[1] Commission nationale de l'informatique et des libertés

Diffusion de la campagne *Fraude Fight Club* à destination des *millennials*

Forts d'une étude mettant en lumière la vulnérabilité des millennials face à la fraude par ingénierie sociale sur Internet, Mastercard et Cybermalveillance.gouv.fr ont lancé le 5 avril *Fraude Fight Club*, une initiative inédite sur Instagram à destination des 25-35 ans. Basée sur la parole des victimes, la campagne vise à aiguiser les réflexes de chacun contre les tentatives de fraude.

CYBERMOI/S 2023 : UN MOIS POUR DEVENIR #CYBERRESPONSABLE

Copiloté en 2022 par l'ANSSI*, l'organisation de la 11e édition du Cybermoi/s a cette année été confiée au dispositif national d'assistance aux victimes d'actes de cybermalveillance, Cybermalveillance.gouv.fr.

TOUS PUBLICS

• Événement de lancement au Campus Cyber

Cybermalveillance.gouv.fr a donné le coup d'envoi de la 11e édition du Cybermoi/s avec un événement de lancement organisé le 2 octobre au Campus Cyber, lieu totem de la cybersécurité en France. À cette occasion, différentes thématiques ont été abordées pour tous les publics sous forme de conférences.

- Un échange institutionnel avec avec Jean-Noël Barrot, ministre délégué chargé du numérique et Charlotte Caubel, secrétaire d'État chargée de l'enfance ;
- 3 tables rondes avec 12 intervenants;
- Près de 150 spectateurs en salle et + de 2000 personnes sur la diffusion en ligne.

#CyberResponsable

• Action citoyenne #CyberResponsable

Afin de mobiliser le plus grand nombre d'internautes autour de cet enjeu sociétal qu'est la cyber, Cybermalveillance.gouv.fr a organisé une action de sensibilisation collective d'envergure sur les réseaux sociaux. Le principe ? Poster ensemble au même moment un conseil cyber accompagné du hashtag #CyberResponsable.

- 6 conseils cyber illustrés associés chacun à une peinture;
- 63 millions d'impressions des hashtags #CyberResponsable et #Cybermois sur X.

• Agenda du Cybermoi/s en France

Fortement plébiscité par les internautes, Cybermalveillance.gouv.fr a mis à disposition de tous les publics, un agenda commun recensant l'ensemble des actions de sensibilisation cyber menées en France durant le mois d'octobre.

- + de 150 événements ont été ainsi référencés sur le territoire français.

* Agence nationale de la sécurité des systèmes d'information

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

• Cyber Quiz Famille en ligne pour tester ses connaissances

Pour la deuxième année consécutive, Cybermalveillance.gouv.fr a organisé le Cyber Quiz Famille, un jeu-concours sur le thème de la cybersécurité pour tester ses réflexes et adopter les gestes essentiels recommandés dans le Cyber Guide Famille.

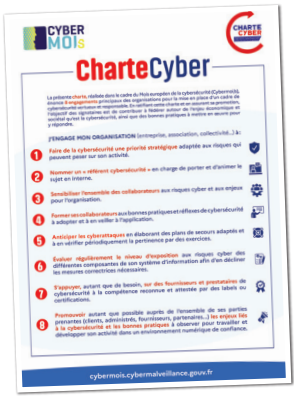
- 10 313 participants ;
- 50 gagnants ;
- + de 3 700 téléchargements du Cyber Guide Famille.

PROFESSIONNELS COLLECTIVITÉS

• CharteCyber

À l'occasion du Cybermoi/s, Cybermalveillance.gouv.fr a édicté une CharteCyber avec pour objectif de positionner la cyber comme un enjeu sociétal majeur et de favoriser la mise en place d'un cadre de cybersécurité vertueux et responsable dans les organisations.

- 8 engagements sur les volets techniques et humains ;
- + de 100 signataires fin octobre ;
- + de 2 000 téléchargements.



• Une action inédite à destination des prestataires informatiques

Pour le Cybermoi/s, Cybermalveillance.gouv.fr a spécifiquement conçu, en partenariat avec le CampusCyber et avec le soutien de l'ensemble des fédérations, syndicats et groupements de prestataires informatiques, une fiche de cybersécurité pour sensibiliser les entreprises.

- 5 recommandations cyber essentielles pour les TPE/PME ;
- Une douzaine de syndicats/fédérations/groupements de prestataires ont diffusé cette fiche auprès de leurs adhérents ;
- + de 10 000 entreprises adressées en direct (hors diffusion via les réseaux sociaux) par près de 600 prestataires.

• Campagnes nationales TV-médias sur France Télévisions et 4 Consomag

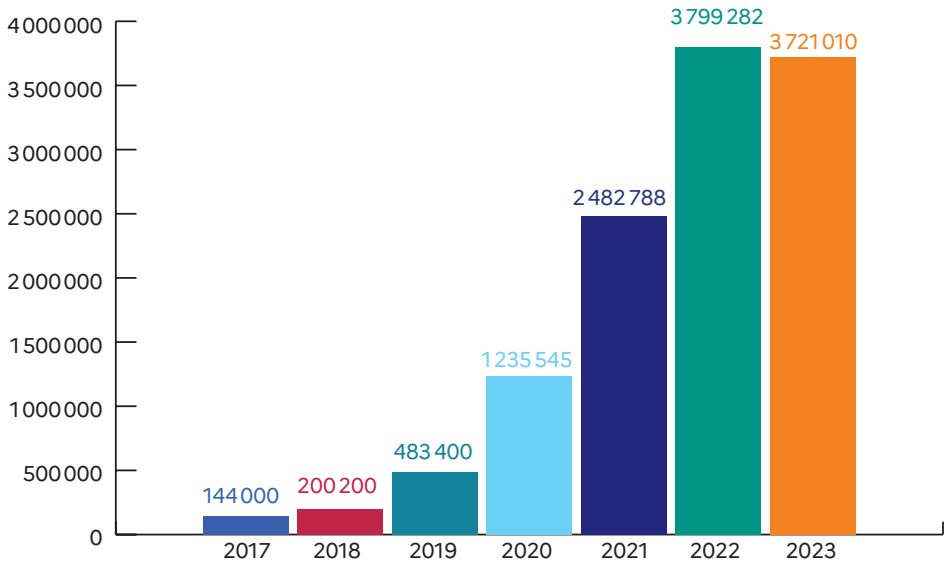
Dans le cadre du Cybermoi/s, Cybermalveillance.gouv.fr a renouvelé son partenariat avec le groupe France Télévisions qui a diffusé la campagne de sensibilisation *Cybersécurité de vraies solutions existent* dédiée aux particuliers, collectivités et entreprises. En parallèle, une nouvelle série d'émissions Consomag a été réalisée en collaboration avec l'INC* et a également été diffusée sur les chaînes du Groupe France Télévisions touchant plusieurs millions de téléspectateurs.

* Institut national de la consommation

ÉTAT DE LA MENACE

FRÉQUENTATION DE LA PLATEFORME CYBERMALVEILLANCE.GOUV.FR

Avec 3,7 millions de visiteurs en 2023, la fréquentation de la plateforme Cybermalveillance.gouv.fr se stabilise à un niveau élevé.



Fréquentation annuelle de la plateforme Cybermalveillance.gouv.fr

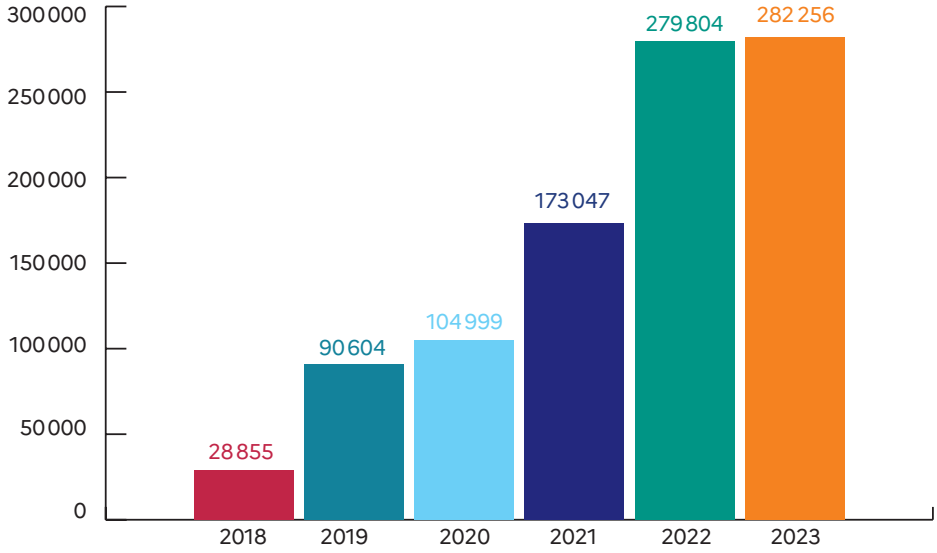
La fréquentation de la plateforme Cybermalveillance.gouv.fr est restée globalement stable en 2023 avec 3,7 millions de visiteurs et reste majoritairement centrée sur les contenus et services d'assistance. À noter que plusieurs phénomènes qui avaient drainé un fort trafic sur le site en 2022 ne se sont heureusement pas reproduits, ou dans une bien moindre mesure : violations de données médicales (Ameli et CHSF), fortes vagues d'hameçonnage à l'infraction pédopornographique, à la livraison de colis, à la vignette Crit'Air, escroqueries au CPF…

Avec plus de 12 millions de visiteurs depuis sa création en 2017, **la plateforme maintient son rang de référence en termes de prévention et d'assistance pour ses publics.** Un palier risque toutefois d'être atteint dans l'état des moyens du dispositif pour promouvoir et développer son action.

3,7 millions de visiteurs en 2023

LES CHIFFRES 2023 DE LA CYBERMALVEILLANCE

L'analyse des plus de 280 000 demandes d'assistance en ligne sur la plateforme Cybermalveillance.gouv.fr donne une vision des différentes formes de cybermalveillance rencontrées par les publics du dispositif.



Évolution des recherches d'assistance

Le service d'assistance en ligne de Cybermalveillance.gouv.fr traite 51 formes différentes de cybermalveillance. Après avoir sélectionné son profil (particulier, entreprises/association, collectivité/administration) la victime est invitée à répondre à quelques questions pour obtenir un diagnostic du phénomène auquel elle est confrontée et disposer des conseils et orientations nécessaires pour y faire face. En fonction de la cybermalveillance qui la touche, la victime peut également se voir proposer d'être mise en relation au besoin avec les 1 250 prestataires référencés par Cybermalveillance.gouv.fr sur l'ensemble du territoire national en capacité de lui apporter une assistance technique de proximité.

282 256 demandes d'assistance en ligne ont été réalisées sur la plateforme en 2023, à un niveau stable par rapport à l'année précédente.

Le taux de satisfaction des publics pour ce service d'assistance en ligne reste élevé (89,5 %).

280 000
demandes d'assistance en ligne en 2023

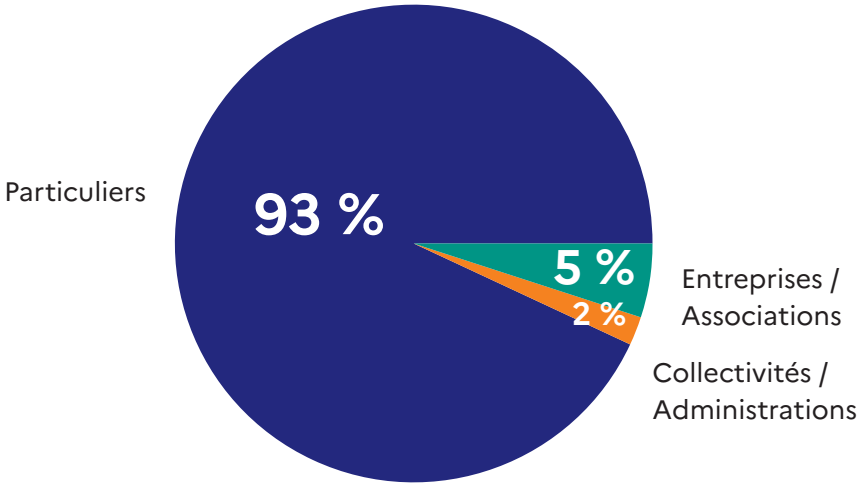
• Répartition des demandes d'assistance

+17 %
de demandes d'assistance de collectivités

Sur la base des demandes d'assistance où la catégorie de public est connue, la répartition des publics demeure quasi stable en proportion en 2023 avec **93 % de particuliers, 5 % d'entreprises/associations et 2 % de collectivités/administrations.**

+13 %
de demandes d'assistance de particuliers

L'analyse rapportée aux volumes respectifs des catégories de publics (68 millions de particuliers, 6 millions d'entreprises et associations, et 36000 collectivités), démontre que pour un particulier qui a eu recours au service d'assistance de la plateforme, on compte environ 1 entreprise/association et 35 collectivités/administrations.



Répartition des demandes d'assistance par catégories de public

Répartition des demandes d'assistance par catégories de public		
	2023	**Variation n-1**
Particuliers	**221 066**	**+13 %**
Professionnels dont :	16 790	+4 %
Entreprises / Associations	**12 668**	**+0 %**
Collectivités / Administrations	**4 122**	**+17 %**

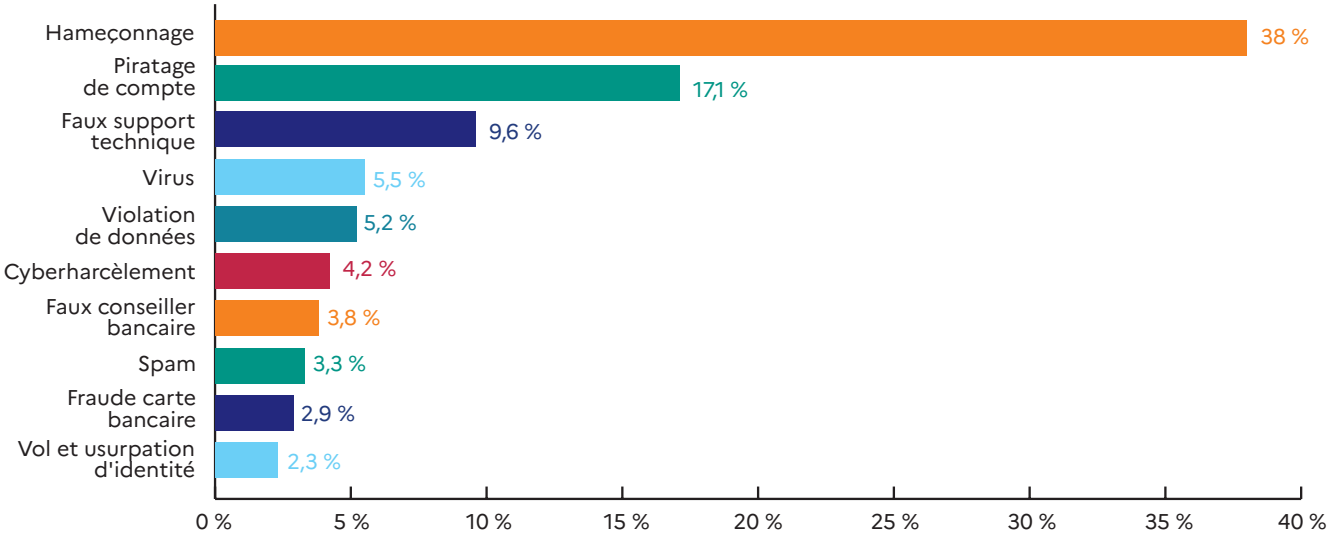
PRINCIPALES MENACES PAR CATÉGORIES DE PUBLIC EN 2023

L'analyse quantitative des 10 principales menaces par catégorie de public sur les 51 que traite l'outil d'assistance en ligne permet de mettre en évidence les grandes tendances de la cybermalveillance et leur évolution.

D'une manière générale et pour toutes les catégories de publics du dispositif, on constate un resserrement des demandes d'assistance sur les menaces du haut du spectre qui gagnent en intensité. Certaines menaces du bas du spectre semblent donc progressivement délaissées par les cybercriminels car sans doute devenues moins rentables.

À noter toutefois que cet indicateur quantitatif ne reflète pas les conséquences qu'une cybermalveillance peut avoir pour une victime, que ce soit sur le plan financier, psychologique, réputationnel, juridique, parfois même dans la durée, et qui peuvent être très différentes d'une victime à l'autre.

• Particuliers



Principales recherches d'assistance pour les particuliers

Avec 38 % des demandes d'assistance, l'**hameçonnage** sous ses différentes formes reste de loin la première menace qui touche les particuliers à un niveau comparable à celui de l'année précédente bien qu'en léger retrait, en volume (-6 %).

Le **piratage de compte** est en seconde position des cybermalveillance les plus fréquentes pour les particuliers et continue de progresser tant en proportion (+3 points) qu'en volume (+22 %).

Particuliers	2023	Variation en volume vs 2022
Hameçonnage	38,0 %	-6 %
Piratage de compte	17,1 %	+22 %
Faux support technique	9,6 %	+2 %
Virus	5,5 %	+67 %
Violation de données	5,2 %	-69 %
Cyberharcèlement	4,2 %	+23 %
Faux conseiller bancaire	3,8 %	+78 %
Spam	3,3 %	+46 %
Fraude carte bancaire	2,9 %	+87 %
Vol et usurpation d'identité	2,3 %	+93 %

Quant au **faux support technique**, il reprend la troisième place à un niveau quasi équivalent en intensité par rapport à l'année antérieure (+2 %).

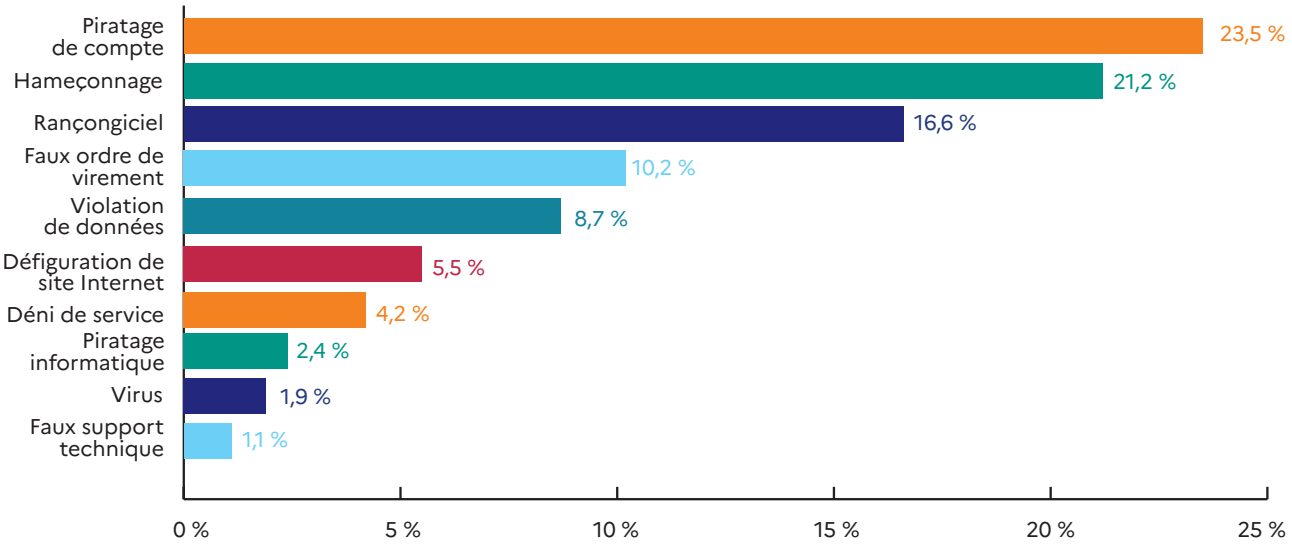
Si la majorité des principales cybermalveillances progressent sensiblement, les augmentations les plus significatives de ce classement concernent les **fraudes à la carte bancaire** (+87 %), les **fraudes au faux conseiller bancaire** (+78 %), les programmes malveillants ou « **virus** » (+67 %) et les **vols et usurpations d'identité** (+93 %).

Le **spam électronique et téléphonique** (+46 %), et les faits de **cyberharcèlement** (+23 %) qui recouvrent un vaste champ d'acceptions pour les victimes, apparaissent également en hausse notable.

En revanche, une baisse importante des demandes d'assistance pour des **violations de données personnelles** est constatée par rapport à 2022 (-69 %) qui avait été une année marquée par des fuites de données personnelles médicales importantes touchant plus de 1,2 million de personnes et qui ne se sont pas reproduites en 2023.

Enfin, des menaces telles que les **escroqueries sentimentales** (+91 %) ou au **placement financier** (+189 %) ne figurent pas dans ce classement, car elles restent relativement faibles en proportion (moins de 1 %), bien qu'en très forte progression et avec des montants de préjudice financier souvent considérables pour les particuliers qui en sont victimes.

• Entreprises et associations



Principales recherches d'assistance pour les entreprises et les associations

Le **piratage de compte** est en 2023 la première cause des recherches d'assistance des entreprises et associations, en hausse notable (+26 % en volume).

L'**hameçonnage** (21 %) et les attaques par **rançongiciel** (17 %) suivent en tête du classement pour cette catégorie de public à un niveau quasi stable, suivi par les **fraudes aux virements** qui se montrent à nouveau sur l'année 2023 en hausse significative en volume (+63 %).

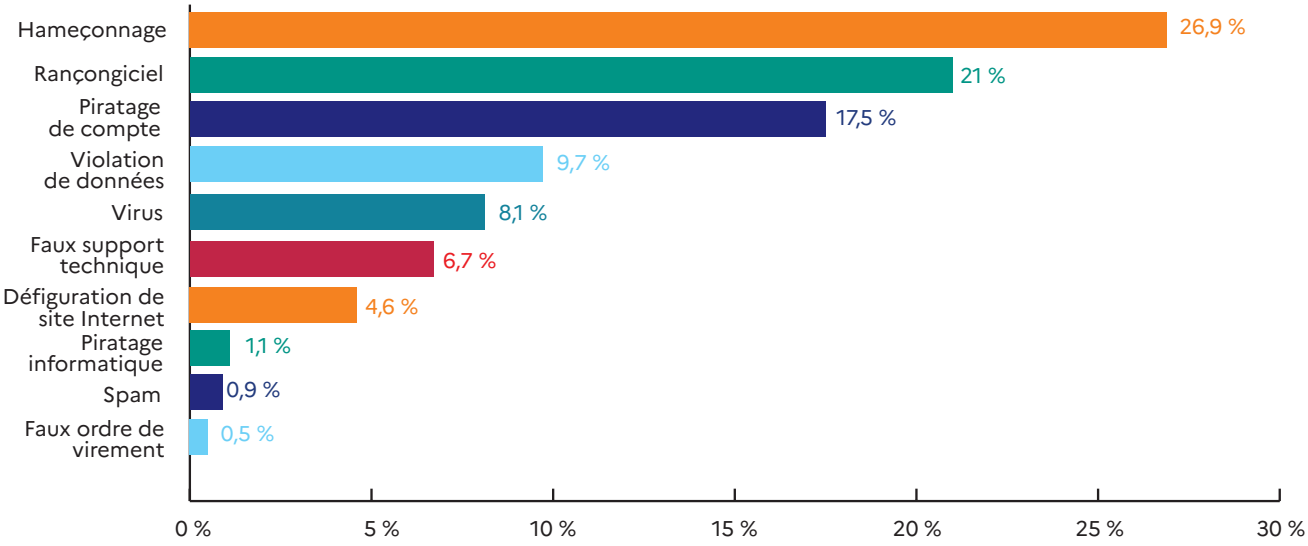
Déjà identifiées en 2022 en résurgence significative, les attaques contre les **sites Internet** des professionnels maintiennent leur position dans ce classement en forte augmentation en volume avec +61 % de recherches d'assistance pour des attaques en **défiguration** et +41 % pour des attaques en **déni de service**.

Pour ce qui concerne les **violations de données**, elles restent à un niveau stable en proportion, bien qu'en augmentation substantielle en volume (+38 %).

Il est ici intéressant de noter que ce classement apparaît très similaire à celui de l'année précédente, ce qui tend à démontrer que les menaces principales sont bien identifiées et que les attaques se resserrent sur le haut du spectre.

Entreprises / Associations	2023	Variation en volume vs 2022
Piratage de compte	23,5 %	+26 %
Hameçonnage	21,2 %	+2 %
Rançongiciel	16,6 %	+8 %
Faux ordre de virement	10,2 %	+63 %
Violation de données	8,7 %	+38 %
Défiguration site Internet	5,5 %	+61 %
Déni de service	4,2 %	+41 %
Piratage informatique	2,4 %	+20 %
Virus	1,9 %	+11 %
Faux support technique	1,1 %	-11 %

• Collectivités et administrations



Principales recherches d'assistance pour les collectivités et les administrations

Pour les collectivités et administrations le classement 2023 des principales de recherches d'assistance sur Cybermalveillance.gouv.fr demeure globalement stable par rapport à l'année précédente.

L'**hameçonnage** reste la principale menace rencontrée pour cette catégorie de public avec 27 % des demandes en augmentation de 26 % en volume.

Il est suivi par les attaques par **rançongiciel** (21 %) et le **piratage de compte** en ligne (17,5 %).
Si les variations en proportions par rapport à l'année 2022 n'apparaissent pas significatives, il n'en va pas de même pour les variations en volumes qui sont souvent en hausse très marquées : +73 % pour les **défigurations de site Internet**, +71 % pour les programmes malveillants **(virus)**, +54 % pour les fraudes au **faux support technique**, +45 % pour les **violations de données**...

Pour les collectivités et administrations, comme pour les entreprises et associations, les principales menaces qui les visent continuent donc de gagner en intensité.

Collectivités	2023	Variation en volume vs 2022
Hameçonnage	26,9 %	+26 %
Rançongiciel	21,0 %	+36 %
Piratage de compte	17,5 %	+22 %
Violation de données	9,7 %	+45 %
Virus	8,1 %	+71 %
Faux support technique	6,7 %	+54 %
Défiguration site Internet	4,6 %	+73 %
Piratage informatique	1,1 %	-21 %
Spam	0,9 %	+43 %
Faux ordre de virement	0,5 %	+150 %

LES **GRANDES TENDANCES DE LA MENACE** EN 2023

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

L'HAMEÇONNAGE (*PHISHING*) : LA MENACE PRÉDOMINANTE POUR TOUS LES PUBLICS

Première menace pour les particuliers et les collectivités et administrations, et seconde pour les entreprises et associations, **l'hameçonnage (*phishing* en anglais) reste en 2023 la principale menace pour toutes les catégories de publics** au niveau élevé d'intensité constaté en 2022.

L'hameçonnage peut prendre de multiples formes : messages électroniques (mail), SMS (*smishing*), messages instantanés, publications sur les réseaux sociaux, liens sponsorisés sur les moteurs de recherches, appels téléphoniques (*vishing*), QR codes frauduleux (*quishing*, voir page 31)...

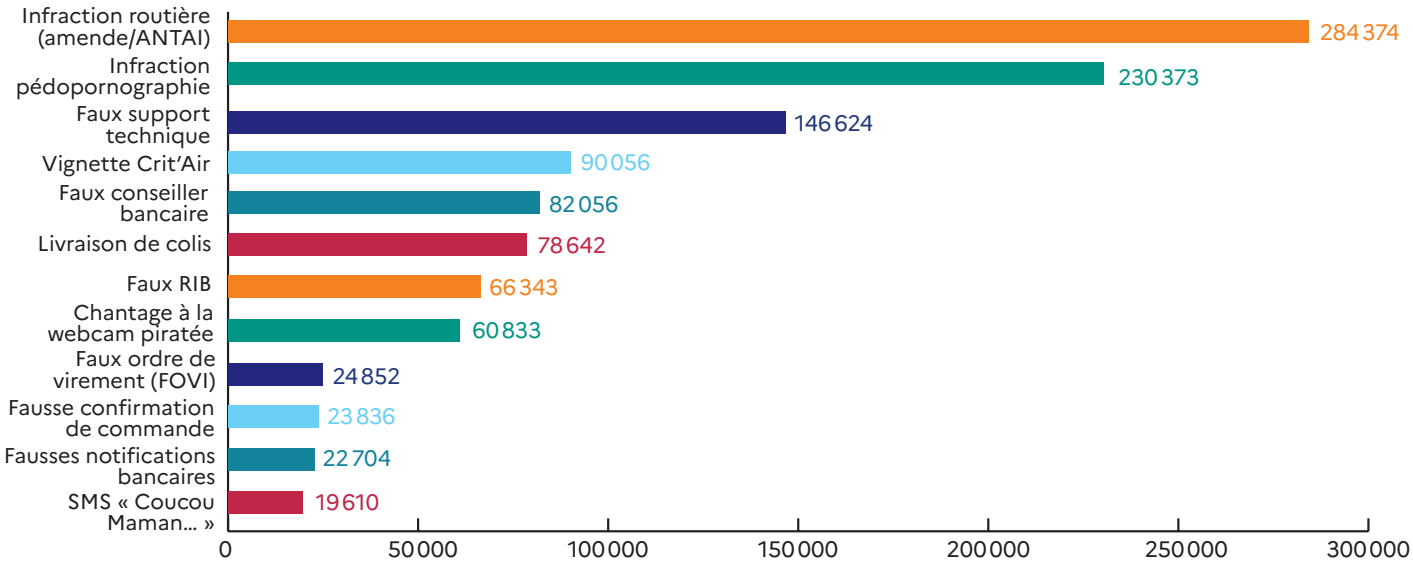
Il vise toujours à créer, sous une apparence légitime et crédible, un sentiment d'urgence ou d'intérêt chez les victimes pour les tromper afin de les inciter à réaliser une action, comme fournir des données personnelles ou confidentielles (mots de passe, coordonnées de carte bancaire, codes de validation...) ou télécharger un programme malveillant (virus) qui prendra le contrôle de leur appareil.

Il existe depuis maintenant plusieurs années **un véritable écosystème cybercriminel de l'hameçonnage** qui commercialise des méthodes, listes d'adresses mail ou de numéros de téléphone actifs, faux messages, faux sites très réalistes, à des tarifs toujours plus compétitifs qui les rendent accessibles à une petite cyberdélinquance en fort développement.

Les informations récupérées suite à un hameçonnage sont revendues sur les places de marché cybercriminelles à toute personne qui se pense en capacité de les exploiter.

Pour les victimes, **les conséquences d'un hameçonnage peuvent être diverses** : piratage de compte, débits bancaires frauduleux, infection virale, attaque par rançongiciel, appel de faux conseillers bancaires...

En 2023, les contenus produits par Cybermalveillance.gouv.fr sur les principales formes d'hameçonnage et les moyens d'y faire face ont recueilli **1,5 million de consultations** et 50 000 particuliers et professionnels ont recherché une assistance sur ce phénomène.



Hameçonnages les plus fréquents en 2023 (nombre de consultations)

Ce classement des types d'hameçonnage les plus fréquents en 2023 montre la grande diversité des prétextes utilisés par les cybercriminels.

Info ANTAI :

Vous avez un retard de paiement de 68,00e, dossier référence 20023099.

Consulter mon dossier d'infraction via : https://antai-amendes-gouv.org/

Avec plus de 280 000 consultations de l'article dédié, l'hameçonnage par mail, et surtout par SMS, à l'**infraction routière** demandant le paiement d'une amende fictive est le phénomène le plus important qui a perduré tout au long de l'année 2023.

L'hameçonnage à l'**infraction pédopornographique**, a quant à lui considérablement baissé en intensité tout en restant à un niveau très élevé de recherches d'assistance. Les multiples communications réalisées sur cette forme de malveillance depuis maintenant trois ans ne sont sans doute pas étrangères à cette baisse, même si un public toujours trop nombreux continue de s'interroger sur ces messages frauduleux.

L'hameçonnage à la **vignette Crit'Air**, qui avait marqué la fin de l'année 2022 jusqu'au début de l'année 2023, s'est finalement tari au premier trimestre, mais pourrait évidemment ressurgir en fonction de l'actualité.

Phénomène de la fin de l'année 2023, l'hameçonnage à l'enfant qui a un problème avec son téléphone (dit « **coucou maman**… ») a rapidement fait une entrée remarquée dans ce classement et pourrait s'installer dans la durée.

Coucou maman, c'est moi. J'ai eu un problème avec mon numéro de téléphone, c'est mon numéro temporaire. Envoie moi un message sur WhatsApp, sur ce numéro le plus rapidement possible ! Je ne pourrai plus te répondre ici comme je n'ai pas de crédit, je dois te parler de quelque chose…

LE « QUISHING » : L'HAMEÇONNAGE PAR QR CODE

À l'instar des codes-barres, un QR code est une image codifiée contenant des informations, comme un lien qui peut rediriger l'utilisateur sur un site ou lui permettre de télécharger une application. Les QR codes se sont largement répandus ces dernières années, car ils présentent un caractère pratique indéniable en permettant d'éviter la saisie manuelle et fastidieuse de liens sur les appareils mobiles en particulier.

Comme pour toute nouveauté technologique, **la démocratisation des QR codes a rapidement attiré l'attention des cybercriminels**. Faux avis de contravention reçus au domicile ou laissés sur les pare-brise de véhicules stationnés dans plusieurs villes de France, faux avis de passage de La Poste déposés dans des boîtes aux lettres, faux QR codes collés sur des parcmètres ou sur des bornes de recharges de véhicule électriques, faux QR codes de confirmation de connexion Office365… Les QR codes frauduleux (appelés *quishing* en anglais) ont commencé à s'inviter régulièrement dans l'actualité nationale de l'hameçonnage en 2023.

Pour Cybermalveillance.gouv.fr, si **des QR codes commencent à être de plus en plus utilisés dans des messages d'hameçonnage pour renforcer leur apparence officielle**, à l'instar des fausses infractions pédopornographiques qui contiennent parfois un QR code qui renvoie sur le vrai site de la gendarmerie, **leur développement reste toutefois encore marginal.**

En effet, l'envoi d'un QR code malveillant par message électronique, s'il peut être massif, peut apparaître incongru, car il faut un second appareil pour le scanner. Cela présente donc de facto un faible taux de réussite possible pour les cybercriminels. En revanche, la distribution physique de QR code, que ce soit pour des notifications d'amende déposées sur les pare-brises ou pour coller des QR codes de substitution, ne peut cibler qu'un nombre limité de victimes potentielles. Par ailleurs, ce type d'opération présente de fait un faible retour sur investissement pour les cybercriminels, et un risque important pour eux de se faire identifier et donc interpeller.

Si la menace des QR codes malveillants reste encore relativement mineure, elle n'en demeure pas moins réelle, car elle joue sur la difficulté que peuvent avoir les victimes à identifier des liens frauduleux, a fortiori lorsqu'ils sont masqués par un QR code qui n'est pas immédiatement lisible. Les QR codes malveillants peuvent alors diriger l'utilisateur abusé vers un site frauduleux ou lui faire télécharger un virus.

Au même titre qu'un lien contenu dans un message, **avant de suivre le lien proposé par un QR code, il convient donc toujours d'en vérifier la vraisemblance et de s'abstenir de l'ouvrir au moindre doute**.

LES RAVAGES DES ESCROQUERIES AU FAUX CONSEILLER BANCAIRE

Identifiées en 2022 comme un nouveau phénomène majeur en devenir, les escroqueries au faux conseiller bancaire ont confirmé cette tendance avec une très forte expansion durant l'année écoulée (+78 %).

Signe de l'ampleur du phénomène, il s'agit de la 7e menace la plus fréquente en 2023 pour les particuliers. Ce sont ainsi **5 000 personnes qui sont venues chercher une assistance sur Cybermalveillance.gouv.fr sur cette forme de cyberescroquerie** et l'article décrivant les moyens d'y faire face a fait l'objet de 80 000 consultations.

Ces escroqueries d'**ingénierie sociale** sont généralement consécutives d'un hameçonnage réussi qui permet aux escrocs de récupérer les informations nécessaires pour crédibiliser leur arnaque (identité, adresse, numéro de carte bancaire, voire mot de passe du compte en ligne…). Dans d'autres cas rapportés, l'hypothèse d'un virus voleur d'informations (infostealer) sur un des appareils de la victime ne peut être exclue.

Les montants de préjudice pour les victimes peuvent être considérables, car en abusant de leur confiance pour leur faire valider des opérations frauduleuses, les escrocs peuvent aller jusqu'à vider l'intégralité de leurs comptes bancaires.

> E-Paiement : Transaction en cours de 899.99€ saisissez le code 244856 ou contactez le centre d'opposition au 0184608228

Ce mode opératoire a vu en 2023 de nombreuses évolutions et déclinaisons différentes. Parmi les principales, des **faux mails ou SMS de validation d'achat** demandant de rappeler un numéro prétendu d'opposition frauduleux. Dans ce cas, ce ne sont plus les escrocs qui contactent la victime, mais la victime elle-même. Paniquée, elle va contacter l'escroc en lui demandant de l'aide. L'escroc pourra alors la manipuler pour lui dérober son numéro de carte bancaire ou même lui pirater ses comptes et en soustraire les fonds.

FAUX SUPPORT TECHNIQUE, DES MODES OPÉRATOIRES TOUJOURS PLUS AGRESSIFS

En 2023, les escroqueries au faux support technique Microsoft ou Apple reprennent la 3e place des principales menaces pour les particuliers et se maintiennent à un niveau très élevé avec 12 000 recherches d'assistance et 140 000 consultations de l'article permettant d'y faire face.

Les professionnels, et surtout ceux qui ne disposent pas de support informatique, ne sont pas épargnés par cette menace.

Les modes de déclenchement d'une alerte anxiogène indiquant une infection virale et demandant d'**appeler en urgence un prétendu support technique** « gratuit » restent globalement similaires. Ils reposent principalement sur un hameçonnage par courrier électronique (fausses notifications ou lettres d'informations par exemple) contenant des liens malveillants ou par des pages frauduleuses sponsorisés sur les moteurs de recherche.

En revanche depuis fin 2022 le mode opératoire des opérateurs de faux support technique, qui repose également sur l'ingénierie sociale, se révèle **beaucoup plus agressif**. Aujourd'hui, les escrocs ne se contentent plus de faire payer un dépannage à distance factice. Les cybercriminels **prennent le contrôle des comptes bancaires en ligne de la victime** au prétexte que la pseudo-infection virale les aurait affectés. Ils vont ensuite manipuler la victime pour lui faire valider des opérations, soi-disant pour « sécuriser » ses comptes bancaires mais qui en réalité vont avoir pour effet de leur permettre de les piller, à l'instar des modes opératoires d'arnaques au faux conseiller bancaire.

Les montants constatés de préjudice pour les victimes d'escroquerie au faux support technique, qui jusqu'alors étaient de quelques centaines d'euros, peuvent aujourd'hui atteindre **plusieurs milliers, voire dizaines de milliers d'euros**.

LE PIRATAGE DE COMPTE EN LIGNE, MENACE MAJEURE QUI DEMEURE EN FORTE EXPANSION

Deuxième menace toutes catégories de publics confondus, **le piratage de compte en ligne continue de progresser fortement en 2023 (+22 %)**. Ce sont ainsi près de 25000 particuliers et professionnels qui ont demandé une assistance sur Cybermalveillance.gouv.fr pour cette menace et les articles dédiés ont fait l'objet de près de 280000 consultations.

Le piratage de compte en ligne concerne tous types de comptes et principalement les messageries, réseaux sociaux, banques, opérateurs téléphoniques, mais également des sites d'administrations (Ameli, impôts, CAF, CPF...). Là aussi, ces piratages sont généralement consécutifs d'un hameçonnage auquel aura répondu la victime, à la réutilisation d'un même mot de passe sur plusieurs accès dont l'un aura été compromis, ou à l'infection d'un de ses appareils par un virus voleur d'information (*Infostealer*).

Les conséquences du piratage d'un compte de messagerie s'avèrent souvent très importantes, car il permet au cybercriminel de pouvoir contrôler tous les comptes qui y sont rattachés (réseaux sociaux, sites administratifs ou de commerce en ligne...) et qui contiennent de nombreuses informations personnelles et confidentielles. Ces conséquences peuvent donc aller **du préjudice financier à l'usurpation d'identité.**

De nombreux témoignages rapportent que les cybercriminels jouent sur la difficulté de récupérer son compte auprès de certaines plateformes et exercent un **chantage** sur les victimes pour leur restituer leur compte contre une rançon, en particulier pour des comptes de réseaux sociaux professionnels, dont la perte pourrait avoir un impact important sur le plan financier ou réputationnel.

LE RETOUR EN FORCE DES PROGRAMMES MALVEILLANTS (VIRUS)

L'activité des programmes malveillants, communément appelés « virus » par le grand public, ne s'est jamais tarie mais connaît une augmentation notable en 2023.

4e menace en termes de demandes d'assistance des particuliers sur Cybermalveillance.gouv.fr, elle se montre en forte progression pour cette catégorie de public (+67 %). Hors rançongiciel, elle est également en progression notable chez les professionnels (+36 %).

Le marché cybercriminel du programme malveillant en tant que service (ou MaaS pour *Malware as a Service* en anglais) s'est fortement développé ces dernières années, rendant facilement accessibles des logiciels malveillants très perfectionnés, toujours plus difficilement détectables par les antivirus et souvent dotés de fonctionnalités délétères multiples.

Au premier rang de ces fonctionnalités : les **voleurs d'informations ou *Infostealers*** en anglais, en très forte expansion, qui visent à dérober des informations particulièrement sensibles comme des identifiants, mots de passe, témoins de connexions (cookies de session), portefeuilles de cryptomonnaies, numéros de cartes bancaires…

D'autres fonctionnalités permettent de **prendre le contrôle de l'appareil**, par exemple pour miner de la cryptomonnaie, ou encore pour l'utiliser à l'insu de son propriétaire comme pour passer des appels surtaxés ou envoyer en masse des SMS frauduleux en utilisant sa ligne.

Une catégorie particulière de ces programmes malveillants sophistiqués, baptisée ***stalkerware*** en anglais, sont spécialisés dans l'**espionnage domestique et conjugal**. Ils visent particulièrement les téléphones mobiles en permettant de les localiser et de surveiller illégalement leurs communications (appels, SMS, mail, chat, réseaux sociaux…) en temps réel. Ils sont également facilement accessibles sur des plateformes spécialisées pour quelques dizaines d'euros et ne requièrent pas de compétence particulière pour les utiliser.

Une caractéristique de ces programmes malveillants est qu'ils vont généralement toujours être **contrôlés à distance par les cybercriminels** qui les opèrent, parfois dans la durée, pour récupérer des informations ou leur faire déclencher des actions.

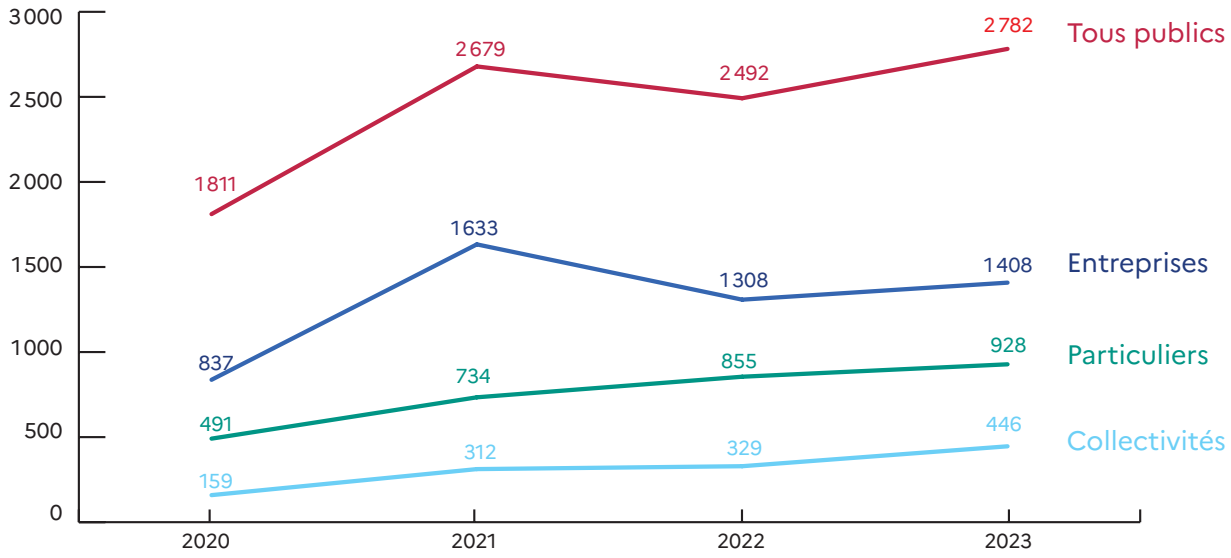
Une tendance observée ces dernières années est que ces programmes malveillants vont **souvent viser les téléphones mobiles** des victimes souvent moins protégés que leurs ordinateurs.

L'infection provient le plus souvent de l'ouverture d'un fichier infecté, ou de l'installation d'une application piégée, comme cela peut être le cas de certaines extensions de jeux ou d'applications piratées ou encore de fausses mises à jour d'applications. Lorsqu'ils arrivent à leurrer les antivirus au moment de l'infection, ces programmes sont **souvent difficiles à détecter pour les personnes qui en sont victimes.**

LES RANÇONGICIELS REPARTENT À LA HAUSSE

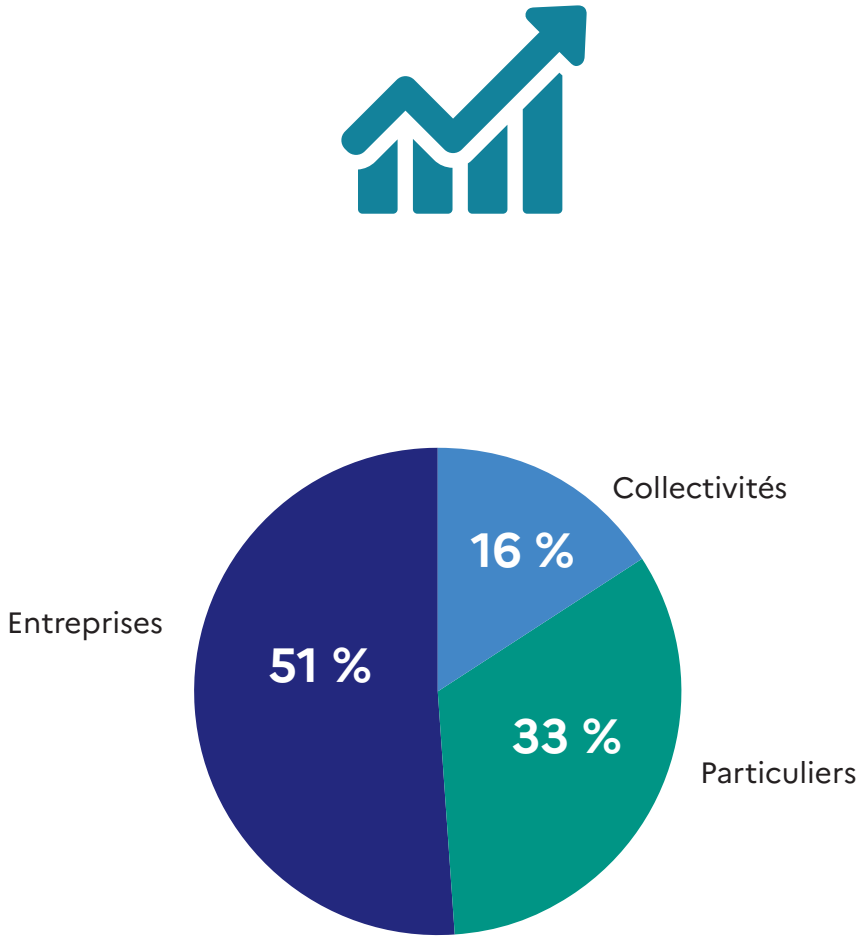
Alors qu'elles avaient amorcé une légère accalmie en 2022, les attaques par rançongiciels ont atteint un niveau record depuis 4 ans.

En proportion, **les attaques par rançongiciel continuent de cibler principalement les professionnels** pour lesquels elles sont l'une des principales causes de recherche d'assistance sur Cybermalveillance.gouv.fr : 3e menace pour les entreprises/associations et 2e menace pour les collectivités/administrations. Les particuliers représentent toujours quant à eux un tiers des demandes d'assistance sur ce phénomène qui ne se positionne qu'en 15e position pour cette catégorie de public.



Évolution des demandes d'assistance pour des attaques par rançongiciels

	2020	2021	2022	2023	Variation n-1
Tous publics	1 811	2 679	2 492	2 782	+12 %
Particuliers	491	734	855	928	+9 %
Entreprises	837	1 633	1 308	1 408	+8 %
Collectivités	159	312	329	446	+36 %



Avec 2 782 demandes d'assistance, les attaques par rançongiciel sont en augmentation sensible pour toutes les catégories de publics en 2023 (+12 %) à un niveau record sur les quatre dernières années.

Si cette augmentation reste mesurée pour les particuliers (+9 %) ainsi que pour les entreprises et associations (+8 %), elle est en revanche en **hausse importante pour les collectivités et administrations (+36 %)**.
Pour ce qui concerne les **particuliers**, les attaques par rançongiciel semblent principalement non ciblées. Elles sont pour l'essentiel consécutives à l'ouverture d'un programme ou fichier infectés, ou à l'utilisation d'un serveur de fichier domestique (NAS) insuffisamment protégé et accessible par Internet. Ces attaques contre les particuliers apparaissent assez peu rentables pour les cybercriminels, car la très grande majorité de ces victimes refusent de payer les rançons demandées et acceptent de perdre leurs données.

En revanche pour les **professionnels**, les attaques sont généralement plus ciblées et le montant des rançons demandées est de ce fait plus élevé, en phase avec leur solvabilité plus importante et les conséquences pour leur activité. Les attaques constatées sur le périmètre de Cybermalveillance.gouv.fr ont principalement pour origine une intrusion des cybercriminels qui ont exploité des failles de sécurité sur les accès externes ou services exposés sur Internet des organisations (RDP, VPN, NAS...).

Le marché des rançongiciels demeure un secteur en fort développement et de plus en plus concurrentiel, ce qui le rend accessible à une petite cyberdélinquance qui s'en prend sans état d'âme et de manière aveugle à tous types de cibles, au risque de mettre en péril l'activité des victimes professionnelles les plus fragiles.

2 782
recherches d'assistance sur des attaques par rançongiciel en 2023

L'INTELLIGENCE ARTIFICIELLE (IA) ENTRE MENACES ET OPPORTUNITÉS

Si les concepts de l'intelligence artificielle datent des années 50 et qu'elle est intégrée dans de nombreuses solutions depuis maintenant plusieurs dizaines d'années, l'année 2023 aura été marquée pour le grand public par la découverte de l'intelligence artificielle générative et notamment celles basées sur les grands modèles de langage.

Compréhension du langage naturel, traduction, production de contenus texte, vidéo ou audio, traitement massif de données, automatisation et résolution de problèmes complexes... Les capacités et l'accessibilité de ces nouveaux modèles d'intelligence artificielle peuvent à la fois émerveiller comme effrayer, tant le champ des possibles semble étendu.

Bien évidemment, **comme toute évolution technologique, les possibilités offertes par l'intelligence artificielle ne peuvent que retenir l'attention des cybercriminels**. Des modèles d'IA générative cybercriminels n'ont d'ailleurs pas tardé à être développés et rendus disponibles (WormGPT, FraudGPT, ThreatGPT...).

En l'état des connaissances encore balbutiantes sur le sujet et au-delà de toute spéculation, **cela ne voudrait toutefois pas pour autant annoncer un bouleversement du panorama des cybermenaces.** En effet, si l'intelligence artificielle peut améliorer la productivité des cybercriminels et la sophistication de leurs modes opératoires, ceux-ci resteront sans doute, du moins encore un temps, très similaires dans leurs principes.

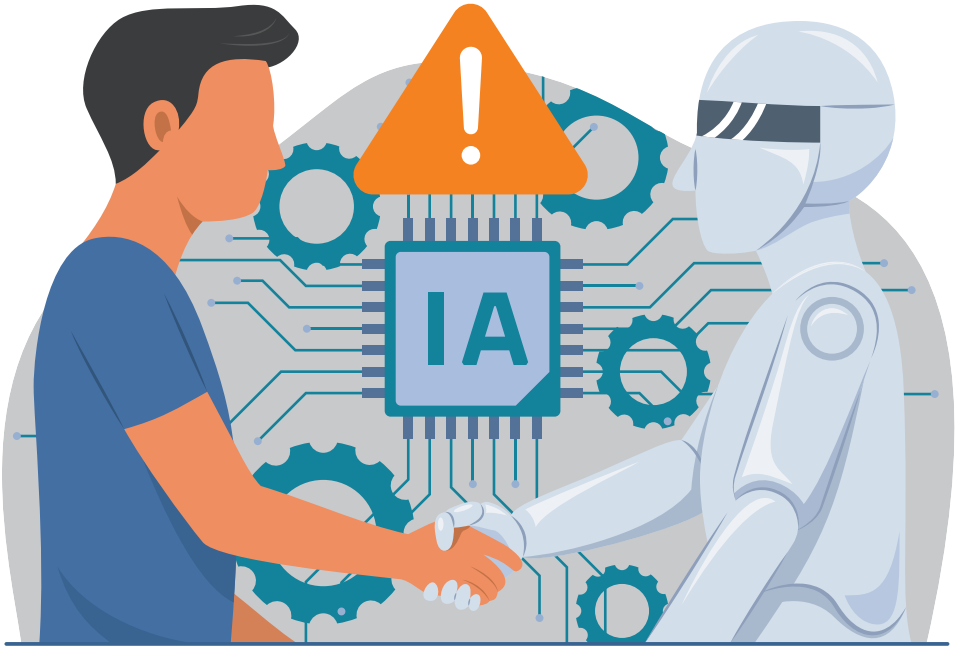
Depuis plusieurs années, la cybercriminalité est devenue de plus en plus facilement accessible à de nouveaux acteurs disposant de faibles compétences techniques, au travers de services spécialisés commercialisés en ligne, notamment sur l'Internet sombre (*darknet*). L'arrivée de l'intelligence artificielle dans ces services ne peut qu'accroître cette tendance. **Le développement de l'utilisation de l'IA à des fins cybercriminelles et l'augmentation du nombre d'acteurs malveillants qui pourra en découler seront très probablement de nature à voir encore s'amplifier le nombre attaques et leur niveau d'élaboration.**

Aucun cas de malveillance pouvant être formellement imputé à l'intelligence artificielle n'a pu être recensé jusqu'à présent par Cybermalveillance.gouv.fr sur son périmètre. Cette imputation restera toutefois souvent difficile à déterminer. En effet, si on peut toujours affirmer qu'un message, une publication ou un programme sont malveillants, il est souvent beaucoup plus délicat de déterminer avec certitude qu'ils ont pu être réalisés par, ou à l'aide, d'une intelligence artificielle.

Plusieurs faits d'utilisation malveillante de l'IA ont toutefois commencé à être rapportés à l'international dans des hypertrucages (deepfakes) audio, vidéo ou photo visant à détourner l'image de célébrités à des fins d'escroquerie, ou de personnalités politiques à des fins de manipulation de l'opinion, ou encore de cyberharcèlement à caractère pornographique...

Cela démontre que le champ des possibles est vaste et qu'**il convient d'aiguiser encore plus son sens critique pour arriver à distinguer le vrai du faux**.

Mais **si l'intelligence artificielle peut constituer une menace dans son utilisation par les cybercriminels, elle s'imposera certainement aussi comme une opportunité d'aider les publics à mieux et plus facilement identifier les menaces et s'en protéger.**



FAITS ET **CHIFFRES CLÉS**

plus de
3 700 000
visiteurs uniques sur la plateforme

plus de
280 000
demandes d'assistance sur la plateforme

Taux de satisfaction des publics pour le service d'assistance en ligne :
89,5 %

62
membres du dispositif

plus de
1 250
prestataires
privés

83 %
des demandes d'assistance des entreprises et des collectivités reçoivent une réponse d'un prestataire référencé **en moins d'1 heure**

19
agents du GIP ACYMA

plus de 200
labellisés
ExpertCyber

66 %
des demandes de sécurisation reçoivent une réponse en **moins de 3 heures**

166
interventions

2 534
retombées médias

Plus de **132 000** **abonnés** sur LinkedIn

Plus 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 sixième année d'exercice. Il tient également à remercier les membres, partenaires et nombreux relais qui soutiennent et contribuent à sa mission d'intérêt général, au rayonnement du dispositif et à la sensibilisation de tous les publics.

Les membres étatiques

- 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 ;
- Ministre délégué chargé du numérique.

Les membres hors étatiques

Aéma Groupe, **AFCDP** (Association française des correspondants à la protection des données à caractère personnel), **Afnic** (Association française pour le nommage Internet en coopération), **AMF** (Association des maires de France et des présidents d'intercommunalité), **ANCT** (Agence Nationale de la cohésion des territoires), **APVF** (Association des Petites Villes de France), **Atempo**, **Avicca** (Association des Villes et Collectivités pour les Communications électroniques et l'Audiovisuel), **AWS** (Amazon Web Services), **Banque des Territoires** (groupe Caisse des Dépôts), **BNP Paribas, Bouygues Telecom**, **CAMF** (Commerçants et Artisans des Métropoles de France, **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), **Déclic**, **EBEN** (Fédération des Entreprises du Bureau et du Numérique), **e-Enfance/3018**, **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), **Mercatel**, **Microsoft France**, **Neuflize OBC**, **Nomios**, **Numeum**, **Orange Cyberdefense**, **Palo Alto Networks**, **Région Pays de la Loire**, **Régions de France**, **Signal Spam**, **Groupe SNCF**, **Stormshield**, **U2P** (Union des entreprises de proximité), **UFC-Que Choisir**, **Unaf** (Union Nationale des Associations Familiales).

Le ministère de l'Europe et des Affaires Étrangères, le ministère de la Transformation et de la Fonction Publiques, la Direction Générale de l'Administration et de la Fonction Publique, le Centre National de la Fonction Publique Territoriale et l'Association nationale pour la formation permanente du personnel hospitalier ainsi que la e-Université France Travail dans le cadre de l'intégration du module de e-sensibilisation SensCyber.

L'Association Delta7, la Médiathèque de Stains et de Saint-Denis, le Cube Garges, le Réseau Pimms Médiation, les Conseillers numériques France Services, les Conseiller.ère.s numériques des Villes de Troyes et de Montigny-lès-Cormeilles ainsi que le GIP « Vendée Numérique » pour le temps accordé et leurs contributions aux contenus de la MalletteCyber.

Les 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 groupements de prestataires aux côtés des fédérations et syndicats : **Alliance du Numérique**, **Groupe Convergence**, **Eurabis**, **Réseau Initia**, **Hexapage**, **Résadia**, **Séquence Informatique**, **FRP2i**, **Green France**.

Les partenaires tels que le CNOEC (Conseil national de l'ordre des experts-comptables), Mastercard ou encore PIX pour la co-création de contenus.

Les **organisateurs et visiteurs des salons et événements** suivants : **AGIR** (Accompagnement par la Gendarmerie de l'Innovation et de la Recherche), **ANCTour**, les **Assises de la sécurité** (La Poste Groupe), les **Assises de la sécurité à Monaco** (Groupe Comexposium), le **Congrès des Maires**, le **coTer numérique**, le **Cybercercle**, les **GS Days – Journées Francophones de la sécurité**, les **Innodays** (Bouygues Telecom), **IT Partners** (RX France), le **NEC – Numérique En Commun[s]**, la **Paris Games Week**.

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

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 **C3NA** (Campus régional de Cybersécurité et de Confiance numérique Nouvelle-Aquitaine) et **le centre de formation de l'ANSSI**.

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

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

GIP ACYMA
6 rue Bouchardon, 75 010 Paris
www.cybermalveillance.gouv.fr

Suivez-nous sur :