RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

RAPPORT D'ACTIVITÉ 2024

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

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

ÉDITOS

2024 a été une année exceptionnelle pour la cybersécurité française. La réussite des Jeux Olympiques et Paralympiques de Paris 2024, dans un contexte de menace cyber élevée, a nécessité un engagement d'ampleur de l'ensemble de l'écosystème cyber public et privé.

Face à cet enjeu, le GIP ACYMA a joué un rôle majeur tant pour la prévention des actes de cybermalveillance, que pour l'accompagnement des victimes. Cette année, ACYMA a une fois de plus démontré son rôle clé d'aiguilleur, aux côtés des acteurs de l'écosystème, gendarmerie et police nationales, CSIRT, prestataires, associations et de l'Agence nationale de la sécurité des systèmes d'information.

Le lancement du 17Cyber, équivalent numérique pour les actes de cybermalveillance de l'appel 17, incarne ce rôle prépondérant du GIP, guichet d'entrée pour les victimes d'infractions numériques. 2025 verra la montée en puissance de ce dispositif, avec l'appui de l'écosystème.

En 2024, ACYMA a également continué de s'imposer comme acteur central de la sensibilisation avec notamment la publication de la 3e étude sur la maturité cyber des collectivités, l'opération ImpactCyber menée conjointement avec le Club EBIOS, la CPME, le MEDEF et l'U2P pour les TPE et PME et enfin la coordination du Cybermoi/s.

Je salue, à ce titre, la publication de la stratégie à cinq ans du GIP qui inscrit à long terme cette ambition d'ACYMA, de l'État et de ses membres de devenir l'outil réflexe face à la cybermalveillance. Ce rapport démontre le chemin parcouru et la pertinence du rôle du GIP. Je remercie ses membres pour leur engagement sans cesse renouvelé. Je remercie également son Directeur Général et son équipe qui mènent au quotidien un travail exigeant. Enfin, j'aurai une pensée particulière pour Jean-Jacques Latour qui a été un maillon essentiel de la construction de ce bel outil au service de notre protection.

Vincent Strubel
Président du GIP ACYMA,
Directeur Général de l'ANSSI[1]

[1] Agence nationale de la sécurité des systèmes d'information

Si la fréquentation de la plateforme avait connu un effet « plateau » en 2023, Cybermalveillance.gouv.fr a vu son audience croître de façon significative en 2024 pour dépasser le cap des 5,4 millions de visiteurs uniques.

Au-delà des projets majeurs qui ont ponctué son actualité ces derniers mois tels que le programme de sensibilisation *SensCyber* décliné pour le grand public et les entreprises, la sensibilisation *Cactus* auprès des collégiens et des lycéens, l'opération *ImpactCyber* pour sécuriser les TPE-PME ou encore le Mooc de gestion de crise *SenCy-Crise* menée de concert avec le COMCYBER-MI et la Gendarmerie nationale et bien évidemment le guichet unique 17Cyber, inauguré en fin d'année avec le Ministère de l'Intérieur, *ce sont les fuites de données* qui ont considérablement marqué 2024.

Véritable phénomène de l'année par leur nombre et la quantité de données exfiltrées, elles ont également démontré que les parties prenantes impliquées (Parquet J3, CNIL, police judiciaire du ministère de l'Intérieur) s'étaient collectivement et rapidement organisées pour nous aider à assister et apporter des réponses aux victimes.

Autre fait marquant, la 12e édition du Cybermoi/s lancée depuis l'Assemblée nationale et dont le mouvement s'est considérablement amplifié cette année. Témoins, les 1 200 entités publiques, privées ou associatives qui ont rejoint son collectif, les 400 événements inscrits à l'agenda mais également les 15 000 marchands de presse qui ont relayé la campagne *Fausse Bonne Idée* pour inciter le public à adopter les bons réflexes de cybersécurité.

Enfin, nous ne pouvions pas refermer le chapitre 2024 sans avoir une pensée émue pour Jean-Jacques Latour, directeur de notre pôle Expertise, trop rapidement disparu en cette fin d'année.

Nous nous emploierons à poursuivre notre démarche d'intérêt public avec la même rigueur qu'il menait sa mission.

Jérôme Notin
Directeur Général du GIP ACYMA[1]

[1] Groupement d'intérêt public pour le dispositif national d'assistance aux victimes d'actes de 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 et au 17Cyber.gouv.fr qui assurent 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 et avec un policier ou un gendarme pour les menaces qui le nécessitent.

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

Gouvernance

Le GIP ACYMA est composé de 65 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

18
agents en 2024

dont 9 mis à disposition par des membres du GIP :

- ANSSI (Service du Premier ministre) ;
- Ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche ;
- Ministère de la Justice ;
- Ministère de l'Intérieur ;
- Ministère des Armées ;
- Groupe SNCF.

2 721 455 €
de budget en 2024

dont

une subvention exceptionnelle pour le projet 17Cyber
300 000 €

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

NOS **MEMBRES**

PREMIER MINISTRE

MINISTÈRE DE L'ÉDUCATION NATIONALE,
DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

MINISTÈRE DE LA JUSTICE

MINISTÈRE DE L'INTÉRIEUR

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES
ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE

MINISTÈRE DES ARMÉES

MINISTÈRE DÉLÉGUÉ CHARGÉ DE L'INTELLIGENCE ARTIFICIELLE ET DU NUMÉRIQUE

Nouveaux membres **en 2024**

« PAROLES DE MEMBRES »

U2P*
Michel Picon
Président de l'U2P

Alors que les cyberattaques se multiplient en direction des petites entreprises, l'U2P a rejoint le GIP ACYMA afin de relayer ses actions de sensibilisation et d'accompagnement face aux enjeux de cybersécurité au plus près des 3,3 millions de TPE-PME artisanales, commerciales et libérales qu'elle représente.

* L'Union des Entreprises de Proximité

APVF*
Christophe Bouillon
Président de APVF

Face à la montée des cybermenaces, les petites villes sont en première ligne, souvent par manque d'accès à l'ingénierie. Cybermalveillance.gouv.fr est un partenaire clé pour sensibiliser élus et agents, et fournir des outils concrets, renforçant la résilience de nos territoires et la sécurité des citoyens.

* L'Association des Petites Villes de France

CNOEC*
Boris Sauvage
Vice-président du CNOEC
en charge du Numérique

Le CNOEC s'engage à sensibiliser les cabinets d'expertise comptable et leurs clients face à la montée en puissance des cyberattaques, l'anticipation est plus que jamais un impératif pour nous tous. Le GIP ACYMA et son dispositif Cybermalveillance.gouv.fr sont les références de la prévention et de l'assistance aux victimes de la cybercriminalité en France.

* Le Conseil national de l'ordre des experts-comptables

AVANT DE CLIQUER
Carl Hernandez
Co-fondateur

Notre collaboration avec Cybermalveillance.gouv.fr vise à sensibiliser les professionnels et particuliers aux risques cyber. Face aux enjeux économiques et sociétaux actuels, nous unissons nos forces pour une sensibilisation globale, essentielle pour protéger et sécuriser notre environnement numérique.

Assemblée nationale
Naïma Moutchou
Vice-présidente de
l'Assemblée nationale

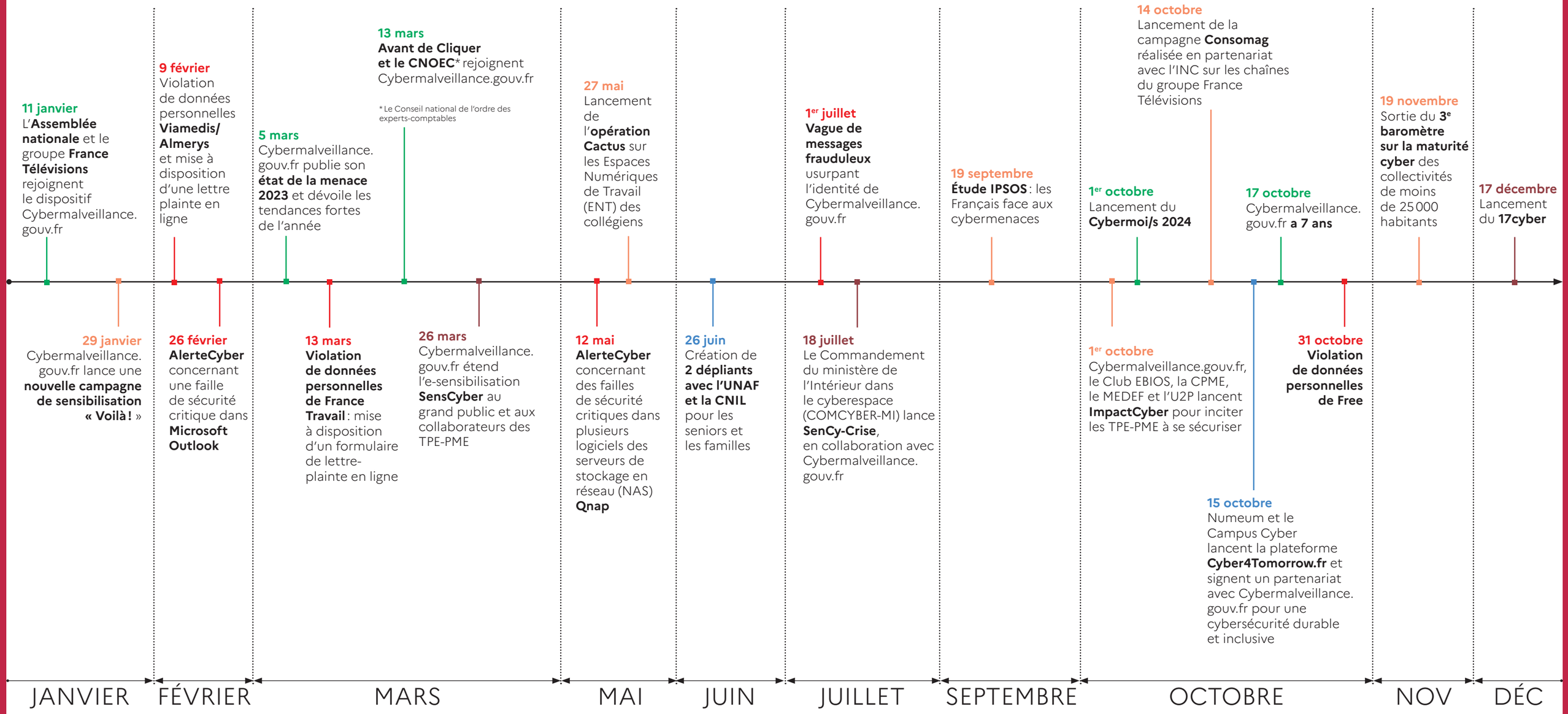
Le partenariat entre l'Assemblée nationale et le groupement d'intérêt public Action contre la Cybermalveillance va permettre de décupler nos moyens de prévention et de réaction, en diffusant les bonnes pratiques et l'accès au dispositif national d'assistance aux victimes dans chaque territoire, auprès des citoyens et de l'ensemble des acteurs locaux.

France TV
Frédéric Brochard
Directeur des Technologies
et des Systèmes
d'Information

La collaboration avec les équipes du GIP offre à nos journalistes un accompagnement afin de mieux appréhender et transmettre à notre public une information claire et précise sur les risques numériques. Cette collaboration s'inscrit pleinement dans notre mission de service public.

LES FAITS MARQUANTS

Annonces de communication institutionnelle · Services & réalisations · Guides & Sensibilisation · Collaborations · Alertes



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en cybersécurité

L'ACTUALITÉ DE L'ANNÉE **2024**

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 2024, ses ressources ont été enrichies de **plus de 170 supports** et notamment de :

- **4 campagnes de communication :** Campagne « Voilà ! » ; campagne ImpactCyber ; campagne INC[1] ; campagne 17Cyber.

- **6 articles « État de la menace » :** *Faux support technique, des modes opératoires toujours plus agressifs ; L'intelligence artificielle (IA), entre menaces et opportunités ; L'hameçonnage (phishing) : la menace prédominante pour tous les publics ; Le « quishing » : l'hameçonnage par QR code ; Les rançongiciels repartent à la hausse ; Le retour en force des programmes malveillants (virus).*

- **4 articles « Menaces » :** *Détournement de loyer ; Accusation de fraude fiscale ; Offres d'emploi d'opérateur marketing sur Internet ; Alerte : vague de messages frauduleux usurpant l'identité de Cybermalveillance.gouv.fr.*

- **2 articles Jeux Olympiques et Paralympiques de Paris 2024 :** *État de la menace et mesures de cybersécurité renforcées pour les petites et moyennes entreprises, associations, collectivités ; Nos conseils pour vivre l'événement en cybersécurité.*

- **3 articles « Top 10 » des cybermenaces les plus fréquentes par public :** particuliers ; entreprises et associations ; collectivités et administrations.

- **1 fiche pratique :** *Sites de vente entre particuliers : 20 conseils pour éviter les arnaques.*

- **3 fiches réflexes :** *Comment réagir en cas d'escroquerie sentimentale ? ; Comment réagir en cas d'arnaques à la location immobilière ? ; Que faire en cas de sextorsion ?*

- **4 articles « Violation de données personnelles » :** Prestataires de tiers payant Viamedis et Almerys : mise à disposition d'un formulaire de lettre-plainte en ligne ; France Travail : mise à disposition d'un formulaire de lettre-plainte en ligne ; Fédération Française de Football (FFF) : mise à disposition d'un formulaire de lettre-plainte en ligne ; Opérateur Free : situation, risques et recommandations.

- **6 autres réalisations :** Le module de e-sensibilisation SensCyber élargi au grand public et aux collaborateurs des TPE-PME ; le MOOC d'initiation à la gestion de crise cyber SencyCrise ; l'étude de maturité cyber de TPE/PME ; le Mémento ImpactCyber à l'attention des dirigeants TPE/PME ; la 3e édition du baromètre sur la maturité cyber des collectivités ; le service d'assistance 17Cyber.gouv.fr

- **2 AlerteCyber** : Failles de sécurité critiques dans les produits Qnap ; Faille de sécurité critique dans Microsoft Outlook. Et **8 alertes de vulnérabilité informatique :** Infection par le virus PlugX ; Multiples vulnérabilités affectant les automates Schneider Electric ; Infection par différents virus (opération ENDGAME) ; Vulnérabilité affectant les produits Check Point ; Vulnérabilité affectant Palo Alto Networks PAN-OS ; Multiples vulnérabilités affectant des produits Ivanti ; Vulnérabilité affectant un produit Barracuda ; Vulnérabilité affectant les équipements Fortinet FortiManager.

- **2 dépliants :** Unaf[2]/CNIL[3] pour les seniors et les familles.

- **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] Mutuelle assurance des instituteurs de France
[3] Union Nationale des Associations Familiales

SENSCYBER POUR LE GRAND PUBLIC ET LES COLLABORATEURS DES TPE-PME

www.cybermalveillance.gouv.fr/sens-cyber/apprendre

Après avoir lancé son programme de e-sensibilisation à la cybersécurité auprès des collectivités en juin 2023, Cybermalveillance.gouv.fr a décidé d'étendre son service SensCyber au grand public et aux collaborateurs des TPE-PME françaises pour sensibiliser l'ensemble de la population aux risques numériques. Résolument accessible et entièrement gratuit, le programme composé de 3 modules repose sur des contenus inclusifs et interactifs avec des tests de connaissances pour permettre à tous les utilisateurs de se familiariser en peu de temps aux enjeux de la cybersécurité à travers une activité ludique.

DE NOUVEAUX SUPPORTS DE SENSIBILISATION POUR LES FAMILLES ET LES SENIORS

www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cybermalveillance-gouv-fr-cnil-unaf-reflexes-cyber-familles-seniors

Pour accompagner les particuliers fortement exposés aux menaces numériques dans leur quotidien, la CNIL, Cybermalveillance.gouv.fr et l'Unaf ont décidé d'éditer deux dépliants intitulés « Cybersécurité : ayez les bons réflexes ». Spécialement conçus pour les familles et les seniors, ces nouvelles ressources visent à sensibiliser et à éduquer les utilisateurs des dangers d'Internet et à adopter les bonnes pratiques pour s'en protéger en leur apportant connaissances et outils nécessaires pour naviguer dans un numérique de confiance.

OPÉRATION CACTUS POUR SENSIBILISER À L'HAMEÇONNAGE SUR LES ENT

Face aux actes de malveillance qui ont touché les espaces numériques de travail (ENT), le ministère de l'Éducation nationale et de la Jeunesse (HFDS-DGESCO-DNE), le ministère de l'Intérieur (COMCYBER-MI), Cybermalveillance.gouv.fr et les magistrats de la section de lutte contre la cybercriminalité ont mené une action de prévention collective forte pour responsabiliser les jeunes à la cybersécurité. Lancée en mai 2024, l'opération Cactus est basée sur une simulation d'hameçonnage, qui constitue la première menace cyber en France. L'objectif ? Alerter les collégiens sur les dangers des liens suspects et les inciter à adopter des comportements prudents en ligne. Déjà mise en place dans les collèges du département des Yvelines (78) et de l'académie d'Orléans-Tours, l'opération sera généralisée dans d'autres académies en 2025.

SENCY-CRISE EN COLLABORATION AVEC LE COMCYBER-MI

www.cybermalveillance.gouv.fr/gestion-de-crise/sency-crise

Fort de son expérience auprès de victimes de cyberattaques et au regard de l'évolution rapide des cybermenaces qui pèsent sur tous les acteurs de la société, le COMCYBER-MI[1] a mis en place SenCy-Crise, un programme de e-sensibilisation pour initier les petites et moyennes structures, publiques et privées, aux fondamentaux de la gestion de crise cyber. Développé avec l'expertise du département de la gestion de crise cyber et des réservistes du COMCYBER-MI et de Cybermalveillance.gouv.fr, ce programme composé de 3 modules fournit les outils et les connaissances pour débuter et améliorer la gestion de crise cyber au sein de son organisation. Gratuite, cette e-sensibilisation est accessible à tous.

[1] Commandement du ministère de l'Intérieur dans le cyberespace

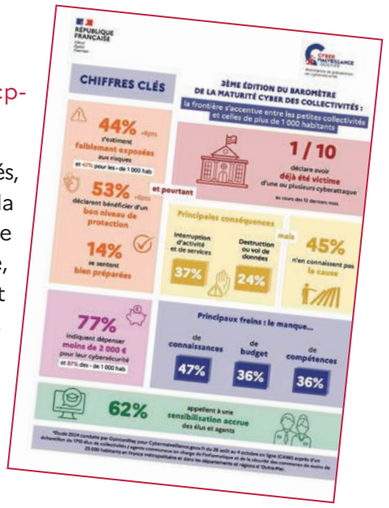
IMPACTCYBER : UNE OPÉRATION POUR CONVAINCRE LES TPE-PME DE SE SÉCURISER

www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/impact-cyber

Face à la vulnérabilité cyber des TPE-PME, Cybermalveillance.gouv.fr, le Club EBIOS, la CPME, le MEDEF et l'U2P ont lancé une opération conjointe en 3 volets afin de les amener à se sécuriser en amont : une étude avec *OpinionWay* pour évaluer le niveau de maturité cyber des entreprises et établir un état des lieux précis de leur gestion de la sécurité informatique, une campagne de communication mettant en avant des entreprises victimes à travers la parole de leurs clients pour les convaincre de se protéger et enfin un mémento pour apporter aux chefs d'entreprise des points de repère en matière de chiffres, témoignages de pairs et recommandations.

3e ÉDITION DU BAROMÈTRE **DE LA MATURITÉ CYBER DES COLLECTIVITÉS**

www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cp-etude-2024-cybersecurite-collectivites



Dans la continuité de ses actions de sensibilisation auprès des collectivités, Cybermalveillance.gouv.fr a mené une nouvelle étude pour évaluer la maturité des collectivités de moins de 25 000 habitants en matière de cybersécurité. Les résultats de cette 3e édition, dévoilés mi-novembre, ont notamment révélé que si 44 % des collectivités s'estiment faiblement exposées et que 53 % pensent bénéficier d'un bon niveau de protection, 1 collectivité sur 10 déclare avoir déjà été victime d'une ou plusieurs cyberattaques durant les 12 derniers mois. Le baromètre révèle également que l'écart se creuse entre les plus petites collectivités et celles de plus de 1 000 habitants qui intensifient leurs efforts.

ORGANISATION DE CYBERMATINALES À L'ASSEMBLÉE NATIONALE

En tant que membre de Cybermalveillance.gouv.fr, l'Assemblée nationale a souhaité se mobiliser en organisant des « Cybermatinales » visant à informer et sensibiliser les parlementaires sur les enjeux cyber et les tendances de la menace. Deux éditions ont eu lieu en 2024 pour présenter le dispositif et ses services.

AUTRES **RÉALISATIONS**

SENSIBILISATION DES BÉNÉVOLES DE LA **FÉDÉRATION NATIONALE DE PROTECTION CIVILE**

« *L'hameçonnage, comment s'en protéger ?* », « *Quelle vigilance sur les réseaux sociaux ?* » ou encore « *Comment se protéger de l'usurpation d'identité ?* » étaient les thèmes abordés dans la série de capsules vidéos réalisées par Cybermalveillance.gouv.fr et la Fédération Nationale de Protection Civile pour sensibiliser les bénévoles de l'association lors de leur congrès annuel. Des séquences depuis diffusées sur les réseaux sociaux de la Fédération pour informer le plus grand nombre sur la cybersécurité.

PARTICIPATION À LA CAMPAGNE **CYBERPREV DE FRANCE ASSUREURS**

À l'occasion de la 21e édition du Safer Internet Day, le 6 février 2024, Assurance Prévention, l'association de France Assureurs dédiée à la prévention, a lancé une campagne de sensibilisation aux risques numériques pour les adolescents. Intitulée CyberPrev, cette campagne abordait des thèmes tels que l'addiction aux écrans, l'exposition à des contenus choquants et le cyberharcèlement. Cybermalveillance.gouv.fr a contribué à cette initiative en participant à un épisode de CyberPrev décode sur le thème « Ados et Familles : comment bien se protéger contre les risques cyber ».

MALLETTECYBER : CAMPAGNE NATIONALE AUPRÈS **DES CONSEILLERS NUMÉRIQUES AVEC L'ANCT ET LA MEDNUM**

www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/lancement-mallette-cyber-inclusion-numerique

Pour soutenir le lancement de la MalletteCyber, outil pédagogique mis en place pour accompagner les plus vulnérables, Cybermalveillance.gouv.fr, l'ANCT et la Mednum ont lancé en 2024 une campagne de diffusion auprès des structures qui accueillent ou emploient des conseillers numériques. En 2024, plus de 1 600 MalletteCyber ont été livrées. En parallèle, de nombreux webinaires ont été organisés (Cybermalveillance.gouv.fr, les Hubs territoriaux, la MedNum…) pour permettre aux bénéficiaires de mieux s'approprier l'ensemble des ressources de la MalletteCyber.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

17CYBER.GOUV.FR

GUICHET UNIQUE D'ASSISTANCE CYBER

17 CYBER
Mon assistance en ligne

Le dispositif 17Cyber (17cyber.gouv.fr), annoncé par le Président de la République, a été lancé le 17 décembre 2024 depuis les locaux du GIP ACYMA en présence du Directeur Général de la Police nationale, du Directeur de la stratégie digitale et technologique de la Gendarmerie nationale, du Président du GIP, également Directeur Général de l'ANSSI et du Directeur Général du GIP ACYMA.

L'outil s'appuie sur la plateforme existante du GIP ACYMA Cybermalveillance.gouv.fr, dispositif national d'assistance aux victimes d'actes de cybermalveillance, et les services de tchat du ministère de l'Intérieur. Le 17Cyber permet :

- **l'accueil des victimes** (particuliers, entreprises, associations et collectivités) sur la plateforme 17cyber.gouv.fr ;
- **la qualification de la menace** et la fourniture des conseils adaptés à celle-ci ;
- **le filtrage des sollicitations de victimes** d'attaque cyber via le parcours adapté ;
- **la mise en relation pour les menaces techniques avec des prestataires** de proximité sur l'ensemble du territoire national (1 200 prestataires référencés et 200 prestataires labellisés ExpertCyber) ;
- **la mise en relation avec les forces de sécurité intérieure** via tchat en 24/7 dans les cas des menaces le nécessitant ;
- **la collecte de l'information dans le cadre des sollicitations** visant à affiner la surveillance et le suivi des cybermenaces et à faciliter la prise en compte des victimes ;
- **la mise à disposition de guides et recommandations** à destination des opérateurs des forces de sécurité intérieure pour l'amélioration de la réponse apportée.

Le service s'adresse à l'ensemble des publics du GIP ACYMA : particuliers, entreprises, associations locales et nationales et collectivités.

La coopération entre le GIP ACYMA et le ministère de l'Intérieur permet d'assurer en commun ces missions de service public. Le service est opéré par le GIP ACYMA.

Un module intégrable sur tout site Web permet à ses visiteurs de bénéficier de l'outil gratuitement.

LA CAMPAGNE **17CYBER**

Pour permettre à tous les français d'être informés du lancement du guichet unique de la cybersécurité, une campagne de communication visant à faire connaître ce service d'assistance en ligne a été spécialement conçue pour l'imposer comme le nouveau réflexe cyber. Composée d'un spot de 30 secondes et déclinée en plusieurs visuels, elle incarne l'accompagnement que propose le 17Cyber avec une mise en relation avec un prestataire de proximité et avec un policier ou un gendarme pour les menaces qui le nécessitent.

FOCUS SUR LES PRINCIPALES CONTRIBUTIONS AVEC
LE MINISTÈRE DE L'ÉDUCATION NATIONALE ET DE LA JEUNESSE

JEU CYBER-ENQUÊTE

En étroite collaboration avec la Direction du Numérique Éducatif (ministère de l'Éducation nationale et de la Jeunesse) Cybermalveillance.gouv.fr a participé à la conception du jeu de société Cyber-Enquête « Sur la piste du hacker », qui a vu le jour au dernier trimestre 2024. Le but ? Sensibiliser de façon ludique les membres de la communauté éducative et les élèves aux enjeux cyber grâce à un escape game basé sur le piratage d'un collège.

3e ÉPISODE DES PODCASTS PARCOURS SENSCYBER

La direction générale de l'enseignement scolaire (DGESCO) et Cybermalveillance.gouv.fr ont réalisé une série de podcasts animés par Stéphane Guérault visant à approfondir et illustrer les connaissances dispensées dans l'e-sensibilisation SensCyber sur la plateforme M@gistère. Destiné au personnel de l'Éducation nationale, chaque épisode fait ainsi l'objet d'échanges et de témoignages avec le retour d'expérience d'un prescripteur de l'Éducation nationale (rssi, enseignant…). Le 10 janvier dernier paraissait ainsi le 3e épisode intitulé « Sensibiliser et transmettre » avec l'intervention d'un chef d'établissement.

OPTIMISATION DU PARCOURS GRAND PUBLIC DE PIX

En tant que contributeur au référentiel cœur de Pix, Cybermalveillance.gouv.fr participe activement à l'amélioration continue des épreuves du parcours grand public en s'appuyant sur les statistiques d'utilisation et les retours des usagers.

TOURS DE FRANCE

NUMÉRIQUE ÉTHIQUE TOUR

Fédéré par la MAIF[1], le Numérique Éthique Tour sillonne la France depuis septembre 2023 pour sensibiliser le plus grand nombre – citoyens, élus, enseignants, entrepreneurs… – aux sujets cyber via des expériences ludiques et immersives. Depuis janvier 2024, la tournée nationale, à laquelle Cybermalveillance.gouv.fr s'est associé, a réalisé 21 étapes, pour un total de 64 journées d'ouverture, et un peu plus de 13 000 visiteurs, dont une grande majorité de publics scolaires.

[1] Mutuelle assurance des instituteurs de France

GOOGLE TOUR

En 2023, Villes de France, Cybermalveillance.gouv.fr et Google France lançaient un programme commun pour sensibiliser les collectivités locales à la cybersécurité. En 2024, cette initiative s'est poursuivie avec plus de 1 000 agents et élus formés dans une vingtaine de collectivités à travers le territoire. Son objectif : réduire les risques de cyberattaques et renforcer la sécurité collective.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

ZOOM

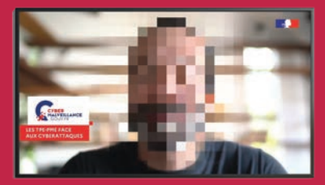
LES CAMPAGNES DE CYBERMALVEILLANCE.GOUV.FR

Outre le soutien à des campagnes nationales, l'année 2024 aura été marquée par la création et la diffusion de spots conçus par le dispositif :

LA CAMPAGNE « VOILÀ ! »

Cybermalveillance.gouv.fr a lancé en janvier sa nouvelle campagne de sensibilisation originale « Voilà ! » afin d'inciter le grand public à retenir les bonnes pratiques cyber en moins d'une minute. Sur un ton décalé faisant directement allusion au tic de langage français qui ponctue nos conversations, la campagne est une saga qui mêle humour et dynamisme pour souligner dans chacun de ses épisodes les réflexes à adopter en matière de mots de passe, de mises à jour et d'hameçonnage.

LA CAMPAGNE IMPACTCYBER



Pour appuyer l'opération ImpactCyber, Cybermalveillance.gouv.fr, Club Ebios, la CPME, le MEDEF et l'U2P ont imaginé une campagne de communication pour rappeler aux entreprises la nécessité de se sécuriser en amont. Pour déclencher une prise de conscience et les convaincre de faire de l'enjeu cybersécurité une priorité, c'est la réputation des TPE auprès de leurs clients qui a été utilisée. Composée de 3 spots inspirés de faits réels, la campagne met en avant les risques encourus par une cyberattaque et se conclut par des conseils pour éviter aux entreprises d'être victimes de cyberattaques, avec le message « Pour garder vos clients, protégez-vous dès maintenant ».

LES PRINCIPALES INTERVENTIONS DE 2024

JANVIER

16 janvier	Prise de parole lors d'une session de l'Observatoire de la Haine en Ligne animé avec l'ARCOM.
24 janvier	Intervention et mise en avant de la MalletteCyber lors d'un webinaire organisé par la Mednum pour la formation des Conseillers Numériques.

FÉVRIER

8 février	Présentation de la MalletteCyber à l'occasion d'une rencontre avec les médiateurs de Plaine Commune.
8 février	Keynote pour la Matinale du CRIP[1] sur le sujet « Comprendre la menace cyber pour agir et réagir efficacement ».
9 février	Table ronde pour le CNOEC[2] sur le thème « Cyberattaque – Construire son plan de continuité d'activité ».
20 février	Sensibilisation des agents de la Région Hauts-de-France sur les risques propres à une collectivité et les bonnes pratiques à adopter.

[1] Club des Responsables d'infrastructure, de technologies et de Production Informatique
[2] Ordre des Experts Comptables

8 février 2024. Présentation de la MalletteCyber à Plaine Commune.

MARS

5-6 mars	Animation d'une webconférence et participation à une table ronde au salon AccessSecurity de Marseille.
12 mars	Cybermatinale Assemblée nationale : lancement de rencontres avec les parlementaires et leurs assistants pour les informer et les sensibiliser aux enjeux de la cyber.
14 mars	Animation d'un webinaire avec lesbonsclics.fr sur les risques en matière de sécurité numérique et introduction de la MalletteCyber aux acteurs de la médiation numérique.
18 mars	Intervention en ouverture de l'édition 2024 de la Semaine de l'Éducation Financière organisée par la Banque de France.
19 mars	Participation à Cyberéco, forum de la sécurité économique et numérique d'Île-de-France au Campus Cyber, en tant qu'exposant et intervenant à la table ronde « Gestion de crise : les clés de l'anticipation ».
28 mars	Table ronde des rencontres territoriales des Systèmes d'Information organisées par le CNFPT[1] pour les collectivités territoriales.

[1] Centre National de la Fonction Publique Territoriale

AVRIL

4 avril	Présentation aux aidants du réseau Inclusion Numérique de la Ville de Paris de l'ensemble des ressources d'accompagnement aux côtés de la CNIL.
9 avril	Interventions au salon Numérique en Commun[s] régional de Strasbourg.

MAI

14 mai	Session de sensibilisation pour les référents sécurité économique de la DNRT[1] et les former en tant qu'ambassadeurs du GIP ACYMA.
24 mai	Présentation de l'offre de service locale et nationale aux 180 élus des collectivités territoriales d'Ille-et-Vilaine.
29 mai	Table ronde lors du colloque de l'AVICCA auprès de ses adhérents.
30 mai	Intervention auprès des Commissaires de justice de la cour d'appel de Paris sur les différentes menaces cyber, leur aspect réglementaire et le programme de sensibilisation SensCyber.

[1] La direction nationale du renseignement territorial

JUIN

4-5 juin	Participation au CoTer Numérique à La Rochelle avec présentation de SensCyber aux élus et démonstration de la MalletteCyber.
18 juin	Webinaire pour l'association 1FO100NUAGES spécialisée dans l'aide à l'autonomie numérique pour partager les bons réflexes cyber auprès des relais locaux en zone rurale.
19 juin	Conférence en ligne pour les adhérents de la MACIF (groupe AÉMA) sur les principales tendances des menaces et les mesures essentielles pour se protéger.
20 juin	Table ronde et atelier MalletteCyber lors d'Aginum[1] organisé par Bordeaux Métropole, fédérant l'ensemble des professionnels de la médiation et de l'inclusion numérique de la région.

[1] Agir pour l'inclusion numérique

10 octobre 2024. Masterclass au salon BIG organisé par BPI France.

JUILLET

2 juillet	Présentation de la e-sensibilisation SensCyber et témoignages d'aidants utilisateurs de la MalletteCyber dans un deuxième webinaire lesbonclics.fr.
2 juillet	Intervention à la matinale CDRT[1] sur les problématiques organisationnelles et humaines complémentaires à la technique dans le domaine de la cybersécurité.
11 juillet	Conférence en ligne BPI FRANCE destinée aux créateurs d'entreprise sur le thème « Fraudes aux entreprises, comment vous en prémunir ? ».

[1] Club des Dirigeants Réseaux et Télécoms

SEPTEMBRE

16 sept	Table ronde France Num sur la transformation numérique des TPE-PME.
19 sept	Prise de parole à l'évènement SecNumÉco organisé par l'ANSSI pour les entreprises de la Région Pays de la Loire.
20 sept	Intervention lors d'un colloque cybersécurité et d'une table ronde organisés par l'AMIF[1] et le SIPPEREC[2].
25-26 sept	Participation au forum national du Numérique en Commun[s] à Chambéry et à une table ronde « Regards Croisés ».

[1] Association des Maires d'Île-de-France
[2] Syndicat intercommunal de la périphérie de Paris pour les énergies et les réseaux de communication

OCTOBRE

1-2 oct	Première présence au salon INNN[1] de Niort avec keynote et table ronde.
3 oct	Intervention en plénière et stand au salon We Ker de Rennes Métropole destiné au grand public.
8 oct	Présentation de la MalletteCyber au Forum Rés'In Lyon pour les acteurs de l'inclusion et de la médiation numérique de la métropole.
10 oct	Masterclass au salon BIG organisé par la BPI à Bercy.
15 oct	Soirée grand public organisée dans le cadre du Cybermoi/s par la commune de Sucy-en-Brie.
17 oct	Sensibilisation des professionnels du transport au sein du groupe Heppner à Rungis à l'occasion du Cybermoi/s.
22 oct	Présentation de l'opération ImpactCyber lors d'une table ronde du Cyber Tour à Toulouse aux côtés de représentants régionaux du MEDEF et de CPME.
25 oct	Intervention au colloque annuel du CEFCYS[2] au Sénat pour le Cybermoi/s.

[1] Salon de l'innovation numérique, de l'insurtech et du risque
[2] CErcle des Femmes de la CYberSécurité

8 octobre 2024. Présentation de la MalletteCyber à Lyon.

1-2 octobre 2024. Au salon INNN de Niort.

NOVEMBRE

6 nov	Intervention lors du salon du Groupement des Hôtelleries et Restaurations de France.
14 nov	Présentation de l'opération ImpactCyber à l'événement de la CPME Nord à Lille.
19 nov	Participation au Salon des Maires et des Collectivités Locales et interventions communes avec la CNIL et l'Unaf, table ronde avec l'APVF et atelier sur la sécurisation.
26 nov	Plénière et atelier à l'occasion du Conseil Régional de l'Ordre des Experts-comptables Grand-Est à Metz.
26 nov	Animation d'un webinaire organisé par CLCV[1] sur les bonnes pratiques lors d'achat en ligne.
28 nov	Webinaire de sensibilisation des agents de la collectivité Hauts-de-France.

[1] Confédération du Logement et du Cadre de Vie

DÉCEMBRE

2 déc	Sensibilisation interne pour Bouygues Telecom.
3 déc	Conférence en ligne auprès des aidants du Réseau d'Inclusion Numérique de Paris.
5 déc	Intervention à la table de ronde de Cinov Digital.
5 déc	Participation au NEC[1] de Dijon pour les professionnels de l'inclusion et de la médiation numérique de la Région Bourgogne Franche-Comté.
12 déc	Journée de sensibilisation réalisée pour les agents de la commune de Massy.

[1] Numérique en Commun[s]

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

FOCUS

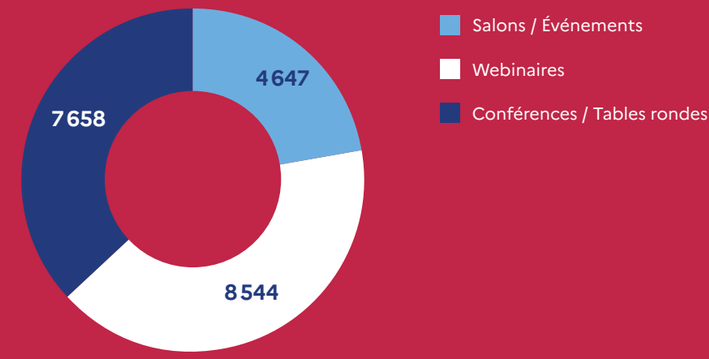
NOS INTERVENTIONS EN DÉTAILS

Sur l'année 2024, le pôle sensibilisation totalise 175 événements incluant webinaires, conférences ou encore tables rondes. Dans 54 % des cas, ces évènements étaient physiques.

NOMBRE DE PERSONNES SENSIBILISÉES PAR TYPOLOGIE D'ÉVÈNEMENT

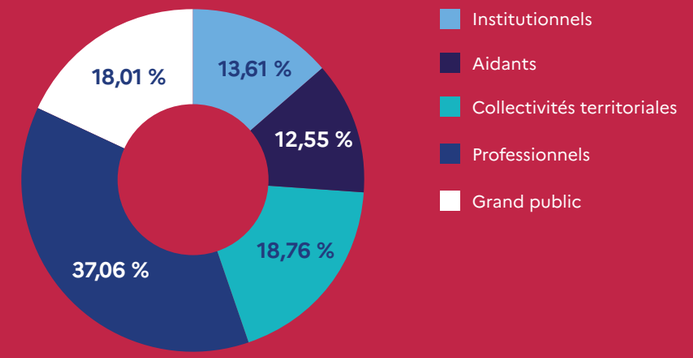
Au total **plus de 20 000 personnes** ont été sensibilisées sur l'année.

7 658 lors de conférences/tables rondes, **4 647** lors de salons et plus de **8 500** à l'occasion d'interventions webinaires.



TYPOLOGIE DES PUBLICS

En 2024, les professionnels représentent **37 %** du public total sensibilisé, contre **18 %** pour le grand public et **19 %** pour les collectivités. Le public des aidants est celui qui affiche la progression la plus marquée, passant à 12,5 % contre seulement 5 % en 2023.

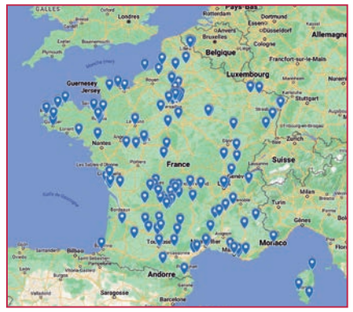


ÉVÉNEMENT DE **LANCEMENT À L'ASSEMBLÉE NATIONALE**

Le 2 octobre 2024 a marqué le lancement officiel du Cybermoi/s à l'Assemblée nationale, membre de Cybermalveillance.gouv.fr

À cette occasion, différents enjeux ont été abordés sur le thème de « la cybersécurité au service de la souveraineté et de la démocratie ».

- Une introduction par Naïma Moutchou, Vice-présidente de l'Assemblée nationale et une intervention de la Direction Générale de la Sécurité Intérieure (DGSI);
- 3 tables rondes avec 12 intervenants;
- 250 spectateurs en salle et + de 950 vues sur la diffusion en ligne.

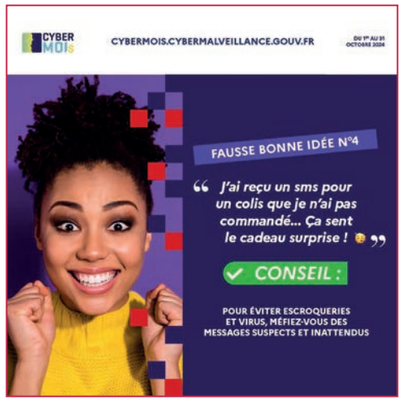


AGENDA DU CYBERMOI/S EN FRANCE

Pour la deuxième année consécutive, les actions de sensibilisation cyber menées durant le Cybermoi/s en France ont été recensées au sein d'un agenda dédié. Plébiscitée par les publics en 2023, la version 2024 a été agrémentée d'une carte interactive et a comptabilisé 417 événements dans des formats les plus divers (goûter, escape game, hackathon, afterwork...) sur l'ensemble du territoire français. La carte a été consultée par plus de 9000 visiteurs.

CAMPAGNE **« FAUSSE BONNE IDÉE »**

Afin de mobiliser le plus grand nombre d'internautes autour de l'enjeu sociétal qu'est la cyber, Cybermalveillance.gouv.fr a créé la campagne de sensibilisation « Fausse Bonne idée ». Celle-ci met en avant 6 personnages avec des idées reçues sur les pratiques numériques et un conseil associé pour éviter de tomber dans le piège des cyberattaques et escroqueries en ligne avec les bons réflexes en matière de cybersécurité. Pour y participer, chacun était invité à relayer les visuels de la campagne sur ses réseaux sociaux accompagnés de #CyberEngagés.



- + de 12000 téléchargements des 6 vignettes « Fausse Bonne Idée »;
- + de 155 millions d'impressions #CyberEngagés et #Cybermois tous réseaux sociaux confondus.

LE CYBER QUIZ FAMILLE POUR FACILITER LE DIALOGUE ENTRE PARENTS ET ENFANTS

Cybermalveillance.gouv.fr a organisé pour la troisième année consécutive le Cyber Quiz Famille, un jeu-concours ludique sur le thème de la cybersécurité pour tester ses connaissances et adopter les bonnes pratiques recommandées dans le Cyber Guide Famille.

- 7838 participants;
- 4460 téléchargements du Cyber Guide Famille entre le 1er octobre et le 31 octobre 2024;
- 50 lots à gagner.

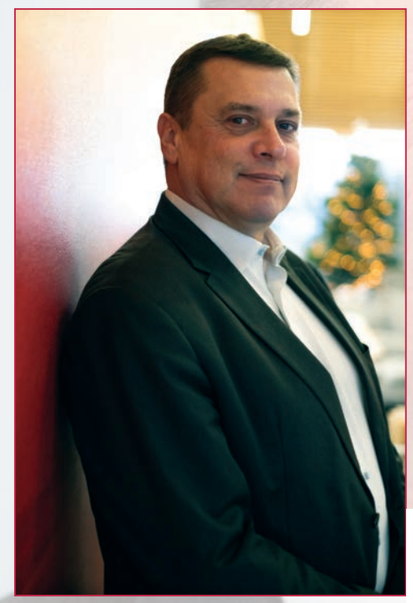
CAMPAGNE NATIONALE 2024 TV-MÉDIAS DE SENSIBILISATION À LA CYBERSÉCURITÉ

Afin de sensibiliser les particuliers aux risques numériques, Cybermalveillance.gouv.fr a renouvelé son partenariat avec l'INC en réalisant une série d'émissions Consomag (fraude au faux RIB, escroquerie sentimentale, arnaque à la location immobilière) diffusées sur les chaînes du groupe France Télévisions du 15 octobre au 21 novembre 2024, ainsi que des capsules La Minute Info (sextorsion, hameconnage "Coucou Papa/Maman", escroquerie détournement loyer, vente entre particuliers). Ces vidéos abordent les cybermenaces qui touchent les consommateurs et les bonnes pratiques à adopter pour s'en prémunir.

ILS NOUS ONT SOUTENU LORS DU CYBERMOI/S:

- **Culture presse, le SNDP et France Messagerie:** diffusion de l'affiche du Cybermoi/s auprès de 15000 marchands de presse.
- **BFMTV:** diffusion de la campagne ImpactCyber.
- **L'Internaute:** relais des messages et des actions de sensibilisation tout au long du mois d'octobre.

HOMMAGE À
JEAN-JACQUES LATOUR



À travers ce rapport d'activité, nous souhaitions également rendre hommage à Jean-Jacques Latour, Directeur de l'équipe Expertise de Cybermalveillance.gouv.fr, disparu en cette fin d'année 2024.

Son engagement et son professionnalisme continuent d'inspirer notre action au quotidien pour poursuivre notre mission d'intérêt public avec la même exigence et la même conviction que celles qui guidaient son travail.

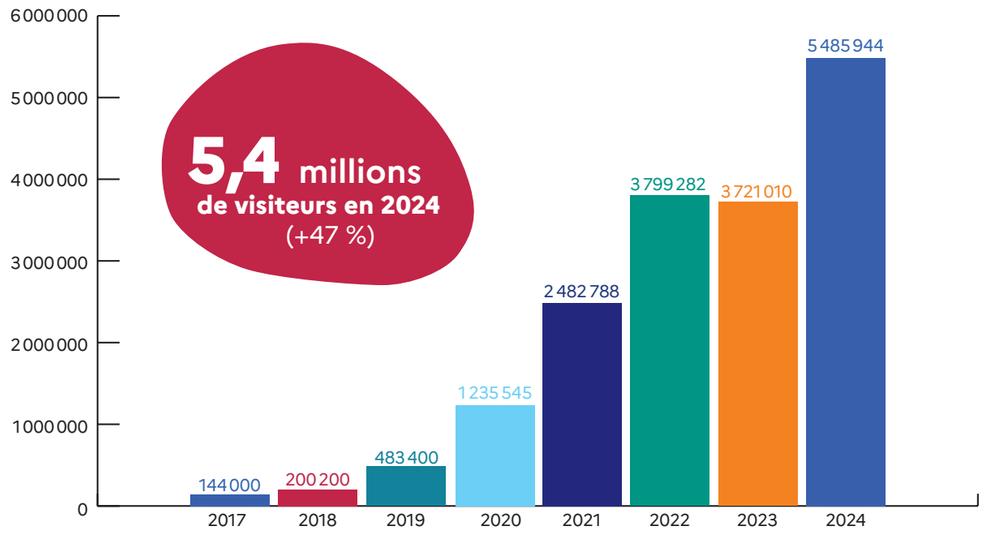
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

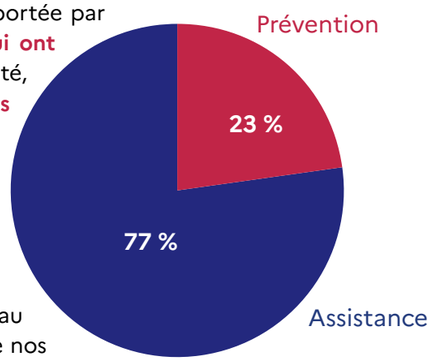
ÉTAT DE LA MENACE

FRÉQUENTATION DE LA PLATEFORME CYBERMALVEILLANCE.GOUV.FR

En 2024, la fréquentation de la plateforme Cybermalveillance.gouv.fr a enregistré une hausse significative (+47 %) avec 5,4 millions de visiteurs. En sept ans d'existence, elle comptabilise plus de 17,5 millions de visiteurs. Comme les années précédentes, elle est majoritairement centrée sur les contenus et services d'assistance qui représentent 77 % de son trafic.



Fréquentation annuelle de la plateforme Cybermalveillance.gouv.fr



La forte hausse de l'audience de la plateforme a été largement portée par les **nombreuses violations de données personnelles massives qui ont marqué l'année** (Free, France Travail, prestataires de mutuelles de santé, enseignes de la distribution…) ainsi que par les **vagues importantes et permanentes de SMS ou mail d'hameçonnage de tout type** (livraison de colis, infraction routière…), pour lesquelles les publics de Cybermalveillance.gouv.fr sont venus s'informer et chercher de l'assistance.

D'autres éléments organiques tendent également à expliquer la forte progression de l'audience :

- la **hausse de la notoriété de Cybermalveillance.gouv.fr**, au travers notamment des sollicitations accrues de l'expertise de nos intervenants par les médias et organisateurs d'événements publics ;
- le **succès de nouveaux services en ligne sur la plateforme**, tels que les modules d'e-sensibilisation SensCyber et Sency-Crise ;
- l'**animation toujours plus fédératrice du Cybermoi/s**, le mois européen de la cybersécurité, dont Cybermalveillance.gouv.fr est pilote en France ;
- l'**enrichissement du service d'assistance avec le lancement du 17Cyber** en collaboration avec le ministère de l'Intérieur ;
- le **besoin croissant des publics de s'informer sur les risques numériques** et les moyens d'y faire face dans un contexte de cybercriminalité toujours en expansion.

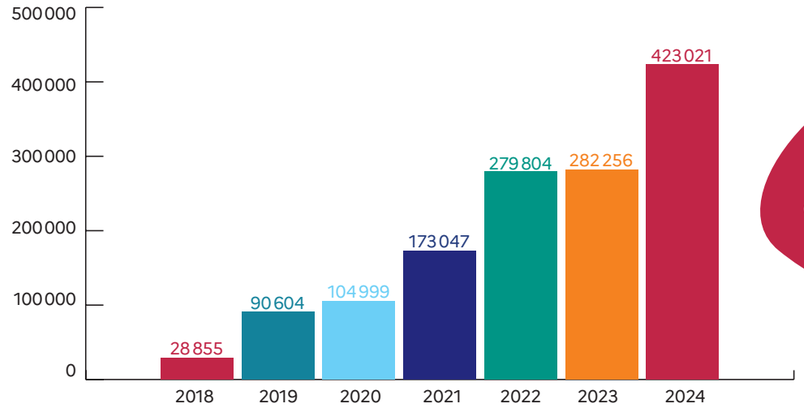
Avec plus de 17,5 millions de visiteurs depuis sa création en 2017, l**a plateforme maintient toujours son rang de référence en matière de prévention et d'assistance pour ses publics.**

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBER MALVEILLANCE GOUV.FR
Assistance et prévention en cybersécurité

LES DEMANDES D'ASSISTANCE 2024

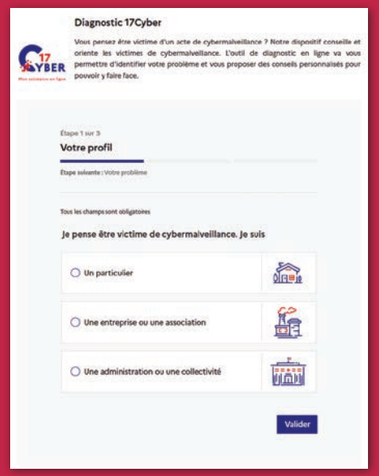
En 2024, la plateforme Cybermalveillance.gouv.fr a enregistré plus de 420 000 demandes d'assistance. Leur analyse offre une vision des différentes formes de menaces auxquelles les publics du dispositif sont confrontés.



Évolution des recherches d'assistance

420 000
demandes d'assistance en ligne en 2024

Le service d'assistance en ligne de Cybermalveillance.gouv.fr, désormais nommé 17Cyber, est le guichet unique de la cybersécurité qui traite 51 formes différentes de cybermalveillance. Après avoir sélectionné son profil (particulier, entreprise/association, collectivité/administration), la victime répond à quelques questions pour obtenir un diagnostic adapté à sa situation et disposer des conseils et orientations pour y faire face. En fonction de la menace diagnostiquée, le 17Cyber permet d'obtenir une assistance technique de proximité avec l'un des 1 200 prestataires référencés et 200 labellisés ExpertCyber par Cybermalveillance.gouv.fr partout en France et un accompagnement par un policier ou un gendarme en 24/7.

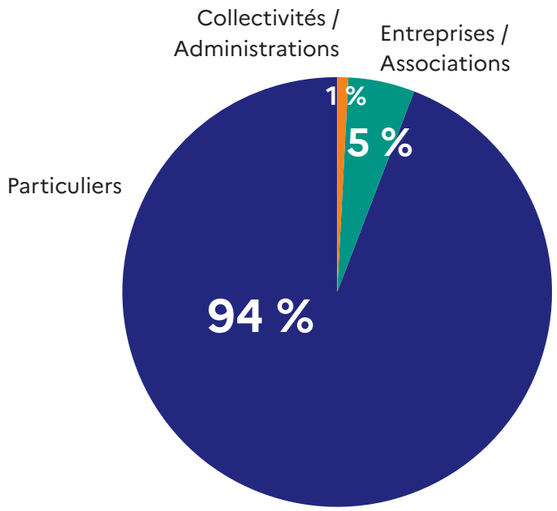


Plus de **420 000 demandes d'assistance en ligne ont été réalisées sur la plateforme en 2024, en progression de 49,9 %.**

En amont du lancement du 17Cyber en fin d'année, la structure de l'outil d'assistance en ligne et les questions posées aux victimes ont été revues courant 2024 dans le but d'améliorer et simplifier l'expérience utilisateur. Les statistiques des parcours d'assistance démontrent que cette évolution s'est avérée bénéfique aux publics.

Le taux de satisfaction des publics pour ce service d'assistance en ligne reste élevé (87,4 %).

• Répartition des demandes d'assistance



Répartition des demandes d'assistance par catégories de public

Sur la base des demandes d'assistance où la catégorie de publics est connue, la proportion des publics est stable en 2024 par rapport à l'année précédente avec **94 % de particuliers, 5 % d'entreprises/associations et 1 % de collectivités/administrations.**

En 2024, 19 600 professionnels (15 655 entreprises et associations et 3 945 collectivités et administrations) sont venus chercher une assistance en ligne sur Cybermalveillance.gouv.fr, ce qui représente une augmentation de 17 % par rapport à l'année précédente (+24 % pour les entreprises/associations et en légère baisse pour les collectivités à -4 %).

+43 %
de demandes
d'assistance de particuliers
•
-4 %
de demandes d'assistance
des collectivités et
administrations
•
+24 %
de demandes d'assistance
des entreprises et
associations

L'analyse rapportée aux volumes respectifs des catégories de publics (68,6 millions de particuliers, 6,4 millions d'entreprises et associations et 36 000 collectivités), démontre que pour un particulier qui a eu recours au service d'assistance de la plateforme, environ 1 entreprise/association et 24 collectivités/administrations ont été assistées.

	2024	%	Variation n-1
Particuliers	**315 205**	**94 %**	**43 %**
Professionnels dont :	19 600	6 %	17 %
Entreprises/Associations	**15 655**	**5 %**	**24 %**
Collectivités/Administrations	**3 945**	**1 %**	**-4 %**

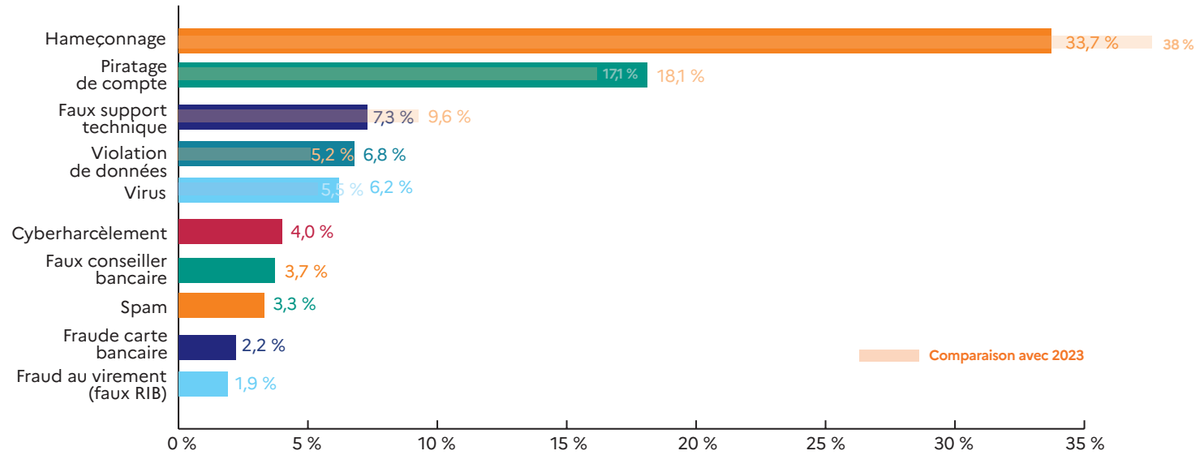
PRINCIPALES MENACES PAR CATÉGORIES DE PUBLIC EN 2024

Sur les 51 formes de cybermalveillance traitées par l'outil d'assistance en ligne en 2024, l'analyse quantitative des principales recherches par catégories de public est un indicateur fort des grandes tendances de la cybermalveillance et de leurs évolutions au niveau national. En effet, les 10 principales cybermenaces par catégories de public représentent à elles seules environ 90 % des recherches d'assistance en ligne sur la plateforme.

Toutefois, les analystes de Cybermalveillance.gouv.fr ont remarqué, et ce pour toutes les catégories de public du dispositif, que les 10 principales cybermenaces avaient légèrement perdu en intensité, passant d'environ 92 % du total des recherches d'assistance en 2023 à 87 % en 2024 pour les particuliers. **Ce qui laisse penser à une menace cybercriminelle plus diverse et diffuse et à un regain d'intérêt des cybercriminels pour des modes opératoires qui étaient jusqu'alors délaissés ou moins exploités.**

Il est important de souligner que cet indicateur quantitatif ne prend pas en compte les conséquences d'une cybermalveillance sur la victime, qu'elles soient financières, psychologiques, réputationnelles, juridiques, y compris dans la durée et peuvent varier considérablement d'une victime à l'autre.

• Particuliers



Principales recherches d'assistance pour les particuliers

Avec près de 34 % des demandes d'assistance, **l'hameçonnage** sous ses différentes formes reste de loin la première menace qui touche les particuliers, en hausse de 23 % en volume.

Le **piratage de compte** se maintient en deuxième position des cybermalveillances les plus fréquentes pour les particuliers et continue de progresser en volume (+47 %).

L'arnaque au faux support technique reste à la troisième place et enregistre une légère hausse par rapport à l'année précédente (+4 %).

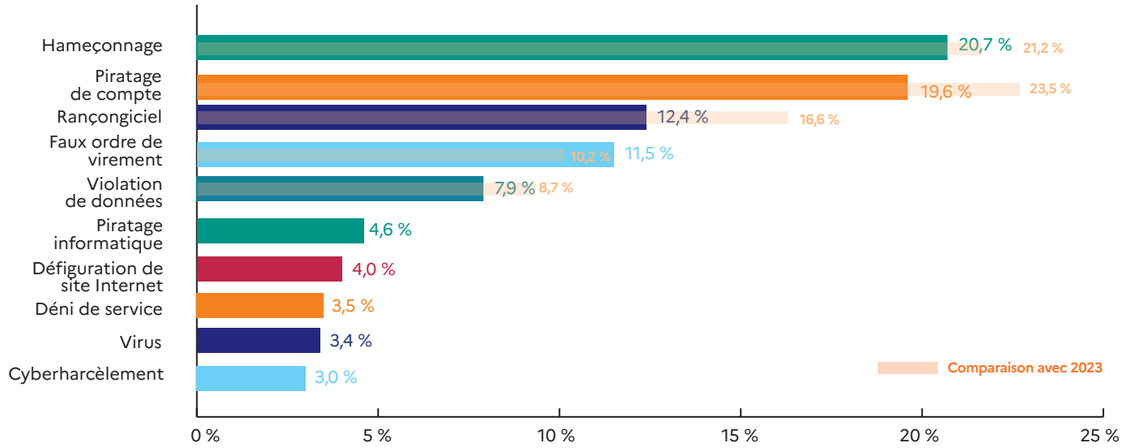
Si la majorité des principales cybermalveillances progresse sensiblement, les augmentations les plus significatives de ce classement concernent les **programmes malveillants ou « virus »** (+58 %), **le spam électronique et téléphonique** (+54 %), les faits de **cyberharcèlement** (+31 %) et **la fraude au faux conseiller bancaire** (+18 %).

Les demandes d'assistance pour des **violations de données personnelles** ont très fortement augmenté (+82 %), en corollaire direct des nombreuses fuites de données qui ont ponctué l'année 2024 et pour lesquelles les particuliers sont venus chercher de l'assistance et des conseils sur la plateforme.

À noter également l'entrée à la dixième place des **fraudes au virement (faux RIB)** qui ont véritablement connu une très forte augmentation (+603 %) par rapport à l'année antérieure.

Enfin, certaines cybermalveillances relativement marginales (moins de 1 %) ont connu des progressions notables. Parmi celles-ci, les **escroqueries au placement financier** continuent d'augmenter fortement en 2024 (+109 %), la **sextorsion** voit le nombre de demandes d'assistance multiplié par dix et les **escroqueries sentimentales** enregistrent toutefois une moindre hausse (+6 %).

• Entreprises et associations



Principales recherches d'assistance pour les entreprises et les associations

En 2024, **l'hameçonnage** reprend la première place du classement avec près de 21 % des recherches d'assistance des entreprises et associations, en hausse de 12 % en volume.

Le **piratage de compte** (20 %), qui occupait la première place en 2023, et les attaques par **rançongiciels** (12 %) complètent la tête du classement pour cette catégorie de publics. À noter toutefois la baisse en volume respective de 4 % et 14 % des recherches d'assistance pour ces deux menaces.

Les **fraudes aux virements** restent à un niveau quasi stable en proportion du nombre de recherches d'assistance mais enregistrent à nouveau une hausse significative en volume (+29 %).

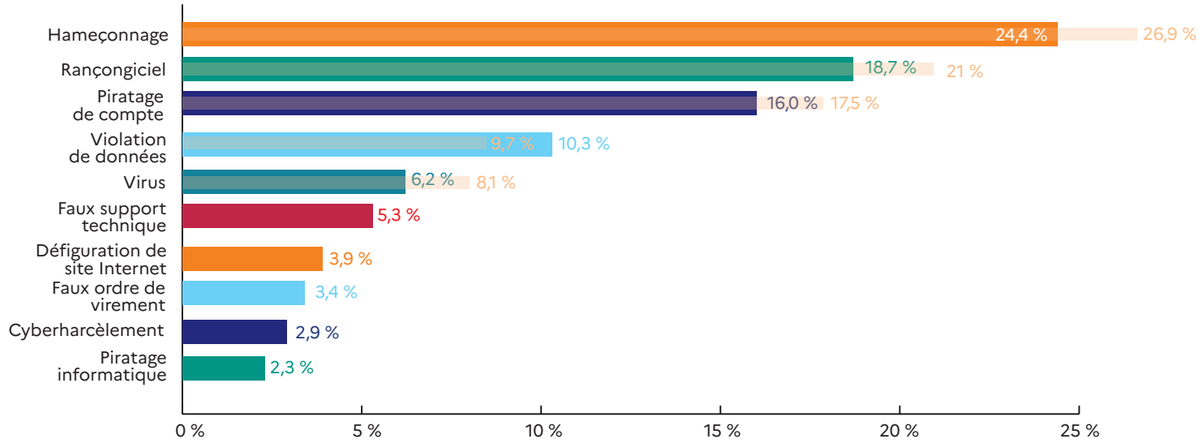
Les attaques contre les **sites Internet** des professionnels sont en baisse en 2024 pour les **attaques en déni de service** (-4 % en volume) et pour les **défigurations de site Internet** (-17 %). Un renversement de tendance notable alors que ces cybermalveillances étaient en forte progression sur la période 2022-2023.

Pour ce qui concerne les **violations de données**, elles restent à un niveau stable en proportion (8 %) et en légère augmentation en volume (+5 %).

Les **programmes malveillants ou « virus »** conservent la neuvième place mais ont connu une forte hausse, tant en proportion (3,4 % contre 1,9 % en 2023) qu'en volume (+ 106 %).

Enfin, les faits de **cyberharcèlement** contre les entreprises et associations ont connu une augmentation très importante (+556 %) par rapport à l'année précédente.

• Collectivités et administrations



Principales recherches d'assistance pour les collectivités et les administrations

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

L'hameçonnage reste la principale menace rencontrée pour cette catégorie de public avec 24 % des demandes, bien qu'en baisse de 17 % en volume.

Il est suivi des attaques par **rançongiciels** (19 %) et du **piratage de compte** en ligne (16 %). Toutefois, en volume, ces deux menaces sont respectivement en retrait de 19 % et 17 %.

Bien que stable en proportion par rapport à l'année 2023, des baisses en volume sont constatées pour les **violations de données** (-4 %), les **défigurations de site Internet** (-23 %), les fraudes au **faux support technique** (-28 %) et les **programmes malveillants/virus** (-31 %).

Les **faux ordres de virement** (FOVI) représentent 3,4 % des recherches d'assistance et connaissent une forte augmentation en volume (+550 %).

Enfin, à l'image des entreprises et associations, les faits de **cyberharcèlement** intègrent le classement des principales menaces. Ils sont en 9e place avec une progression en volume très importante (+533 %).

LES GRANDES TENDANCES **DE LA MENACE**

2024, UNE ANNÉE MARQUÉE PAR UN NOMBRE RECORD DE VIOLATIONS DE DONNÉES PERSONNELLES

Free, France Travail, Viamedis et Almerys, Boulanger, Cultura… L'année 2024 aura été incontestablement marquée par un nombre record de violations de données personnelles, dont certaines très massives, concernant des dizaines de millions de Français.

12 400
demandes
d'assistance
•
706 000
consultations
des articles dédiés

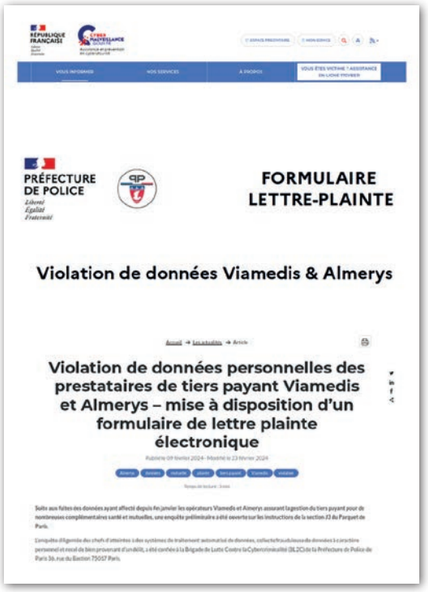
Phénomène marquant de l'année 2024 tant par leur nombre que par le volume de données exfiltrées, les violations de données ont concerné de nombreux secteurs d'activité, publics ou privés: télécom, distribution, santé, sport, transport, maintenance automobile, emploi, banque/assurance, presse… En corollaire direct, le nombre de demandes d'assistance de particuliers sur Cybermalveillance.gouv.fr pour des violations de données personnelles a très fortement augmenté (+82 %).

Dans une large majorité des cas, les fuites de données massives ont été consécutives à des défauts de sécurisation des infrastructures informatiques: utilisation d'identifiants de comptes compromis, intrusion dans un système d'information ou encore « attaques de la chaîne d'approvisionnement » visant à cibler un fournisseur, un sous-traitant ou un partenaire externe ayant accès aux données d'une ou plusieurs organisations.

Les données dérobées lors des attaques concernent en grande partie des données personnelles (nom, prénom, adresse mail ou postale, numéro de sécurité sociale…) **et, dans certains cas, des informations bancaires** (RIB…). **Ces données revêtent une grande valeur pour les cybercriminels** qui peuvent les utiliser pour tenter des escroqueries ciblées ou bien les revendre à d'autres cybercriminels qui essaieront de les exploiter à leur tour.

Selon la nature des informations dérobées, les conséquences d'une violation de données personnelles peuvent être très diverses: hameçonnage (phishing), piratage de comptes, tentatives d'escroqueries ou d'usurpation d'identité, détournement de ligne téléphonique mobile (« *SIM swapping* »), prélèvements non autorisés…

Ces violations de données personnelles et confidentielles suscitent toujours une forte inquiétude des populations sur l'usage frauduleux qui pourrait en être fait. C'est pourquoi, Cybermalveillance.gouv.fr s'est efforcé d'accompagner au mieux les victimes en leur prodiguant les conseils contextualisés nécessaires pour faire face aux cybermalveillances qui peuvent être consécutives à ce type d'incident. **Des articles spécifiques à plusieurs de ces fuites de données ont notamment été publiés et, pour certaines d'entre elles (Viamedis et Almerys, France Travail et la Fédération Française de Football), une lettre plainte a été mise à disposition des victimes en coopération avec les services du ministère de la Justice et du ministère de l'Intérieur.**



L'HAMEÇONNAGE, PREMIÈRE MENACE POUR TOUS LES PUBLICS

1,9 M
de consultations
d'articles (+13 %)
•
64 000
recherches
d'assistance
(+22 %)

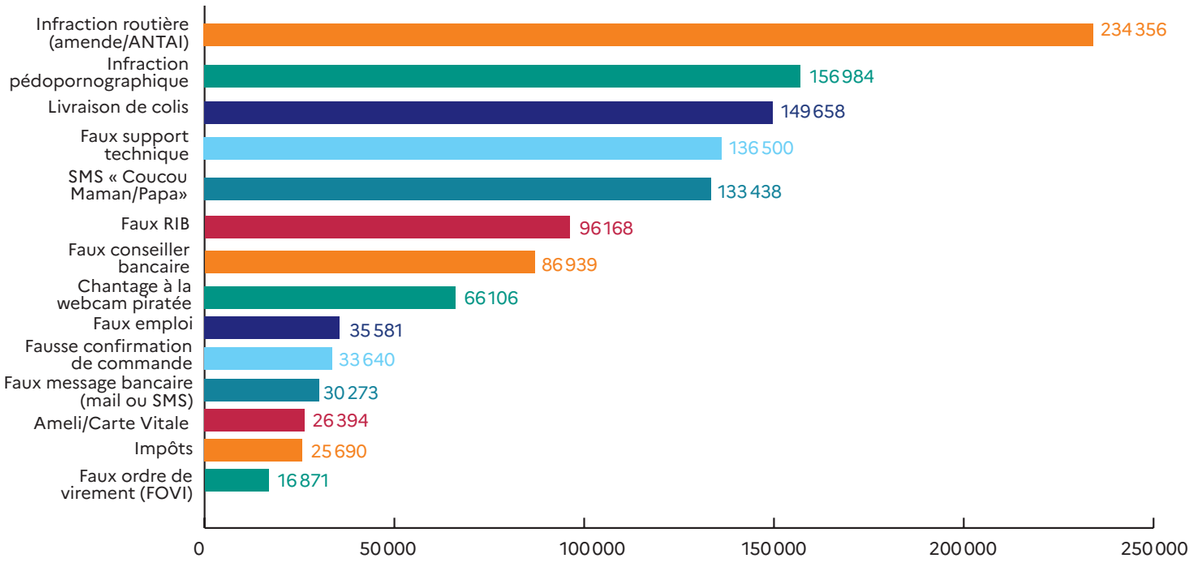
L'hameçonnage (*phishing*) est en tête des préoccupations des visiteurs de la plateforme Cybermalveillance.gouv.fr, qu'ils soient particuliers ou professionnels, et gagne encore en intensité.

SMS, mails, messages privés ou publications sur les réseaux sociaux, messages instantanés, liens sponsorisés et publicités en ligne, appels téléphoniques… Tous types de canaux sont utilisés par les escrocs pour leurs opérations d'hameçonnage. Sous une apparence qu'ils tentent de rendre légitime et crédible, ils cherchent à créer un sentiment d'urgence, d'opportunité ou encore d'empathie chez les victimes afin de les amener à réaliser une action : communiquer des données personnelles et/ou confidentielles (mots de passe, coordonnées de carte bancaire, codes de validation…) ou télécharger un programme malveillant (virus).

L'écosystème cybercriminel de l'hameçonnage est bien établi depuis plusieurs années. Il est essentiellement organisé selon une logique de vente ou de location d'outils, de données personnelles de potentielles victimes ou encore de méthodes clés en main. Cela permet à des cyberdélinquants, sans compétence technique particulière, de dérober des informations ou d'infecter des appareils qu'ils tenteront d'exploiter pour leur propre compte ou dont ils revendront les accès à d'autres acteurs malveillants.

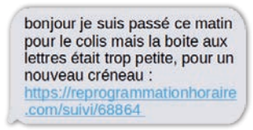
L'hameçonnage est à l'origine de nombreuses autres cybermalveillances quand il est utilisé pour récupérer des informations sur la victime (piratage de compte, fraude au faux conseiller bancaire et autres hameçonnages ciblés…) ou infecter son appareil par un virus (violation de données, espionnage, utilisation malveillante de l'appareil…).

Il peut aussi être une finalité en soi (infraction pédopornographique, « coucou Maman/Papa »…). Il se présente ainsi sous de multiples formes (liste des plus fréquents ci-dessous). L'ingénierie sociale mise en œuvre utilise diverses thématiques et approches rendant son champ d'action très large et diffus, tout en impliquant une multitude d'acteurs malveillants.



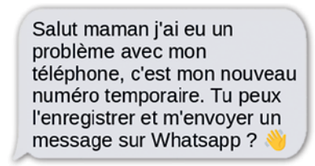
Hameçonnages les plus fréquents en 2024 (nombre de consultations)

L'hameçonnage à l'infraction routière (Amendes.gouv.fr / ANTAI), par mail ou SMS, est cette année encore l'article sur le phishing le plus consulté. Essentiellement diffusée par SMS en 2023, cette escroquerie a été beaucoup plus présente par mail en 2024.
***234 000** consultations de l'article (-17 %)*



Les SMS et mails d'**escroquerie à la livraison de colis** se sont multipliés en 2024, surtout massivement adressés par SMS avec, en général, un faux prétexte de problème de livraison et, systématiquement, un lien renvoyant vers un site malveillant pour prétendument reprogrammer la réception du colis.
***150 000** consultations de l'article (+90 %)*

La consultation de notre article sur **l'hameçonnage à l'infraction pédopornographique** est en baisse mais reste à un niveau élevé, tandis que les recherches d'assistance sont en légère progression. Depuis plus de quatre ans, les auteurs de ces escroqueries continuent d'envoyer en masse leurs messages malveillants à la recherche de victimes, suscitant les interrogations d'une partie des publics. Toutefois, nombreux sont ceux qui s'informent uniquement pour savoir comment signaler ces messages qu'ils considèrent comme abjects. Ce type de phishing s'est tristement inscrit dans le paysage de la cybermalveillance touchant le grand public en France.
***157 000** consultations de l'article (-17 %)*
***6 000** recherches d'assistance (+7 %)*



Apparus fin 2022 puis très largement diffusés fin 2023 - début 2024, les **SMS d'hameçonnage à l'enfant qui a un problème avec son téléphone** (dits « coucou papa/maman… ») se sont, comme pressenti, installés dans la durée. Les vagues d'envois de ces messages se sont en effet poursuivies tout au long de l'année 2024. Dans certains cas, les montants de préjudice se sont élevés à plusieurs milliers d'euros pour les victimes qui ont échangé avec les escrocs.
***133 000** consultations de l'article*

L'hameçonnage aux couleurs de l'Assurance Maladie est en nette résurgence en 2024. Il avait connu une baisse notable en 2023 après avoir été très fortement présent l'année précédente, essentiellement par SMS. En 2024, le canal mail a été beaucoup plus utilisé que les années précédentes pour ce type de phishing. Le thème du renouvellement de la Carte Vitale avec menace de suspension de droits est toujours le plus courant.
***26 000** consultations de l'article (+140 %)*
***2 500** recherches d'assistance (+190 %)*

FOCUS

LES FRAUDES AU FAUX CONSEILLER BANCAIRE TOUJOURS EN HAUSSE

87 000
consultations de l'article (+6 %)
•
6 000
recherches d'assistance (+18 %)

Les hameçonnages à l'infraction routière, à la livraison de colis et à l'Assurance Maladie décrits précédemment sont utilisés pour collecter des données personnelles et de carte bancaire qui seront, en général, exploitées par la suite pour des **escroqueries au faux conseiller bancaire**. Peu de temps après avoir été piégée par l'hameçonnage, la victime reçoit un appel téléphonique d'un supposé service anti-fraude de sa banque qui l'alerte à propos d'opérations suspectes sur son compte.

Les établissements bancaires communiquent fortement sur ces arnaques auprès de leurs clients mais, malgré cela, les escrocs parviennent encore à créer un sentiment d'urgence chez de nombreuses victimes en les manipulant afin de leur faire valider des opérations bancaires frauduleuses.

Pour la deuxième année consécutive, Cybermalveillance.gouv.fr a observé une hausse de la fréquentation de sa plateforme concernant les fraudes au faux conseiller bancaire.

Une déclinaison de ce mode opératoire observée en 2023 s'est intensifiée en 2024 : l'hameçonnage aux **fausses confirmations de commande**, généralement par mail mais aussi par SMS. Ces messages impersonnels informent d'une supposée validation d'achat en ligne par la victime et l'invitent à appeler un numéro de téléphone donné si elle n'est pas à l'origine du paiement. Dans ce cas, c'est la victime qui contacte l'escroc qui tentera de la manipuler pour arriver à ses fins.


DARTY

Nous vous informons que votre commande **DARTY** pour un **iphone 13** d'une valeur de **960.00 €** est en cours de traitement, et sera livré dans les prochains jours. Si vous n'êtes pas à l'origine de ce paiement veuillez contacter :

NUMERO VERT : 0 9[redacted]308

Cordialement,
client Darty.

SAS au capital de 23 470 382 Euros Siège social : ZAC Port d'Ivry - 9 rue des Bateaux Lavoirs – 94200 IVRY-SUR-SEINE.

Par ailleurs, les informations personnelles et bancaires dérobées (identité, RIB…) lors des nombreuses violations de données qui ont ponctué l'année 2024 auraient également été utilisées par les escrocs pour opérer des fraudes au faux conseiller bancaire.

Enfin, la récupération d'informations personnelles et bancaires suite à un **piratage de compte mail**, l'**infection par un virus** ou toute autre **cybermalveillance** ne sont pas à exclure comme origine des fraudes au faux conseiller bancaire.

FOCUS

L'ARNAQUE AU FAUX SUPPORT TECHNIQUE, UNE ANCIENNE ESCROQUERIE QUI PERDURE

136 500
consultations de l'article (-7 %)
•
13 500
recherches d'assistance (+4 %)

En 2024, les **escroqueries au faux support technique restent à un niveau globalement stable**. Elles concernent uniquement les ordinateurs et ciblent majoritairement les usages d'Internet de particuliers. Les professionnels en sont également victimes, particulièrement ceux qui ne disposent pas de service ou support informatique.

La mécanique n'a pas changé. Il s'agit toujours d'**une page Internet agressive qui alerte d'une supposée infection de l'appareil et affiche le numéro de téléphone** d'un support informatique se disant être Microsoft ou Apple selon le système d'exploitation de l'équipement de la victime.

En 2024, la plupart des déclenchements de ces pages de faux support ont eu lieu suite à un clic sur un contenu sponsorisé (premiers résultats de moteurs de recherche, publicités et titres d'articles racoleurs sur des sites Internet ou les réseaux sociaux). À noter que les mails d'hameçonnage menant à de l'arnaque au faux support technique n'ont pas été observés cette année, contrairement aux années précédentes et en particulier en 2020 pendant les confinements.

Pour rappel, depuis fin 2022, certains faux supports techniques ciblent aussi le compte bancaire de leurs victimes en leur faisant croire qu'il a été piraté lors de la supposée infection de leur appareil. S'en suit une manipulation de la victime pour lui faire valider des opérations bancaires, selon des méthodes similaires à celles des **fraudes au faux conseiller bancaire**. Les multiples facturations de la fausse réparation sont elles aussi régulièrement pratiquées sous le prétexte que les premiers paiements auraient échoué.

Cybermalveillance.gouv.fr observe également une diversification des moyens de paiement utilisés par les escrocs. S'ils recouraient quasi systématiquement au paiement par carte bancaire, désormais, ils utilisent aussi des paiements par virement, coupon PCS ou par des mandats internationaux type Western Union.

Contrairement aux années précédentes, les faux supports techniques transmettent moins fréquemment aux victimes des documents d'apparence officielle tels que des contrats, des factures, etc. Ainsi, ils tentent moins de légitimer leur prétendue activité en privilégiant des modes opératoires plus agressifs et nécessitant moins de travail « administratif », les rendant ainsi plus « rentables ».

LE PIRATAGE DE COMPTE EN LIGNE, UNE MENACE TOUJOURS EN EXPANSION

Le piratage de compte en ligne continue de fortement progresser en 2024. Il concerne tous types de comptes mais les messageries (mail) et les comptes de réseaux sociaux sont particulièrement ciblés par les cybercriminels.

430 000 consultations d'articles (+55 %)

•

35 000 recherches d'assistance (+42 %)

Ces piratages peuvent avoir pour origine un hameçonnage, l'utilisation d'un même mot de passe pour différents comptes dont l'un a été compromis, le piratage d'un appareil ou son infection par un virus qui a permis le vol d'identifiants de connexion.

Les **comptes de messagerie (mail)** sont toujours des cibles privilégiées pour les cybercriminels. Ils contiennent en général de nombreuses informations sur leurs propriétaires et leurs interactions avec leurs contacts personnels, contractuels, administratifs et professionnels.

Le piratage d'une **messagerie personnelle** peut permettre à un cybercriminel de nombreuses autres cybermalveillances. Parmi les conséquences les plus observées en 2024 figurent :

- **la réinitialisation de mots de passe d'autres comptes de la victime** pour les pirater à leur tour (administrations et services publics, réseaux sociaux, services de VOD, sites de commerce en ligne…) ;
- **l'usurpation de l'identité de la victime auprès de ses contacts** pour des tentatives d'escroquerie (arnaque au proche en situation d'urgence…) ;
- **la collecte d'informations suffisantes pour usurper l'identité d'un créancier de la victime** afin de détourner un paiement (fraude au virement).

Le piratage d'une **messagerie professionnelle** est également une porte d'entrée vers d'autres cybermalveillances, globalement similaires à celles concernant les particuliers mais elles peuvent aussi, d'une façon plus spécifique :

- servir à **l'envoi de mails d'hameçonnage en tout genre aux contacts de la victime** ;
- permettre à un cybercriminel de **mettre un premier pied dans le réseau informatique d'une organisation pour opérer une cyberattaque ultérieure** contre ce réseau ou celui d'une organisation partenaire, par exemple en diffusant un virus (rançongiciel) auprès des contacts internes ou externes de la victime.

En 2024, **il est important de souligner la forte recrudescence des messages d'hameçonnage qui visent à récupérer des mots de passe de messagerie mail. Particulièrement, des mails qui informent d'un supposé document à télécharger** (acte notarié, facture, devis ou autre document contractuel…). La victime, qu'il s'agisse d'un particulier ou d'un professionnel, est redirigée vers un site Internet frauduleux sur lequel elle doit saisir ses identifiants de compte de messagerie pour accéder au document qu'elle ne pourra pas consulter, en général, puisqu'il n'existe pas. Dans quelques cas, la victime pourra quand même télécharger un document qui ne la concerne pas mais qui peut contenir un virus susceptible d'infecter son appareil.

Une des multiples variantes de ce type de phishing cible les **identifiants d'un compte de service d'hébergement de fichiers** (WeTransfer, Dropbox, OneDrive…). Pour les professionnels, il peut s'agir des **identifiants du portail Chorus Pro**, la plateforme des administrations publiques pour la réception des factures de leurs fournisseurs.

Les **comptes de réseaux sociaux** ont cette année encore été très convoités par les escrocs.
Les comptes de réseaux sociaux piratés font l'objet de divers types d'escroqueries. Parmi les plus constatées en 2024,

- **l'identité de la victime est usurpée auprès de ses contacts :**
  - pour demander de l'aide afin de résoudre un problème supposé, en général lié à son téléphone (ex : carte SIM bloquée). L'escroc demande alors de lui transmettre des codes de validation que la victime reçoit par SMS. Ces codes lui permettent de pirater à son tour le compte du contact sollicité ou, dans de nombreux cas, d'effectuer des achats débités sur la facture de son abonnement téléphonique ;
  - pour faire la promotion d'escroqueries, en général liées à des investissements en cryptomonnaie ;
- la victime fait l'objet de **chantage pour pouvoir récupérer son compte ou éviter la diffusion de contenus compromettants** que l'escroc aura récupérés dans les messages privés du compte piraté ;
- s'il s'agit d'un compte professionnel, le compte publicitaire lié au compte peut servir à **diffuser des publications sponsorisées malveillantes.**

Force est de constater qu'il est souvent très difficile pour la victime du piratage de son compte de réseau social de le récupérer malgré ses démarches auprès de la plateforme.

LES RANÇONGICIELS, UNE ACCALMIE EN 2024 MAIS UNE MENACE QUI RESTE TOUJOURS À UN NIVEAU ÉLEVÉ

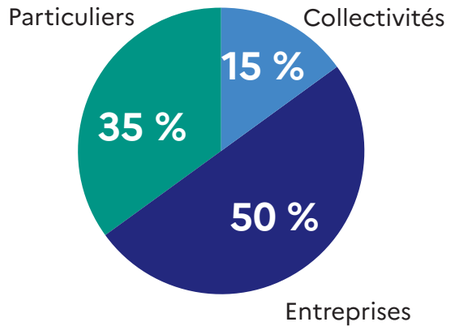
Les attaques par rançongiciel affichent leur plus bas niveau depuis 4 ans après avoir connu un niveau record en 2023.

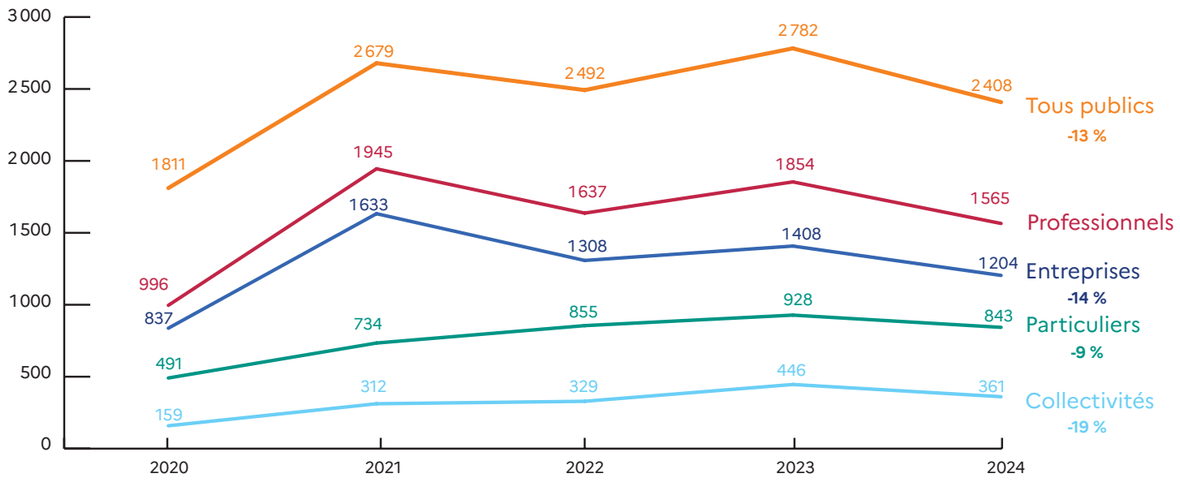
2 408 recherches d'assistance (-13 %)

Les attaques par rançongiciel continuent de cibler majoritairement les professionnels (65 %) et restent l'un des principaux motifs de recherche d'assistance sur la plateforme pour cette catégorie de publics : 3e menace pour les entreprises/associations et 2e menace pour les collectivités/administrations. **Les particuliers représentent un peu plus d'un tiers des demandes d'assistance (35 %)** pour cette cybermalveillance qui figure en 20e position.

Avec 2 408 demandes d'assistance, les attaques par rançongiciel sont en baisse pour toutes les catégories de publics en 2024 (-13 %), soit leur plus bas niveau des quatre dernières années.

Si cette baisse reste mesurée pour les particuliers (-9 %), elle est revanche plus marquée chez les professionnels (-16 %) avec, dans le détail, -14 % pour les entreprises et associations et -19 % pour les collectivités et administrations.





Évolution des demandes d'assistance pour des attaques par rançongiciels

Cette relative accalmie des attaques par rançongiciel peut notamment être imputée aux nombreuses opérations internationales qui auront marqué l'année 2024. En effet, les forces de l'ordre de plusieurs pays ont procédé à des opérations de démantèlement des infrastructures informatiques appartenant à des groupes d'attaquants et à la mise en cause de leurs membres, sans oublier la mise hors ligne de nombreuses plateformes du darknet qui étaient utilisées pour l'achat et la vente de services cybercriminels. Cette réponse collective des forces de l'ordre a vraisemblablement fragilisé l'écosystème du rançongiciel qui avait pourtant gagné en sophistication, structuration et professionnalisme au cours des dernières années, au point de devenir l'une des activités les plus lucratives de la cybercriminalité. Les services spécialisés français ont d'ailleurs pour nombre de ces actions joué un rôle majeur.

Par ailleurs, les efforts en matière de sensibilisation à destination des structures professionnelles (TPE/PME, associations, collectivités territoriales…) **semblent avoir amorcé une prise de conscience de l'importance de la cybersécurité pour leur activité** et donc une sécurisation accrue des parcs informatiques au travers de l'application de bonnes pratiques, de la formation des collaborateurs et d'une offre grandissante de produits et de services de sécurité, publique ou privée, adaptée aux petites organisations.

Toutefois, si les baisses des demandes d'assistance pour ce type d'attaques peuvent sembler importantes, le nombre de demandes d'assistance est toujours à un haut niveau. Ceci suggère que l'activité des groupes cybercriminels opérant ce type d'attaques reste toujours importante.

En matière de modes opératoires, l'analyse des demandes d'assistance pour ce type de cybermalveillance ne montre pas d'évolution notable quant aux vecteurs d'attaques exploités par les cybercriminels.

Pour les particuliers, les attaques par rançongiciel sont généralement consécutives à l'ouverture d'un fichier infecté ou à l'utilisation d'un serveur de stockage de fichiers (NAS) insuffisamment protégé et accessible depuis Internet.

En revanche, pour les professionnels, les attaques par rançongiciel trouvent essentiellement leur origine dans une intrusion au sein du système d'information de l'organisation ciblée au travers de l'exploitation de failles de sécurité affectant les accès externes ou des services exposés sur Internet (RDP, VPN, NAS…).

Les procédés d'extorsion employés par les groupes d'attaquants connaissent une évolution sensible : là où il y a plusieurs années les cybercriminels chiffraient uniquement les données, ils sont ensuite passés au principe de la « double extorsion » en les chiffrant après les avoir exfiltrées de l'organisation ciblée, pour aujourd'hui se limiter parfois à la seule violation des données et menacer la victime de les rendre publiques, tout en les proposant à la vente sur des plateformes spécialisées.

FOCUS

L'ARNAQUE À LA TÂCHE : L'ESCROQUERIE À L'EMPLOI 3.0

19 600 consultations de l'article

De nombreuses campagnes d'offres d'emploi frauduleuses par SMS, messageries instantanées ou sur les réseaux sociaux ont été observées par Cybermalveillance.gouv.fr. Ces emplois ne nécessitent pas de compétences particulières et font miroiter des rémunérations attractives.

En principe, ils reposent sur la réalisation de tâches « simples » en ligne : rédiger des commentaires, noter des produits… **Mais la particularité de cette escroquerie requiert d'acheter un lot de tâches à accomplir pour obtenir le versement de la rémunération sur une cagnotte, généralement en cryptomonnaie, si l'objectif est réalisé.**

Pour mettre en confiance la victime, les premières tâches sont gratuites, simples à exécuter et la victime a la possibilité de récupérer sa rémunération. Par la suite, elle doit acheter des lots de tâches avec une promesse de rémunération toujours plus importante, à des prix de plus en plus élevés. Finalement, les objectifs de ces tâches s'avèrent impossibles à atteindre, empêchant la victime de récupérer les fonds de sa cagnotte. Durant ce processus, elle est entraînée dans une spirale infernale, tout en subissant une forte pression psychologique des escrocs qui la culpabilisent de ne pas avoir atteint ses objectifs.

Lorsque la victime ne sera plus en mesure de payer, les escrocs pourront bloquer son compte, la « renvoyer », voire devenir injoignables du jour au lendemain.

Cybermalveillance.gouv.fr a publié un article sur ce type d'escroquerie élaborée qui semble l'œuvre de groupes très organisés fonctionnant à l'international.

FOCUS

LES FRAUDES AU VIREMENT

121 000 consultations de l'article (+33 %)

•

6 000 recherches d'assistance (+18 %)

Les fraudes au virement (faux RIB ou FOVI) consistent à usurper l'identité d'une personne ou d'une organisation afin de détourner un virement de fonds planifié qui finalement sera au bénéfice d'un escroc. Dans certains cas pour les professionnels, il s'agit d'obtenir un virement imprévu (fraude au président).

Depuis 2022, ce type d'escroquerie touche de plus en plus les particuliers, par usurpation de l'identité d'un créancier avec lequel la victime est en relation (artisan, notaire, avocat, propriétaire/bailleur…). Pour tromper les professionnels, l'usurpation d'identité peut concerner un fournisseur mais également un employé afin de lui dérober son salaire.

En général, cette fraude fait suite au piratage du compte mail de la victime ou de celle du créancier. L'escroc y aura identifié une facture en attente de règlement ou un paiement récurrent et tentera de les détourner à son profit.

En 2024, Cybermalveillance.gouv.fr a publié un article sur l'escroquerie au détournement de loyer. Il s'agit d'une forme de fraude au virement qui passe par l'envoi de mails d'hameçonnage impersonnels semblant provenir d'un propriétaire/bailleur qui informent d'un changement de coordonnées bancaires pour le paiement du loyer faisant, en général, mention d'un impayé.

FOCUS

LA SEXTORSION, UNE MENACE GRANDISSANTE NOTAMMENT CONTRE LES JEUNES

25 300 consultations de l'article

En 2024, Cybermalveillance.gouv.fr a constaté une augmentation très marquée du nombre de demandes d'assistance pour des faits de sextorsion (+924 %) ainsi que de nombreux témoignages de victimes. Au cours de l'année, un article a été publié sur cette menace. Dans ce type d'escroquerie, un escroc, sous une fausse identité, cherche à obtenir de la victime des échanges en vidéo ou des photos à caractère sexuel pour la faire chanter ensuite en la menaçant de les divulguer. Le but est de lui soutirer de l'argent ou d'autres contenus intimes.

D'une manière générale, les victimes sont approchées sur un site de rencontre, un réseau social ou bien une messagerie instantanée.

Dans certains cas identifiés par Cybermalveillance.gouv.fr, il n'y a pas eu d'échange préalable entre la victime et le maître chanteur. En effet, ce dernier aura pu récupérer des contenus intimes suite au piratage d'un compte de la victime ou bien en réalisant un montage en apposant le visage de la victime sur des images à caractère sexuel.

Cybermalveillance.gouv.fr a observé un élargissement de la typologie des victimes de ce phénomène : alors que les adultes constituaient les principales victimes jusque-là, les jeunes, notamment les jeunes hommes, en sont aussi la cible, particulièrement sur les réseaux sociaux tels qu'Instagram, TikTok ou Snapchat.

Enfin, il est important de souligner que les contenus intimes soutirés auprès des victimes peuvent revêtir une certaine valeur, tant pour une finalité financière dans le cadre de chantage que pour alimenter des sites pornographiques, voire la sphère pédocriminelle dans le cas de jeunes victimes.

FOCUS

LE CYBERHARCÈLEMENT, UNE MENACE QUI TOUCHE AUSSI LES PROFESSIONNELS

58 600 consultations de l'article
•
7 600 demandes d'assistance

En 2024, le cyberharcèlement pour les professionnels a fait une entrée notable dans le classement des principaux motifs de recherches d'assistance sur la plateforme en se positionnant à la 9e place pour les collectivités/administrations et à la 10e pour les entreprises/associations. Les progressions sont par ailleurs très marquées pour ces deux catégories de publics avec respectivement +533 % et +566 %.

En parallèle, une hausse des demandes d'assistance de 31 % pour les particuliers victimes ou témoins de harcèlement en ligne a été observée.

Ces chiffres de recherche d'assistance témoignent d'une véritable préoccupation pour les publics professionnels, qu'ils appartiennent au secteur privé, public ou associatif. Le cyberharcèlement aurait ainsi dépassé la sphère privée, sociale et communautaire pour s'étendre au monde professionnel.

À l'image des témoignages d'élus et agents d'établissements publics qui relatent des situations d'incivilité et d'agressions verbales, voire physiques, de la part d'administrés ou d'usagers, ces comportements auraient de manière croissante leur équivalent en ligne. Mécontentement, opposition, agitation, concurrence, activisme… Les entreprises, associations et autres professionnels (libéraux, indépendants, personnalités publiques…) feraient eux aussi face à des propos virulents et répétés sur les sites de partages d'avis d'internautes, à des envois de messages par mail et formulaires de contact ou sur leurs comptes de réseaux sociaux, en privé ou publiquement.

Le cyberharcèlement contre les organisations, leurs dirigeants ou leurs collaborateurs peut être le fait d'employés anciens ou en poste, de clients, d'administrés, d'usagers, d'opposants ou encore de concurrents.

FOCUS

ARNAQUE AU RECOUVREMENT : CYBERMALVEILLANCE.GOUV.FR VICTIME DE L'USURPATION DE SON IDENTITÉ

En 2024, Cybermalveillance.gouv.fr a été victime de l'usurpation de son identité au cours de deux vagues (juillet et décembre) de messages frauduleux dits « d'arnaque au recouvrement », également appelée « escroquerie à l'indemnisation ».

Dans ces messages remontés à nos services par les destinataires, des escrocs prétendaient être agents de Cybermalveillance.gouv.fr et contactaient de potentielles ou anciennes victimes d'escroquerie financière. Elles étaient alors incitées à communiquer des données personnelles sous le faux prétexte de les indemniser de leur préjudice passé. Elles devaient toutefois engager en amont à nouveau des frais pour espérer pouvoir retrouver les sommes perdues initialement.

Ce type d'escroquerie, qui n'est pas nouveau, a connu une résurgence dans divers pays dont la France en 2024.

Afin de prévenir les risques potentiels de ces deux campagnes d'hameçonnage (*phishing*), Cybermalveillance.gouv.fr a publié sur son site Internet et ses comptes de réseaux sociaux des alertes pour inviter les destinataires à ne pas y donner suite. Des actions ont été entreprises avec les autorités compétentes et des plaintes ont été systématiquement déposées.

FOCUS

L'INTELLIGENCE ARTIFICIELLE (IA) : DES RISQUES CROISSANTS MAIS PAS DE BOULEVERSEMENT EN 2024

Dans son rapport d'activité 2023, Cybermalveillance.gouv.fr indiquait « qu'aucun cas de malveillance pouvant être formellement imputé à l'intelligence artificielle n'avait pu être recensé sur son périmètre ». Ce constat est identique en 2024, mais l'utilisation croissante de l'IA en tant qu'outil à des fins malveillantes est à prévoir.

En effet, bien que les possibilités et les applications de l'intelligence artificielle soient très importantes, elle reste un « outil » aux côtés de l'arsenal déjà très fourni des cybercriminels et de leur montée en compétence, bien antérieure à l'apparition des services d'IA générative. Son principal intérêt est d'augmenter la productivité des attaquants, d'améliorer la sophistication et l'efficacité de leurs attaques, ainsi que la crédibilité de leurs escroqueries voire de les réaliser dans des langues qu'ils ne maîtrisent pas. Par exemple en 2024, des actes de cybermalveillance sophistiqués ont fort probablement été élaborés à l'aide de l'IA : hameçonnage, escroqueries financières et sentimentales, sextorsion ou hypertrucages (*deepfakes* audio, vidéo ou photo).

Par ailleurs, nombre d'organisations expriment des craintes relatives à une utilisation mal maîtrisée par leurs collaborateurs des systèmes d'IA génératives. En effet, ces systèmes sont en majorité des solutions externes à l'organisation et leurs utilisateurs peuvent leur confier des données sensibles, ce qui peut présenter des risques en matière de confidentialité.

Bien que les risques soient réels et que quelques cas aient été largement relayés par la presse, l'IA ne semble pas, pour le moment, avoir permis à l'écosystème cybercriminel de développer des capacités nouvelles, les modes opératoires et le panorama des cybermenaces restant globalement identiques.

AUTRES PHÉNOMÈNES OBSERVÉS

Plusieurs « phénomènes » ont particulièrement retenu l'attention des analystes de Cybermalveillance.gouv.fr dans leur mission de veille et d'observation de la menace.

LE VOL D'IDENTITÉ LORS D'UNE RECHERCHE DE LOCATION IMMOBILIÈRE

De nombreux particuliers font état de la récupération frauduleuse de copies de leurs documents personnels et d'identité, particulièrement lors de recherches d'une location de logement sur des sites/applications d'annonces immobilières ou de vente entre particuliers. Ils ont été trompés par de faux propriétaires ou bailleurs qui publient des annonces frauduleuses et demandent aux personnes intéressées des copies de document d'identité, des justificatifs de revenus et de domicile pour supposément constituer leur dossier.

Cybermalveillance.gouv.fr a observé que, fréquemment, ces faux propriétaires ne demandaient pas d'argent et interrompaient les échanges après avoir obtenu les documents. **Il en ressortirait que ce type d'escrocs ait pour seul objectif le vol d'identité qu'ils utiliseront pour leur propre compte ou qu'ils revendront à des fins d'usurpation d'identité. Dans certains cas toutefois, les escrocs tentent également de soutirer de l'argent pour le paiement du premier loyer ou d'une caution.**

En 2024, Cybermalveillance.gouv.fr a publié une fiche réflexe sur les escroqueries à la location immobilière, donnant des conseils pour s'en prémunir et réagir si on en est victime. Ce contenu traite aussi des escroqueries spécifiques aux locations saisonnières.

LES ESCROQUERIES SUR LES PLATEFORMES DE VENTE ENTRE PARTICULIERS

Les sites et applications de vente entre particuliers sont le terrain de multiples cybermalveillances.

De faux vendeurs ou de faux acheteurs mettent en œuvre différents modes opératoires pour soutirer de l'argent ou des informations personnelles aux utilisateurs de ces plateformes : usurpations d'identité de services de paiements (PayPal, Paylib, Wero…) ou de plateformes de vente elles-mêmes, notamment Leboncoin, sous la forme d'appels téléphoniques de faux conseillers ou encore de sites d'hameçonnage. Il peut aussi s'agir de piratage de compte pour dérober la cagnotte d'un vendeur ou usurper son identité auprès d'acheteurs.

En 2024, Cybermalveillance.gouv.fr a publié un article donnant 20 conseils pour éviter les arnaques sur les sites de vente entre particuliers.

L'USURPATION DE NUMÉRO DE TÉLÉPHONE MOBILE

De nombreux témoignages d'utilisateurs de la plateforme et un nombre croissant d'interventions des prestataires référencés par le dispositif font état de ce type de nuisance touchant essentiellement les particuliers.

En effet, leur numéro de téléphone mobile apparaît comme émetteur de nombreux SMS d'hameçonnage (*smishing*), concernant essentiellement de fausses livraisons de colis. Si l'analyse de leur ligne téléphonique et de leur appareil ne révèle aucune compromission, ils reçoivent en retour des réponses, parfois très violentes, de personnes agacées par le message qu'elles ont reçu. Cette nuisance peut être très stressante pour les victimes et durer quelques jours consécutifs.

Une hypothèse très vraisemblable est l'utilisation par des acteurs malveillants de services illégaux, dits de « *spoofing* », leur permettant d'afficher un numéro d'appel qui ne leur appartient pas pour mener des campagnes de *smishing* et préserver la ligne téléphonique réellement utilisée pour envoyer des messages frauduleux.

Sur le même principe, d'autres personnes témoignent de l'utilisation de leur numéro de téléphone mobile pour passer des appels en nombre qui raccrochent aussitôt que les destinataires les reçoivent. Il est fort probable que cette méthode soit utilisée par des cybercriminels qui, à l'aide d'outils dédiés, établissent ainsi des listes de numéros de téléphone mobile valides qu'ils commercialiseront par la suite.

Enfin, ces méthodes de *spoofing* sont également utilisées pour des appels de démarchage commercial illégal, concernant bien souvent des travaux de rénovation énergétique.

Depuis le 1er juin 2024 avec application à grande échelle le 1er octobre 2024, la loi dite Naegelen impose aux opérateurs téléphoniques un mécanisme d'authentification des numéros (MAN) visant à lutter contre le *spoofing* téléphonique. Cela concerne actuellement les numéros de téléphone fixe et les SMS adressés avec un nom d'expéditeur à la place d'un numéro de téléphone. Les communications ne respectant pas le MAN doivent être désormais automatiquement bloquées par les opérateurs.

Il est probable que les acteurs malveillants aient dû s'adapter pour contourner ces nouvelles contraintes légales et technologiques en recourant aux méthodes d'usurpation de numéro téléphone mobiles qui se sont développées courant 2024. En effet, ils utilisaient auparavant bien souvent des noms d'expéditeurs pour les SMS, ce qui leur est désormais impossible. De même, nombre d'appels d'hameçonnage (*vishing*) et de démarchage illégal ou abusif passaient auparavant par l'affichage de numéros de téléphone fixes aléatoires ou volontairement choisis (ex : usurpation des véritables numéros de banques pour opérer des fraudes au faux conseiller bancaire).

L'extension du mécanisme d'authentification des numéros aux téléphones mobiles est en cours de déploiement début 2025. Cette évolution pourra ainsi renforcer significativement la lutte contre les usurpations de numéros de téléphone.

JEUX OLYMPIQUES ET PARALYMPIQUES DE PARIS 2024

Les Jeux Olympiques et Paralympiques (JOP) de Paris 2024 se sont déroulés en France métropolitaine et d'outre-mer l'été dernier et ont braqué les projecteurs du monde entier sur le pays.

En matière de cybersécurité :
- **l'Agence nationale de la sécurité des systèmes d'information (ANSSI)** a piloté et coordonné l'ensemble des parties prenantes et des acteurs étatiques dans l'organisation de l'événement ;
- **Viginum**, le dispositif national de lutte contre les ingérences numériques étrangères, a mené une veille active et opérationnelle sur les campagnes de désinformation liées de près ou de loin aux JOP 2024 ;
- **les services spécialisés du ministère de l'Intérieur** ont agi pour anticiper, identifier et neutraliser les activités cybercriminelles.

Il en ressort que chacun de ces acteurs publics a tiré un bilan positif de l'événement et s'est félicité de sa réussite.

Sur le périmètre de Cybermalveillance.gouv.fr et dans le cadre de sa mission d'observation de la menace, des escroqueries à la revente de billets sur les réseaux sociaux et des sites de commerce en ligne frauduleux en lien avec l'évènement ont été identifiées.

Concernant la sensibilisation aux risques numériques et l'assistance aux victimes, Cybermalveillance.gouv.fr a publié deux contenus dédiés au JOP 2024 à destination de ses publics :
- « État de la menace et mesures de cybersécurité renforcées » pour les petites et moyennes entreprises, associations et collectivités ;
- « Conseils pour vivre l'événement en cybersécurité » pour les particuliers.

Pour les particuliers également, une fiche à portée plus générale mais pouvant s'appliquer au contexte de l'événement a également été diffusée avant l'été 2024 : « Les escroqueries à la location immobilière », pour faire face aux arnaques à la location saisonnière.

Cybermalveillance.gouv.fr a également collaboré avec les organisateurs des JOP 2024 à la sensibilisation des athlètes participant à l'événement.

FAITS ET **CHIFFRES CLÉS**

5,4 millions
de visiteurs uniques sur la plateforme

420 000
demandes d'assistance sur la plateforme

65
membres du dispositif

plus de **1 200** **prestataires** privés

175
interventions

18
agents du GIP ACYMA

plus de **200** **labellisés** ExpertCyber

67,6 %
des demandes de sécurisation reçoivent une réponse en **moins de 3 heures**

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

Taux de satisfaction des publics pour l'assistance en ligne : **87,4 %**

Plus de **165 000** **abonnés** sur LinkedIn

Plus de **46 300** **abonnés** sur X

Plus de **32 000** **abonnés** sur Facebook

Près de **830** **abonnés** sur Instagram

REMERCIEMENTS

Cybermalveillance.gouv.fr remercie celles et ceux qui ont apporté leur témoignage dans ce rapport d'activité pour sa septième 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

- Premier ministre (ANSSI) ;
- Ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche ;
- Ministère de la Justice ;
- Ministère de l'Intérieur ;
- Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique ;
- Ministère des Armées ;
- Ministère délégué chargé de l'Intelligence artificielle et 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), **Assemblée nationale**, **Atempo**, **Avant de Cliquer**, **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, **CCI France** (Chambre de Commerce et d'Industrie), **CCR** (Caisse centrale de réassurance), **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**, **CNOEC** (Conseil National de l'Ordre des Experts-Comptables), **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 Télévisions**, **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**, **Régions de France**, **Signal Spam**, **Groupe SNCF**, **Stormshield**, **U2P** (Union des entreprises de proximité), **UFC-Que Choisir**, **Unaf** (Union Nationale des Associations Familiales).

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 **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** (La Poste Groupe), les **Assises de la sécurité à Monaco** (Groupe Comexposium), le **coTer numérique**, le **Cybercercle**, le **Forum InCyber**, 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**, le **Salon des Maires et des Collectivités Locales**.

Ses partenaires **médias**, tels que **Culture presse, France Messagerie, Groupe BFM**, **L'Internaute** (Groupe CCM Benchmark) et le **SNDP**.

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 cybersécurité

GIP ACYMA
www.cybermalveillance.gouv.fr

Suivez-nous sur :