RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

RAPPORT D'ACTIVITÉ

Au cœur de l'action cyber

2025

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

www.cybermalveillance.gouv.fr

SOMMAIRE

Directeur de la publication : Jérôme Notin
Coordination éditoriale : Béatrice Hervieu, Pauline Fabry, Stella Azzoli et Maïlys Derville
Conception graphique : Elsa Godet
Crédits photos : p. 3 : © Pierre Morel – MEN / p. 7 : © Hugo Renard, © Maxime HURIEZ

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

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

ÉDITOS

La Revue nationale stratégique, publiée en juillet 2025, fixe l'ambition d'une résilience cyber collective, qui appelle à une synergie renforcée entre l'État et l'ensemble des parties prenantes de la Nation (les collectivités territoriales, les entreprises et la société civile dans son entièreté). Alors que la menace cyber s'intensifie, la revue fait le constat que l'État ne pourra pas y faire face seul. À ce titre, le Groupement d'intérêt public Action contre la cybermalveillance (GIP ACYMA) fait figure de modèle précurseur, en fédérant acteurs publics et privés au service de la prévention et de l'assistance aux victimes d'actes cybermalveillants.

Au premier rang de ses actions, le 17Cyber favorise l'articulation entre les acteurs de l'assistance aux victimes de cybermalveillance et offre aux individus et organisations une porte d'entrée connue vers ces acteurs. Après son lancement fin 2024, le 17Cyber est monté progressivement en puissance en 2025, avec sa diffusion et l'intégration dans son parcours de premiers centres de réponse à incident cyber (CSIRT[1]) territoriaux et l'élargissement des types de menaces pouvant faire l'objet d'une demande d'assistance. Cet effort de diffusion devra se poursuivre en 2026 afin de faire du 17Cyber un réflexe pour toutes et tous.

Cette année également, le Cybermois a de nouveau constitué une belle réussite dont l'équipe du GIP et ses membres peuvent se féliciter tout comme l'opération Cactus, fruit d'un travail collectif pour sensibiliser les élèves aux risques cyber. La prévention sera un axe d'effort majeur en 2026, avec l'ambition de massifier la diffusion de contenus de sensibilisation. Des dispositifs cœur du GIP, comme le label ExpertCyber, seront aussi conduits à être renforcés pour accompagner l'ambition fixée par la Revue nationale stratégique.

Au regard de ces nombreux défis, je remercie l'ensemble des membres et l'équipe du GIP pour leur investissement sans faille, et j'appelle les organisations qui ne seraient pas encore membres à franchir le pas. Nous avons plus que jamais besoin de vous.

Vincent Strubel
Président du GIP ACYMA,
Directeur Général de l'ANSSI[2]

[1] *Computer Security Incident Response Team*
[2] Agence nationale de la sécurité des systèmes d'information

L'année 2025 a été, tout comme la précédente, particulièrement marquée par les fuites de données. TPE, opérateurs télécoms, services publics, établissements de santé, collectivités territoriales ou encore fédérations sportives ont été nombreux à être confrontés à des incidents de cybersécurité.

Témoins les chiffres de consultation de Cybermalveillance.gouv.fr qui ont dépassé les 5 millions de visiteurs et surtout les 504 000 demandes d'assistance en hausse de plus de 20 %.

Ces attaques qui touchent d'autant plus les cibles vulnérables justifient à elles seules le renouvellement d'opérations telles que Cactus, pour protéger les jeunes, ImpactCyber pour inviter les entreprises à se sécuriser en amont ou encore la lettre ouverte adressée aux élus à l'occasion du Salon des Maires et des Collectivités locales.

Par ailleurs, le 17Cyber lancé en partenariat avec la Gendarmerie nationale et la Police nationale, continue de se déployer et intègre désormais l'offre d'assistance téléphonique des CSIRT[1] territoriaux afin d'optimiser la prise en charge des victimes professionnelles avec un guichet unique et une assistance de proximité, notamment grâce aux prestataires de confiance.

Une collaboration étroite que nous nouons tout au long de l'année avec les acteurs locaux lors de nos 185 interventions, renforcée en 2025 par le 1er tour de France étatique consacré à la cybersécurité à l'occasion du Cybermois.

Enfin, nous remercions nos membres sans lesquels de nombreux projets ne pourraient prendre vie.

Nous poursuivrons ces initiatives qui nous permettent d'aller directement à la rencontre des particuliers, entreprises et collectivités pour les sensibiliser face à la menace et qui s'inscrivent pleinement dans notre démarche d'intérêt public.

Jérôme Notin
Directeur Général du GIP ACYMA[3]

[3] 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, collectivités, 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 et entitées assujetties à la directive NIS2).

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 au 17Cyber qui propose un service en ligne 24h/7j aux victimes de cybermalveillance, et une mise en relation, selon la menace, avec des professionnels en cybersécurité référencés ou labellisés, ou avec un policier ou un gendarme.

2. PRÉVENIR LES RISQUES ET SENSIBILISER SUR LA CYBERSÉCURITÉ

avec la réalisation de campagnes de sensibilisation et de prévention contre les cybermenaces, de 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 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.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en cybersécurité

Services

• 17Cyber.gouv.fr

Lancé en partenariat avec le Ministère de l'Intérieur, le 17Cyber est un service en ligne disponible 24h/7j. Ce guichet unique permet à tous les Français de qualifier la menace dont ils sont victimes, d'obtenir une assistance et, si besoin, une mise en relation avec un prestataire de proximité et avec un policier ou un gendarme pour les menaces qui le nécessitent.
17Cyber.gouv.fr doit être un réflexe pour tous afin de se protéger face aux menaces cyber.

• Mon ExpertCyber

Lancé en 2021, Mon ExpertCyber est le service de sécurisation proposé par Cybermalveillance.gouv.fr aux entreprises, associations, collectivités ou encore administrations, pour leur permettre de protéger leurs systèmes d'information. Pour en bénéficier, il suffit de répondre à quelques questions pour être mis en relation avec des prestataires labellisés ExpertCyber via la plateforme Cybermalveillance.gouv.fr.

• SensCyber

SensCyber est un programme de e-sensibilisation à la cybersécurité destiné aux particuliers, TPE-PME et agents de la fonction publique. Il repose sur des contenus accessibles, inclusifs et interactifs pour aider chacun à comprendre les risques numériques et adopter les bons réflexes au quotidien. Structuré en trois modules, SensCyber propose une approche pédagogique et ludique pour se familiariser rapidement avec les enjeux de la cybersécurité.

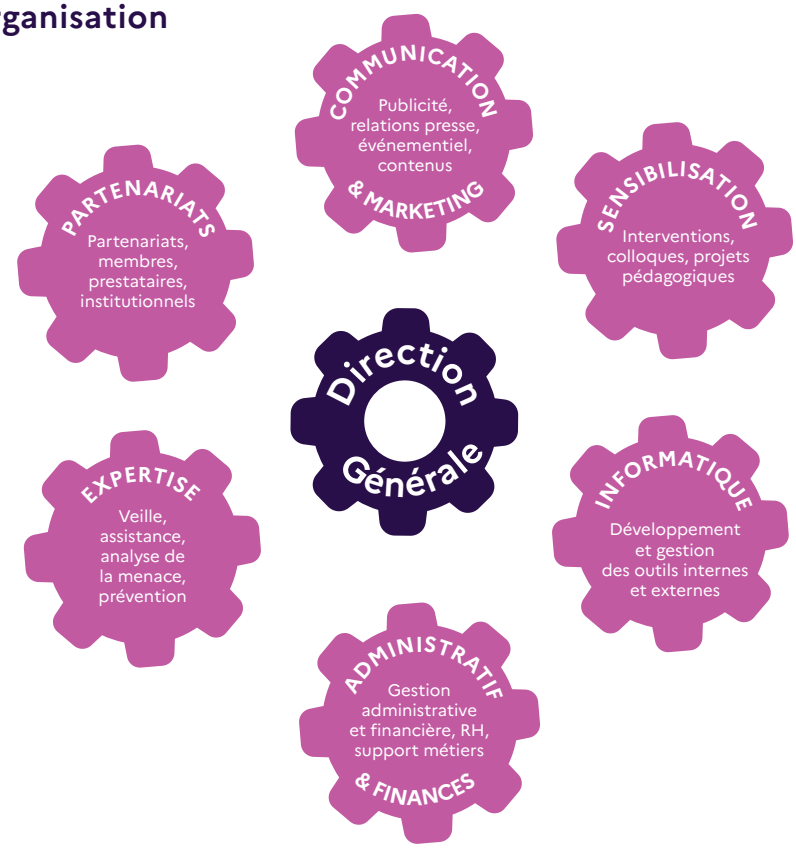
Gouvernance

Le GIP ACYMA est composé de 64 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



20
agents en 2025

dont 8 mis à disposition par des membres du GIP :

- ANSSI (Service du Premier ministre) ;
- Ministère de l'Intérieur ;
- Ministère de l'Éducation nationale ;
- Les Ministères économiques et financiers ;
- Groupe SNCF.

3 412 155 €
de budget en 2025

dont
une subvention exceptionnelle pour le projet 17Cyber
300 000 €

et
une subvention exceptionnelle pour l'intégration des territoriaux
410 700 €

NOS MEMBRES

PREMIER MINISTRE (ANSSI)

MINISTÈRE DE L'INTÉRIEUR

MINISTÈRE DES ARMÉES ET DES ANCIENS COMBATTANTS

MINISTÈRE DE LA JUSTICE

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

MINISTÈRE DE L'ÉDUCATION NATIONALE

MINISTÈRE DÉLÉGUÉ CHARGÉ DE L'INTELLIGENCE ARTIFICIELLE ET DU NUMÉRIQUE

Nouveau membre **en 2025**

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en cybersécurité

PAROLES DE MEMBRES

Aéma Groupe
Adrien Couret
Directeur Général

En tant que groupe d'assurance mutualiste protégeant plus de 12 millions de Français au quotidien, l'engagement d'Aéma Groupe aux côtés de Cybermalveillance.gouv.fr s'inscrit dans la continuité de nos valeurs qui placent la prévenance et la prévention au cœur de ses enjeux. Le GIP ACYMA nous permet d'agir concrètement pour une sécurité numérique inclusive et solidaire.

Bouygues Telecom
Jean-Paul Arzel
Directeur Général Adjoint
Technique SI et Réseau

Bouygues Telecom est fier d'être membre de Cybermalveillance.gouv.fr depuis 2017. Nous sommes convaincus qu'une action collective est essentielle pour sensibiliser et protéger tous les publics face aux menaces numériques. En tant qu'opérateur télécom, nous œuvrons chaque jour pour un numérique sûr et inspirant.

Ministère de l'Éducation nationale
Édouard Geffray
Ministre de l'Éducation nationale

S'engager avec Cybermalveillance.gouv.fr, c'est porter une ambition collective nationale pour faire progresser la sécurité numérique. Avec le Cybermois et l'opération Cactus, nous outillons les jeunes et les familles face aux risques et renforçons la résilience de la Nation.

Afnic*
Pierre Bonis
Directeur Général

Cybermalveillance.gouv.fr représente un lieu unique de coopération entre les pouvoirs publics et les acteurs privés et associatifs pour renforcer la résilience numérique française en accompagnant chaque utilisateur, chaque entreprise. L'Afnic, plus que jamais, soutient cet effort indispensable et au sein duquel le.fr doit tenir toute sa place pour représenter un espace de confiance et de sécurité.

* Association française pour le nommage Internet en coopération

CCI* France
Alain Di Crescenzo
Président

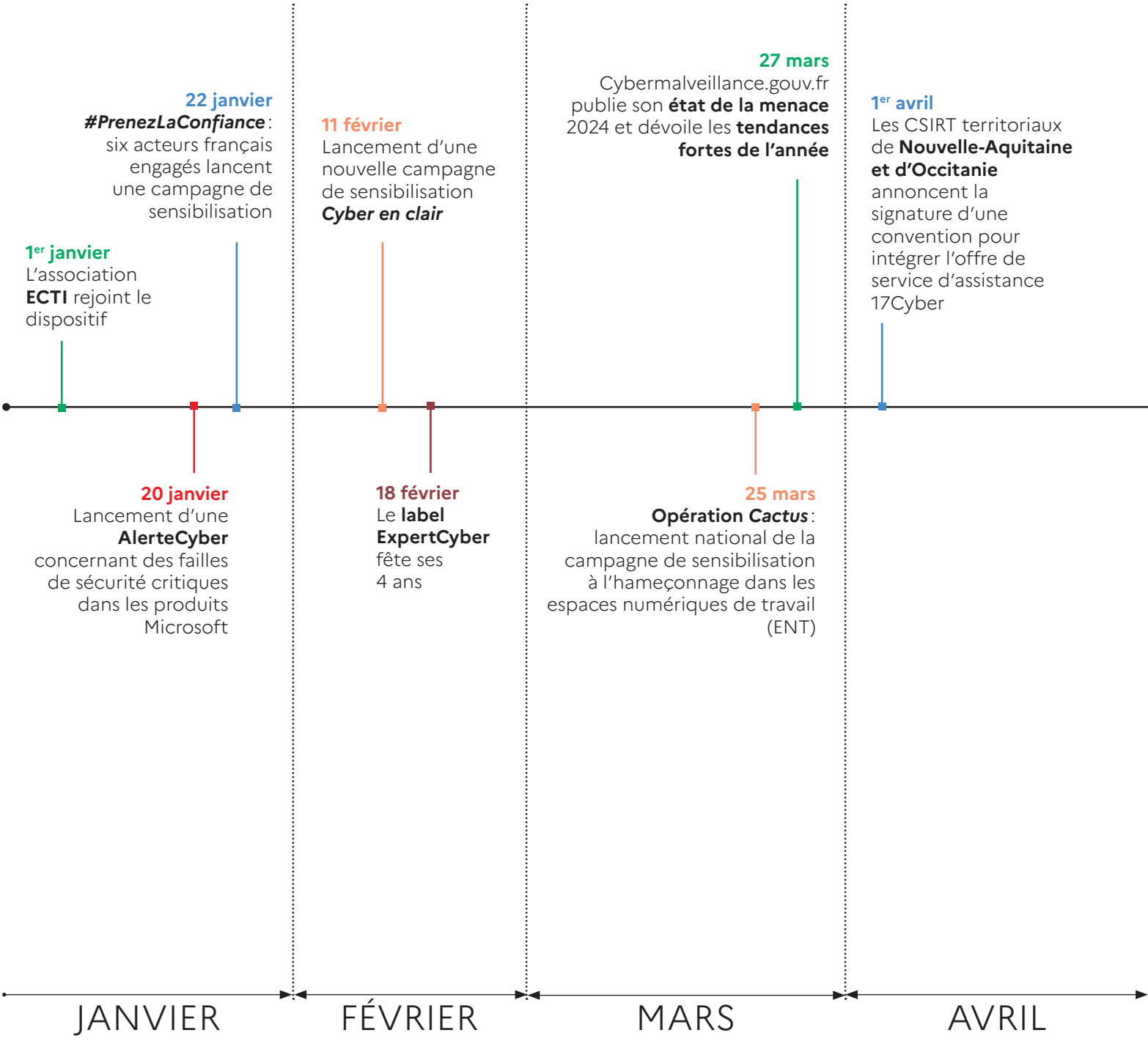
La cybersécurité est un enjeu vital pour nos TPE-PME. Partenaire engagé, le réseau des CCI s'appuie sur l'expertise de Cybermalveillance.gouv.fr pour sensibiliser et protéger les dirigeants. Ce dispositif est le tiers de confiance essentiel pour sécuriser notre tissu économique face aux risques numériques.

* Chambre de commerce et d'industrie

Groupe SNCF
Jean-Christophe Mathieu
Directeur Sécurité numérique

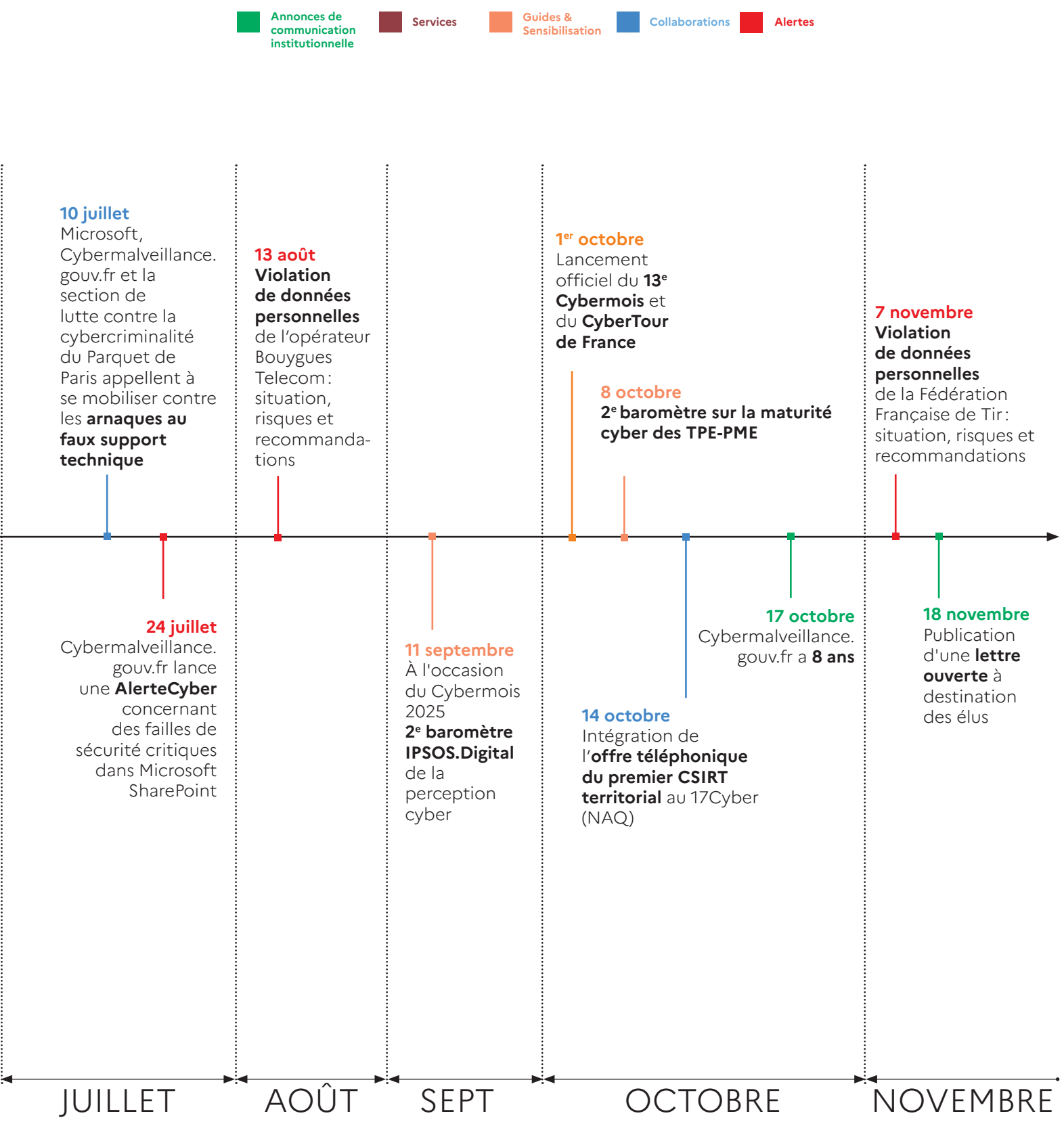
Soutenir Cybermalveillance.gouv.fr c'est apporter à nos collaborateurs des ressources claires pour se protéger dans leurs usages personnels mais aussi renforcer nos travaux de sensibilisation interne. Cela renforce les réflexes face aux attaques, réduit le stress en cas d'incident, et développe une culture cyber partagée.

LES FAITS MARQUANTS



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité


Annonces de communication institutionnelle
Services
Guides & Sensibilisation
Collaborations
Alertes
10 juillet
Microsoft, Cybermalveillance.gouv.fr et la section de lutte contre la cybercriminalité du Parquet de Paris appellent à se mobiliser contre les arnaques au faux support technique
24 juillet
Cybermalveillance.gouv.fr lance une AlerteCyber concernant des failles de sécurité critiques dans Microsoft SharePoint
13 août
Violation de données personnelles de l'opérateur Bouygues Telecom : situation, risques et recommandations
11 septembre
À l'occasion du Cybermois 2025
2e baromètre IPSOS.Digital de la perception cyber
1er octobre
Lancement officiel du 13e Cybermois et du CyberTour de France
8 octobre
2e baromètre sur la maturité cyber des TPE-PME
14 octobre
Intégration de l'offre téléphonique du premier CSIRT territorial au 17Cyber (NAQ)
17 octobre
Cybermalveillance.gouv.fr a 8 ans
7 novembre
Violation de données personnelles de la Fédération Française de Tir : situation, risques et recommandations
18 novembre
Publication d'une lettre ouverte à destination des élus
JUILLET
AOÛT
SEPT
OCTOBRE
NOVEMBRE

L'ACTUALITÉ DE L'ANNÉE **2025**

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 2025, ses ressources ont été enrichies de **plus de 103 supports** et notamment de :

• **3 campagnes de communication :** Campagne ***Cyber en Clair*** ; Campagne ***#PrenezLaConfiance*** ; Campagne ***Histoire de Cyber*** pour le Cybermois ;

• **1 article « État de la menace » :** *2024, une année marquée par un nombre record de violations de données personnelles* ;

• **1 article « Menaces » :** *L'hameçonnage au faux numéro d'opposition bancaire* ;

• **2 articles « Top 10 » des cybermenaces les plus fréquentes par public :** particuliers et professionnels ;

• **2 fiches réflexes :** *Que faire en cas d'escroquerie au placement financier ?* et *Rançongiciel ou ransomware : que faire si votre organisation est victime d'une attaque ?* ;

• **2 articles « Violation de données personnelles » :** *Bouygues Telecom : situation, risques et recommandations* ; *Fédération Française de Tir (FFTir) : situation, risques et recommandations* ;

• **2 AlerteCyber :** Failles de sécurité critiques dans les produits Microsoft ; failles de sécurité critiques dans Microsoft SharePoint. Et **3 alertes de vulnérabilité informatique** : Infection par le virus Bumblebee ; compromission de produits Fortinet ; vulnérabilité affectant des produits Fortinet ;

• **1 fiche mémo :** *Cyber réflexes – Maison et travail* (avec la CNIL[1]) ;

• **1 lettre d'information mensuelle :** tous publics et sa déclinaison sur LinkedIn *La Lettre Cyber* ;

• **1 *Flash info* :** pour les prestataires informatiques ;

• **1 lettre mensuelle *Info ExpertCyber* :** pour les prestataires labellisés ;

• **1 sélection presse hebdomadaire :** revue de presse pour les membres et les prestataires du dispositif ;

• **Autres réalisations :** 2e édition du baromètre national de la maturité cyber des TPE-PME ; 2e édition du Mémento ImpactCyber avec mise à jour du baromètre ; lettre ouverte aux élus à l'occasion du Salon des Maires et des Collectivités locales.

[1] Commission Nationale de l'Informatique et des Libertés

CYBERMALVEILLANCE.GOUV.FR DÉVOILE SA STRATÉGIE 2025-2030

Cybermalveillance.gouv.fr a rendu publique en mars sa stratégie 2025-2030 à l'occasion de la présentation de son rapport d'activité et des tendances de la menace cyber en France. Élaborée à la suite des recommandations de la Cour des comptes et en cohérence avec la stratégie nationale de cybersécurité, cette feuille de route à cinq ans fixe le cadre d'évolution du GIP ACYMA pour répondre aux défis croissants de la menace numérique. Elle présente le contexte dans lequel le dispositif évolue, décrit la méthodologie utilisée pour déterminer ses priorités et objectifs, dresse le bilan des actions menées et définit les objectifs stratégiques qui guideront son développement au service des particuliers, des entreprises et des collectivités.

INTÉGRATION PROGRESSIVE DE L'OFFRE D'ASSISTANCE DES CSIRT TERRITORIAUX

En avril, Cybermalveillance.gouv.fr a engagé, avec les centres de réponse à incident (CSIRT) territoriaux, une démarche visant à optimiser la prise en charge des victimes professionnelles à travers un service d'assistance de proximité. Cette initiative permet à des entreprises ou collectivités victimes de bénéficier d'un accompagnement téléphonique avec un opérateur de leur CSIRT régional pour gérer leur incident de cybersécurité de premier niveau. À la fin de l'année 2025, une étape importante a été franchie avec l'intégration du service d'assistance téléphonique de leur CSIRT de 5 premières régions au dispositif 17Cyber : Nouvelle-Aquitaine, Occitanie, Réunion, Grand Est et Caraïbes. Cette dynamique, menée en lien étroit avec les acteurs territoriaux et le soutien de l'ANSSI, renforce le positionnement du 17Cyber comme point d'entrée national de l'assistance cyber en France.

WEBINAIRE EXPERTCYBER : ACCOMPAGNER LA MONTÉE EN PUISSANCE DU LABEL

Cybermalveillance.gouv.fr a organisé le 3 juin le webinaire *Comment se faire labelliser ExpertCyber ?*, afin d'accompagner les prestataires informatiques dans l'accès au label ExpertCyber. Conçu avec le Groupe AFNOR, le Groupe Conty et la Fédération EBEN, cet événement présentait les critères d'éligibilité, le processus de labellisation et les exigences associées, avec le témoignage de structures déjà labellisées pour illustrer concrètement la démarche. Le webinaire est disponible en rediffusion afin de permettre aux professionnels intéressés de préparer leur candidature.

MALLETTECYBER : UN DÉPLOIEMENT NATIONAL AU SEIN DE 3 000 LIEUX DE MÉDIATION NUMÉRIQUE AVEC L'ANCT ET LA MEDNUM

Après la livraison de 1 600 MalletteCyber en 2024, Cybermalveillance.gouv.fr, l'ANCT[1] et la Mednum ont poursuivi en 2025 la diffusion de cet outil au sein des réseaux de médiation numérique. À l'issue de cette nouvelle phase de déploiement, 3 000 acteurs de médiation sont désormais équipés de la MalletteCyber sur l'ensemble du territoire pour accompagner des publics plus vulnérables.

[1] Agence Nationale de la Cohésion des Territoires

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

OPÉRATION IMPACTCYBER : 2e ÉDITION DU BAROMÈTRE NATIONAL DE LA MATURITÉ CYBER DES TPE-PME

Dans la continuité de ses actions de sensibilisation auprès des entreprises, Cybermalveillance.gouv.fr a publié en octobre la 2e édition du baromètre national de la maturité cyber des TPE-PME[1], réalisée avec la CPME[2], le MEDEF[3] et l'U2P[4]. Les résultats montrent une amélioration de la perception des risques et des dispositifs de sécurité, avec une hausse des protections et des procédures internes mises en place. Ils soulignent toutefois des fragilités persistantes : 6 entreprises sur 10 semblent toujours ne pas savoir évaluer les conséquences d'une cyberattaque et elles sont encore 80 % à estimer ne pas être suffisamment préparées. Les contenus de sensibilisation associés ont bénéficié d'une large visibilité médiatique, notamment grâce à une diffusion massive de spots sur BFM Business et BFM Radio, renforçant la portée des messages de prévention auprès des dirigeants de TPE-PME.

LETTRE OUVERTE AUX MAIRES DE FRANCE POUR RENFORCER LA CYBERSÉCURITÉ

À l'occasion du Salon des Maires et des Collectivités locales, Cybermalveillance.gouv.fr et un collectif d'acteurs engagés ont publié en novembre une *lettre ouverte*, avec le soutien de l'ANSSI, APVF, AVICCA, coTer numérique, Déclic, invitant les maires de France à renforcer la cybersécurité de leur commune. Malgré une meilleure conscience des risques, seules 14 % des collectivités se déclarent bien préparées face aux cyberattaques. La lettre rappelle les pratiques essentielles : sécuriser les infrastructures, sensibiliser élus et agents, et intégrer la cybersécurité dans les plans de continuité. Elle présente également des services clés pour accompagner les collectivités, dont SensCyber, Mon ExpertCyber, MesServicesCyber, la Suite territoriale et le 17Cyber. Cette initiative vise à faire de la cybersécurité un enjeu structurant de gouvernance locale et de résilience territoriale.

CYBERMALVEILLANCE.GOUV.FR DÉVOILE UN LIVRET POUR LES ENFANTS DE 9–12 ANS : « LE NUMÉRIQUE, PAS DE PANIQUE ! »

Pendant le Cybermois, Cybermalveillance.gouv.fr a lancé le livret *Le numérique, pas de panique !*, destiné aux enfants de 9 à 12 ans pour les aider à identifier et prévenir les principaux risques numériques tels que le cyberharcèlement, l'hameçonnage, les fraudes en ligne ou l'exposition à des contenus malveillants. Issu d'un mécénat dans le cadre d'un groupe de travail dédié, ce support a été conçu avec le soutien de l'Afnic et produit en partenariat avec Bayard Média Développement et Astrapi.

Diffusé auprès des abonnés du magazine Astrapi (73 000 exemplaires), relayé par le ministère de l'Éducation nationale, et téléchargeable gratuitement sur la plateforme (6 500 téléchargements), il a généré au total 135 000 impressions. Afin de faciliter son appropriation en milieu scolaire, un support pédagogique a été mis à disposition des enseignants, ainsi qu'un contenu dédié permettant à des intervenants de présenter le livret sous forme d'ateliers auprès de classes ou de groupes d'enfants. Le livret a également été décliné en exposition itinérante en Bretagne et en Nouvelle-Aquitaine, renforçant sa diffusion auprès du jeune public et des communautés éducatives.

[1] Très Petites Entreprises - Petites et Moyennes Entreprises
[2] Confédération des petites et moyennes entreprises
[3] Mouvement des Entreprises de France
[4] Union des Entreprises de Proximité

LES MEMBRES DU **GT MÉCÉNAT**

Mené entre 2024 et 2025, ce groupe de travail s'est régulièrement réuni afin d'identifier des projets susceptibles d'être réalisés dans le cadre d'un mécénat lié aux missions du GIP.

afnic — anct agence nationale de la cohésion des territoires — bouygues telecom — france•tv — Microsoft

Ministère de l'Économie, des Finances et de la Souveraineté industrielle, énergétique et numérique — Direction générale du Trésor — Cyberdefense — paloalto networks — Unaf Unis pour les familles

NOS COLLABORATIONS

SENSIBILISATION DE 190 000 POSTIERS AVEC LA POSTE GROUPE

Cybermalveillance.gouv.fr et La Poste Groupe ont co-élaboré un support de sensibilisation diffusé début février auprès de 190 000 postiers, via une insertion dans le magazine de communication interne *Forum*. Conçu comme un support opérationnel, ce prospectus présente les principales fraudes en circulation, les bons réflexes à adopter et les modalités de signalement en cas d'incident. Cette action vise à renforcer la vigilance des agents face aux cybermenaces et à accompagner la montée en compétence des équipes dans leurs pratiques numériques quotidiennes.

ORGANISATION DU COLLOQUE SUR LES IMPACTS PSYCHOLOGIQUES DES CYBERATTAQUES AVEC AÉMA GROUPE ET FRANCE VICTIMES

À l'initiative d'Aéma Groupe, et en partenariat avec France Victimes, un colloque consacré aux impacts psychologiques des cyberattaques a été organisé avec les équipes de Cybermalveillance.gouv.fr le 13 février dernier. Il a ainsi mis en lumière un volet encore peu traité de la cybermalveillance : les répercussions humaines et émotionnelles pour les victimes. En réunissant acteurs publics, experts, associations et représentants du secteur assurantiel, l'événement a inscrit cette dimension dans une approche plus globale de la cybersécurité. Des agents de Cybermalveillance.gouv.fr ont pu échanger avec le public et proposer les ressources du dispositif.

CYBERMALVEILLANCE.GOUV.FR, MEMBRE FONDATEUR DE L'ÉQUIPE DE FRANCE DU NUMÉRIQUE DE NUMEUM

En juin, Cybermalveillance.gouv.fr est devenu membre fondateur de l'Équipe de France du Numérique portée par Numeum. Cette initiative constituée de plus de 70 organisations, vise à fédérer les acteurs du secteur, améliorer la lisibilité de l'écosystème et structurer des prises de parole communes sur les enjeux clés du numérique en France. Par sa participation active, Cybermalveillance.gouv.fr partage son expertise, contribue aux travaux collectifs et soutient l'émergence d'une vision commune d'un numérique responsable, engagé et accessible à tous.

MOBILISATION CONJOINTE CONTRE LES ARNAQUES AU FAUX SUPPORT TECHNIQUE AVEC MICROSOFT ET LE PARQUET DE PARIS

Microsoft, Cybermalveillance.gouv.fr et la section de lutte contre la cybercriminalité du Parquet de Paris se sont associés en juillet dernier pour renforcer la prévention autour des arnaques au faux support technique, 4e menace cyber touchant les particuliers. Face à l'augmentation des préjudices et à la sophistication des modes opératoires, cette collaboration a permis de rappeler les bons réflexes à adopter. Deux supports de sensibilisation ont été produits : une fiche destinée aux jeunes et une autre dédiée aux seniors, afin d'adapter les messages aux publics les plus concernés. Ces ressources visent à faciliter l'identification de ce type d'arnaque, encourager les gestes de protection essentiels et orienter les victimes potentielles vers 17Cyber.gouv.fr

PLAN D'ACTION CONJOINT AVEC LE CNOEC POUR LA CYBERSÉCURITÉ DES CABINETS D'EXPERTISE-COMPTABLE

Cybermalveillance.gouv.fr a conduit en 2025 une collaboration étroite avec le CNOEC[1] afin d'accompagner la profession face à l'évolution des risques numériques. Cette démarche s'est concrétisée par une intervention lors du webinaire *Cybersécurité et intelligence artificielle : nouvelle donne pour les cabinets d'expertise-comptable*, organisé le 25 juin aux côtés du ComCyberMI[2], ainsi que par une prise de parole lors du 80e Congrès national des experts-comptables le 18 septembre. Enfin deux articles sont venus compléter le dispositif de sensibilisation en octobre.

[1] Conseil national de l'ordre des experts-comptables
[2] Commandement du ministère de l'Intérieur dans le cyberespace

SENSIBILISATION DES ÉQUIPES DE L'ASSOCIATION E-ENFANCE/3018

Cybermalveillance.gouv.fr est intervenu auprès des écoutants du 3018 et des responsables des actions de prévention en milieu scolaire dans le cadre de la formation continue de l'association e-Enfance/3018. Cette session a permis de présenter de manière exhaustive les missions du dispositif, ses publics, ses ressources ainsi que le service 17Cyber, afin d'enrichir les solutions d'assistance et les ressources disponibles pour les jeunes, les éducateurs et les victimes. Une initiative qui participe activement à renforcer l'action des équipes engagées quotidiennement dans la protection des mineurs face aux risques numériques.

PARCOURS CYBERSÉCURITÉ D'ORANGE : DES ATELIERS ENRICHIS EN COLLABORATION AVEC CYBERMALVEILLANCE.GOUV.FR

Utiliser le numérique en toute sécurité, *Éviter les arnaques en ligne* et *Sécuriser ses données personnelles* : les trois ateliers numériques du parcours cybersécurité d'Orange Cyberdéfense ont été revus et enrichis en 2025 avec l'appui de Cybermalveillance.gouv.fr afin de renforcer leur portée pédagogique. Ouverts à tous les publics souhaitant développer leurs compétences numériques, ces ateliers, proposés en ligne comme en présentiel, sont animés par des ambassadeurs Orange et contribuent à diffuser largement les bons réflexes de sécurité numérique sur l'ensemble du territoire.

SENSIBILISATION AUX HYPERTRUCAGES AVEC MACIF ASSURANCES

Cybermalveillance.gouv.fr et Macif Assurances (Aéma Groupe) ont co-produit une vidéo de sensibilisation aux hypertrucages (*deepfakes*), diffusée le 22 décembre sur TikTok avec la créatrice de contenus @creatwithamy. En s'appuyant sur une mise en situation d'usurpation d'identité, le format permet de mieux appréhender ce phénomène et les risques associés. La vidéo apporte également des repères de prévention, en mettant en avant trois réflexes clés pour se prémunir des hypertrucages et renforcer la sécurité numérique du grand public.

FOCUS SUR LES PRINCIPALES CONTRIBUTIONS AVEC **LE MINISTÈRE DE L'ÉDUCATION NATIONALE**

PARTICIPATION AU **PRIX *NON AU HARCÈLEMENT***

En mars, Cybermalveillance.gouv.fr a renouvelé sa participation au Prix *Non au harcèlement*, en siégeant au jury de pré-sélection et au jury national. Organisé par le ministère de l'Éducation nationale, avec le soutien de la MAE[1], ce prix vise à donner la parole aux élèves, du CP à la terminale, à travers la création d'affiches ou de vidéos de prévention contre le harcèlement et le cyberharcèlement en milieu scolaire. Cette mobilisation s'est conclue par une cérémonie de remise des prix le 21 mai 2025 au Palais de l'Élysée. Par son engagement, Cybermalveillance.gouv.fr soutient l'expression des élèves et contribue au renforcement de la prévention du harcèlement et du cyberharcèlement, en lien avec les actions éducatives portées par l'institution.

[1] Mutuelle Assurance de l'Éducation

OPÉRATION *CACTUS*: SENSIBILISATION NATIONALE À L'HAMEÇONNAGE DANS LES ENT

Face à la multiplication des attaques ciblant les ENT[1], le ministère de l'Éducation nationale, le ministère de l'Intérieur, Cybermalveillance.gouv.fr, la CNIL et la juridiction nationale de lutte contre la cybercriminalité ont lancé l'opération *Cactus* pour sensibiliser collégiens et lycéens aux risques d'hameçonnage et des virus collectant des mots de passe (*infostealers*). Après une expérimentation réussie en 2024, la campagne a été généralisée à l'échelle nationale du 19 au 21 mars 2025. 2,5 millions d'élèves dans 4 700 établissements ont ainsi reçu un message les incitant à cliquer sur un lien de jeux piratés, redirigeant vers une vidéo pédagogique. Celle-ci expliquait les mécanismes de l'hameçonnage, présentait des conseils de prévention et rappelait les sanctions encourues. Un kit pédagogique a été mis à disposition des enseignants pour accompagner un dispositif appelé à être reconduit d'année en année, complété par des actions menées en classe pour renforcer durablement les bonnes pratiques numériques des élèves.

[1] Espaces Numériques de Travail

GUIDE NATIONAL DE LA PARENTALITÉ NUMÉRIQUE

Cybermalveillance.gouv.fr a contribué au *guide national de la parentalité numérique* publié en juillet dernier par le ministère de l'Éducation nationale. Le dispositif y est référencé comme ressource clé pour accompagner les familles dans leurs usages numériques, notamment via le *Cyber Guide Famille*, renforçant ainsi son rôle dans la sensibilisation et l'éducation au numérique. Ce guide vient compléter le lancement par le ministère d'un jeu familial gratuit, l'*Odyssée du numérique*, conçu pour favoriser l'apprentissage des bons usages en ligne de manière ludique et encourager le dialogue intergénérationnel autour des pratiques numériques.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

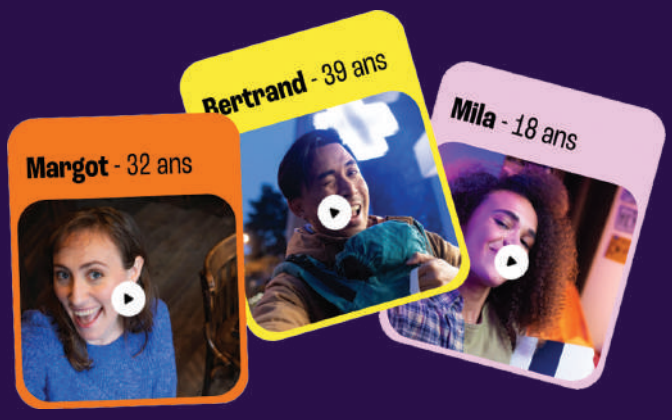
LES **CAMPAGNES DE COMMUNICATION**

LA CAMPAGNE ***CYBER EN CLAIR***

À l'occasion de la 22e édition du *Safer Internet Day*, Cybermalveillance.gouv.fr a lancé une mini-série destinée à sensibiliser les jeunes, leurs familles et acteurs éducatifs aux usages numériques du quotidien. Les trois premiers épisodes – *Les téléchargements*, *Les réseaux sociaux* et *L'hameçonnage* – apportent des réponses simples aux questions que se posent les enfants et préadolescents sur les risques en ligne et rappellent les bons réflexes à adopter pour naviguer en sécurité. Cette campagne vise, elle aussi, à rendre la cybersécurité plus accessible et compréhensible par les jeunes publics.

LA CAMPAGNE ***#PRENEZLACONFIANCE***

Le 20 janvier, la Caisse des Dépôts, la Croix-Rouge française, Cybermalveillance.gouv.fr, Docaposte, Inria et Orange ont lancé *#PrenezLaConfiance*, une campagne nationale issue du consortium *Confiance numérique du quotidien*. Face au constat d'un manque de confiance persistant dans les usages numériques, la campagne rappelle les bons réflexes pour un numérique plus sûr à travers trois courts métrages, une déclinaison sur les réseaux sociaux et un site dédié Prenezlaconfiance.fr. Relayée par l'ensemble des partenaires, elle encourage chaque citoyen à adopter des pratiques numériques simples et sécurisées.



NOS PRINCIPALES INTERVENTIONS

JANVIER

9 janvier	Intervention auprès des étudiants de l'école 2600 sur les enjeux organisationnels et humains de la cybersécurité.
17 janvier	Présentation des ressources Cybermalveillance.gouv.fr et du 17Cyber aux conseillers France services de la Ville de Paris.
24 janvier	Webinaire France Travail organisé dans le cadre de la Semaine du Numérique pour sensibiliser les demandeurs d'emploi parisiens aux arnaques les plus courantes et leur présenter Cybermalveillance.gouv.fr et le 17Cyber.
28 janvier	Ouverture de la plénière du salon GSDays avec la présentation du 17Cyber.

28 janvier 2025. Ouverture de la plénière du salon GSDays.

FÉVRIER

5 février	Webinaire des *Experts du Numérique en Entreprise* (ENE) en Auvergne-Rhône-Alpes auprès des adhérents de la Fédération des Entreprises du BTP de la région pour sensibiliser les dirigeants de TPE-PME aux risques cyber et leur présenter le 17Cyber.
5 février	Intervention auprès des élèves officiers de l'Académie militaire de la Gendarmerie nationale dans le cadre d'une session "cyber".
7 février	Sensibilisation des dirigeants et cadres de TPE-PME sur les menaces actuelles et les bonnes pratiques cyber lors d'un webinaire organisé pour l'UNEA[1].
27 février	Animation d'un webinaire organisé par la Préfecture de la Sarthe pour sensibiliser les élus locaux aux menaces ciblant les collectivités ainsi qu'aux ressources et service de sécurisation proposés par Cybermalveillance.gouv.fr

[1] Union Nationale Des Entreprises Adaptées

MARS

13 mars	Sensibilisation auprès de l'association Les Enfants du Mékong pour présenter l'état de la menace et les moyens de s'en prémunir.
13 mars	Animation d'un webinaire organisé par la CNAV[1] au profit de ses personnels.
13 mars	Animation d'une conférence lors du Salon des Seniors à Paris, sur invitation de la CNIL.
20 mars	Intervention en plénière aux Journées de la Cyber du Collectif ENE AuRA au Campus du Numérique.
28 mars	Participation en distanciel à une table ronde organisée lors du Salon 3S'EXPO Tour Martinique - Sécurité • Sûreté • Sérénité - consacrée aux acteurs étatiques opérant dans la lutte contre la cybercriminalité et la protection des entreprises.

[1] Caisse nationale d'assurance vieillesse

AVRIL

3 avril	Soirée grand public organisée par les caisses locales Groupama de Reims, centrée sur le thème des cybermenaces.
8 avril	Animation d'un webinaire organisé par le CTRC[1] AuRA au profit des permanents des associations de défense des consommateurs de la région.
9 avril	Participation aux Rencontres Territoriales des Systèmes d'Information organisées par le CNFPT, pour les RSSI[2] et DSI[3] des collectivités territoriales.
24 avril	Intervention lors d'un webinaire grand public organisé par WeTechCare (Lesbonsclics.fr).
28 avril	Webinaire pour l'Académie de Martinique consacré aux principales cybermalveillances touchant les administrations avec une présentation du 17Cyber et de l'opération Cactus.
28 avril	Animation d'un webinaire de la Macif destiné aux acteurs de l'économie sociale et solidaire pour présenter les menaces qui touchent les professionnels et le 17Cyber.

[1] Centre Technique Régional de la Consommation
[2] Responsable Sécurité des Systèmes d'Information
[3] Directeur des Systèmes d'Information

MAI

20 mai	Webinaire organisé par la FFMAS[1] pour ses adhérents.
20 mai	Intervention devant le collège des Commissaires de la CNIL.
22 mai	Participation au premier Forum InCyber des territoires au Creusot.

[1] Fédération Française des Métiers de l'Assistanat et du Secrétariat

JUIN

2 juin	Participation au séminaire de sensibilisation aux enjeux cyber organisé pour les collectivités territoriales par la Direction départementale des finances publiques.
3 juin	Prises de parole à l'occasion d'une campagne de sensibilisation organisée par la Communauté de Communes Bretagne Porte de Loire pour les élus locaux ainsi que les aidants, suivies d'une conférence pour les administrés.
11 et 13 juin	Interventions à Caen et Rouen auprès des conseillers et médiateurs numériques normands, coordonnées par le Hub Numi, pour présenter aux usagers les dernières actualités et supports de Cybermalveillance.gouv.fr
12 juin	Participation au webinaire organisé par France Num pour les entreprises.
16 juin	Conférence hybride lors du L'Oréal Cyberday sur les menaces touchant les particuliers et les réflexes à adopter.
17 et 18 juin	Participation à l'événement annuel du CoTer numérique à Clermont-Ferrand.
19 juin	Conférence lors de la première édition du Numérique En Commun[s] local dans le Lot.
23 juin	Conférence lors du séminaire organisé par la sous-préfecture de Dieppe à Forges-les-Eaux pour présenter aux élus locaux les services 17Cyber et Mon ExpertCyber.
25 juin	Animation d'un webinaire du CNOEC.
25 juin	Participation à l'événement Innodays de Bouygues Telecom pour présenter les services et supports de Cybermalveillance.gouv.fr dont SensCyber et le 17Cyber.
30 juin	Conférence devant les élus de l'Eure lors d'un évènement organisé par le département et Eure Normandie Numérique pour les informer des solutions d'assistance et d'accompagnement de Cybermalveillance.gouv.fr

JUILLET

1er juillet	Intervention lors d'un webinaire de l'Incubateur des territoires de l'ANCT destiné aux élus et cadres locaux bénéficiant de l'ANSM[1].
16 juillet	Prise de parole lors d'un grand débat consacré aux risques liés aux réseaux sociaux, organisé par la revue Risques (France Assureurs).
24 juillet	Animation d'un webinaire pour les conseillers numériques des Alpes-Maritimes afin de présenter le 17Cyber, la MalletteCyber et le Cybermois.

[1] Accompagnement Numérique Sur Mesure

SEPTEMBRE

17 et 18 sept	Table ronde animée par le CLUSIR sur le panorama des cybermenaces au Salon Lyon Cyber Expo aux côtés du CESIN et d'Hexatrust et conférence plénière sur le thème de la souveraineté européenne.
18 sept	Conférence au 80e Congrès du CNOEC à Lyon sur les menaces visant la profession des experts-comptables et présentant les services de Cybermalveillance.gouv.fr
18 sept	Participation à un événement cyber organisé par la CCI Meuse Haute-Marne sur la base aérienne 113 de Saint-Dizier.

18 septembre 2025. Événement cyber organisé par la CCI Meuse Haute-Marne sur la base aérienne 113 de Saint-Dizier.

OCTOBRE

1er oct	Lancement du Cybermois et du CyberTour de France à Rennes depuis l'hôtel de Courcy.
2 oct	Présentation des menaces, des bonnes pratiques et du Cybermois lors du 2e webinaire WeTechCare.org (Lesbonsclics.fr).
2 oct	Ouverture du *Digital Day* de la Brasserie du Digital au Puy-en-Velay dans le cadre du Cybermois, avec conférence plénière, atelier France services et podcast.
6 oct	1re étape du CyberTour de France à Périgueux au théâtre de l'Odyssée.
7 oct	Webinaire du CERT Santé pour les professionnels du secteur consacré aux menaces, ressorts psychologiques des escrocs et bonnes pratiques à observer.
7 au 10 oct	Participation aux Assises de la cybersécurité à Monaco.
8 oct	Participation aux Cyberdays pour évoquer l'engagement cyber de BNP PARIBAS en tant que membre de Cybermalveillance.gouv.fr et mettre en avant le 17Cyber en présentiel et en distanciel.
8 oct	Conférence donnée à Orléans lors du séminaire national annuel des DSI[1] de la DRASI[2] (Éducation nationale).
9 oct	Table ronde sur la cybersécurité lors des rencontres nationales de DÉCLIC à Tours.
13 oct	Intervention lors d'un webinaire ECTI, avec une mise en avant du 17Cyber auprès d'un public éloigné du numérique, principalement des seniors.
14 oct	À l'occasion du Cybermois, table ronde pour France TV lors d'un événement interne.
14 oct	Intervention lors de la rencontre avec la Mission cinéma du Ministère de l'Intérieur.
15 oct	Participation à la conférence hybride de l'association 1FO100NUAGES à Brasles sur les bons réflexes à adopter en cas de suspicion d'escroquerie.
15 oct	2e étape du CyberTour à Lille, organisée avec le Campus Cyber Hauts-de-France, Euratechnologies et la ville de Lezennes au Kiabi Village.

17 oct	Participation à la conférence-débat du SHFD[3] du Ministère de l'Intérieur dans le cadre du Cybermois, avec présentation du 17Cyber et de SensCyber auprès de l'ensemble des agents.
17 oct	3e étape du CyberTour à Rouen organisée avec le Campus Normandie Cyber et la Métropole à Seine Innopolis.
27 oct	Clôture du CyberTour de France au Campus national Cyber de la Défense dans le cadre d'une matinée de sensibilisation à l'hygiène numérique.
29 et 30 oct	Intervention en distanciel au SecNumÉco de La Réunion (Saint-Denis et Saint-Pierre).
29 et 30 oct	Salon Numérique En Commun[s] à Strasbourg, organisé par le programme Société Numérique de l'ANCT avec animation d'un atelier sur le 17Cyber, contribution à un *Regards croisés* consacré à la formation des élus locaux et échanges avec le public sur le stand.
30 oct	Sensibilisation des députés et sénateurs à l'Assemblée nationale.

[1] Directeur des Systèmes d'Information
[2] Direction Régionale Académique des Systèmes d'Information
[3] Service du haut fonctionnaire de défense

18-20 novembre 2025. Participation au 107e Congrès et Salon des Maires et des collectivités locales.

NOVEMBRE

18-20 nov	Participation au 107e Congrès et Salon des Maires et des collectivités locales avec publication d'une lettre ouverte aux élus, conférence sur la protection nécessaire des entités publiques face aux menaces croissantes et table ronde animée par Cybermalveillance.gouv.fr sur la gestion des enjeux cyber dans le cadre d'un mandat.
25 nov	Présentation de Cybermalveillance.gouv.fr et du service Mon ExpertCyber lors d'un événement organisé par DEV'UP Centre–Val de Loire sur la transition numérique, avec témoignage d'un professionnel labellisé.
26 nov	7e édition de la Cyber Business Convention à Toulouse : stand et table ronde avec le MEDEF auprès des entreprises sur le thème du levier de compétitivité que représente la cybersécurité.
27 nov	Webinaire pour la Réserve Cyber de la Police nationale (ReCym), coordonnée par la DNPJ[1]-OFAC[2], pour présenter le 17Cyber et les ressources de Cybermalveillance.gouv.fr

[1] Direction nationale de la Police judiciaire
[2] Office anti-cybercriminalité

DÉCEMBRE

4 déc	Participation à la 1re édition de Numérique En Commun[s] organisée par le département du Tarn à Albi, à destination des aidants numériques et des collectivités territoriales. Intervention en plénière pour présenter le 17Cyber et les ressources de Cybermalveillance.gouv.fr
8 déc	Webinaire pour l'association CLCV[1] consacré aux menaces cyber, aux bonnes pratiques de prévention et à la présentation du 17Cyber.
8 déc	Participation à la 1re édition régionale de Numérique En Commun[s] en Auvergne-Rhône-Alpes. Intervention lors d'une session *Regards croisés* sur la formation des élus et animation d'un atelier consacré au 17Cyber.
15 déc	Webinaire pour la Fédération Nationale des OGEC[2] autour des cybermalveillances, des moyens de s'en protéger et du 17Cyber.
18 déc	Sensibilisation pour la CNDP[3] dédiée aux bonnes pratiques cyber et aux ressources de Cybermalveillance.gouv.fr

[1] Consommation Logement Cadre de Vie
[2] Organismes de gestion de l'Enseignement catholique
[3] Commission Nationale du Débat Public

FOCUS

NOS INTERVENTIONS EN DÉTAIL

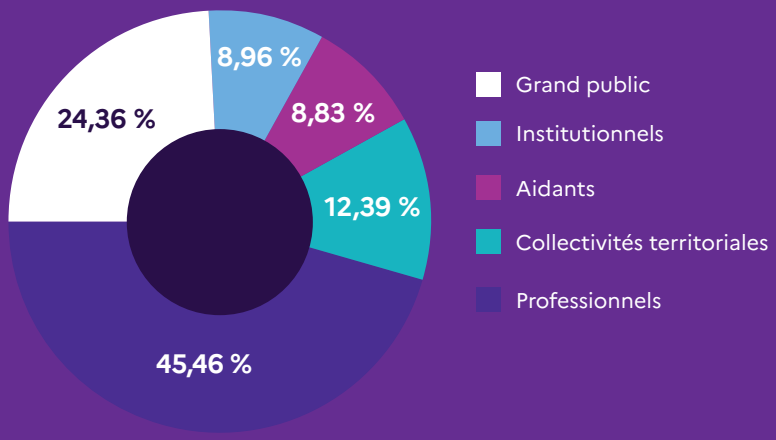
Sur l'année 2025, le pôle sensibilisation a réalisé 185 interventions parmi lesquelles des webinaires, conférences ou encore tables rondes. 55 % des événements étaient physiques.

AUDIENCE **PAR TYPOLOGIE D'ÉVÈNEMENTS**

Au total, **20 537 personnes ont été sensibilisées sur l'année 2025 :** 7 925 lors de conférences ou tables rondes, 3 540 lors de salons et 9 072 à l'occasion d'interventions dans des webinaires.

TYPOLOGIE **DE PUBLICS SENSIBILISÉS**

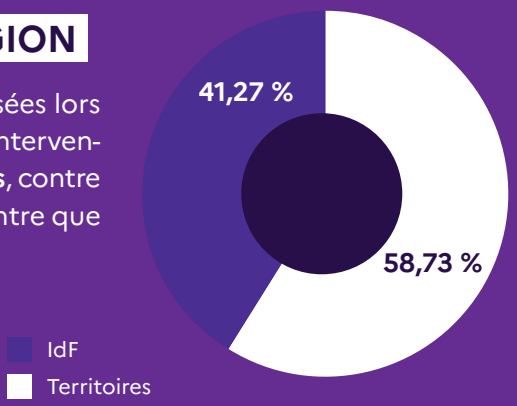
En 2025, les professionnels représentent 45 % du public total sensibilisé soit une augmentation de 22,7 % par rapport à 2024. Le grand public représente 24 % et les collectivités 12 %.



Typologie des publics sensibilisés (par nombre de personnes)

UNE FORTE SENSIBILISATION **EN RÉGION**

Sur l'année 2025, **11 465 personnes** ont été sensibilisées lors d'interventions en présentiel. Bien que le nombre d'interventions soit plus élevé en **Île-de-France** (**72 interventions**, contre **55 autres**), la répartition des publics sensibilisés montre que 6 personnes sensibilisées sur 10 résident **en région**.



Répartition géographique des personnes sensibilisées lors d'interventions en présentiel.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

Dans le cadre de sa 13e édition, le Cybermois a mobilisé 1500 entités qui se sont engagées à relayer nos messages et à organiser de nombreux événements ou actions de sensibilisation.

AGENDA NATIONAL DU CYBERMOIS
UNE MOBILISATION RENFORCÉE EN 2025

Pour la 3e année consécutive, Cybermalveillance.gouv.fr a mis à disposition un agenda national qui recense, suite à leur inscription, des événements de sensibilisation cyber menés durant le Cybermois. Cet outil a connu une évolution significative, de 400 événements enregistrés en 2024 à 1300 en 2025, avec des formats variés : ateliers, conférences, goûters, webinaires, formations, expositions, jeux pédagogiques… L'agenda s'affirme désormais comme une vitrine du Cybermois qui offre une visibilité sur la mobilisation collective et la diversité des actions réalisées par des acteurs publics, privés et associatifs engagés dans la sensibilisation.

CAMPAGNE *HISTOIRE DE CYBER* :
HUMOUR ET CULTURE AU SERVICE DE LA SENSIBILISATION

Comment attirer l'attention et responsabiliser le grand public à la cyber ? C'est tout l'objet de la campagne *Histoire de Cyber* qui revisite de grands épisodes de l'Histoire, du naufrage du Titanic à la bataille de Waterloo, en passant par le siège d'Alésia.
L'objectif ? Sensibiliser le grand public aux enjeux de la cybersécurité de manière originale et pédagogique. Chaque visuel établit un parallèle clair entre un événement historique emblématique et un risque numérique du quotidien (hameçonnage, double authentification, exposition des données, faux conseiller bancaire etc.) pour inviter les publics à jouer un rôle clé et prendre en main leur propre histoire, en respectant les bonnes pratiques.
Dans une logique de mobilisation collective, la campagne appelait également les organisations et les citoyens à relayer les contenus via #CyberEngagés (57M d'impressions). Diffusée également sous forme d'affiches, elle a bénéficié d'une visibilité nationale avec 22000 supports mis à disposition dans les maisons France services et les marchands de presse.

CHASSE AU TRÉSOR NUMÉRIQUE : UN FORMAT INTERACTIF
POUR ENCOURAGER L'EXPLORATION DES RESSOURCES

Du 1er au 31 octobre, Cybermalveillance.gouv.fr a proposé une chasse au trésor numérique destinée à encourager l'exploration de ses contenus pédagogiques et l'adoption des bons réflexes numériques. Les participants devaient retrouver cinq caractères dissimulés sur différentes pages du site afin de reconstituer un mot de passe mystère et tenter de remporter un lot. Cette initiative ludique a contribué à renforcer la découverte active des ressources, des bonnes pratiques et à aborder la cybersécurité sous un format accessible, interactif et engageant.

NOS COLLABORATIONS

ANCT ET RÉSEAU FRANCE SERVICES: UN RELAIS TERRITORIAL CLÉ

Cybermalveillance.gouv.fr et l'ANCT ont conduit une action de sensibilisation d'envergure au sein du réseau France services. Agents et coordinateurs ont été associés dès le lancement de l'opération au travers de communications internes, d'un webinaire dédié et de réunions d'information. Pour soutenir la diffusion territoriale, 6 000 affiches de la campagne *Histoire de Cyber* ont été distribuées pour les publics de 2 600 maisons France services. Cette mobilisation a abouti à l'organisation de 800 événements cyber à travers la France et à une participation active aux cinq étapes du CyberTour de France, renforçant l'ancrage territorial du dispositif auprès des usagers.

PROGRAMME DE SENSIBILISATION DES JEUNES PUBLICS AVEC LE MINISTÈRE DE L'ÉDUCATION NATIONALE

Depuis de nombreuses années, le ministère de l'Éducation nationale, membre actif de Cybermalveillance.gouv.fr, a déployé différentes actions pour sensibiliser les scolaires aux enjeux numériques.

Pour mieux cerner les besoins des jeunes élèves, une enquête menée en septembre 2025 auprès de 4 264 élèves dans les Territoires Numériques Éducatifs (TNE) a permis de dresser un premier état des lieux de leurs usages, de leur exposition aux risques et de leurs connaissances en matière de cybersécurité. Ces enseignements témoignent parfaitement des efforts de sensibilisation qui doivent être mis en place auprès des plus jeunes.

C'est pourquoi, face à cet enjeu sociétal, l'Éducation nationale a décidé de mettre en place plusieurs actions visant plus particulièrement les 9-12 ans (cycle 3) et correspondant aux premiers usages autonomes d'outils numériques.

Ce travail a conduit à la diffusion du livret *Le numérique, pas de panique !* et de son support pédagogique pour les enseignants, à la mise en avant du *Cyber Guide Famille* ainsi qu'à la publication de deux vidéos tournées pour illustrer de manière concrète et accessible, les risques numériques et les bons réflexes à adopter.

Enfin, un défi créatif national invite les classes du CM1 à la terminale à produire leurs propres supports de sensibilisation d'ici la fin de l'année scolaire. Les réalisations seront valorisées sur les espaces pédagogiques du ministère.

L'ensemble de ces actions s'inscrit dans une démarche ministérielle de prévention et de responsabilisation pour répondre à l'usage précoce du numérique chez les jeunes et initier ainsi un maximum d'élèves à la cybersécurité de façon durable.

FRANCE TÉLÉVISIONS : UN ACTEUR MÉDIA PLEINEMENT ENGAGÉ DANS LA PRÉVENTION CYBER

France Télévisions a engagé, en lien avec Cybermalveillance.gouv.fr, un ensemble d'actions de sensibilisation auprès de ses publics et de ses collaborateurs. Cette mobilisation s'inscrit dans une approche globale autour de plusieurs priorités : protection des infrastructures et des salariés, prévention des cybermalveillances, lutte contre les phénomènes de désinformation et de cybermanipulation, ainsi que protection de l'écosystème médiatique, culturel et sportif face au piratage des contenus. Dans ce cadre, des messages de sensibilisation ont été diffusés sur les antennes du groupe et sur ses réseaux sociaux. Un clip dédié au Cybermois, plusieurs vidéos intégrant des interventions de Cybermalveillance.gouv.fr, ainsi qu'une collection de programmes consacrés aux cybermenaces sur France.tv, ont contribué à toucher un large public.

En interne, cette dynamique a été complétée par l'organisation de conférences destinées aux équipes, portant notamment sur les risques d'hameçonnage, l'exposition à l'Internet sombre (*darkweb*) ou les ingérences étrangères. De plus, ces actions ont été enrichies par des temps d'échange entre les équipes de Cybermalveillance.gouv.fr et les collaborateurs de France Télévisions pour les informer et répondre à leurs questions sur la cybersécurité et les dispositifs d'assistance existants. Enfin, une campagne d'envergure sur le 17Cyber a été massivement diffusée sur de nombreuses chaînes du groupe.

COLLABORATION AVEC ORANGE CYBERDÉFENSE : OUTILLER LES AMBASSADEURS D'ORANGE

Cybermalveillance.gouv.fr a collaboré avec Orange Cyberdéfense pour accompagner la montée en compétence de la communauté des ambassadeurs d'Orange. Une synthèse pédagogique des principaux risques et des bons réflexes numériques leur a été fournie afin qu'ils puissent, à leur tour, sensibiliser efficacement tout au long du mois d'octobre. Cette action a renforcé la capacité de diffusion des messages du dispositif au sein d'un réseau interne à fort potentiel de démultiplication.

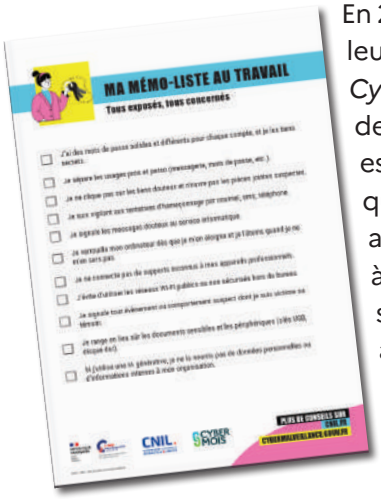
DIFFUSION DE MESSAGES CLÉS DE PRÉVENTION AUPRÈS DU GRAND PUBLIC AVEC GMF ASSURANCES

GMF Assurances (Groupe Covéa) et Cybermalveillance.gouv.fr ont produit une vidéo de sensibilisation rappelant trois règles essentielles pour protéger ses données : utiliser des mots de passe robustes et différents pour chaque compte, sauvegarder régulièrement ses informations et éviter de partager des données sensibles par messagerie ou téléphone. Diffusée sur les réseaux sociaux, cette vidéo invitait le grand public à adopter de bons réflexes numériques et à se tourner vers le 17Cyber en cas de doute ou d'incident. Une collaboration qui a contribué à amplifier la portée des messages de prévention auprès du grand public.

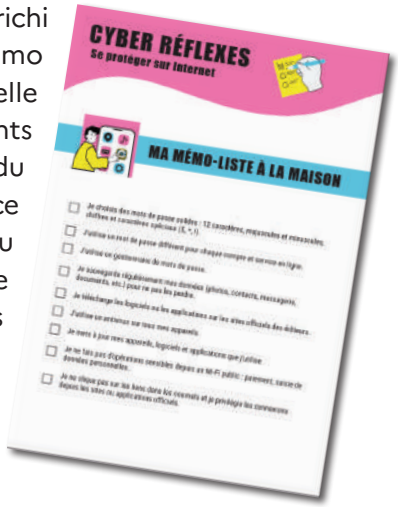
SENSIBILISATION À L'HAMEÇONNAGE
PAR DES FORMATS PÉDAGOGIQUES GRAND PUBLIC AVEC LA **MAIF**

Cybermalveillance.gouv.fr et la MAIF ont réalisé une vidéo de sensibilisation consacrée à l'hameçonnage, qui met en évidence la manière dont les attaquants jouent sur les émotions pour piéger leurs victimes. Diffusée sur numeriqueethique.fr, sur les réseaux sociaux et relayée dans une lettre d'information dédiée, elle explique comment repérer les pièges et adopter les bons réflexes face à un message suspect – notamment ceux envoyés par de faux livreurs – et invite à se tourner vers le 17Cyber pour obtenir assistance et conseils adaptés.

CYBER RÉFLEXES : UN MÉMO PRATIQUE
POUR LA MAISON ET LE TRAVAIL PRODUIT AVEC LA **CNIL**



En 2025, la CNIL et Cybermalveillance.gouv.fr ont enrichi leur collaboration avec la création d'une fiche mémo *Cyber réflexes – maison et travail*. Ce support rappelle de manière simple et accessible les comportements essentiels à adopter face aux risques numériques du quotidien : mises à jour, mots de passe, vigilance face aux arnaques et aux sollicitations en ligne. Conçu à partir des besoins constatés lors des actions de sensibilisation, il vient renforcer les ressources mises à disposition des particuliers et des professionnels pour encourager l'adoption de bonnes pratiques cyber.



ILS ONT SOUTENU L'ÉDITION 2025 DU CYBERMOIS :

- **Culture presse, le SNDP[1] et France Messagerie :** diffusion de l'affiche du Cybermois auprès de 15 000 marchands de presse.
- **BFM Business :** diffusion de la campagne *ImpactCyber*.
- **L'Internaute :** relais des messages et des actions de sensibilisation tout au long du mois d'octobre.
- **Le Parisien :** insertion de l'affiche du Titanic en clôture du Cybermois.

[1] Syndicat National des Dépositaires de Presse

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

ZOOM

ZOOM SUR LE
CYBERTOUR DE FRANCE

CYBERTOUR DE FRANCE :
LA CYBERSÉCURITÉ AU CŒUR DES TERRITOIRES

Cybermalveillance.gouv.fr a inauguré en 2025 un CyberTour de France afin de renforcer la sensibilisation aux enjeux de cybersécurité en allant à la rencontre des territoires. Organisé en collaboration avec les Campus Cyber territoriaux et les acteurs locaux, ce dispositif a permis de déployer des actions de prévention au plus près des publics, en s'adressant aux élèves, aux familles, aux professionnels ou encore aux collectivités.

Articulé autour de cinq étapes, le CyberTour de France a ainsi proposé à un vaste public conférences, ateliers, démonstrations, expositions et de nombreux échanges avec des experts. Des expositions issues du livret *Le numérique, pas de panique !*, des séances dédiées au cyberharcèlement, des ateliers d'hygiène numérique ou encore une *Fresque de la cybersécurité* ont permis d'aborder les risques de manière pédagogique. Cette initiative s'inscrit dans une dynamique collective visant à faire de la cybersécurité un enjeu partagé à tous les échelons du territoire.

1er octobre

Le coup d'envoi du Cybermois et du CyberTour de France a été donné cette année en Bretagne depuis l'hôtel de Courcy en présence du Vice-Président de Rennes Métropole et du conseiller régional délégué au Numérique et à l'IA auprès de 150 élèves de primaire, collège et de lycée installés dans l'hémicycle et de 60 élèves de Vannes et Lannion en duplex. Rencontres, échanges, ateliers avec deux hackers éthiques, conférences organisées, par exemple par des professeurs de la Sorbonne, ont ponctué cette matinée de lancement.

ZOOM SUR LE
CYBERTOUR DE FRANCE

6 octobre

1re étape du CyberTour de France, Périgueux a réuni sur toute une journée 650 personnes au théâtre de l'Odyssée, autour de thématiques touchant collégiens, étudiants, particuliers, entreprises et collectivités, en présence du Président du Département, de représentants du Préfet, de la Région, du Maire et du Recteur de l'Académie. L'annonce de la création d'une licence Informatique en cybersécurité à Périgueux réalisée en collaboration avec le CNED[1] a conclu le programme de la journée.

[1] Centre national d'enseignement à distance

15 octobre

2e étape du CyberTour à Lille, organisée avec le Campus Cyber Hauts-de-France, Euratechnologies et la Ville de Lezennes au Kiabi Village. L'événement a été marqué par une conférence, différents ateliers (Sec-Cure, France services), l'inauguration de l'exposition inspirée du livret *Le numérique, pas de panique !*, l'annonce de l'instauration de Cyber Breakfasts pour les entreprises et de l'initiative CyberKids pour sensibiliser les plus jeunes.

17 octobre

La 3e étape du CyberTour, orchestrée par la Métropole Rouen Normandie et le Campus Normandie Cyber à Seine Innopolis, a rassemblé 130 personnes (élèves, particuliers et chefs d'entreprise) autour d'interventions de Cybermalveillance.gouv.fr, de la Gendarmerie nationale, de tables rondes avec des conseillers France services et de professionnels sur les métiers de la cyber.

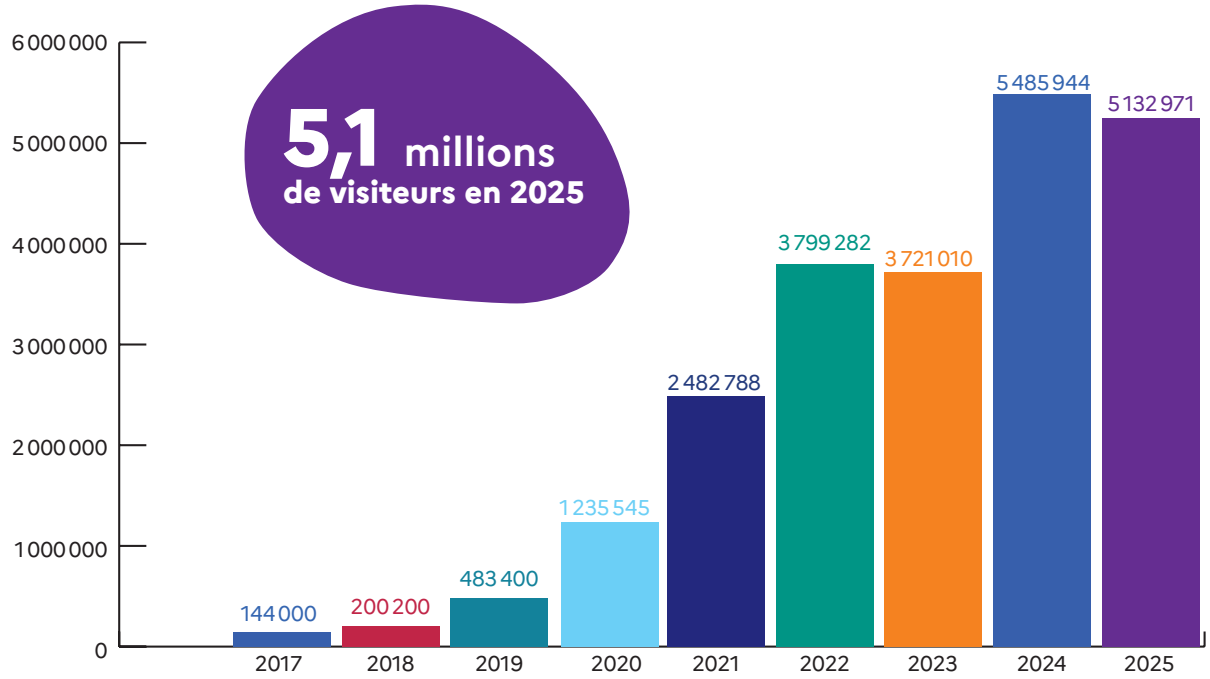
27 octobre

Clôture du CyberTour de France au Campus Cyber national de la Défense dans le cadre d'une matinée de sensibilisation à l'hygiène numérique via la *Fresque des Cybercitoyens* d'Advens for People and Planet et la *Fresque Cyber & vie privée* de Cyberludik, référencées au sein du catalogue Cyber4Tomorrow.

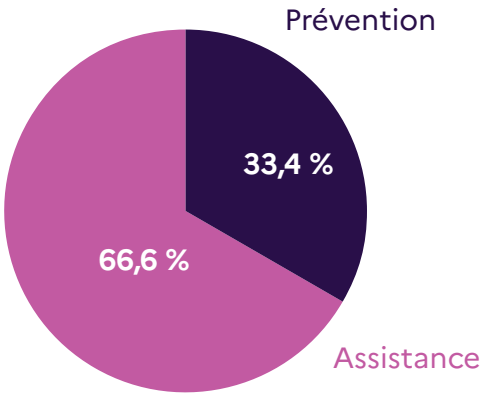
ÉTAT DE
LA MENACE

FRÉQUENTATION DE LA PLATEFORME CYBERMALVEILLANCE.GOUV.FR

Pour la deuxième année consécutive, la fréquentation de la plateforme Cybermalveillance.gouv.fr dépasse le seuil des 5 millions de visiteurs uniques et confirme sa place de site de référence pour l'assistance et la prévention face aux actes de cybermalveillance pour les particuliers, les entreprises TPE - PME et les collectivités territoriales. En huit années d'existence, elle comptabilise plus de 22,6 millions de visiteurs.



Fréquentation annuelle de la plateforme Cybermalveillance.gouv.fr



La forte audience observée a été soutenue par des besoins d'assistance et de conseils suite aux **multiples violations de données personnelles qui ont marqué l'année** (commerces en ligne ou physiques, fédérations et opérateurs sportifs, de l'emploi, services en santé, sociétés de logistique et de livraison, acteurs de l'assurance et mutuelles...).

L'exploitation malveillante de ces fuites de données a eu pour conséquences d'importantes **vagues d'hameçonnage par SMS, courriels ou appels audio afin de réaliser de nombreuses tentatives d'arnaques** (fausse livraison de colis, fausse commande, faux conseiller bancaire...) et de **piratages de compte en ligne** (dont découlent les fraudes au virement, usurpations d'identité, intrusions informatiques...) pour lesquelles les publics de Cybermalveillance.gouv.fr sont venus s'informer et chercher de l'assistance.

Les publics ont consulté, **pour les deux tiers, des contenus d'assistance** et pour le dernier tiers, des contenus de prévention et d'actualité.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en cybersécurité

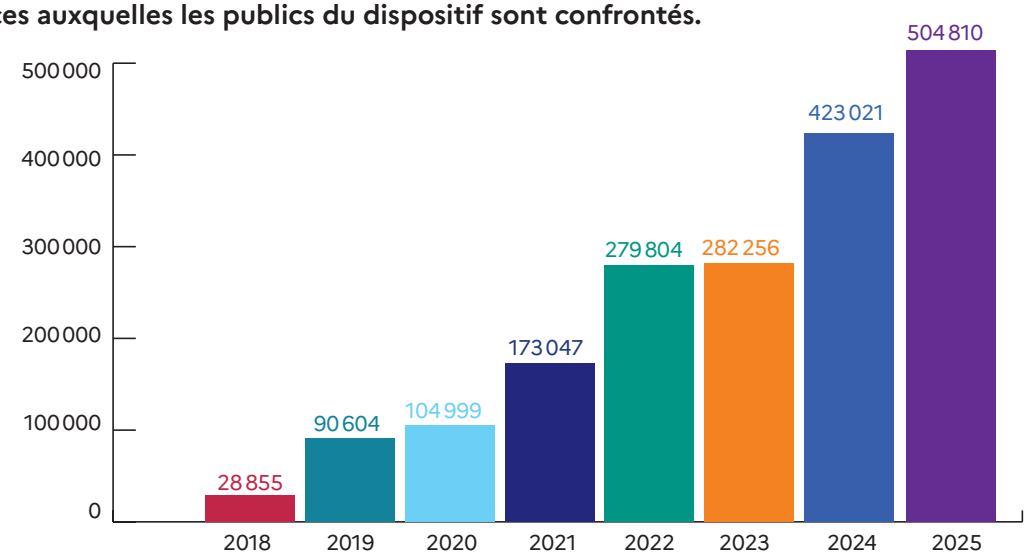
D'autres éléments organiques expliquent également cette audience :

- les communications relatives au lancement du **17Cyber.gouv.fr**, en collaboration avec le ministère de l'Intérieur ;
- la consultation des contenus de la **campagne nationale de sensibilisation à l'hameçonnage auprès de collégiens et lycéens** (**opération Cactus** en mars 2025), en collaboration avec le ministère de l'Éducation nationale et d'autres partenaires étatiques ;
- de nombreuses **prises de parole auprès de la presse régionale et nationale** sur les réflexes et bonnes pratiques préconisés par Cybermalveillance.gouv.fr ;
- **l'animation du Cybermois 2025**, le mois européen de la cybersécurité, dont Cybermalveillance.gouv.fr est pilote en France ;
- le **besoin des publics de s'informer sur des menaces numériques** actives, de disposer de conseils adaptés ou d'être orientés pour y faire face (dépôt de plainte, associations d'aides aux victimes…).

22,6 millions de visiteurs depuis 2017

LES CHIFFRES 2025 DE LA CYBERMALVEILLANCE

En 2025, la plateforme Cybermalveillance.gouv.fr a enregistré plus de 504 000 demandes d'assistance (+20%) associées à 51 types de menaces. Leur analyse offre une vision des différentes formes de menaces auxquelles les publics du dispositif sont confrontés.



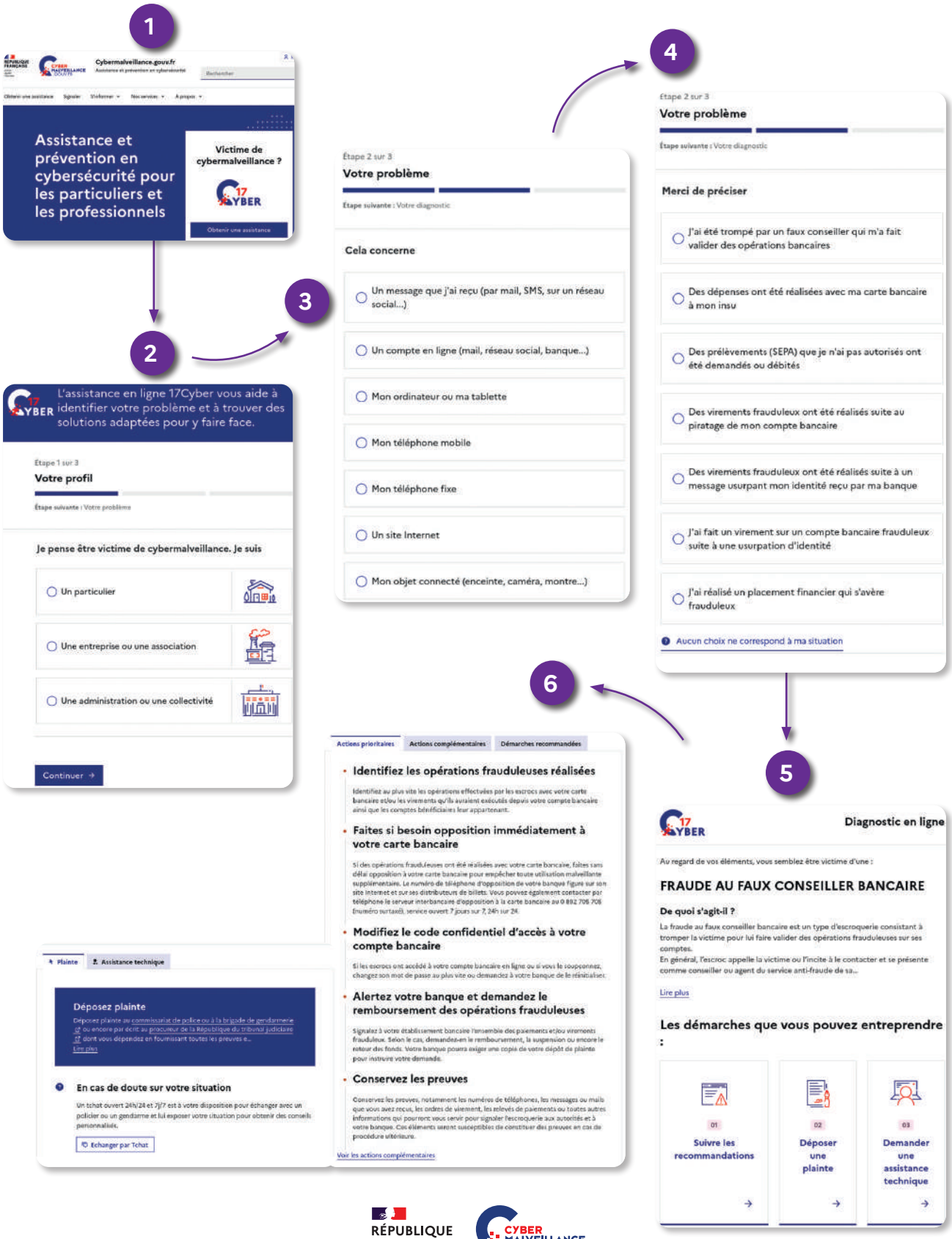
Évolution des recherches d'assistance

504 000 demandes d'assistance en ligne en 2025

Le lancement du 17Cyber (déc. 2024) a permis de **simplifier les parcours des usagers** en réduisant l'orientation vers des pages Internet externes, notamment en début d'assistance. Désormais, les recherches d'assistance sont comptabilisées uniquement à partir des parcours réalisés via *Obtenir une assistance* du site Cybermalveillance.gouv.fr et du 17Cyber.gouv.fr. Ce choix apporte une meilleure stabilité de l'indicateur et permettra d'observer plus finement l'évolution des menaces dans le temps.

Le parcours d'assistance 17Cyber est le fruit de plusieurs années d'expertise de Cybermalveillance.gouv.fr sur les menaces et les recommandations. Il permet aux usagers d'être guidés dans leur recherche d'assistance, de bénéficier de recommandations adaptées au contexte, et, si nécessaire, d'être mis en relation avec des policiers et gendarmes, d'être orientés vers des prestataires référencés ou labellisés ExpertCyber ou encore vers des associations spécialisées dans l'aide aux victimes.

Le taux de satisfaction des publics pour ce service d'assistance en ligne est de 84,2 % d'avis positifs exprimés.



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

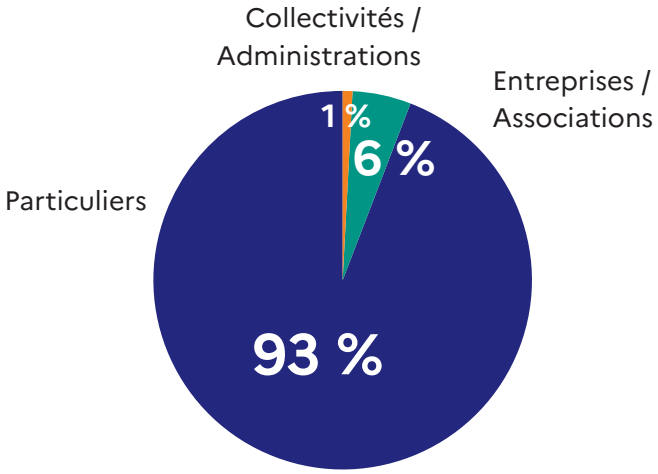
RÉPARTITION DES DEMANDES D'ASSISTANCE

La répartition est quasiment stable avec **93 % de particuliers, 6 % d'entreprises/associations et 1 % de collectivités/administrations.**

La progression de la volumétrie des demandes d'assistance est **plus marquée en 2025 pour les publics professionnels**, notamment pour les entreprises et associations :

- **+47% pour les particuliers**
- **+63% pour les professionnels dont :**
  - **› +73% pour les entreprises et associations,**
  - **› +22% pour les collectivités et administrations.**

En 2025, 33 012 professionnels (27 934 entreprises ou associations et 5 078 collectivités et administrations) et **471 798 particuliers** ont bénéficié d'une assistance 17Cyber.



Répartition des demandes d'assistance par catégorie de publics

+47 % de demandes d'assistance de particuliers

+73 % de demandes d'assistance des entreprises et associations

+22 % de demandes d'assistance des collectivités et administrations

Cette répartition, rapportée à des volumes comparables de catégorie de publics, permet d'énoncer qu'en 2025 :

- **Pour 1 000 particuliers, 7 ont eu recours à l'assistance 17Cyber,**
- **Pour 1 000 entreprises ou associations, 3 ont eu recours à l'assistance 17Cyber,**
- **Pour 1 000 collectivités territoriales, 141 ont eu recours à l'assistance 17Cyber.**

PRINCIPALES MENACES PAR CATÉGORIE DE PUBLICS EN 2025

Sur les 51 formes de cybermalveillance traitées par l'outil d'assistance en ligne en 2025, l'analyse quantitative des principales recherches par catégorie de publics est un indicateur fort des grandes tendances de la cybermalveillance et de leurs évolutions au niveau national.

La tendance observée se poursuit vers **une plus grande dilution et variété de menaces et de modes opératoires**. Sur ces trois dernières années, le volume des dix principales cybermenaces traitées dans l'assistance représentait :

- 92 % des assistances sur les 10 principales menaces en 2023,
- 87 % des assistances sur les 10 principales menaces en 2024,
- **81 % des assistances sur les 10 principales menaces en 2025.**

Le phénomène déjà identifié en 2024 se confirme en 2025 : **la menace cybercriminelle est plus diverse et diffuse. On remarque un regain d'intérêt des cybercriminels pour des modes opératoires qui étaient délaissés, en les réactualisant et en développant de nouvelles variantes.**

Les cybercriminels disposent désormais de nombreuses données personnelles, issues des fuites de données et de précédentes campagnes d'hameçonnage, ce qui facilite **la diffusion des menaces avec une plus grande efficacité.**

La professionnalisation et la spécialisation des cybercriminels se confirment. **Les plateformes de vente de données « fuitées », la location ou la vente de kits prêts à l'emploi pour réaliser des campagnes malveillantes, l'existence de centres d'appels de faux téléconseillers** (parfois contre leur gré), **permettent de cibler plus de victimes et de maximiser les rendements.**

Pour certaines malveillances, **la frontière entre le cyberespace et l'espace physique tend à se réduire. Certains cybercriminels recrutent des équipes sous-traitantes sur le terrain qui prennent part au délit en opérant sur une zone géographique donnée** : récupération de cartes bancaires à domicile par un faux livreur-porteur (tel que documenté dans l'arnaque au faux conseiller bancaire), menaces physiques voire séquestration de détenteurs de cryptomonnaies, cambriolages chez des licenciés de tir sportif…

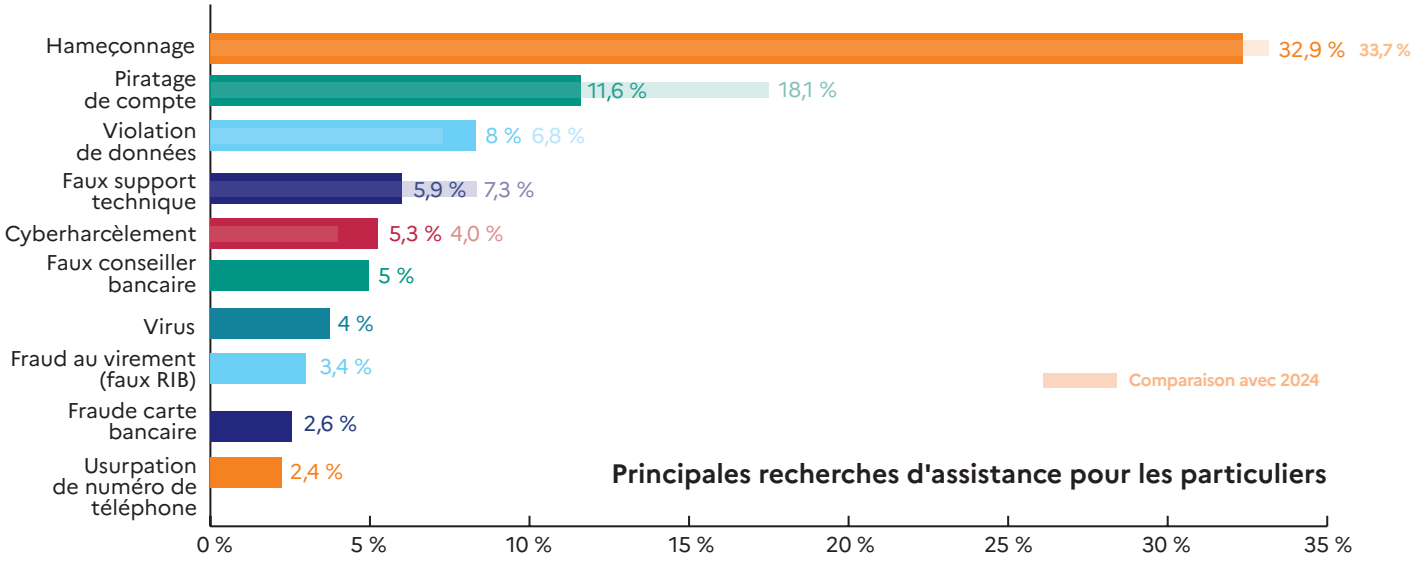
ET L'IA DANS TOUT ÇA ?

Les cybercriminels ont également pris en compte l'IA, en particulier pour optimiser la diffusion des cybermenaces (traductions automatisées d'hameçonnage en plusieurs dizaines de langues, textes et visuels générés par IA) et gagner en agilité (génération assistée de faux sites, développements assistés de kits malveillants…). Néanmoins, si les cybermalveillants ont intégré cette facilité, les campagnes malveillantes de masse entièrement pilotées par IA ne sont pas attestées à ce stade.

Après de nombreuses fuites de données qui ont souvent concerné des entités disposant de grandes masses de données (secteur commercial, opérateurs de sports et de loisirs, organismes de l'emploi et de la santé…), **la perspective pour 2026** laisse présager de nouveau, **des volumes importants d'hameçonnage, de piratages de compte**, d'**usurpations d'identité** ou d'autres tentatives d'arnaques, probablement mieux personnalisées, plus réalistes et plus ciblées.

Une probabilité qui incite à poursuivre et renforcer la sensibilisation des publics aux menaces (hameçonnage et ses conséquences en particulier), à accentuer l'intérêt pour la protection des comptes d'accès numériques (usage de l'authentification à double facteur) et, d'une manière plus générale, à continuer de communiquer sur les bonnes pratiques d'hygiène numérique et de sécurisation informatique pour le grand public et les professionnels.

• L'assistance aux particuliers en 2025



Principales recherches d'assistance pour les particuliers

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

Avec près de 33 % des demandes d'assistance, l'**hameçonnage** sous ses différentes formes reste de loin la première menace qui touche les particuliers. Les recherches d'assistance associées sont en hausse de 71 % par rapport à 2024.

Avec plus de 11 % des assistances, le **piratage de compte** se maintient en deuxième position des cybermalveillances les plus vécues pour les particuliers, bien qu'en légère baisse en volume (-2 %).

L'année 2025 a vu **la tendance des fuites de données se perpétuer** avec un grand nombre de **violations de données**, encore plus médiatisées, ce qui explique la **multiplication par 2** des **demandes d'assistance** (+107%). Les recherches d'assistance suite aux violations de données se positionnent au 3e rang des menaces pour les particuliers (6,6 % des assistances).

Au-delà de ces cybermalveillances majeures, les volumes d'assistance et leurs variations pour les particuliers se répartissent comme suit :

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

L'**arnaque au faux support technique** descend à la quatrième place (5,9 % des assistances). Suite à des actions judiciaires en 2024, les acteurs de la menace ont semblé marquer une pause de quelques mois, avant **de relancer le procédé au début 2025. Les demandes d'assistance sont à nouveau en augmentation sur 2025** (+39 % d'assistances par rapport à 2024).

Les recherches d'assistance pour **cyberharcèlement**, généralement lié à des dénigrements, à des menaces via les réseaux sociaux ou à des appels audio masqués, **progressent** (**+134 %**) et s'établissent désormais à 18000 recherches d'assistance par an.

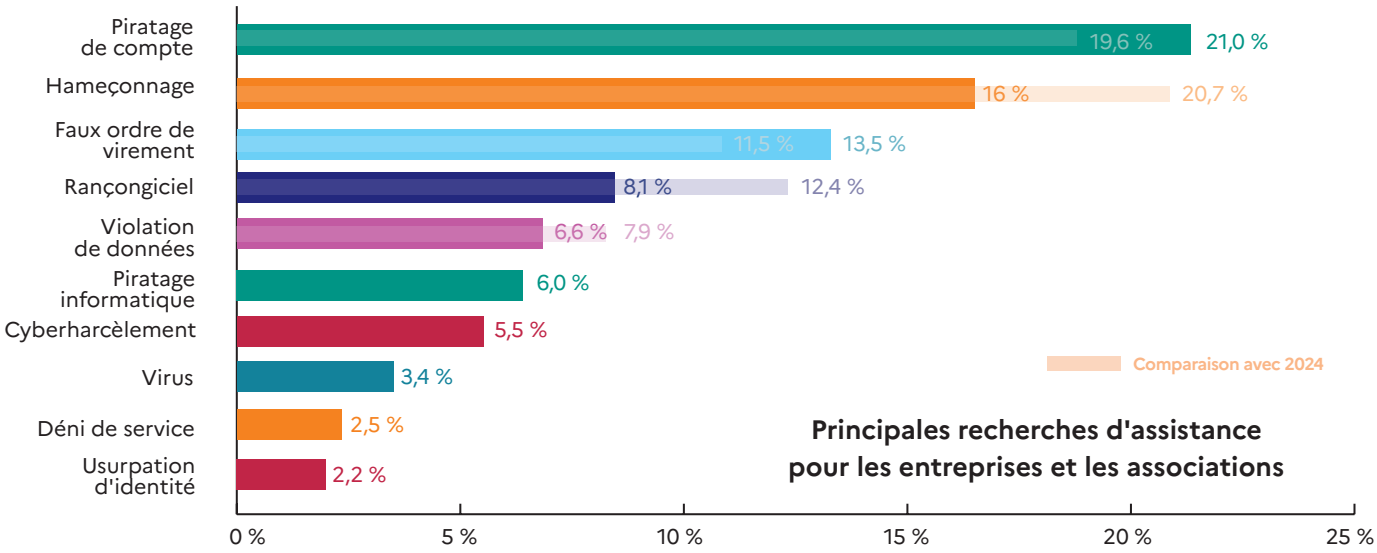
L'arnaque au **faux conseiller bancaire connaît une progression importante** (+159 %) et représente 15000 recherches d'assistance sur l'année (voir en page « Focus »).

Bien qu'en légère hausse en termes de volume (+8 %), l'assistance pour **virus informatique** passe de la 5e à la 7e place.

Par ailleurs, les **fraudes au virement** (faux ordre virement ou détournement de RIB) continuent leur forte progression (+196 %) et représentent 13000 assistances par an (voir Focus page 53). Elles sont suivies par les **fraudes à la carte bancaire,** toujours en 9e position malgré un volume d'assistance en hausse de +96 %.

Enfin, certaines cybermalveillances plus marginales (moins de 10000 par an) accusent des progressions notables. Parmi celles-ci, l'**usurpation de numéro de téléphone enregistre un bond de +517 %**, à suivre de près en regard des nouvelles modalités de protection des numéros de téléphone entrées en vigueur au 1er janvier 2026 (voir Focus page 57).

• L'assistance aux entreprises et associations en 2025



Conséquence des violations de données et des campagnes d'hameçonnage réussies, les **piratages de compte** représentent aujourd'hui la 1re menace pour les entreprises et associations avec **21 % des parcours d'assistance** réalisés, **en croissance de 52%.**

L'**hameçonnage reste à un niveau particulièrement significatif** et représente en 2025 le second motif des parcours d'assistance pour les entreprises et associations avec **16 % des diagnostics**, **en augmentation de 29 %**.

La fraude au virement fait son entrée dans les trois principales menaces pour les entreprises et associations. Elle représente **13,5 % des assistances** avec un nombre de diagnostics en progression de **93 % par rapport à 2024**.

FRAUDE AU VIREMENT

Cette catégorie regroupe une grande diversité de procédés qui évoluent dans le temps et ciblent des processus financiers des entreprises et associations : usurpation d'identité de créancier, arnaque au président, piratage de compte de messagerie pour envoi de demande de changement de RIB ou pour envoi de facture avec un RIB usurpé…

Voir rubrique « Grandes tendances »

Au-delà de ces principales cybermalveillances, les recherches d'assistance et leurs variations pour les entreprises et associations ont été recensées comme suit :

ENTREPRISES ET ASSOCIATIONS		
Plus de 2000 assistances	**Entre 1000 et 2000 assistances**	**Moins de 1000 assistances**
• Piratage de compte (+52%) • Hameçonnage (+29%) • Fraude au virement (+93%)	• Rançongiciel (+8%) • Violation de données (+40%)	• Piratage informatique (+112%) • Cyberharcèlement (+205%) • Virus (+59%) • Déni de service (+17%) • Usurpation d'identité (+213%)

Les **rançongiciels** prennent la quatrième place en 2025 avec **8,1 % des demandes d'assistance** mais avec un volume en légère augmentation, ce qui peut indiquer une amorce de reprise du phénomène, en hausse de **9 % de l'ensemble des parcours d'assistance**. Cette menace reste la **plus redoutable et la plus impactante pour une organisation.**

Les recherches d'assistance d'entreprises et associations pour des **violations de données** représentent **6,6 % des assistances, en augmentation de +40 %**.

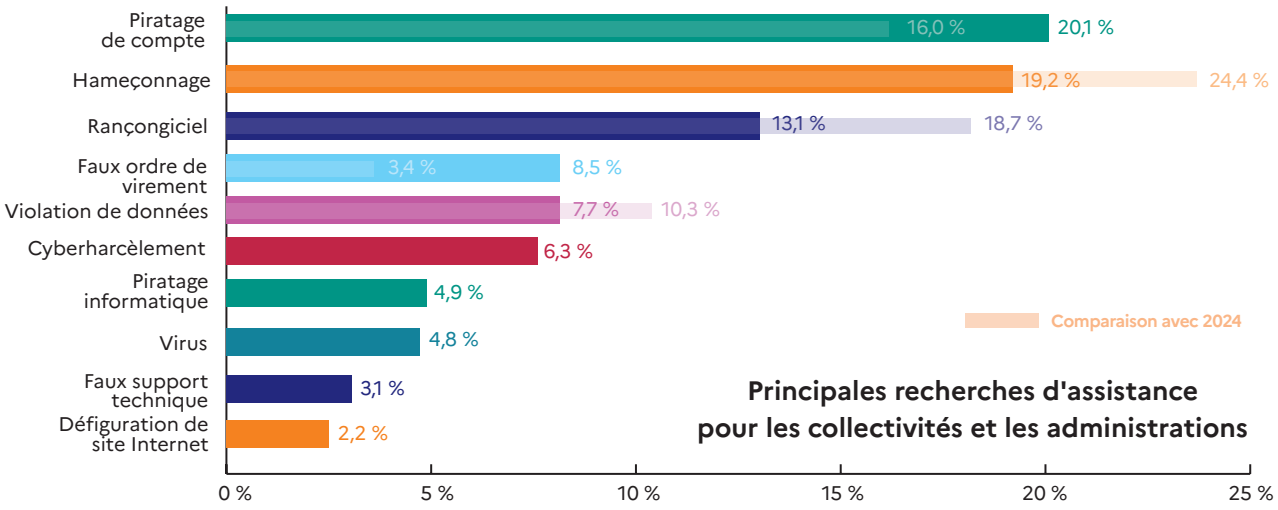
Certaines cybermalveillances plus marginales (moins de 1000 par an) ont aussi connu des progressions notables.

Ainsi, les **piratages informatiques** (6 % des demandes d'assistance) **sont en hausse de 112 %**. Cette évolution est liée aux hameçonnages réussis et aux violations de données : les comptes fuités ou hameçonnés constituent un accès initial dans les systèmes d'information.

Les **cyberharcèlements** visant les entreprises, associations – particulièrement leurs dirigeants, employés ou les pages de sociétés sur les réseaux sociaux -, concernent **5,5 % des assistances** et poursuivent **leur progression (+205%)**.

Enfin, si le volume reste stable, les assistances pour les **virus informatiques** (3,4 % des assistances), les **dénis de service** (2,5 % des assistances) et les **usurpations d'identité** (2,2 % des assistances) de dirigeants, d'employés, de sociétés ou d'associations sont également en hausse.

• L'assistance aux collectivités territoriales et aux administrations en 2025



Le **piratage de compte** est désormais le principal objet de recherches d'assistance avec **20,1 % des parcours d'assistance** et un **volume en hausse de 14 %**.
Dans une proportion très proche, l'**hameçonnage** (soit 19,2 % des demandes), s'il augmente en nombre de demandes (+14%), **prend néanmoins la deuxième position.**
Le rançongiciel perd également une place (13,1 % des assistances) tout en conservant une volumétrie équivalente (+1 %).
Au-delà de ces cybermalveillances, les recherches d'assistance et augmentations les plus remarquables pour les collectivités et administrations sont les suivantes :

COLLECTIVITÉS TERRITORIALES ET ADMINISTRATIONS		
Plus de 300 assistances	**Entre 100 et 300 assistances**	**Moins de 100 assistances**
• Piratage de compte (+14%) • Hameçonnage (+14%) • Rançongiciel (+1%)	• Fraude au virement (+262%) • Violation de données (+9%) • Cyberharcèlement (+209%)	• Piratage informatique (+146%) • Virus (+12%) • Faux support informatique (-16 %) • Défiguration de site (-20 %)

La **fraude au virement** enregistre une progression significative avec la 4e place (soit 8,5 % des besoins d'assistance) et un **volume en très forte hausse de +262%.**

Les **violations de données** redescendent au 5e rang (7,7 % des demandes d'assistance, volume à +9 %).

Les recherches d'assistance pour **cyberharcèlement** intègrent les principales menaces en 6e place (6,3 % des assistances) avec une **progression importante (+209%)**, qui représente néanmoins moins de 300 recherches d'assistance.

S'il ne reflète que 4,9 % des parcours d'assistance (moins de 100 demandes), le **piratage informatique** affiche toutefois une **hausse de 146 %**. Il est souvent lié à des hameçonnages réussis ou des violations de données, les comptes fuités constituant un vecteur d'accès initial dans les systèmes d'information.

Les **virus** (4,8 % des assistances) **restent présents** avec une progression moins marquée (+12 %).

Enfin, les **arnaques au faux support informatique** (-16 %) ainsi que les **défigurations de site (-20 %)** s'inscrivent **en baisse**.

LES GRANDES TENDANCES **DE LA MENACE**

LES DONNÉES PERSONNELLES : UN INTÉRÊT CROISSANT ET UN BESOIN PERMANENT POUR LES CYBERCRIMINELS

Depuis plusieurs années, Cybermalveillance.gouv.fr observe qu'un nombre toujours plus important de modes opératoires vise à récupérer, directement ou indirectement, des données personnelles par :

- **hameçonnages** via de nombreux procédés tels que courriels, SMS, messages de réseaux sociaux, faux liens publicitaires, fausses offres de location ou d'emploi… ;
- **piratages de compte** faisant suite à des hameçonnages réussis, ou indirectement en testant sur d'autres services numériques les comptes fuités (disposant souvent de mots de passe identiques), infection par virus collectant les mots de passe (« *infostealer* »)… ;
- **violations massives de données personnelles**, obtenues en exploitant des comptes compromis pour obtenir l'accès à des fonctionnalités privilégiées ou d'exports insuffisamment protégés, défauts de sécurisation…

Tous les types de données personnelles, qu'elles soient sensibles ou non, **suscitent l'intérêt des cybercriminels** : identité (nom, prénom, date de naissance, n° de sécurité sociale, copies de documents d'identité…), informations de contact (adresse courriel et postale, n° de téléphone…), données bancaires (IBAN/BIC, n° de carte de bancaire…), données de connexion (identifiant, mot de passe), justificatifs de revenus et de domicile, informations médicales ou encore numéro de plaque d'immatriculation, adresse IP, etc.

En outre, **une donnée personnelle récente aura davantage de valeur qu'une donnée ancienne**, devenue invalide ou qui nécessitera des vérifications supplémentaires pour en confirmer la validité. **Cet intérêt croissant des cybercriminels pour les données personnelles s'explique par le besoin permanent de se constituer des identités ou des profils**, aisément mobilisables, **dans le but** :

- **de commettre d'autres cybermalveillances en usurpant l'identité de victimes** (fraude financière ou bancaire, escroquerie auprès des proches, création de comptes sur les réseaux sociaux, etc.) ;
- **de disposer d'un « vivier » de victimes potentielles** dont l'approche (hameçonnage, fraude au faux conseiller…) pourra être facilitée grâce aux informations personnelles récoltées ;
- **d'ouvrir des comptes bancaires afin de permettre le transit et le blanchiment des fonds générés par les activités criminelles** (cyber ou traditionnelles), ceci nécessitant une identité "plausible" pour procéder à l'ouverture de comptes auprès d'établissements moins vigilants ;
- **de revendre les informations dérobées à d'autres cybercriminels qui les utiliseront à leur tour.**

Dans un contexte d'accélération des violations de données personnelles qui entraînent l'exposition, parfois massive, d'informations de millions de personnes, une **offre pléthorique de données récentes est désormais disponible**.

Ces données sont commercialisées sur l'Internet sombre (*darknet*), sur des forums clandestins spécialisés et sur des chaînes de messageries chiffrées dédiées à la revente de données personnelles. Les prix varient essentiellement en fonction de la sensibilité des données proposées, du volume disponible et de la "fraîcheur" des informations. Des bases de données entières contenant des milliers voire des millions, d'enregistrements peuvent aussi être mises en libre accès ou à des prix parfois dérisoires.

Après achat, les informations contenues dans ces bases de données sont ensuite triées et enrichies (croisement avec d'autres données issues d'autres fuites) par les cybercriminels **dans le but de créer des identités ou d'affiner les futures cibles d'escroqueries et autres cybermalveillances.** Certains acteurs, spécialisés dans la revente de ces données structurées, vont jusqu'à proposer **des identités "clés en main" qui pourront être directement utilisées par des criminels dans le cyberespace ou l'espace réel.**

Avec les années, ce marché souterrain de la donnée personnelle et de l'identité en ligne a gagné en sophistication, structuration et professionnalisme. Il tend à devenir un marché mature où les données personnelles se vendent comme des produits de consommation, en suivant la logique de l'offre et de la demande.

L'HAMEÇONNAGE (« *PHISHING* ») : UNE MENACE OMNIPRÉSENTE, MASSIVE ET DIVERSIFIÉE

À l'image de la profusion de messages malveillants que chacun d'entre nous a pu recevoir tout au long de l'année, l'hameçonnage figure au premier rang des menaces avec 1/3 des assistances tous publics confondus. Le *phishing*, par courriel et SMS, envoyé par vagues à un très grand nombre de destinataires s'est une nouvelle fois concentré autour de thématiques présentes depuis des années et peu de nouveautés ont été constatées. Ces hameçonnages poursuivent divers objectifs :

108 000 demandes d'assistance **+70%**

1. La collecte d'informations personnelles (nom, prénom, adresse postale et courriel, numéro de téléphone) **et de coordonnées de carte bancaire** (numéro, date d'expiration et code de vérification) **sur un site frauduleux.**

Menace n°1 pour les particuliers avec **32,9 %** des demandes d'assistance

Pour cette catégorie d'hameçonnage, les données collectées ne sont généralement pas exploitables directement du fait de l'obligation d'une authentification forte pour les paiements en ligne. À noter que, sauf exception, la transaction de paiement n'est pas réellement effectuée dans ce type d'hameçonnage. Les informations dérobées seront ensuite exploitées pour d'autres escroqueries : pour la grande majorité associées à ce type de phishing de masse, il s'agit de fraudes au faux conseiller bancaire (voir la page dédiée).

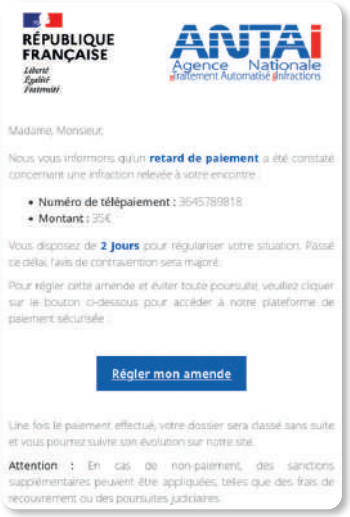
Menace n°2 pour les professionnels avec **16,4 %** des demandes d'assistance

Parmi les types d'hameçonnage, voici ci-dessous les plus couramment observés en 2025.

- **L'hameçonnage à la livraison de colis :** l'accroche est systématiquement un supposé problème de livraison et la victime est invitée à choisir un réacheminement qui nécessiterait le paiement d'une somme de l'ordre de 1 à 2 euros. La marque la plus usurpée est, comme en 2024, Mondial Relay.

Une variante largement diffusée a été observée à l'été 2025 : des SMS avec le simple message "Bonjour, vous êtes chez vous ?". Il s'agissait de faire réagir le destinataire pour contourner une sécurité anti-hameçonnage. En effet, pour lutter contre l'hameçonnage par SMS (« smishing »), certaines applications de messages désactivent les liens qui proviennent de numéros inconnus. Mais si on répond, la conversation est considérée comme légitime et les messages suivants pourront alors contenir des liens actifs. C'est en fait un système automatisé qui interagit avec les victimes en envoyant des réponses pré-rédigées.

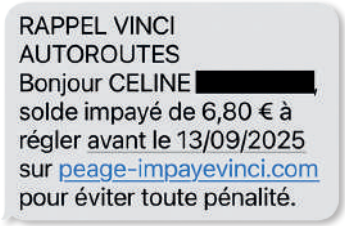
- **L'hameçonnage à la contravention routière** aux couleurs d'ANTAI et d'Amendes.gouv.fr. La victime est informée du prétendu non-paiement d'une amende à régulariser sans tarder sous peine de majoration.



Variante observée : Quelques sites d'hameçonnage disposaient d'un véritable module de paiement, contrairement à tous les autres. Dans ces campagnes, les escrocs dérobaient alors 135 € par victime et les informations de carte bancaire étaient également récupérées pour une exploitation ultérieure.

- **La fausse confirmation de commande** a été bien plus présente en 2025 que les années précédentes, particulièrement au travers de campagnes de courriels frauduleux aux couleurs d'Amazon envoyés en très grand nombre. **Ces messages étaient personnalisés avec des informations personnelles et bancaires (IBAN/BIC) des destinataires. Il est probable que ces informations provenaient de diverses violations de données incluant des IBAN en 2024 et 2025.**

- **Nouveauté en 2025** des **messages demandant de régler un supposé impayé de trajet autoroutier** usurpant l'identité des gestionnaires Vinci Autoroutes (ULYS) et SANEF. Les escrocs ont ainsi exploité le récent déploiement des péages autoroutiers dits en "flux libre" pour lequel l'automobiliste doit effectuer un paiement dématérialisé de son trajet. À noter que ce type d'hameçonnage apparu début 2025 est beaucoup moins observé depuis fin décembre 2025.


RAPPEL VINCI AUTOROUTES
Bonjour CELINE [redacted],
solde impayé de 6,80 € à régler avant le 13/09/2025 sur peage-impayevinci.com pour éviter toute pénalité.

- **Les traditionnels hameçonnages aux couleurs des impôts et de l'Assurance Maladie ont été moins présents en 2025** mais de larges campagnes pour de prétendus renouvellements de cartes Vitale ont été observées à la toute fin 2025.

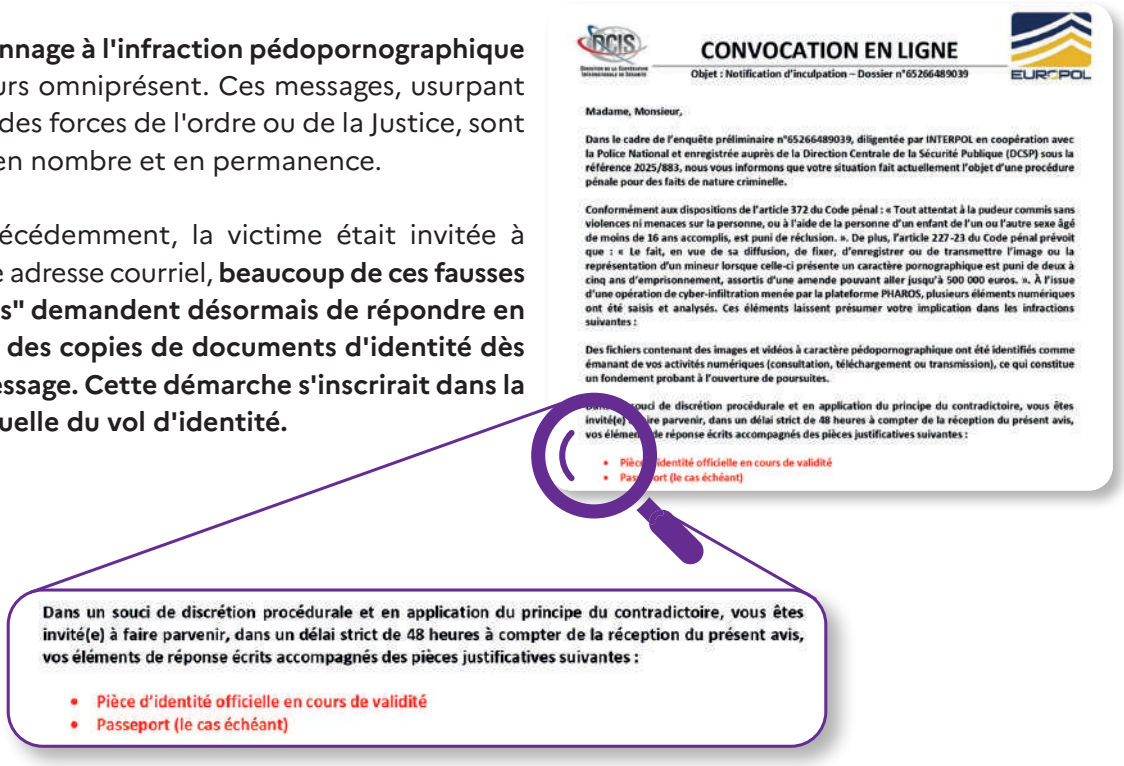
- **Plusieurs autres campagnes de masse aux couleurs de différentes administrations ou entreprises ont régulièrement été vues en 2025.** À titre d'exemples: SNCF (carte Avantage en promotion), EDF (remboursement de trop-perçu), Amazon (annulation de commande) etc.

2. Les messages d'escroquerie incitant à contacter les cybercriminels

Ces modes **opératoires** n'orientent pas vers un site d'hameçonnage mais incitent les destinataires à répondre au message reçu ou à contacter un numéro de téléphone donné, comme le décrivent les exemples ci-dessous.

- **L'hameçonnage à l'infraction pédopornographique** est toujours omniprésent. Ces messages, usurpant l'identité des forces de l'ordre ou de la Justice, sont adressés en nombre et en permanence.

Alors que précédemment, la victime était invitée à contacter une adresse courriel, **beaucoup de ces fausses "convocations" demandent désormais de répondre en transmettant des copies de documents d'identité dès le premier message. Cette démarche s'inscrirait dans la tendance actuelle du vol d'identité.**


CONVOCATION EN LIGNE
Objet : Notification d'inculpation – Dossier n°65266489039
EUROPOL

Madame, Monsieur,

Dans le cadre de l'enquête préliminaire n°65266489039, diligentée par INTERPOL en coopération avec la Police National et enregistrée auprès de la Direction Centrale de la Sécurité Publique (DCSP) sous la référence 2025/883, nous vous informons que votre situation fait actuellement l'objet d'une procédure pénale pour des faits de nature criminelle.

Conformément aux dispositions de l'article 372 du Code pénal : « Tout attentat à la pudeur commis sans violences ni menaces sur la personne, ou à l'aide de la personne d'un enfant de l'un ou l'autre sexe âgé de moins de 16 ans accomplis, est puni de réclusion. ». De plus, l'article 227-23 du Code pénal prévoit que : « Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque celle-ci présente un caractère pornographique est puni de deux à cinq ans d'emprisonnement, assortis d'une amende pouvant aller jusqu'à 500 000 euros. ». À l'issue d'une opération de cyber-infiltration menée par la plateforme PHAROS, plusieurs éléments numériques ont été saisis et analysés. Ces éléments laissent présumer votre implication dans les infractions suivantes :

Des fichiers contenant des images et vidéos à caractère pédopornographique ont été identifiés comme émanant de vos activités numériques (consultation, téléchargement ou transmission), ce qui constitue un fondement probant à l'ouverture de poursuites.

Dans un souci de discrétion procédurale et en application du principe du contradictoire, vous êtes invité(e) à faire parvenir, dans un délai strict de 48 heures à compter de la réception du présent avis, vos éléments de réponse écrits accompagnés des pièces justificatives suivantes :

- Pièce d'identité officielle en cours de validité
- Passeport (le cas échéant)

Dans un souci de discrétion procédurale et en application du principe du contradictoire, vous êtes invité(e) à faire parvenir, dans un délai strict de 48 heures à compter de la réception du présent avis, vos éléments de réponse écrits accompagnés des pièces justificatives suivantes :

- Pièce d'identité officielle en cours de validité
- Passeport (le cas échéant)

Par ailleurs, en 2025, quelques campagnes ont été réalisées par envoi de messages privés sur WhatsApp alors qu'elles se faisaient exclusivement par courriel jusqu'alors.

- Les **SMS d'hameçonnage à l'enfant qui a un problème avec son téléphone** (dits « coucou papa/maman… ») s'installent dans la durée. Cette année encore, certains montants de préjudice se sont élevés à plusieurs milliers d'euros pour les victimes qui pensaient échanger avec un proche en difficulté.

- L'**hameçonnage au faux numéro d'opposition bancaire** s'est fortement répandu en 2025 en vue d'escroqueries de type fraude au faux conseiller bancaire (voir en page 54).

- Depuis des années, le **chantage à l'ordinateur et à la webcam prétendus piratés** fait très régulièrement l'objet de vagues de courriels d'hameçonnage dans lesquels un "*hacker*" dit avoir pris le contrôle de l'appareil de la victime. Une rançon en cryptomonnaie est demandée pour éviter la diffusion de contenus compromettants. Certains envois utilisent une technique (dite de "*spoofing*") pour tenter de faire croire aux victimes que le message a été envoyé depuis leur propre boîte courriel, d'autres contiennent un mot de passe de la victime issu d'une autre fuite de données pour renforcer la crédibilité de la menace.

3. La collecte d'identifiants et de mots de passe

L'hameçonnage ayant pour objectif le piratage de compte en ligne est toujours très présent. Les messageries électroniques (courriel) et les comptes bancaires sont parmi les plus visés mais un grand nombre de types de comptes peut également faire l'objet de phishing de masse : services publics (CAF, Assurance Maladie, Chorus Pro…), opérateurs de télécommunications (Orange, SFR, Free…), transports publics (RATP / Île-de-France Mobilités), commerces en ligne (Amazon…) etc.

Focus sur les comptes de messageries électroniques et bancaires :

- Les **messageries électroniques personnelles et professionnelles sont toujours très ciblées** pour la richesse des informations et documents qu'elles peuvent contenir, pour accéder aux autres comptes en ligne de la victime, tenter des usurpations d'identité auprès de ses contacts ou encore réaliser des campagnes d'hameçonnage par l'envoi de messages en nombre.
  L'une des méthodes les plus utilisées concerne des courriels qui informent d'un soi-disant document à télécharger (courrier recommandé en ligne (AR24), acte de notaires, facture, devis ou autre document contractuel…). Le site Internet vers lequel la victime est dirigée demande de saisir ses identifiants de compte de messagerie pour supposément accéder au document de manière sécurisée. Plus spécifiquement pour les professionnels, les messages indiquent fréquemment une procédure de changement de mot de passe obligatoire, un renforcement de la sécurité de la messagerie, etc., et concernent par exemple Microsoft Outlook/Office365 ou Zimbra.

- **Comptes bancaires, services de paiement ou autres services financiers.** Certains sites d'hameçonnage de données bancaires sont dotés de **fonctionnalités permettant d'intercepter la double authentification**, ce qui permet de créer simultanément une session active sur un appareil du cybercriminel. En plus des identifiants de connexion, **quelques sites demandent également à la victime de renseigner son numéro de téléphone et le code RIO** (relevé d'identité opérateur) **qui lui est associé**. À l'aide de cet identifiant, les cybercriminels tenteront de s'approprier la ligne téléphonique de la victime pour accéder à son compte bancaire et commettre d'autres cybermalveillances.

UNE PERSONNALISATION DES MESSAGES D'HAMEÇONNAGE DE PLUS EN PLUS OBSERVÉE

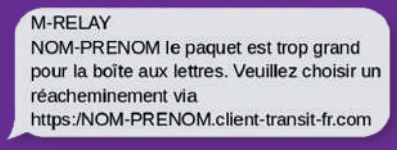
Même si la pratique existe depuis des années, un nombre croissant de SMS et courriels d'hameçonnage sont personnalisés avec les informations du destinataire. Cette méthode a pour but de lui faire croire que le message lui est spécialement destiné et envoyé par une organisation susceptible de détenir ses données. De plus, ce mode opératoire détourne son attention de ce qui est réellement important : les coordonnées de l'expéditeur (adresse courriel ou numéro de téléphone), l'URL du site vers lequel il est dirigé, voire la cohérence du message lui-même.

La profusion des informations disponibles suite aux nombreuses violations de données qui se sont déroulées ces deux dernières années permet aux opérateurs d'hameçonnage de disposer d'un volume conséquent de données riches et "fraîches". Ils peuvent ainsi acquérir des listes d'informations personnelles sélectionnées et structurées, à l'image de fichiers marketing de l'économie légale.

Outre un envoi personnalisé avec a minima des noms et prénoms, on observe un nombre croissant de messages avec des informations précises et contextualisées. Quelques exemples identifiés en 2025 :

- IBAN/BIC affiché dans des messages de fausses confirmations d'abonnement par prélèvement ou d'hameçonnage au faux numéro d'opposition bancaire ;
- Numéro de plaque d'immatriculation et modèle de véhicule dans certains hameçonnages au paiement de trajet autoroutier ;
- Numéro de client dans de faux messages de sécurité ou usage des noms et prénoms en les utilisant dans le lien malveillant afin d'abuser la victime.

Les sites de phishing vers lesquels sont orientées les victimes restent, quant à eux, génériques et ne sont que très rarement personnalisés avec les informations propres à la victime, créant une rupture de cohérence avec le message.



LE PIRATAGE DE COMPTE EN LIGNE

41 000
demandes d'assistance réalisées en 2025
+17%

Le piratage de compte en ligne continue de progresser en 2025 et devient la menace n° 1 pour les publics professionnels. Il concerne toujours tous types de comptes mais les messageries électroniques (courriel) et les comptes de réseaux sociaux restent particulièrement ciblés par les cybercriminels.

S'agissant des modes opératoires, l'année 2025 ne montre pas d'évolution notable quant aux vecteurs de compromission des comptes : hameçonnage, mot de passe trop simple, réutilisation d'un même mot de passe sur plusieurs sites dont l'un a été piraté, piratage d'un appareil ou encore infection par un logiciel malveillant (par exemple virus collectant les mots de passe, via le téléchargement de logiciels piégés).

L'ingénierie sociale est fréquemment observée dans le piratage de compte. Exemples de modes opératoires :

- Sur les plateformes de vente entre particuliers (Leboncoin, Vinted, Facebook MarketPlace), de faux vendeurs ou acheteurs cherchent à pirater les comptes de leurs interlocuteurs en les orientant vers des sites d'hameçonnage pour le paiement ou la confirmation du paiement, souvent avec l'appel d'un complice qui se fait passer pour un conseiller de la plateforme ou d'un service de paiement. Les escrocs ciblent ainsi les comptes des victimes sur les plateformes de vente mais également leurs comptes bancaires.
- Pour un professionnel, il peut s'agir de l'appel d'un faux conseiller Google My Business pour pirater son compte, s'approprier sa fiche d'établissement et, le cas échéant, son compte publicitaire. L'envoi de liens vers des sites d'hameçonnage et/ou la demande d'un code d'authentification sont utilisés dans ce type d'approche.

Les comptes de messagerie électronique demeurent des cibles privilégiées pour les cybercriminels en raison des nombreuses informations personnelles, administratives et parfois professionnelles qu'ils contiennent, ainsi que des échanges avec les différents contacts de la victime. La compromission d'une messagerie peut constituer un point d'entrée vers d'autres formes de cybermalveillance, notamment la prise de contrôle d'autres comptes par réinitialisation de mots de passe, d'usurpations d'identité à des fins d'escroquerie ou encore de fraudes financières (fraude au virement notamment).

Les comptes de réseaux sociaux restent fortement ciblés et sont régulièrement exploités dans le cadre de diverses escroqueries : chantage pour récupérer son compte ou pour éviter la diffusion de contenus compromettants, usurpation de l'identité de la victime auprès de ses contacts, promotion d'escroqueries liées, en général, à des investissements en crypto-actifs.

D'autres types de comptes peuvent également susciter l'intérêt des escrocs : compte de plateformes de commerce en ligne ou de sites de vente entre particuliers, compte bancaire, compte de carte de fidélité, compte de gestion des tickets-restaurants, Pass Culture etc. À ce titre, les recherches d'assistance sur **le service 17Cyber pour un piratage de compte bancaire ont progressé de 205 %** en 2025.

Le piratage de compte est devenu en 2025 le premier motif de recherche d'assistance pour les professionnels (+45%) avec :

- +52 % pour les entreprises/associations ;
- +14 % pour les collectivités/administrations.

Menace n°1
pour les professionnels
avec **20,9 %**
des demandes d'assistance

La compromission d'un compte professionnel peut constituer une porte d'entrée vers d'autres cybermalveillances, comparables à celles affectant les particuliers, tout en présentant des spécificités propres au contexte professionnel, par exemple pour mettre un premier pied dans le réseau informatique d'une organisation, mener une cyberattaque ultérieure ou pour réaliser des fraudes au virement en trompant les clients ou les fournisseurs de l'organisation.

Les comptes de messageries professionnelles sont fortement ciblés : ainsi, les prestataires référencés et **labellisés ExpertCyber** de Cybermalveillance.gouv.fr sont régulièrement **intervenus pour des cas de piratage de comptes** Microsoft Office 365 ou des piratages de systèmes d'information qui avaient pour origine la compromission d'un tel compte. En effet, cette solution utilisée par de nombreuses structures professionnelles offre des services de gestion des identités et des accès qui sont particulièrement prisés des cybercriminels pour obtenir un premier point d'entrée dans les systèmes d'information de l'organisation ciblée.

Des victimes professionnelles assistées en 2025 dans le cadre du service 17Cyber ont également remonté des cas de piratage plus spécifiques. À titre d'exemples :

- piratage de compte d'un logiciel de facturation pour mener des fraudes au virement ;
- piratage de compte Booking.com d'hôtels menant à des tentatives d'hameçonnage ciblé auprès des clients de l'établissement. Les associations professionnelles du secteur hôtelier alertent régulièrement leurs adhérents sur le piratage de ce type de compte de gestion de réservations ;
- piratage de compte Colissimo Entreprise puis utilisation pour plusieurs milliers d'euros de préjudice ;
- piratage de compte Meta Business pouvant mener au lancement de campagnes de publicité frauduleuses ;
- piratage d'un compte de formation professionnelle auprès d'un opérateur de compétences (OPCO) puis inscription à des formations pour plusieurs milliers d'euros ;
- piratage d'un compte de services d'envoi de courriels Courrieljet avec création de listes de contacts et envoi massif de courriels menant à une facturation supplémentaire.

Menace n°2
pour les particuliers
avec **11,6 %**
des demandes d'assistance

LES VIOLATIONS DE DONNÉES : UNE ACCÉLÉRATION AVEC DES CONSÉQUENCES TRÈS DIVERSES

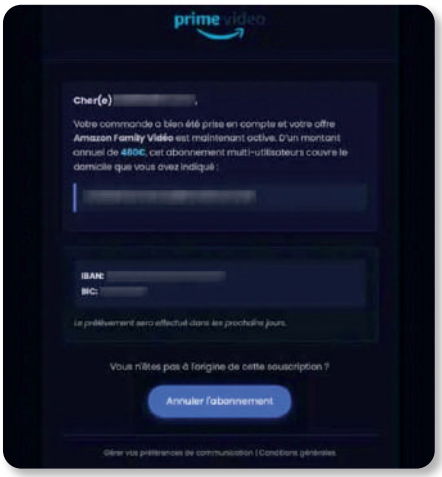
Dans la continuité de l'année 2024, l'année 2025 a été marquée par une accélération des violations de données personnelles. De nombreux incidents, dont certains considérables, ont affecté des organisations publiques et privées, entraînant l'exposition des données personnelles de millions de Français. Les conséquences de ces fuites s'avèrent très diverses.

Différents types d'acteurs ont été touchés : fédérations et opérateurs sportifs, organismes de services en santé, acteurs du commerce en ligne ou physique, de l'assurance ou des mutuelles, opérateurs de logistique et de livraison, France Travail…

En conséquence directe, le nombre de demandes d'assistance de particuliers sur la plateforme a connu une hausse significative (+107 %, suivant +82 % en 2024), témoignant d'une **accélération du phénomène**.

Comme les années précédentes, **la majorité des violations de données personnelles constatées en 2025 résulte de défauts dans la sécurisation des systèmes d'information, de compromissions d'identifiants de comptes, d'intrusions** dans les infrastructures informatiques ou d'**incidents liés à des prestataires ou des partenaires** (attaques de la chaîne d'approvisionnement)…

Les données compromises concernent principalement des informations à caractère personnel (nom, prénom, adresse courriel ou postale, n° de téléphone ou de sécurité sociale…) **et, dans certains cas, des données bancaires (RIB). Ces informations constituent une cible privilégiée pour les cybercriminels,** qui peuvent les exploiter à des fins d'escroquerie ou bien les revendre à d'autres cybercriminels qui essaieront de les exploiter à leur tour.



À titre d'exemple, elles peuvent être utilisées dans le cadre de campagnes d'hameçonnage, parfois massives, personnalisées avec des informations appartenant au destinataire du message frauduleux, à l'image de la campagne de phishing aux couleurs du service Amazon Prime Family au printemps dernier où les messages contenaient le nom, prénom, adresse postale et IBAN de la victime. Ceci a pu être la conséquence de violations massives de données personnelles incluant des IBAN en 2024 et 2025 (SFR, Free, CNFPT, AIDES, Direct Assurance, etc.).

La réutilisation de données bancaires fuitées peut mener à divers types d'escroqueries par ingénierie sociale : fraude au faux conseiller bancaire, fraude au virement…

Par ailleurs, **les informations dérobées peuvent aussi être utilisées à des fins de piratage de compte ou encore à des tentatives d'usurpation d'identité pour mener nombre d'actions frauduleuses** (souscription de crédits, détournement de ligne téléphonique mobile ("*SIM swapping*"…).

Autre conséquence pouvant survenir suite à des fuites de données: des tentatives de vols par ruse et par effraction ont été commises auprès de certains licenciés de la Fédération Française de Tir qui a connu une violation de données personnelles en octobre 2025. Dans le cadre de cet incident, Cybermalveillance.gouv.fr en lien avec le Parquet de Paris et la Préfecture de Police de Paris s'est mobilisé pour diffuser massivement une alerte et prodiguer des conseils de prudence et de conduite à tenir.

Enfin, **suite à des violations de données personnelles dans le secteur des crypto-actifs, des tentatives de détournement de ces actifs ont été identifiées** sur un mode opératoire similaire à celui utilisé dans la fraude au faux conseiller bancaire. Dans les situations les plus graves, des malfaiteurs sont allés **jusqu'à menacer et agresser physiquement les victimes ou leur entourage proche afin de les extorquer.** Plusieurs situations ont été signalées aux forces de sécurité intérieure en 2025 et début 2026.

In fine, les nombreuses situations associées aux violations de données personnelles confirment qu'elles alimentent une multitude de cybermalveillances, qui ne se limitent plus à l'espace cyber mais qui se poursuivent aussi dans l'espace physique avec parfois de graves conséquences (enlèvement, séquestration, tortures et actes de barbarie). Dans la majorité des cas, les informations dérobées permettent aux escrocs de renforcer le ciblage et la crédibilité de leur approche auprès des victimes pour parvenir à leurs fins.

LES RANÇONGICIELS :
UNE MENACE AUSSI PERSISTANTE QUE REDOUTABLE

2 700
demandes d'assistance en 2025
+10%

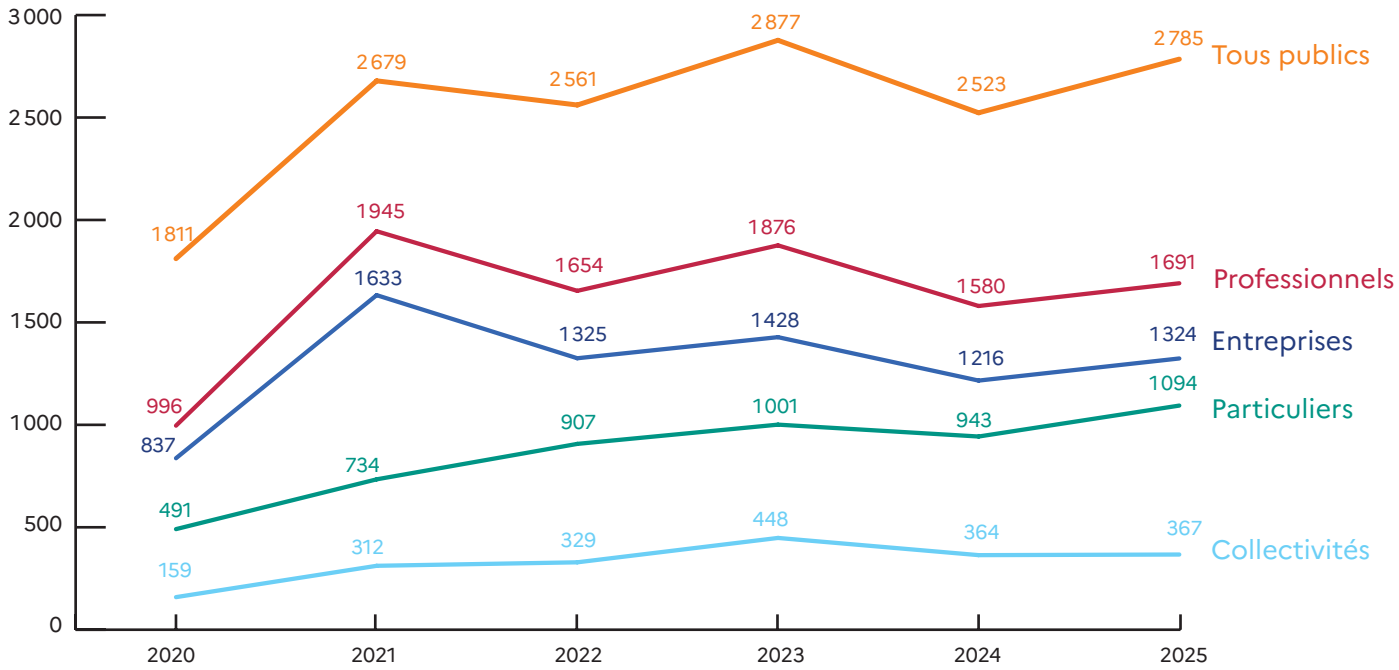
Après avoir connu une accalmie en 2024, les attaques par rançongiciel affichent leur niveau le plus élevé pour la deuxième fois depuis 5 ans (+7% pour les professionnels), ce qui pourrait augurer d'une tendance de nouveau en hausse.

Le rançongiciel est l'un des principaux motifs de recherches d'assistance sur la plateforme pour cette catégorie de publics. Cette menace est répertoriée comme la **4e pour les entreprises et associations et 3e pour les collectivités et administrations** pour un total de **1691 demandes d'assistance.**

Dans le détail, cette hausse est davantage marquée pour les entreprises et associations (+9 %) que pour les collectivités et administrations (+1%).

Côté **particuliers, le rançongiciel enregistre une hausse de 16 % des demandes d'assistance avec 1094 demandes** et figure en 21e position.

Les statistiques concernant les particuliers sont néanmoins à relativiser car Cybermalveillance.gouv.fr constate que nombre de ceux qui s'estiment victimes de rançongiciel font en fait face à un virus et/ou un dysfonctionnement de leur appareil, ou encore à des escroqueries avec des procédés d'extorsion (arnaque au faux support technique, certains piratages de compte, chantage à la webcam/ordinateur prétendu piraté…).



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

À l'image de l'année 2024, l'année 2025 aura été marquée par des opérations judiciaires internationales visant au démantèlement d' infrastructures informatiques appartenant à des groupes d'attaquants ou à la mise hors ligne de nombreuses plateformes et services cybercriminels de l'Internet sombre (*darknet*).

Ces opérations des forces de l'ordre, parfois en collaboration avec des entreprises privées, **ont contribué à fragmenter l'écosystème du rançongiciel**. Néanmoins, de nouvelles franchises de rançongiciels issues de rapprochements et de partenariats entre les différents acteurs cybercriminels existants sont apparues. **Si ces opérations ont mis à mal une partie de l'écosystème du rançongiciel** qui avait pourtant gagné en sophistication, structuration et professionnalisme au cours des dernières années, **l'activité des groupes cybercriminels opérant ce type d'attaques demeure à un haut niveau.**

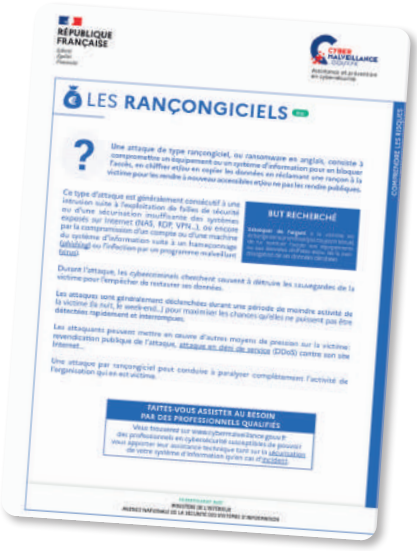
S'agissant des modes opératoires, l'année 2025 ne montre pas d'évolution notable quant aux vecteurs d'attaques exploités par les cybercriminels.

Pour les professionnels, les attaques par rançongiciel résultent le plus souvent d'une **intrusion dans le système d'information** de l'organisation ciblée, rendue possible par l'exploitation de **failles de sécurité** touchant les **accès externes** ou des **services exposés sur Internet** (RDP, VPN, NAS, etc.), des **équipements de bordure et de sécurité** (pare-feu, passerelle de filtrage…) ou encore des **logiciels de virtualisation** (hyperviseur).

Concernant les particuliers, les rançongiciels surviennent notamment suite à l'ouverture d'un fichier malveillant ou par la compromission d'un **serveur de stockage en réseau (NAS) insuffisamment sécurisé et exposé sur Internet**.

Selon son ampleur, **une attaque par rançongiciel peut aller jusqu'à interrompre totalement l'activité de l'organisation ciblée,** si celle-ci ne dispose pas des ressources et des moyens adéquats pour y faire face. **De plus, les conséquences financières, réputationnelles voire juridiques peuvent être lourdes pour les organisations victimes. Les effets psycho-sociaux sur les équipes ne sont pas non plus à négliger.**

Enfin, dans l'objectif d'accompagner au mieux ses publics professionnels et de leur prodiguer les conseils les plus pertinents pour se protéger et réagir lorsque l'on est victime, Cybermalveillance.gouv.fr a publié en juin 2025 une version mise à jour et enrichie de son article sur les rançongiciels.



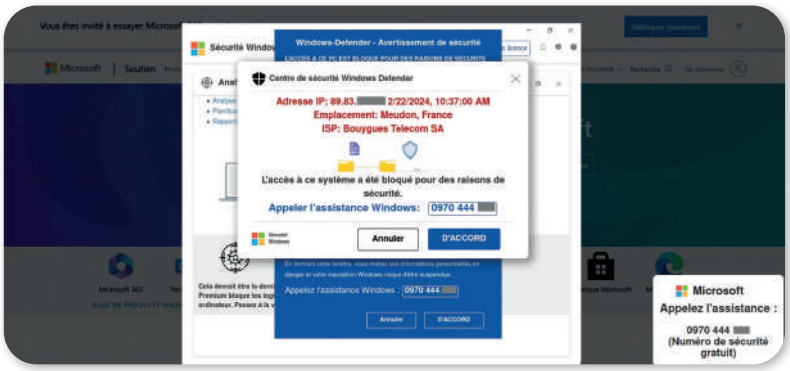
L'ARNAQUE AU FAUX SUPPORT TECHNIQUE : UNE MENACE TOUJOURS PRÉSENTE

Menace n°4
pour les particuliers
avec **5,9 %**
des demandes d'assistance

Année après année, **les escroqueries au faux support technique, aussi appelées fraudes à la réparation informatique, se sont installées dans le paysage des principales menaces affectant les particuliers** (4e position en 2025) et plus ponctuellement, les professionnels.

18 000
demandes d'assistance réalisées
+39%

Ces arnaques ciblent exclusivement les ordinateurs sous la forme d'une page Internet agressive qui s'affiche en plein écran dans le navigateur Internet, faisant croire à l'utilisateur non averti que son appareil est "bloqué". Cette page alerte d'un supposé problème de sécurité critique et enjoint d'appeler le numéro de téléphone affiché d'une prétendue "assistance" Microsoft ou Apple, selon le système d'exploitation de l'ordinateur.



Comme en 2024, **la plupart de ces faux messages d'alerte se produisent suite à un clic sur un contenu sponsorisé malveillant** : premiers résultats de moteurs de recherche, publicités trompeuses et titres d'articles attisant la curiosité sur des sites Internet grand public d'information ou sur les réseaux sociaux, en particulier sur Facebook.

Si la victime appelle, un faux technicien prend la main sur l'ordinateur pour effectuer un dépannage fictif et bien souvent faire souscrire un abonnement à de faux services de sécurité qui seront facturés quelques centaines d'euros. Il n'est pas rare que les paiements soient effectués plusieurs fois sous le prétexte que les précédents auraient échoué.

En 2023 et 2024, Cybermalveillance.gouv.fr avait aussi constaté qu'un nombre croissant de faux supports ciblaient parfois les comptes bancaires des victimes en leur faisant croire qu'ils avaient été piratés. **Ces dérives, similaires aux fraudes au faux conseiller bancaire, ainsi que le sabotage des appareils de victimes qui refusent de payer, ont été moins observés en 2025 mais sont toujours présents.**

En juillet 2025, Cybermalveillance.gouv.fr s'est associé à *Microsoft* et à la section de lutte contre la cybercriminalité (J3) du Parquet de Paris pour une nouvelle campagne de sensibilisation aux arnaques au faux support technique, à destination des seniors qui sont les principales victimes de ce type d'escroquerie.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en cybersécurité

LA FRAUDE AU VIREMENT : UNE CROISSANCE QUI PERDURE

Les fraudes au virement (faux RIB ou faux ordres de virement dits « FOVI ») consistent à usurper l'identité d'une personne ou d'une organisation afin de détourner un virement de fonds planifié au bénéfice d'un escroc. Ce type d'escroquerie est en constante augmentation pour tous les publics depuis plusieurs années. L'année 2025 confirme cette tendance.

13 000 recherches d'assistance **+170%**

Dans la majorité des cas, cette fraude fait suite au piratage d'un compte de messagerie (courriel) du débiteur/client ou de son créancier/fournisseur. L'escroc identifie une facture en attente de règlement ou un paiement récurrent et tente de les détourner à son profit. Pour cela, il se fait passer pour le créancier par courriel et prétexte un changement de coordonnées bancaires. Dans certains cas, pour les professionnels, il s'agit d'obtenir un virement imprévu en usurpant l'identité d'un dirigeant de l'entreprise (fraude au président). **Il est important de rappeler qu'une simple vérification auprès du créancier permet d'éviter ce type de fraude.**

Exemples de variantes de fraudes au virement et campagnes d'hameçonnage inédites :

- l'une des variantes de la fraude au virement concerne le **détournement de salaire des employés.** Une nouveauté a été observée au dernier trimestre 2025 : **les escrocs tentent le détournement de salaire auprès des employeurs en ayant préalablement ouvert un compte bancaire au nom de la victime après avoir usurpé son identité.** Cette évolution semble s'inscrire en réponse à la mise en place en octobre 2025 d'un système interbancaire de vérification d'identité automatique pour tout virement SEPA. Les escrocs disposent donc au préalable de suffisamment de documents au nom de la victime pour pouvoir ouvrir un compte bancaire à son nom. Leur provenance peut être le vol physique, l'usurpation d'identité lors d'escroqueries (arnaques à la location immobilière ou à l'emploi), le piratage d'un appareil ou d'un compte de messagerie, ou encore une fuite de données dans une organisation.
- des entreprises constatant sur le tard un **accès frauduleux à leur logiciel de facturation** qui avait conduit à une modification de leurs coordonnées bancaires. Des factures ont ainsi été émises et payées par leurs clients à des escrocs.
- une autre variante concerne le **détournement de prestations sociales**. Cybermalveillance.gouv.fr recueille régulièrement des témoignages de victimes, qui n'ayant pas perçu les versements attendus, ont découvert la modification de leurs coordonnées bancaires au profit d'un escroc dans l'espace personnel de leur compte CAF, retraite, Assurance Maladie ou chômage.
- en février 2025, des **campagnes d'hameçonnage par courriel usurpant l'identité de nombreuses communes françaises ont été identifiées. Ces messages étaient adressés aux entreprises et associations locales et informaient d'un changement de coordonnées bancaires de leur mairie avec un RIB en pièce jointe**. Les escrocs disposaient donc de listes de contacts professionnels et associatifs des zones géographiques ciblées et misaient sur le fait que certains destinataires étaient susceptibles d'effectuer des paiements ponctuels ou récurrents à la collectivité.

Selon les responsabilités de chaque partie dans ces types d'incident, le créditeur ne recevra pas le paiement qui lui est dû ou le débiteur devra s'acquitter d'un deuxième paiement.

Mais les conséquences des fraudes au virement ne sont pas uniquement financières. Ainsi, la détermination des responsabilités peut entraîner une dégradation des relations entre les deux parties. Par ailleurs, les conséquences psychologiques et professionnelles pour la personne qui a réalisé le virement aux escrocs ne sont pas à négliger. Elle peut développer un sentiment de culpabilité, voire être sanctionnée ou déconsidérée professionnellement si son action est jugée fautive.

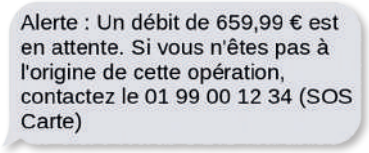
Menace n°3 pour les professionnels avec **12,8 %** des demandes d'assistance

LA FRAUDE AU FAUX CONSEILLER BANCAIRE : EN FORTE HAUSSE MALGRÉ LA SENSIBILISATION

15 000
demandes d'assistance
+159%
pour les particuliers

Les fraudes au faux conseiller bancaire poursuivent leur forte progression et ce, malgré la forte médiatisation du phénomène, les nombreuses communications des établissements bancaires auprès de leurs clients ainsi que les mises en garde affichées lors de la réalisation d'opérations bancaires en ligne. En 2025, les précédents modes opératoires se sont confirmés et des évolutions ont également été constatées :

- **l'hameçonnage du grand public par courriel et par SMS a toujours pour objectif de collecter des données personnelles et de carte bancaire qui seront, en grande majorité, exploitées par la suite pour des appels de faux conseillers bancaires.** Parfois, les escrocs évoquent même cet hameçonnage qui a piégé la victime pour justifier la supposée fraude en cours ;



- **l'hameçonnage au faux numéro d'opposition bancaire, spécifiquement dédié à ce type d'escroquerie, existe depuis plusieurs années mais il est devenu massif en 2025.** Cybermalveillance.gouv.fr a alerté sur ce phénomène dans lequel ce n'est plus l'escroc qui contacte la victime mais bien cette dernière qui l'appelle ;

- **l'exploitation de données personnelles (identité, coordonnées…) et bancaires (IBAN) qui ont fait l'objet de violations lors de fuites massives de données. Des escrocs en possession de ces informations ont directement contacté des victimes en se faisant passer pour des agents de leur banque.** En effet, un IBAN permet de déterminer l'établissement et l'agence bancaire auxquels un compte est rattaché ;

- la création de compte bancaire ou de cryptomonnaies lors de l'appel est une pratique courante. **Les escrocs parviennent à convaincre leurs victimes de créer un compte "de secours" dans un établissement tiers pour y transférer leurs avoirs afin de les sécuriser. Ils arrivent aussitôt à s'approprier ce compte** qui pourra éventuellement être réutilisé ou revendu pour d'autres escroqueries ;

- **l'utilisation de la messagerie WhatsApp par les escrocs pour contacter les victimes a régulièrement été observée en 2025.** Elle leur permet d'afficher le logo d'une banque ou d'un organisme public en tant que photo de profil pour rendre plus crédible leur approche. De plus, certains arnaqueurs incitent leurs victimes à activer la fonctionnalité de partage d'écran de la messagerie pour les guider dans la supposée sécurisation de leur compte et ont ainsi une vue en temps réel de leur application bancaire.

- Cybermalveillance.gouv.fr a également observé une augmentation des appels frauduleux de **faux conseillers de plateformes ou de services de cryptomonnaies** (Binance, Ledger, Coinhouse, etc.) selon des modes opératoires similaires à la fraude au faux conseiller bancaire.

Enfin, d'autres cybermalveillances peuvent être à l'origine des fraudes au conseiller bancaire : **piratage de compte de messagerie** (courriel), **infection par un virus** (récupération de mots de passe par exemple).
Face à cette menace toujours croissante, il est important de rappeler que ces escroqueries existent et qu'un agent d'une banque, d'un service anti-fraude, des forces de l'ordre ou de tout autre organisme privé ou public n'appellera jamais par téléphone ses clients pour leur demander leurs identifiants, codes ou mots de passe, les inciter à réaliser des opérations sur leurs comptes bancaires sous prétexte de les sécuriser ou encore de remettre leur carte de paiement, voire leurs biens de valeur, à une personne qui viendra les chercher à domicile.

L'ESCROQUERIE AU FAUX PLACEMENT FINANCIER : UNE MENACE QUI GAGNE EN INTENSITÉ

6 000
demandes d'assistance
+277%
pour les particuliers

En 2025, Cybermalveillance.gouv.fr a enregistré une nette augmentation des recherches d'assistance concernant les escroqueries au faux placement financier.

Menace n°6
pour les particuliers
avec **5 %**
des demandes d'assistance

Ces arnaques sont largement promues par des publicités ou des contenus sponsorisés sur les réseaux sociaux, des sites Internet ou par courriel, usurpant parfois l'identité de grands médias nationaux et de personnalités publiques.

Sur les messageries instantanées, particulièrement WhatsApp, des invitations non sollicitées à rejoindre des "groupes d'investisseurs" frauduleux sont monnaie courante. Les réseaux sociaux, forums de discussion ou encore les applications de rencontres constituent un terrain de chasse pour des rabatteurs qui entrent individuellement en contact avec leurs victimes et leur vantent des solutions de placements censées rapporter de grands rendements. L'ingénierie sociale est au cœur de ces arnaques où la victime, une fois accrochée, est incitée à investir toujours plus.

Pour crédibiliser l'escroquerie, les cybercriminels disposent d'outils tels que de faux sites Internet d'apparence professionnelle qui laissent croire aux victimes que leurs placements fructifient. Ils produisent éventuellement de faux documents ou formulaires administratifs pour donner un cadre d'apparence légitime à leur activité.

Bien que tous types de placements soient concernés, les cryptomonnaies sont fortement représentées dans les escroqueries au placement.

Les préjudices pour les victimes vont de quelques centaines d'euros (nombre d'escroqueries commencent par un premier "placement" de 250 €), notamment pour ceux qui ont su identifier l'arnaque suffisamment tôt pour ne pas perdre plus d'argent. Certaines victimes déplorent la perte de la totalité de leur épargne qui, pour certaines, peut s'élever à plusieurs centaines de milliers d'euros.

Les arnaques au recouvrement

Quelque temps après l'escroquerie qu'elles ont subie, de nombreuses victimes sont contactées par des escrocs sous des qualités usurpées (forces de l'ordre, autorités administratives, avocats, etc.). Ils prétendent que les fonds dérobés ont été retrouvés et, ont bien souvent, enregistré de fortes plus-values.

Leur objectif est de manipuler ces anciennes victimes pour les escroquer à nouveau (paiement de taxes pour débloquer les avoirs, par exemple). Ces relances peuvent être le fait des mêmes escrocs ou celui d'autres cybercriminels qui auraient racheté aux premiers les "dossiers" de leurs anciennes victimes.

En 2025, Cybermalveillance.gouv.fr a publié un article sur les escroqueries au placement financier présentant cette menace et donnant des conseils pour s'en prémunir et réagir lorsqu'on en est victime.

FOCUS SUR LES **MENACES EN FORTE ACCÉLÉRATION**

FOCUS

L'USURPATION DE NUMÉRO DE TÉLÉPHONE

7 000
demandes d'assistance
+517%
pour les particuliers

Phénomène marquant de l'année 2024, l'usurpation de numéro de téléphone a perduré en 2025 malgré les dispositifs réglementaires et techniques mis en place pour endiguer cette pratique malveillante, avec la loi dite "Naegelen" introduisant notamment un renforcement du mécanisme d'authentification des numéros.

En effet, les cybercriminels ont trouvé des parades pour continuer à afficher des numéros de leur choix ou aléatoires pour passer des appels ou envoyer des SMS malveillants. Les recherches d'assistance pour cette escroquerie ont ainsi poursuivi leur croissance (+ 517%) pour devenir la 10e menace la plus fréquente pour les particuliers.

L'Arcep[1] a elle aussi constaté la poursuite de ces pratiques frauduleuses et, malgré l'entrée en vigueur de nouvelles mesures au 1er janvier 2026 (affichage de numéros masqués pour les appels non authentifiés), elle souligne que le phénomène persiste. En conséquence, l'Arcep a lancé une enquête administrative afin d'identifier plus en profondeur l'ensemble des opérateurs impliqués dans l'acheminement des appels frauduleux.

Les personnes qui sont victimes d'usurpation de téléphone le découvrent lorsqu'elles sont contactées par des particuliers qui leur signifient qu'elles les ont appelés ou lorsqu'elles reçoivent des réponses à des SMS qu'elles n'ont pas envoyés.

Ces contre-appels et messages reçus peuvent être parfois très virulents car, en général, les appels émis avec leur numéro de téléphone sont des appels en absence de type démarchage commercial non sollicité et les messages sont des SMS d'hameçonnage.
Ces nuisances peuvent être très stressantes pour les victimes et durer plusieurs jours consécutifs.

Actuellement, à moins de paramétrer temporairement son appareil pour ne plus recevoir d'appels ou de messages de numéros inconnus, il n'existe pas de parade à cette arnaque.

[1] Autorité de régulation des communications électroniques, des postes et de la distribution de la presse

Nouvelle entrée
dans les principales menaces ciblant les particuliers,
avec 2,4 % des demandes d'assistance

LES ESCROQUERIES COMMERCIALES POURSUIVENT LEUR CROISSANCE

7 600
recherches d'assistance
+170%

Les utilisateurs du service d'assistance 17Cyber sont de plus en plus souvent confrontés à de faux sites de commerce en ligne et à des arnaques sur les plateformes de vente entre particuliers.

1. Les sites de commerce frauduleux ont proliféré en 2025, concernant une grande diversité de produits : habillement, concerts grand public, pellets ou bois de chauffage, équipements domestiques, sportifs et de loisirs, matériel agricole professionnel, etc.

La plupart de ces sites Internet n'envoient pas de produits une fois les commandes passées et ont un pseudo service clients peu actif ou inexistant. D'autres expédient des **produits dont la qualité est très inférieure** à celle annoncée de façon mensongère. Certains sites envoient même **des colis dont le contenu sans valeur n'a aucun rapport avec le produit commandé**. Enfin, de faux commerces en ligne **honorent les commandes pendant un certain temps pour acquérir une bonne réputation puis cessent les envois par la suite**. En général, ces sites ont une durée de vie limitée et continuent à encaisser les montants des commandes tant qu'ils sont en ligne.

La promotion de ces sites se fait essentiellement sur les **réseaux sociaux** avec des **comptes frauduleux** et des **campagnes publicitaires accrocheuses**, ciblées sur les intérêts des utilisateurs qui sont en permanence collectés par ces plateformes. La publicité se fait aussi sur divers sites Internet ou apparaît en **résultats sponsorisés** dans les moteurs de recherche.

De plus, les prix pratiqués sont très compétitifs et ces sites sont en général bien conçus, présentant un aspect professionnel pour mieux tromper les victimes.

Outre les clients escroqués, de nombreux entrepreneurs déplorent l'usurpation d'identité de leur entreprise ou de leur marque par des faux sites d'e-commerce qui reprennent leur raison sociale, coordonnées postales et numéro de SIRET dans leurs mentions légales. Seules les coordonnées téléphoniques et l'adresse courriel de contact sont celles des escrocs.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

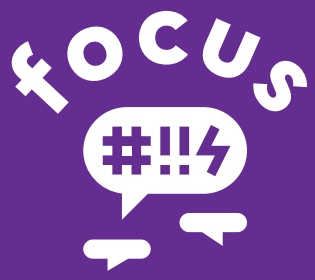
CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

Une fois qu'ils ont été trompés, des acheteurs, parfois nombreux, contactent l'entreprise légitime pour effectuer des réclamations. Certains la suspectent d'être à l'origine de l'arnaque et publient des avis négatifs en ligne à son encontre. Ces méfaits peuvent durer tant que le site frauduleux est en ligne et constituent une situation stressante et chronophage pour les entreprises victimes dont la réputation peut, à tort, être mise à mal.

2. Les sites et applications de vente entre particuliers sont le terrain de multiples cybermalveillances toujours plus présentes sur ces plateformes. De faux vendeurs ou de faux acheteurs mettent en œuvre divers modes opératoires de plus en plus complexes et trompeurs pour voler le bien, soutirer de l'argent ou des informations personnelles aux utilisateurs de ces plateformes.

Parmi ces méthodes, Cybermalveillance.gouv.fr observe un recours croissant aux pratiques suivantes lors des ventes : usurpation d'identité de services de paiement (Paylib/Wero, PayPal…) ou des plateformes de vente elles-mêmes (Leboncoin, Vinted) sous la forme d'appels de faux conseillers, envois de messages frauduleux orientant vers des sites d'hameçonnage. Ils ont pour objectif de faire croire qu'un paiement a bien été effectué pour récupérer un bien, gratuitement.

À l'inverse, il s'agira de détourner un paiement avant de disparaître sans expédier le bien vendu. Ces modes opératoires visent aussi fréquemment à pirater le compte de la victime sur le site de vente, pour y dérober sa cagnotte puis usurper son identité auprès d'autres utilisateurs.



LE CYBERHARCÈLEMENT : VERS UNE BANALISATION DU PHÉNOMÈNE ?

18 000
demandes d'assistance
+138%
pour tous les publics

Après avoir fait une entrée notable dans le classement des principaux motifs de recherches d'assistance des professionnels sur la plateforme en 2024, le cyberharcèlement contre ce public a continué à progresser en 2025 et tend à s'installer durablement.

Il se positionne ainsi à la 6e place pour les collectivités/administrations (+209 % ; 10e en 2024) et à la 7e pour les entreprises/associations (+205 % ; 9e place en 2024). Parallèlement, **une augmentation de 134 % des demandes d'assistance** émanant de particuliers victimes ou témoins de harcèlement en ligne a été enregistrée l'année dernière, passant de la 6e à la 5e place entre 2024 et 2025. **Si le sujet du cyberharcèlement constitue toujours une véritable préoccupation pour les publics particuliers ou professionnels,** sa matérialisation diffère selon la sphère, privée ou professionnelle, dans laquelle il est commis.

Dans la sphère privée, cela peut prendre la forme **d'intimidations, d'insultes, de menaces, de rumeurs ou de publications de photos ou vidéos compromettantes** sur les réseaux sociaux, les messageries, les forums ou les blogs.

En revanche, **dans la sphère professionnelle, le harcèlement en ligne ne vise pas seulement des individus ou groupes d'individus mais également des organisations**. Il peut s'illustrer par des propos virulents et répétés envoyés par courriel, via des formulaires de contact ou sur les comptes de réseaux sociaux d'une entité, d'avis négatifs sur Google ou sur des plateformes permettant à d'anciens ou actuels employés de s'exprimer sur leur entreprise.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

Ainsi, bien que marginal, un nouveau mode opératoire d'escroquerie a été identifié en 2025: des escrocs publient en masse des avis négatifs sur Google concernant une organisation et demandent une rançon contre l'arrêt de ces publications.

Ces faits de cyberharcèlement dans la sphère professionnelle peuvent ainsi toucher des entreprises, des artisans, des professions libérales, des indépendants, des personnalités publiques, des associations etc. Toutefois, contrairement aux grandes organisations qui gèrent leur e-réputation et l'image de leur dirigeant, **les petites structures (TPE-PME, associations, collectivités…) se retrouvent démunies face à de telles situations**. Par exemple, pour les petites entreprises, les réseaux sociaux sont un véritable moyen d'acquérir de la notoriété à un faible coût et une campagne ciblée de cyberharcèlement peut fortement réduire à néant les efforts de plusieurs années pour construire une image positive et une bonne évaluation sur les plateformes en ligne.

Menace n°5
pour les particuliers
avec **5,3 %**
des demandes d'assistance

Enfin, si le harcèlement en ligne n'est pas nouveau, Cybermalveillance.gouv.fr a constaté depuis plusieurs mois un durcissement, voire une violence assumée, dans les propos tenus par les cyberharceleurs et dans les pratiques employées pour harceler les victimes.

FAITS ET CHIFFRES CLÉS

5,1 millions

de visiteurs uniques sur la plateforme

Plus de **504 000**

demandes d'assistance sur la plateforme

64

membres du dispositif

20

agents du GIP ACYMA

466

demandes de souscription au module 17Cyber

1 250

prestataires de service référencés

200

prestataires labellisés **ExpertCyber**

Taux de satisfaction pour l'assistance en ligne :

84,2 %

87 %

des demandes d'assistance des entreprises et des collectivités reçoivent une réponse d'un prestataire

en moins d'1 heure

63 %

des demandes de sécurisation reçoivent une réponse en

moins de 3 heures

185 000 **abonnés** sur LinkedIn

46 000 **abonnés** sur X

33 000 **abonnés** sur Facebook

2 000 **abonnés** sur Instagram

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

NOS REMERCIEMENTS

Cybermalveillance.gouv.fr remercie celles et ceux qui ont apporté leur témoignage dans ce septième rapport d'activité. 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'Intérieur;
- Ministère des Armées et des Anciens combattants;
- Ministère de la Justice;
- Ministère de l'Économie, des Finances et de la Souveraineté industrielle, énergétique et numérique
- Ministère de l'Éducation nationale;
- 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**, **Association E-Enfance/3018**, **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 Digital**, **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), **CNOEC** (Conseil National de l'Ordre des Experts-Comptables), **coTer numérique**, **Covéa**, **CPME** (Confédération des Petites et Moyennes Entreprises), **Déclic**, **ECTI**, **Fédération EBEN** (Fédération des Entreprises du Bureau et du Numérique), **FEVAD** (Fédération du e-commerce et de la vente à distance), **France Assureurs**, **France Télévisions**, **France Victimes**, **Google France**, **Hucency**, **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**, **Nomios**, **Numeum**, **Orange Cyberdefense**, **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 participent activement, aux côtés de Cybermalveillance.gouv.fr, à l'assistance des victimes et à la sécurisation des professionnels sur l'ensemble du territoire.

Les groupements de prestataires aux côtés des fédérations et syndicats : **Alliance du Numérique**, **Groupe Convergence**, **ESCRIM**, **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 cybersécurité à Monaco** (Groupe Comexposium), **CBC**, le **coTer numérique**, le **Forum InCyber**, les **GS Days – Journées Francophones de la sécurité**, les **Innodays** (Bouygues Telecom), **IT Partners** (RX France), **Lyon CyberExpo**, le **NEC – Numérique En Commun[s]**, **Universités d'Été de la Cyber et du Cloud de confiance** (Hexatrust), le **Salon des Maires et des Collectivités Locales**.

Ses partenaires lors du Cybermois tels que **BFM Business**, **Culture Presse**, **France Messagerie**, **L'internaute**, **Le Parisien**, **Match Group** et le **SNDP**, ainsi que les **campus territoriaux de Bretagne**, **Nouvelle-Aquitaine**, **Hauts-de France**, **Normandie**, le **campus national (Campus Cyber)**, **Rennes Métropole**, la **Ville de Périgueux**, **ATD24**, **EuraTechnologies**, la **Ville de Lezennes**, la **Métropole Rouen Normandie**, et les structures gouvernementales notamment l'**ANCT**, le **ministère des Armées et des Anciens combattants**, le **ministère de la Justice**, le **Haut-Commissariat à l'Enfance**, le **ministère de l'Agriculture, de l'Agro-alimentaire et de la Souveraineté alimentaire**, le **ministère de l'Éducation nationale** et le **ministère de la Culture** et le **ministère chargé de l'Intelligence artificielle et du Numérique**.

Plus généralement, Cybermalveillance.gouv.fr remercie **l'ensemble des acteurs de l'écosystème avec lesquels il interagit.**

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention
en cybersécurité

GIP ACYMA
www.cybermalveillance.gouv.fr

Suivez-nous sur :