RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

COMMUNIQUÉ DE PRESSE

Cybermalveillance.gouv.fr dévoile les tendances de la menace cyber en France

26 mars 2026

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

Cybermalveillance.gouv.fr
dévoile les tendances de la menace cyber en France

Paris le 26 mars 2026 - À l'occasion de la publication de son rapport d'activité, Cybermalveillance.gouv.fr présente les tendances de la menace observées pour l'année 2025

Un cap franchi pour l'assistance des victimes

Pour la deuxième année consécutive, Cybermalveillance.gouv.fr a dépassé le seuil de 5 millions de visiteurs sur sa plateforme et enregistre une audience cumulée de 22 millions depuis sa création en 2017.
Cette activité s'explique en partie par le lancement du 17Cyber (fin 2024), l'opération Cactus auprès des collégiens et lycéens, la campagne du Cybermois et son CyberTour de France ainsi que par les recherches de conseils et d'assistance.

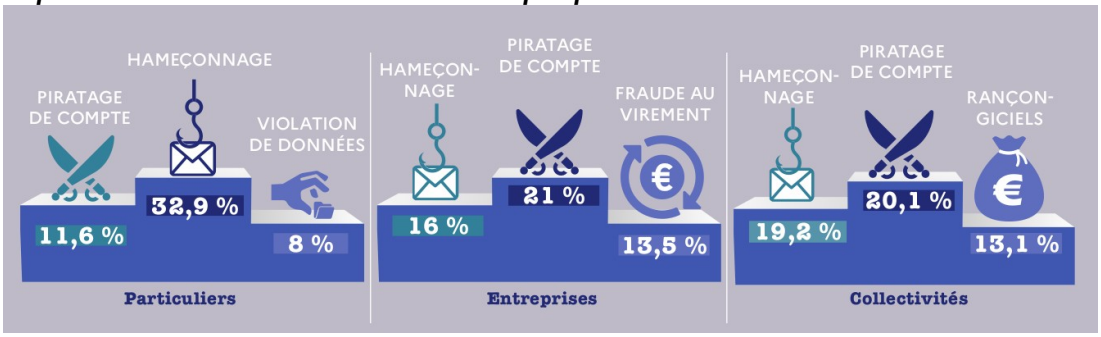
En termes d'assistance, le dispositif national de prévention **a franchi un cap avec plus de 500 000 victimes assistées, en hausse de 20 % par rapport à 2024**.
Cette augmentation du nombre de diagnostics a été générée en particulier par les **nombreuses fuites de données** survenues dans différents secteurs d'activité et par leurs conséquences (commerces en ligne ou physiques, fédérations sportives, opérateurs télécom, sociétés de livraison, acteurs du monde de l'emploi, de la santé ou encore de l'assurance et des mutuelles etc).

Une menace cyber qui s'intensifie

L'année passée s'est en particulier caractérisée par une **accélération des violations de données** qui ont affecté des organisations publiques et privées et entraîné l'exposition de données personnelles de millions de Français. Ce phénomène s'est traduit par un **bond de 107 % des demandes d'assistance concernant les violations de données, tous publics confondus.**

L'exploitation malveillante de ces données fuitées conduit à faire figurer **l'hameçonnage au premier rang des menaces**, tous publics confondus, **en augmentation de 70 %**. 2025 a ainsi été marquée par de multiples vagues d'hameçonnage par SMS, courriels ou même appels audio, de plus en plus variées et personnalisées, pour réaliser des tentatives d'arnaques ou encore **des piratages de comptes en ligne, en tête des menaces touchant les professionnels** (+45%).

Répartition des demandes d'assistance par public :



Un marché de la donnée de plus en plus mature

Si tous les types de données suscitent l'intérêt des cybercriminels et notamment la «donnée fraîche », leur appétence a été favorisée par plusieurs facteurs.
Le marché souterrain de la donnée volée est désormais structuré et piloté par des acteurs spécialisés, des plateformes d'échanges dédiées (« marketplaces »), des kits d'hameçonnage et d'arnaques prêts à l'emploi et même des centres d'appels composés de faux téléconseillers spécialisés en manipulation.
De ce fait, une offre pléthorique de données fraîches et de profils clés en main est commercialisée sur l'Internet sombre (*darkweb*), des forums plus ou moins clandestins et des chaînes de messageries chiffrées.
Cette industrialisation de l'exploitation des données témoigne, d'une part, du niveau de sophistication et de maturité des cybercriminels et explique, d'autre part, la facilité avec laquelle ils peuvent élaborer de nouvelles arnaques et piéger des victimes.

Un regain d'intérêt pour les fraudes et arnaques à objectif financier

En 2025, nombre de données personnelles ont été mises au profit d'arnaques financières. Souvent consécutives à un piratage de compte, **les fraudes au virement**, en constante augmentation pour tous les publics depuis des années, **s'intensifient** (+170%) et se sont étendues à des domaines comme la facturation électronique ou la gestion de la paie.

Par ailleurs, malgré les efforts de communication des acteurs du secteur, **la fraude au faux conseiller bancaire poursuit une forte progression** (+159%) avec quelques évolutions telles que l'hameçonnage au faux numéro d'opposition et le recours à la messagerie WhatsApp pour abuser les victimes.

Le faux placement financier gagne également en intensité auprès des particuliers (+277%) avec des appâts sur les réseaux sociaux ou de faux sites d'apparence professionnelle. Une menace où WhatsApp est aussi mis à contribution par des rabatteurs pour inviter leurs victimes à rejoindre des groupes d'investisseurs.
Les cryptomonnaies occupent elles-aussi une place dans ces escroqueries, avec des tentatives de détournement d'actifs ou des systèmes de fructification frauduleux.

Des menaces en forte accélération

Parmi les cybermalveillances qui s'amplifient très fortement, **l'usurpation de numéro de téléphone affiche une augmentation de 517 %** et ce malgré les dispositifs réglementaires et techniques (Loi « Naegelen ») mis en place pour l'endiguer.

Les escroqueries commerciales poursuivent leur croissance (+ 170 %), notamment au travers de sites frauduleux qui ont proliféré en 2025 ou avec des sites et applications de vente en ligne qui constituent le terrain de multiples malveillances telles que l'usurpation de services de paiement ou de plateformes de vente avec l'appel de faux conseillers ou l'envoi de messages frauduleux.

Enfin, véritable préoccupation pour les particuliers et les professionnels, **le cyberharcèlement progresse et tend à s'installer durablement** (+138% tous publics, dont +209 % pour collectivités et +205 % pour les entreprises)**.** S'il prend la forme d'intimidations, d'insultes ou de publications indésirables sur les réseaux sociaux, dans la sphère professionnelle, cette menace peut mettre à mal la réputation d'entreprises (artisans, professions libérales, personnalités, associations) parfois démunies face à de nouveaux modes opératoires tels que les avis négatifs fallacieux.

Une frontière entre cyber et espace physique qui s'estompe

2025 a également vu la ligne entre les mondes numérique et réel se réduire avec des modes opératoires plus singuliers ou quelquefois extrêmes.

Pour certaines menaces, les criminels n'ont pas hésité à se reposer sur des équipes « terrain » sous-traitantes, mandatées par exemple dans le cas d'une arnaque au faux conseiller bancaire pour récupérer des cartes de paiement à domicile par de « faux coursiers».

Des fuites de données ont également occasionné des délits (cambriolages) ou des visites de faux policiers ou gendarmes auprès de licenciés de la Fédération française de Tir. En lien avec le Parquet et la Préfecture de Paris, Cybermalveillance.gouv.fr s'est mobilisé pour diffuser massivement une alerte et des conseils de prudence et de conduite à tenir.

Enfin, toujours dans un contexte d'exploitation de fuites de données, des menaces physiques ou des crimes ont été commis envers des détenteurs de crypto-actifs voire de leurs proches : enlèvement, séquestration, tortures et actes de barbarie.

« *Si 2025 nous montre que nous avons passé un cap avec plus d'un demi-million de victimes assistées, les conséquences de certaines menaces attestent qu'un seuil a été franchi par les cybercriminels. Avec un marché qui s'est structuré et qui a gagné en sophistication et en maturité, la perspective de 2026 augure encore de fortes vagues d'hameçonnage de plus en plus personnalisées, de piratages de compte et de violations de données qui vont nourrir des arnaques multiples et variées. Enfin, le contexte géopolitique instable et la frontière entre les mondes cyber et physique est devenue très poreuse. Ceci nous appelle plus que jamais à démultiplier la sensibilisation de nos publics et à mettre en œuvre les dispositifs permettant de renforcer significativement la protection cyber de tous les Français* », a déclaré Jérôme Notin, Directeur Général de Cybermalveillance.gouv.fr

Contacts Presse Cybermalveillance.gouv.fr
presse@cybermalveillance.gouv.fr
Béatrice Hervieu - 01 83 75 14 10 - Pauline Fabry - 01 83 75 14 19 - Stella Azzoli - 01 83 75 14 09

À propos de Cybermalveillance.gouv.fr
Cybermalveillance.gouv.fr est la plateforme du Groupement d'Intérêt Public Action contre la cybermalveillance (GIP ACYMA). Créé en 2017, ce dispositif national a pour missions l'assistance aux victimes d'actes de cybermalveillance, la protection des organisations, la sensibilisation aux risques numériques, et l'observation de la menace sur le territoire français, qui s'illustrent notamment au travers du service d'assistance 17Cyber.
Ses 62 membres issus du secteur public, du privé et du domaine associatif contribuent à sa mission d'intérêt général pour ses 3 publics : particuliers, entreprises et collectivités. En 2025, Cybermalveillance.gouv.fr a accueilli 5,1 millions de visiteurs uniques sur son site Internet et plus de 504 000 personnes ont réalisé un parcours d'assistance. www.cybermalveillance.gouv.fr

PREMIER MINISTRE

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