RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

RAPPORT D'ACTIVITÉ 2021

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

Directeur de la publication : Jérôme Notin
Coordination éditoriale : Clémentine Lemal et Maïlys Derville
Conception graphique : Elsa Godet
Crédits photos : © Guillaume Lechat - photos des agents du GIP ACYMA pp. 5, 12, 14, 17 haut / © Photos fournies par les organismes concernés pp. 4, 17, 23, 28, 29 / © Freepik pp. 45, 46, 53

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

SOMMAIRE

ÉDITOS 4
Guillaume Poupard 4
Jérôme Notin 5

1/ LES FAITS MARQUANTS DE L'ANNÉE 2021 6
LES FAITS MARQUANTS 8
FAIRE CONNAÎTRE LES MISSIONS DU DISPOSITIF AU PLUS GRAND NOMBRE 10
Multiplication des événements 10
Des relations médias renforcées 10
Le développement des réseaux sociaux 11
Stratégie de contenus 11
FOCUS. Une notoriété croissante 11
LES PROJETS PHARES DE L'ANNÉE 2021 12
Lancement public du label ExpertCyber 12
FOCUS. Lancement de la campagne de sensibilisation 14
Les collectivités au cœur des actions de sensibilisation 16

2/ LES MISSIONS ET L'ORGANISATION DU GIP 18
Présentation du dispositif 20
Dates clés de la création du GIP 20
Gouvernance et organisation du GIP 21
Les membres du GIP 22
Paroles de membres 23

3/ UN PARTENARIAT PUBLIC – PRIVÉ AU SERVICE D'UNE MISSION D'INTÉRÊT GÉNÉRAL 24
EXEMPLES DE COLLABORATIONS EN 2021 26
Association e-Enfance/3018 26
Tournée de sensibilisation et de formation des entreprises par Google France 26
Ma PME Numérique de Microsoft France 27
Lancement du dispositif « Alerte Cyber » 27
FOCUS. Un guide en ligne pour les dirigeants de TPE-PME-ETI 28
I.M.M.U.N.I.T.É.Cyber : un questionnaire pour sensibiliser les élus à la cybersécurité 29

4/ LA SENSIBILISATION, PREMIÈRE ARME CONTRE LES CYBERMALVEILLANCES 30
SENSIBILISATION ET ÉVÉNEMENTS 32
Tous publics 32
Professionnels 33
Campagne nationale d'information et de sensibilisation « Consomag » 34
Contenus de prévention et d'assistance publiés sur la plateforme 35

5/ L'ASSISTANCE AUX VICTIMES : UN BESOIN, UNE NÉCESSITÉ 36
AMÉLIORATION CONTINUE DE WWW.CYBERMALVEILLANCE.GOUV.FR 38
Optimisation des services proposés 38
LA RÉPONSE À UN BESOIN TOUJOURS PLUS FORT DES POPULATIONS 40
Une fréquentation en hausse 40
Une fréquentation majoritairement centrée sur l'assistance 41
L'intérêt pour le curatif l'emporte toujours très largement sur le préventif 41

6/ OBSERVER LA MENACE POUR MIEUX L'ANTICIPER ET ADAPTER L'OFFRE D'ASSISTANCE 42
LES CHIFFRES DE LA CYBERMALVEILLANCE EN 2021 44
Les principales menaces par catégories de publics en 2021 46
LES GRANDES TENDANCES DE LA MENACE EN 2021 48
L'hameçonnage, principal vecteur de cybermalveillances 48
Le piratage de compte : les messageries de plus en plus ciblées 50
FOCUS. 2021, une année marquée par les fuites de données personnelles médicales 51
Les rançongiciels, principale menace pour les professionnels 52

REMERCIEMENTS 54

ÉDITOS

GUILLAUME **POUPARD**

*Président du Conseil d'administration du GIP ACYMA**
Dispositif Cybermalveillance.gouv.fr

Si l'année 2021 a sans conteste fait l'objet d'une professionnalisation des cyberattaques et d'une multiplication des escroqueries numériques, elle a également vu croître les efforts déployés pour y faire face. Alors que la menace se complexifie, et face à des enjeux cyber plus que jamais d'actualité, les acteurs de la cybersécurité se mobilisent pour accroître la prévention et accompagner l'ensemble des victimes, publiques comme privées, grandes comme petites.

Alliant agilité, expertise et confiance, les missions de prévention et d'assistance du dispositif Cybermalveillance.gouv.fr renforcent au quotidien la sensibilisation aux risques numériques. Les actions concrètes du dispositif sont nombreuses et bénéficient pleinement à nos concitoyens.

C'est en renforçant la cybersécurité de chaque pan de la société, de l'individu aux entreprises, que nous assurerons collectivement notre protection. Avec le lancement du label ExpertCyber, des services de qualité et un accompagnement adapté à certains besoins, de la part de prestataires à l'expertise certifiée, sont désormais facilement identifiables.

Créer des synergies, anticiper toujours mieux les défis à venir, améliorer les compétences… tels sont les piliers d'une protection efficace de notre société. Au cœur de cette dynamique, Cybermalveillance.gouv.fr œuvre de manière toujours plus essentielle en faveur de la sécurité numérique de nos concitoyens.

Merci à nos membres pour leur implication remarquable, à nos partenaires toujours plus nombreux, à tous ceux qui donnent sans compter au quotidien au sein du GIP sous la direction de Jérôme ! Vous contribuez de manière essentielle à l'efficacité et à la cohérence de notre dispositif global de sécurité numérique ; vous pouvez en être fier.

JÉRÔME **NOTIN**

*Directeur général du GIP ACYMA**
Dispositif Cybermalveillance.gouv.fr

2021 a une nouvelle fois été une année très prolifique pour Cybermalveillance.gouv.fr avec près de 2,5 millions de visiteurs sur notre plateforme. Une audience qui a doublé par rapport à 2020, confirmant l'intérêt des populations pour les services offerts et les nombreux contenus originaux produits à destination de tous les publics.

Cette année, notre dispositif et ses membres ont également œuvré pour que les entreprises, collectivités et associations soient mieux accompagnées dans leur cybersécurité afin de faire face à la professionnalisation et la complexité des cyberattaques. Parmi nos actions phares : le lancement officiel d'un service de sécurisation pour les professionnels par des prestataires labellisés ExpertCyber et la mise en place d'un programme de sensibilisation au profit des collectivités.

Enfin, si 2021 a été marquée par la continuité de la crise sanitaire, Cybermalveillance.gouv.fr a su s'adapter pour accompagner ses publics en multipliant ses interventions, aussi bien en présentiel qu'en distanciel, à l'occasion de partenariats, événements et opérations ponctuelles, dans le respect des règles sanitaires.

Ces résultats sont dus à la mobilisation active de nos 53 membres issus des secteurs public et privé, l'engagement des professionnels référencés et labellisés et l'implication des agents du GIP tout au long de l'année, et nous exhortent à continuer de développer nos services et nos actions au service de l'intérêt général.

* GIP ACYMA : Groupement d'Intérêt Public (GIP) Actions contre la cybermalveillance (ACYMA)

LES FAITS MARQUANTS 2021

LES FAITS MARQUANTS 2021

JANVIER

1er janvier : Avicca et la MACIF[1] rejoignent Cybermalveillance.gouv.fr

Communication du président de la République le 18 février 2021 dans le cadre de la Stratégie nationale pour la cybersécurité.

FÉVRIER

5 février : alerte faille de sécurité critique Google Chrome

11 février : lancement de la 2e étape du programme de sensibilisation aux risques numériques auprès des élus

18 février : lancement public du label ExpertCyber dans le cadre de la Stratégie nationale pour la cybersécurité présentée par le président de la République

25 février : alerte vagues de messages d'hameçonnage bancaire (DSP2)

MARS

3 mars : alerte vulnérabilités critiques Microsoft Exchange Server

4 mars : le ministère des Armées réaffirme son engagement au sein du GIP par la signature d'un protocole d'accord

9 mars : le ministère de l'Éducation nationale, de la Jeunesse et des Sports, Cisco, Club EBIOS et la SNCF rejoignent Cybermalveillance.gouv.fr

11 mars : alerte nouvelle campagne d'escroquerie aux faux kits de confinement gratuits de Santé publique France

AVRIL

15 avril : Cybermalveillance.gouv.fr publie son rapport d'activité et état de la menace 2020

Sortie d'un guide pratique pour les dirigeants de TPE-PME-ETI.

MAI

2 mai : alerte escroqueries à la loterie, en collaboration avec le groupe Française des jeux

11 mai : alerte failles de sécurité critique Apple

14 mai : alerte faille de sécurité critique Adobe Acrobat et Acrobat Reader

20 mai : Cybermalveillance.gouv.fr et Bpifrance publient un guide de cybersécurité dédié aux PME, TPE et ETI

27 mai : lancement de la 3e étape du programme de sensibilisation aux risques numériques auprès des élus

JUIN

9 juin : participation à l'événement Paris Cyber Week

10 juin : alerte failles de sécurité critiques Windows et Windows Server

23 juin : lancement d'une enquête sur la notoriété du dispositif Cybermalveillance.gouv.fr et la perception du risque numérique, en partenariat avec l'INC[2]

29 juin : Régions de France et Région Pays de la Loire rejoignent Cybermalveillance.gouv.fr

[1] MACIF : Mutuelle d'assurance des commerçants et industriels de France

[2] INC : Institut National de la Consommation

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

JUILLET/AOÛT

20 juillet : lancement du dispositif « Alerte Cyber » à l'attention des entreprises, par Cybermalveillance.gouv.fr, le MEDEF[3], l'ANSSI[4], la CPME[5] et U2P[6]
31 août : alerte vulnérabilités critiques Microsoft Exchange Server

NOVEMBRE

Lancement d'une campagne de sensibilisation à l'attention des entreprises et collectivités

8 novembre : lancement de l'étude quantitative auprès des petites collectivités de moins de 3 500 habitants sur leurs usages en matière de sécurité numérique
12 novembre : alerte vulnérabilité critique Microsoft Exchange Server
16 novembre : conférence en ligne « Protéger sa vie privée sans se priver d'Internet » co-organisée par Cybermalveillance.gouv.fr, AFCDP[10] et UFC-Que Choisir, en partenariat avec Clubic
16 novembre : diffusion d'une vidéo de Cédric O sur la nécessité de l'accompagnement des entreprises et collectivités pour faire face aux risques numériques
17 novembre : lancement de la campagne de sensibilisation « Face aux risques cyber, faites confiance à un véritable expert » dédié aux collectivités et aux entreprises
30 novembre : Alerte Cyber Microsoft Windows et Windows Server

SEPTEMBRE

6 septembre : le ministère de l'Intérieur dévoile le dispositif I.M.M.U.N.I.T.É.Cyber au profit des collectivités, porté par la Gendarmerie nationale et réalisé avec l'AMF[7] et Cybermalveillance.gouv.fr
6 septembre : diffusion d'une vidéo de présentation du label ExpertCyber par Cédric O, secrétaire d'État chargé de la Transition numérique et des Communications électroniques
du 7 au 9 septembre : participation au Forum International de la Cybersécurité (FIC) à Lille (13 000 participants)
du 28 au 30 septembre : participation au salon Expoprotection sécurité à Paris (plus de 6 400 visiteurs)
du 29 au 30 septembre : participation au salon IT Partners à Marne-la-Vallée (près de 8 000 participants)

DÉCEMBRE

17 décembre : Alerte Cyber vulnérabilité critique Apache Log4j

OCTOBRE

Cybermalveillance.gouv.fr est partenaire du mois européen de la cybersécurité « Cybermoi/s »

1er octobre : participation au lancement d'un CyberTour pour former les TPE et PME en partenariat avec Google, la FEVAD[8] et les CCI[9]
13 au 15 octobre : participation aux Assises de la cybersécurité à Monaco (plus de 1 200 invités)
14 octobre : alerte faille de sécurité critique Apple iOS et iPadOS
22 octobre : sortie officielle de l'édition spéciale des Incollables® « Deviens un super-héros du Net » réalisée conjointement par l'Association e-Enfance/3018 et Cybermalveillance.gouv.fr

25 octobre : diffusion de la campagne de sensibilisation TV Consomag réalisée en partenariat avec l'INC sur les chaînes du groupe France Télévisions

[3] MEDEF : Mouvement des entreprises de France
[4] ANSSI : Agence nationale de la sécurité des systèmes d'information
[5] CPME : Confédération des petites et moyennes entreprises
[6] U2P : Union des entreprises de proximité
[7] AMF : Association des Maires de France
[8] FEVAD : Fédération du e-commerce et de la vente à distance
[9] CCI : Chambre de commerce et d'industrie
[10] AFCDP : Association Française des Correspondants à la protection des Données à caractère Personnel

LES FAITS MARQUANTS 2021

FAIRE CONNAÎTRE LES MISSIONS DU DISPOSITIF AU PLUS GRAND NOMBRE,
L'UN DES ENJEUX DE CYBERMALVEILLANCE.GOUV.FR

Particuliers, entreprises, associations ou collectivités : tous sont exposés quotidiennement à des cyberattaques. Tout au long de l'année, Cybermalveillance.gouv.fr a orienté sa stratégie de communication vers la démultiplication et la diversification de ses actions et outils adressés à ces différents publics.

Multiplication des événements

Alors que la crise sanitaire avait bouleversé le calendrier et la tenue des événements en 2020, le dispositif s'est adapté et a renforcé ses actions de sensibilisation aussi bien lors de rendez-vous physiques qu'à distance. En 2021, Cybermalveillance.gouv.fr a participé à **120 événements externes ou organisés par le dispositif** et ses membres, tels que des salons, des conférences en ligne, des tables rondes, ou encore des interventions, dans le respect des règles sanitaires (voir page 33).

55
événements
en 2020

120
événements
en 2021

Des relations médias renforcées

Le dispositif a fait l'objet d'une importante couverture médiatique en 2021 par la presse écrite et télévisée, **avec 1929 retombées média.** Le lancement du label ExpertCyber (voir page 12), la multiplication des actions de sensibilisation menées avec les membres (voir page 26) et les alertes d'escroqueries et cyberattaques furent notamment les temps forts de relais dans les médias.

Journal télévisé diffusé sur la chaîne M6 – 7 septembre 2021

Journal télévisé diffusé sur la chaîne TF1 – 22 mars 2021

1031
retombées
média
en 2020

+87%

1929
retombées média
en 2021

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

Le développement des réseaux sociaux

Dès sa création, le dispositif Cybermalveillance.gouv.fr a utilisé les réseaux sociaux pour faire connaître son action et diffuser ses messages de prévention et d'assistance à ses publics. L'année 2021 a vu une croissance significative de son activité sur ses réseaux sociaux.

Stratégie de contenus

Tout au long de l'année, Cybermalveillance.gouv.fr a déployé et maintenu une stratégie de publication sur son site Internet, alternant contenus de fonds, contenus d'actualité et ressources sous différents formats. Cette stratégie de contenus est accompagnée par la lettre d'information adressée à tous les publics, et diffusée chaque mois à **plus de 28 000 abonnés en 2021**. Celle-ci vise à informer des nouvelles menaces, à dispenser les conseils pour s'en prémunir, à valoriser les actions de sensibilisation et initiatives menées avec les membres du dispositif ainsi qu'à relayer les alertes et actualités concernant les risques numériques.

FOCUS
Une notoriété croissante

En partenariat avec l'INC*, Cybermalveillance.gouv.fr a renouvelé en 2021 son étude de notoriété annuelle. Celle-ci vise à connaître l'exposition aux risques des internautes ainsi que le niveau de notoriété du dispositif auprès du grand public, pour mieux adapter ses outils et messages de prévention.

D'après l'étude, près de la moitié des répondants affirme ne pas savoir à qui s'adresser en cas de problème et ne peut citer de sites ou d'organismes pour les aider en cas de cybermalveillance. En revanche, 7 % des internautes ont mentionné spontanément Cybermalveillance.gouv.fr, ce qui indique une nette percée en comparaison des années précédentes.

En notoriété assistée, l'étude souligne également des résultats en progression : 51 % des répondants déclarent avoir entendu parler de Cybermalveillance.gouv.fr et 9 % d'entre eux ont utilisé le service. La première source de notoriété est la recherche sur Internet (29 %), suivie de la presse (16 %) puis des réseaux sociaux (13 %).

La croissance progressive de la notoriété du dispositif révélée dans cette étude se confirme également par la fréquentation de la plateforme en ligne, qui a doublé en un an, avec **près de 2,5 millions de visiteurs** (voir page 40).

* INC : Institut national de la consommation

LES PROJETS PHARES DE L'ANNÉE 2021

Lancement public du label ExpertCyber

Lancé en 2020 auprès des professionnels de la cybersécurité, le label ExpertCyber de Cybermalveillance.gouv.fr a été publiquement dévoilé le 18 février 2021, dans le cadre de la Stratégie nationale pour la cybersécurité présentée par le président de la République. À cette occasion, les 50 premiers prestataires labellisés ont été référencés sur la plateforme afin d'apporter un service immédiat au public professionnel.

Développé par Cybermalveillance.gouv.fr à l'issue d'un travail de réflexion avec les principaux syndicats professionnels du secteur (Fédération EBEN, CINOV Numérique, Numeum), France Assureurs et le soutien de l'AFNOR*, le label ExpertCyber permet d'offrir aux entreprises, collectivités et associations une meilleure lisibilité de la qualité des prestations et services en cybersécurité, avec un accompagnement dédié. Il vise également à reconnaître l'expertise des professionnels en cybersécurité assurant des **prestations de sécurisation, de maintenance et d'assistance en cas d'incident**.

Les professionnels en sécurité numérique sont au cœur du fonctionnement du dispositif Cybermalveillance.gouv.fr, notamment en ce qui concerne l'assistance aux victimes. Aux professionnels historiquement référencés sur la plateforme s'ajoutent désormais les professionnels labellisés ExpertCyber, dans une approche à la fois différente et complémentaire.

* AFNOR : Association française de normalisation

Mise à l'honneur des 50 premiers professionnels labellisés à l'occasion du lancement du label ExpertCyber.

Franck **GICQUEL**
Responsable des partenariats
Cybermalveillance.gouv.fr

« Le label ExpertCyber a été pensé pour toutes les entités justifiant d'une activité professionnelle, quel que soit leur secteur ou leur taille. Les prestataires labellisés ExpertCyber s'adressent ainsi à tous types de publics professionnels y compris les plus petites structures, tels que les TPE, PME et petites collectivités qui ne trouvent pas forcément des prestataires dimensionnés pour les accompagner sur des besoins plus modestes. »

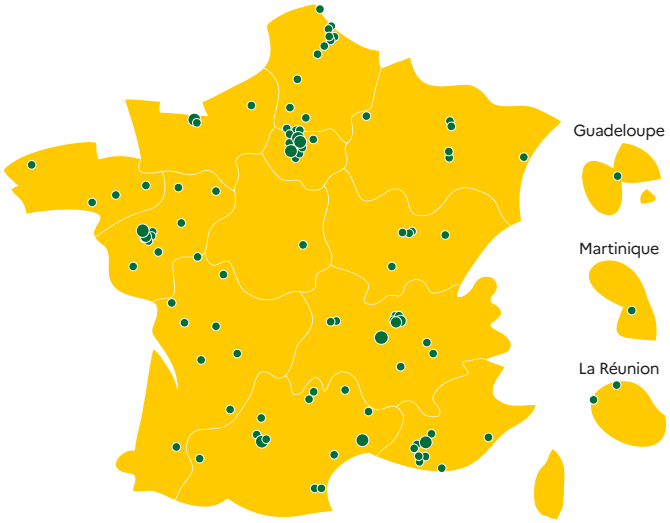
La mise en relation avec les professionnels labellisés ExpertCyber

Cybermalveillance.gouv.fr a créé sur sa plateforme un nouveau service dédié à la sécurisation des systèmes d'information en complément du diagnostic d'assistance aux victimes déjà existant. Cette nouvelle entrée permet aux publics professionnels de bénéficier d'une mise en relation avec un prestataire labellisé de proximité disposant des compétences pour répondre au besoin identifié, comme l'installation d'un nouveau système d'information, ou encore la sécurisation d'un système existant. Ce service est accessible à l'adresse suivante : **securisation.cybermalveillance.gouv.fr**

En parallèle, l'outil de diagnostic et d'assistance en ligne peut également offrir aux entreprises, collectivités et associations la possibilité d'être assistées par au moins un professionnel labellisé parmi les prestataires référencés pour venir en aide à la remédiation d'un incident.

En 2021, **161 entreprises de services informatiques** de toutes tailles ont été labellisées ExpertCyber sur l'ensemble du territoire national. Pour ce faire, les candidats ont dû justifier leurs compétences en cybersécurité dans le cadre d'un audit réalisé par l'AFNOR.

Si l'objectif initial consistait à valoriser des professionnels qui disposaient déjà du niveau d'expertise attendu, Cybermalveillance.gouv.fr accompagne désormais les prestataires dans leur montée en compétence en cybersécurité, pour obtenir la labellisation.



161 prestataires labellisés en 2021

LABELLISÉ ExpertCyber

Les nouveaux domaines de compétences couverts par les prestataires labellisés

- Poste de travail fixe
- Poste de travail nomade (ordinateur portable, tablette…)
- Serveur
- Site Internet
- Téléphonie fixe
- Téléphonie mobile
- Équipement de sécurité (antivirus, pare-feu, supervision…)
- Réseau
- Sauvegarde

Grâce aux prestataires labellisés, un nouveau service de sécurisation des systèmes d'information est désormais disponible sur Cybermalveillance.gouv.fr.

FOCUS

Lancement de la campagne de sensibilisation : « Face aux risques cyber, faites confiance à un véritable expert »

Pour poursuivre ses actions sur la mise en avant des labellisés et dans le cadre du volet cybersécurité du plan de relance dédié aux entreprises et collectivités, Cybermalveillance.gouv.fr a lancé le 17 novembre 2021 une campagne de sensibilisation à destination des professionnels : « Face aux risques cyber, faites confiance à un véritable expert ».

L'objectif de cette campagne est de faire connaître le label ExpertCyber au plus grand nombre afin de sensibiliser les professionnels à la nécessité de faire appel à des experts en cybersécurité pour se protéger efficacement et être correctement assistés en cas d'attaque.

Au travers d'une série de trois films et de déclinaisons des messages en infographies disponibles aux formats numériques et physiques, la campagne illustre sur un ton humoristique et décalé le quotidien de nombreuses entreprises et collectivités qui confient leur sécurité numérique à des entreprises ou des personnes de leur entourage qui ne sont pas nécessairement qualifiées pour cela.

Chacune des vidéos se conclut par l'adresse du service de mise en relation avec des prestataires labellisés ExpertCyber.

Le neveu.

Le jardinier.

La voyante.

Jérôme **NOTIN**
Directeur général de
Cybermalveillance.gouv.fr

> « Nous avons souhaité interpeller avec légèreté les publics professionnels afin de les inviter à s'interroger sur la façon dont est pris en compte ce sujet critique de la gestion de leur sécurité numérique, tout en leur faisant découvrir le label ExpertCyber pour les aider dans leur choix de prestataires. »

Une mobilisation active des membres

Les membres investis dans le groupe de travail dédié à la création du label ont pleinement contribué à la mise en place des premiers professionnels labellisés en 2020. En mobilisant leur réseau respectif, CINOV Numérique, la Fédération EBEN, France Assureurs et Numeum, avec le soutien de l'AFNOR, ont permis aux entreprises et collectivités de bénéficier d'une mise en relation avec un prestataire labellisé dès le lancement public d'ExpertCyber.

Cette mobilisation s'est poursuivie tout au long de l'année 2021, avec également Eset, Kaspersky et Microsoft France, avec pour objectif d'encourager de nouveaux prestataires à candidater au label. Le développement de ces actions a contribué à l'enrichissement du réseau des professionnels labellisés ExpertCyber, **passant ainsi de 50 à 161 prestataires**.

En parallèle, Cybermalveillance.gouv.fr a multiplié ses actions pour faire connaître le label auprès des bénéficiaires, avec l'accompagnement du MEDEF*, de la CPME** ou encore de CCI*** France, par le biais de conférences, webinaires ou encore interviews croisées avec un prestataire labellisé.

Interview croisée avec un prestataire labellisé ExpertCyber, réalisée par CCI France.

* MEDEF : Mouvement des entreprises de France
** CPME : Confédération des petites et moyennes entreprises
*** CCI : Chambre de Commerce et d'Industrie

Soutien au label

Le secrétaire d'État chargé de la Transition numérique et des Communications électroniques Cédric O a témoigné son soutien au label ExpertCyber à travers deux vidéos diffusées les 6 septembre et 16 novembre 2021, à la veille du salon du FIC* puis à l'occasion du lancement de la campagne de sensibilisation. Cédric O y présente le label ExpertCyber et explique l'importance pour les professionnels d'être accompagnés par des prestataires de confiance pour faire face aux risques numériques.

* FIC : Forum international de la cybersécurité

En communiquant le plus largement possible sur le label ExpertCyber, les prestataires labellisés voient leur expertise en cybersécurité valorisée. Ils peuvent ainsi offrir aux entreprises et collectivités une meilleure lisibilité de la qualité de leur offre de services.

Pour plus d'information : **www.expertcyber.fr**

LES PROJETS PHARES DE L'ANNÉE 2021

Les collectivités au cœur des actions de sensibilisation

Les cyberattaques sont une réelle menace pour les collectivités territoriales. Si certaines communes ont pris conscience des risques, elles sont encore trop peu à les anticiper. Afin d'aider les élus à prendre en considération ces enjeux, Cybermalveillance.gouv.fr a mené avec ses membres plusieurs actions de prévention et de sensibilisation au cours de l'année 2021.

Nouvelles étapes du programme de sensibilisation des élus

En 2020, Cybermalveillance.gouv.fr a initié un groupe de travail avec le concours de la Banque des Territoires, la fédération Déclic, CoTer Numérique, l'ANSSI* et le ministère de l'Intérieur, dans le but de mener des travaux destinés à interpeller les élus sur la cybersécurité. C'est dans ce contexte que le programme de sensibilisation aux risques numériques avait été lancé, dont la première étape avait été dévoilée à l'automne 2020.

L'arrivée d'Avicca puis de Régions de France et la Région des Pays de la Loire en 2021 dans le groupe de travail dédié aux collectivités a permis de poursuivre les actions auprès de ces publics. Dans la seconde étape de ce programme, dévoilée en février 2021, Cybermalveillance.gouv.fr a publié le témoignage de deux communes victimes de cyberattaques, et dispensé ses conseils sur les bonnes pratiques à adopter en cybersécurité. En mai, une nouvelle étape mettait à l'honneur six collectivités ayant entrepris des actions de sensibilisation aux risques numériques.

Ce programme a été largement relayé par des prescripteurs (associations, syndicats, médias…) qui ont accepté de s'associer étroitement à cette initiative.

*ANSSI : Agence nationale de la sécurité des systèmes d'information

Des ressources spécifiques pour les collectivités

En complément de ces étapes, Cybermalveillance.gouv.fr et les membres impliqués dans le groupe de travail ont également travaillé à la mise en œuvre de nouvelles ressources adaptées aux enjeux des collectivités. À l'automne 2021, le dispositif dévoilait une fiche A4 et une infographie sous forme d'affiche au format A3 listant les actions essentielles à mener en cas de cyberattaque, depuis les premiers réflexes jusqu'à la sortie de la crise. D'autres supports, déployés en parallèle du programme, sont venus compléter la liste des ressources dédiées à ces publics, à l'instar d'I.M.M.U.N.I.T.É.Cyber, un auto-diagnostic simplifié au profit des élus (voir page 27).

Amandine **DEL-AMO**
Chargée des partenariats
Cybermalveillance.gouv.fr

« Durant la crise sanitaire, les collectivités ont connu une hausse significative de cyberattaques, il était donc essentiel de développer notre action de sensibilisation avec des outils et des messages adaptés à ces publics. Nous avons la chance d'être soutenu par des membres pleinement investis au sein du groupe de travail « Collectivités », que nous remercions vivement pour leur implication dans ce projet. »

Campagne de sensibilisation interrégionale

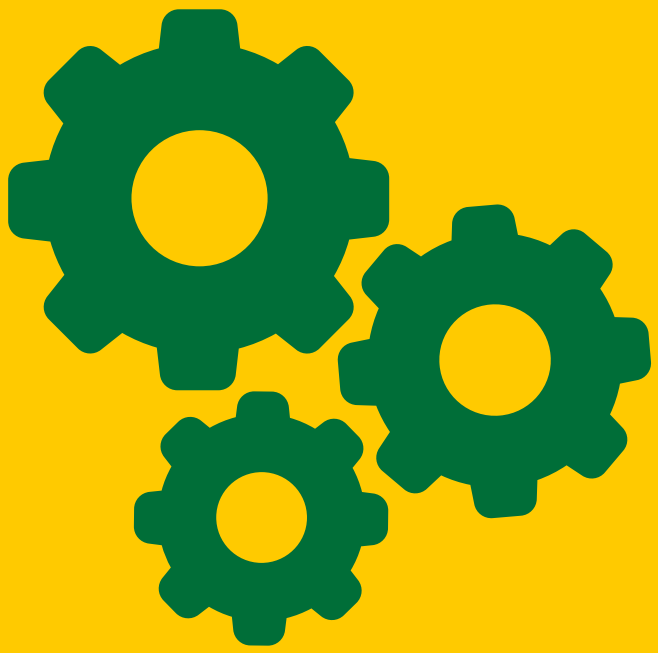
Avec le soutien de Cybermalveillance.gouv.fr, les directions des systèmes d'information (DSI) des dix-huit régions ont entrepris une campagne de sensibilisation des élus lors des élections régionales et départementales en juin 2021. Plusieurs contenus du dispositif ont ainsi été adaptés pour répondre aux problématiques des collectivités : trois mémos synthétiques et trois fiches détaillées relatifs à la gestion des mots de passe, aux usages élus / professionnels / personnels et au risque d'hameçonnage. Ces supports ont ensuite été diffusés aux nouveaux élus.

Région Normandie.

Région Centre-Val de Loire.

UNE ENQUÊTE AUTOUR DES RISQUES NUMÉRIQUES

Afin de sensibiliser les élus à la sécurité numérique, une enquête financée dans le cadre du volet cybersécurité du plan de relance a été lancée au cours de l'année 2021. Adressé aux collectivités de moins de 3500 habitants, ce sondage doit permettre de mieux comprendre les usages en matière de cybersécurité des petites communes et d'identifier les risques dans ce type de structures afin de leur apporter des réponses pertinentes et concrètes.



MISSIONS ET ORGANISATION DU GIP

MISSIONS ET ORGANISATION DU GIP

PRÉSENTATION DU DISPOSITIF

Piloté par le Groupement d'intérêt public (GIP) ACYMA, le dispositif Cybermalveillance.gouv.fr s'adresse aux particuliers, aux associations, aux entreprises et collectivités territoriales (hors opérateurs d'importance vitale et opérateurs de services essentiels). Ses missions sont :

1

L'ASSISTANCE AUX VICTIMES D'ACTES DE CYBERMALVEILLANCE
avec, notamment, la mise en relation avec des professionnels de proximité susceptibles de les assister.

2

LA PRÉVENTION ET LA SENSIBILISATION DES PUBLICS SUR LA CYBERSÉCURITÉ
au travers de contenus et de campagnes.

3

L'OBSERVATION DU RISQUE NUMÉRIQUE
pour mieux l'anticiper et y réagir.

DATES CLÉS DE LA CRÉATION DU GIP

16 octobre 2015

Annonce dans la **STRATÉGIE NATIONALE POUR LA SÉCURITÉ DU NUMÉRIQUE** par le Premier ministre de la création d'un dispositif répondant au besoin des populations : *« Le dispositif adoptera une forme juridique et une organisation lui permettant de bénéficier de l'apport des acteurs économiques du secteur de la cybersécurité (éditeurs de logiciels, plates-formes numériques, fournisseurs de solutions). Grâce aux technologies mises en œuvre, le dispositif devra proposer aux victimes des solutions techniques s'appuyant sur des acteurs de proximité et faciliter les démarches administratives, notamment afin de favoriser le dépôt de plainte. »*

2016-2017

INCUBATION PAR L'ANSSI
en copilotage avec le ministère de l'Intérieur, et le soutien des ministères de la Justice, de l'Économie et des Finances et du secrétariat d'État chargé du Numérique

3 mars 2017

CRÉATION DU GROUPEMENT D'INTÉRÊT PUBLIC POUR LE DISPOSITIF NATIONAL D'ASSISTANCE AUX VICTIMES D'ACTES DE CYBERMALVEILLANCE
(GIP ACYMA – Actions contre la cybermalveillance - NOR : PRMD1704935A).

17 octobre 2017

LANCEMENT NATIONAL DE LA PLATEFORME CYBERMALVEILLANCE.GOUV.FR

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

GOUVERNANCE ET ORGANISATION DU GIP

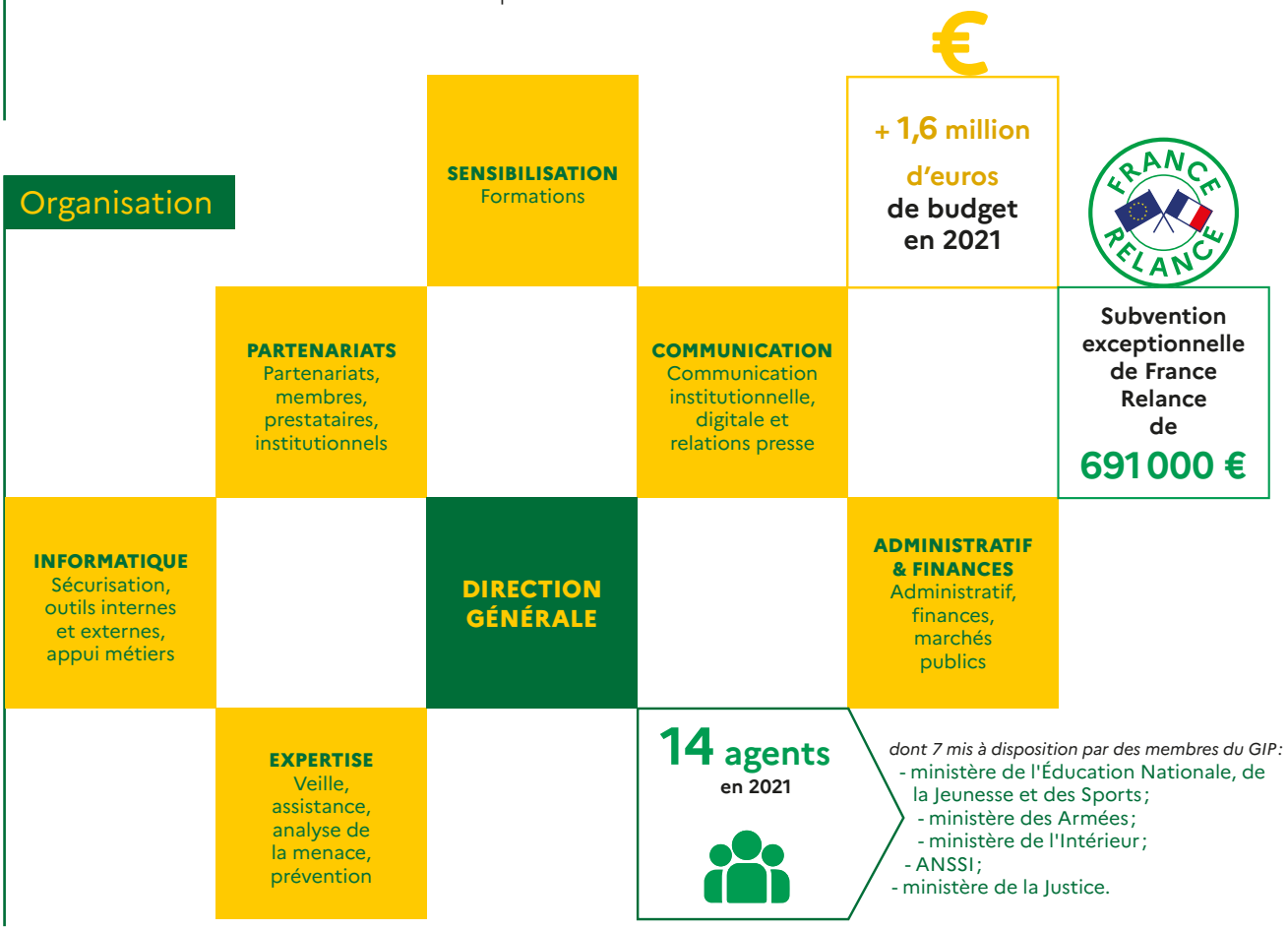
Gouvernance

Le GIP ACYMA est composé de **53 MEMBRES**, d'un président du Conseil d'administration et d'un directeur général. Les membres sont répartis en quatre collèges représentant l'ensemble de l'écosystème :

- **Les étatiques** : ministères et secrétariat d'État ;
- **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



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 portant sur l'assistance aux particuliers, aux entreprises 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 reprise d'activité d'équipement(s) informatique(s) 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.

MISSIONS ET ORGANISATION DU GIP

LES MEMBRES DU GIP

Les membres de Cybermalveillance.gouv.fr sont des organismes privés et publics qui ont souhaité s'engager dans l'action du dispositif et contribuer à l'accomplissement de ses missions. En participant aux travaux du dispositif, ces membres témoignent de leur implication sur le sujet de la sécurité numérique auprès du public.

PREMIER MINISTRE

MINISTÈRE DE L'ÉDUCATION NATIONALE, DE LA JEUNESSE ET DES SPORTS

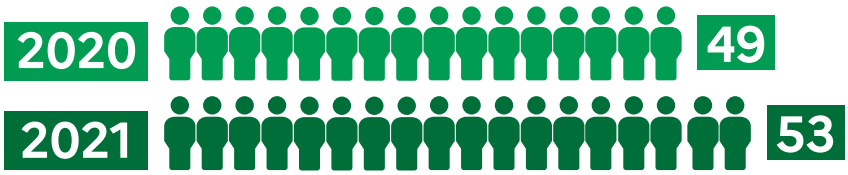
MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA RELANCE

MINISTÈRE DES ARMÉES

MINISTÈRE DE L'INTÉRIEUR

MINISTÈRE DE LA JUSTICE

SECRÉTARIAT D'ÉTAT CHARGÉ DE LA TRANSITION NUMÉRIQUE ET DES COMMUNICATIONS ÉLECTRONIQUES



LES NOUVEAUX MEMBRES EN 2021

Collège étatique : MINISTÈRE DE L'ÉDUCATION NATIONALE, DE LA JEUNESSE ET DES SPORTS

Collège utilisateurs : avicca, CLUBEBIOS, RÉGIONS DE FRANCE, Région PAYS DE LA LOIRE

Collège offreurs de solutions et services : MACIF, SNCF, CISCO

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

PAROLES DE MEMBRES

« L'engagement du ministère au sein du dispositif Cybermalveillance.gouv.fr constitue une avancée importante. En 2021, la généralisation du programme PHARe, le renforcement de l'éducation aux médias et à l'information et le développement des compétences numériques permettent de garantir à chaque élève un environnement numérique sûr et de confiance et qui trouvent un prolongement concret dans le dispositif Cybermalveillance.gouv.fr. »

Jean-Michel BLANQUER
Ministre de l'Éducation Nationale, de la Jeunesse et des Sports

« Dans un contexte d'aggravation de la menace cyber, Cybermalveillance.gouv.fr est un partenaire incontournable pour accompagner les entreprises. Cybermalveillance.gouv.fr offre une capacité inédite d'agir en écosystème : le MEDEF se félicite de la création aux côtés du GIP ACYMA de l'Alerte Cyber. »

Christian POYAU
Coprésident de la Commission Mutations Technologiques et Impacts Sociétaux du Mouvement des Entreprises de France

« Protéger nos systèmes d'informations, c'est protéger nos trains, nos matériels, nos agents et bien sûr nos clients. La Cybersécurité est un élément indispensable des fondamentaux du groupe SNCF. Aussi, face à l'augmentation constante des cybermenaces touchant tant nos vies personnelles et professionnelles, rejoindre le GIP ACYMA, c'est pour nous la volonté de pouvoir contribuer concrètement aux actions de sensibilisation aux risques cyber. »

Gilles BERTHELOT
Directeur sécurité numérique du groupe SNCF

« La Région des Pays de la Loire est la première Région française à avoir rejoint dès 2021 Cybermalveillance.gouv.fr. C'est un acte fort qui témoigne notre volonté d'accompagner nos entreprises à renforcer leur sécurité numérique en s'appuyant sur une communauté de compétences reconnue. »

Christelle MORANÇAIS
Présidente du conseil régional des Pays de la Loire

« La cybersécurité est l'affaire de tous et c'est un enjeu de société : une entreprise sur deux n'a pas de politique cyber et les trois quarts sont persuadées de ne pas pouvoir y faire face. Au-delà de notre expertise technologique, il est de la responsabilité de Cisco d'accompagner le plus grand nombre d'organisations publiques et privées aux côtés de Cybermalveillance.gouv.fr. »

Laurent DEGRÉ
Président de Cisco France

« Cybermalveillance.gouv.fr est incontournable en matière d'assistance aux victimes et de sensibilisation des publics. Numeum, en tant que membre fondateur, est fier de contribuer à ces missions depuis sa création. La cybersécurité constitue un axe stratégique pour tous dans le cadre de la construction d'un espace numérique de confiance. »

Godefroy DE BENTZMANN et Pierre-Marie LEHUCHER
Coprésidents de Numeum

UN PARTENARIAT PUBLIC-PRIVÉ AU SERVICE D'UNE MISSION D'INTÉRÊT GÉNÉRAL

UN PARTENARIAT PUBLIC-PRIVÉ
AU SERVICE D'UNE MISSION D'INTÉRÊT GÉNÉRAL

EXEMPLES DE COLLABORATIONS EN 2021

Original et efficace, le partenariat public-privé du GIP regroupe des acteurs de l'État, tels que l'ANSSI, différents ministères, ainsi que des membres privés. Le dispositif noue également des partenariats plus spécifiques pour des opérations ponctuelles afin de développer des actions ciblées auprès des différents publics.

Association e-Enfance/3018 : une édition spéciale des Incollables® sur la cybersécurité

Pour aider les parents à sensibiliser leurs enfants aux dangers d'Internet, l'Association e-Enfance/3018 et Cybermalveillance.gouv.fr ont réalisé une édition spéciale des Incollables® « Deviens un super-héros du Net ».

Destiné aux classes de primaire et aux parents voulant jouer avec leurs enfants, le jeu éducatif regroupe 84 questions-réponses ludiques avec différents niveaux de difficulté pour tester ses connaissances sur les usages numériques, la sécurité en ligne, les dangers potentiels et les bons réflexes à adopter. Cette édition a été présentée en avant-première au salon du FIC le 7 septembre 2021 par Jérôme NOTIN et Justine ATLAN, directrice générale de l'Association e-Enfance et du 3018.

Créée avec le soutien de Google.org, une version interactive est également disponible sur le site Internet de l'éditeur Play Bac.

Présentation en avant-première de l'édition spéciale des Incollables au salon du FIC par Jérôme Notin et Justine Atlan à Lille.

Lancement d'une tournée de sensibilisation et de formation des entreprises par Google France

À l'occasion du mois européen de la cybersécurité (Cybermoi/s), Google France a lancé le CyberTour, une tournée de sensibilisation et de formation des entreprises à travers 11 villes de France, avec Cybermalveillance.gouv.fr, la FEVAD* et de nombreuses CCI.

Dans la continuité du programme de formation lancé en octobre 2020, CyberTour visait à sensibiliser les TPE et PME françaises aux menaces auxquelles elles sont confrontées en ligne et leur donner des conseils et des outils-clés pour guider leur stratégie de cybersécurité.

Un cours en ligne gratuit regroupant les modules de formations dispensés au sein des Google Ateliers Numériques venait également compléter cette initiative, pour permettre d'identifier les principales menaces cyber et apprendre à s'en protéger grâce à des méthodes, des outils et des conseils pratiques. Ce programme de formation, créé en partenariat avec Cybermalveillance.gouv.fr et la FEVAD, s'adressait prioritairement aux salariés et dirigeants de TPE-PME, aux commerces de proximité et aux petites entreprises de services.

* FEVAD : Fédération du e-commerce et de la vente à distance

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

La sensibilisation des entreprises à la cybersécurité avec Ma PME Numérique de Microsoft France

La plateforme Ma PME Numérique, pilotée par Microsoft France, a mis à disposition un cours en ligne pour sensibiliser les entreprises aux risques de cybermenaces et aux bonnes pratiques en partenariat avec Cybermalveillance.gouv.fr.

Lancée en juin 2021, Ma PME Numérique est une initiative destinée à apporter des solutions concrètes aux enjeux de reprise économique des TPE et PME. Alors que les entreprises ont été particulièrement impactées par les actes de cybermalveillance depuis le début de la crise sanitaire, la formation vise à informer les professionnels sur des enjeux de la cybersécurité, et les sensibiliser sur les risques cyber et les bonnes pratiques à adopter pour s'en prémunir.

Le cours en ligne se compose de deux modules, et permet notamment de bénéficier des contenus de sensibilisation de Cybermalveillance.gouv.fr.

Lancement du dispositif « Alerte Cyber » avec le MEDEF, l'ANSSI, la CPME et l'U2P

Afin de protéger les entreprises de campagnes de cyberattaques massives, un nouveau dispositif d'alerte de cybersécurité a été mis en place dès juillet 2021.

En détaillant la nature de la menace et les risques pour l'entreprise, les alertes permettent à chaque société d'être informée à temps et prendre ainsi les décisions les mieux adaptées pour se protéger ou gérer une crise.

Le dispositif Alerte Cyber a été élaboré par Cybermalveillance.gouv.fr, le MEDEF et l'ANSSI. En pratique, la diffusion des alertes est notamment prise en charge par la CPME, l'U2P*, le MEDEF, les réseaux consulaires des CCI et des CMA** auprès de leurs très nombreux adhérents, ainsi que par le portail public France Num qui accompagne la transformation numérique des petites entreprises.

3 Alertes Cyber

diffusées en 2021


ALERTE CYBERSÉCURITÉ

Faille de sécurité critique dans plusieurs produits Apple

Date de l'alerte : 14 octobre 2021

Risques

Description

Systèmes concernés

Mesure à prendre

Procédure

Besoin d'assistance ?

RÉPUBLIQUE FRANÇAISE

Exemple de notice d'alerte envoyée aux bénéficiaires

* U2P : Union des entreprises de proximité
** CMA : Chambres de Métiers et de l'Artisanat

UN PARTENARIAT PUBLIC-PRIVÉ
AU SERVICE D'UNE MISSION D'INTÉRÊT GÉNÉRAL

FOCUS

Un guide pratique pour les dirigeants de TPE-PME-ETI

Dans l'intérêt commun d'accompagner les entreprises face aux risques croissants de cyberattaques, Cybermalveillance.gouv.fr s'est associé en 2021 à Bpifrance, filiale du groupe Caisse des Dépôts qui figure parmi les membres du dispositif. Cette collaboration s'est concrétisée par la réalisation d'un guide pratique et pédagogique dédié aux TPE, PME et ETI, publié le 20 mai.

Ce guide présente les enjeux de la cybersécurité, décrit les principales menaces de manière détaillée et donne également des recommandations préventives concrètes ainsi qu'un plan d'action à activer en cas d'attaque. Des témoignages d'entrepreneurs et des récits de victimes de cyberattaques complètent cette publication.

Le guide a été imprimé grâce au soutien du ministère des Armées et distribué lors des événements auxquels le dispositif a participé.

Pascal **LAGARDE**
Directeur exécutif en charge de l'International, de la Stratégie, des Études et du Développement de Bpifrance

> "Jusqu'alors les entreprises restaient vulnérables face à des cybercriminels très bien préparés et organisés, notamment les PME qui disposent de moyens limités pour faire face à ces attaques. Nous sommes à leurs côtés pour les accompagner au travers d'outils simples et faciles d'accès qui leur permettront de s'armer et de renforcer leur niveau de maturité en cybersécurité."

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

I.M.M.U.N.I.T.É.Cyber : un questionnaire pour sensibiliser les élus à la cybersécurité

En partenariat étroit avec l'AMF*, la Gendarmerie nationale a mis en place avec Cybermalveillance.gouv.fr une offre de diagnostic simplifié au profit des collectivités.

Reposant sur neuf questions simples couvertes par l'acronyme I.M.M.U.N.I.T.É.Cyber, l'objectif est de sensibiliser les élus aux enjeux de la cybersécurité en les aidant à mieux appréhender les risques qu'ils encourent. Le projet leur permet ainsi d'auto-évaluer leur capacité à se prémunir et à réagir à une cyberattaque, en leur proposant si nécessaire un accompagnement.

Adressé par l'AMF à ses adhérents début septembre 2021, le formulaire I.M.M.U.N.I.T.É.Cyber s'ajoute à la liste des ressources mises à disposition par Cybermalveillance.gouv.fr et ses membres dans le cadre du programme de sensibilisation des élus aux risques numériques (voir page 16).

* AMF : Association des maires de France

Marc **BOGET**
Général de division, commandant de la gendarmerie dans le cyberespace

> « S'appuyant sur une infographie simple et accessible à tous, l'outil de diagnostic I.M.M.U.N.I.T.É.Cyber vise à aider les élus dans l'évaluation des faiblesses potentielles de leurs infrastructures numériques. Développé par le COMCYBERGEND fidèle à la volonté de la Gendarmerie nationale de #RépondrePrésent et en lien étroit avec l'AMF et le dispositif Cybermalveillance.gouv.fr, il permet d'avoir une démarche proactive face aux cybermenaces dont les collectivités territoriales sont régulièrement victimes. »

Auto-diagnostic envoyé à
à l'ensemble des collectivités
par l'AMF

Présentation de I.M.M.U.N.I.T.É.Cyber au salon du FIC par le général BOGET, auprès de Cédric O, secrétaire d'État chargé de la Transition numérique et des Communications électroniques.

LA SENSIBILISATION
PREMIÈRE ARME
CONTRE LES CYBERMALVEILLANCES

SENSIBILISATION ET ÉVÉNEMENTS

Prévenir les populations des risques liés à la cybermalveillance et favoriser les bonnes pratiques à mettre en œuvre constituent l'une des missions du dispositif Cybermalveillance.gouv.fr. Outre la production en propre de contenus de sensibilisation et la contribution aux contenus produits en collaboration avec ses membres et d'autres partenaires, Cybermalveillance.gouv.fr a participé ou lancé en 2021 diverses actions destinées à tous les publics.

Tous publics

Une conférence en ligne sur la protection des données sur Internet

Le 16 novembre 2021 s'est tenue une conférence en ligne intitulée « Comment protéger sa vie privée sans se priver d'Internet ? », coorganisée par Cybermalveillance.gouv.fr, AFCDP* et UFC-Que Choisir.

La table ronde centrée sur la prévention des risques cyber a permis aux experts présents d'expliquer les enjeux et les bons réflexes à adopter pour renforcer sa cybersécurité.

Animée par le journaliste Olivier Bouzereau, et en partenariat média avec Clubic, la conférence était accessible à tous et diffusée en direct. L'événement a comptabilisé 1192 participants, avec un taux de satisfaction de 88 % sur la qualité des contenus et des intervenants.

Conférence en ligne du 16 novembre 2021 coorganisée par Cybermalveillance.gouv.fr, AFCDP et UFC-Que Choisir.

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

Participation au CYBERMOI/S 2021 : toutes les clés pour protéger son identité numérique

La campagne de sensibilisation du Cybermoi/s pilotée par l'ANSSI en octobre 2021 a prodigué aux professionnels et aux particuliers les bonnes pratiques pour gérer leurs mots de passe, indispensables pour sécuriser les comptes en ligne. Si le dispositif s'est appuyé sur ses membres pour démultiplier ses actions de sensibilisation, il a aussi apporté sa contribution active, notamment en sensibilisant sur les cybermenaces liées à l'identité numérique :

- **Une campagne d'information** tout au long du mois d'octobre sur les réseaux sociaux et le site Internet www.cybermalveillance.gouv.fr avec la publication d'articles de prévention et de sensibilisation, en particulier autour de l'identité numérique (usurpation d'identité, hameçonnage, etc.) ;
- **La mise à disposition de nombreuses ressources** à destination des professionnels et du grand public sur le site dédié à l'événement Cybermoi/s ;
- **Une campagne médias auprès des consommateurs, en partenariat avec l'INC sur les chaînes du groupe France Télévisions** et de nombreux médias en ligne, du 25 octobre au 13 novembre 2021 (lire page 34).

Professionnels

Alors que la crise sanitaire avait bouleversé le calendrier et la tenue des événements en 2020, le dispositif s'est adapté et a renforcé ses actions de sensibilisation auprès de ses publics aussi bien lors de rendez-vous physiques qu'en ligne. Durant l'année écoulée, Cybermalveillance.gouv.fr a participé à 120 événements externes ou organisés par le dispositif et ses membres, dans le respect des règles sanitaires. Salons, conférences en ligne ou tables rondes, la multiplication des interventions principalement adressées aux professionnels est notamment due à l'implication active des membres du dispositif qui contribuent au relais des missions de sensibilisation et de prévention de Cybermalveillance.gouv.fr.

Cybermalveillance.gouv.fr a eu l'opportunité de prendre part aux nombreux événements organisés par les membres en 2021:
Le ministère de l'Éducation nationale, de la Jeunesse et des Sports, le Ministère de l'Économie, des Finances et de la Relance, le ministère des Armées, le ministère de l'Intérieur, ANSSI, le secrétariat d'Etat chargé de la Transition numérique et des Communications électroniques, AFNIC, Avicca, réseau des CCI, CoTer Numérique, CPME, FEVAD, France Victimes, Harmonie Technologie, Neuflize OBC, La Poste Groupe, Régions de France, SNCF.

Rencontres Cybersécurité d'Occitanie à Toulouse.

Intervention aux webinaires de Foliweb organisés par l'AFNIC.

Cybermalveillance.gouv.fr a participé à divers événements et salons en lien avec son écosystème professionnel. En 2021, le dispositif a été présent sur quatre salons majeurs dans les domaines de l'informatique et de la cybersécurité :

- **Le Forum International de la Cybersécurité (FIC)** à Lille (13 000 visiteurs) ;
- **IT Partners** à Marne-la-Vallée (près de 8 000 participants) ;
- **Les Assises de la Cybersécurité** à Monaco (plus de 1 200 invités) ;
- **Expoprotection Sécurité** à Paris (plus de 6 400 visiteurs).

Forum International de la Cybersécurité (FIC) à Lille.

Visite du stand de Cybermalveillance.gouv.fr aux Assises de la Cybersécurité, avec notamment les députés Anissa KHEDHER, Philippe LATOMBE et Valéria FAURE-MUNTIAN, et Mauna TRAIKIA, conseillère territoriale en charge du développement numérique de Plaine Commune (métropole du Grand Paris, Seine-Saint-Denis).

Tour de France Cyber

Cybermalveillance.gouv.fr était une nouvelle fois partenaire du Tour de France de la Cybersécurité (TDFCyber) 2021 organisé par le CyberCercle. À travers ses étapes en région, le TDFCyber a pour vocation de porter les sujets de sécurité et de confiance numériques au plus près des acteurs présents sur les territoires, tels que les secteurs public et privé, élus, spécialistes de la cybersécurité nationaux, européens et locaux, associations, collectivités, etc.

Paris Cyber Week (PCW)

Cybermalveillance.gouv.fr a été partenaire de l'édition 2021 de PCW. Cet événement, qui s'est déroulé les 8 et 9 juin, a rassemblé les acteurs du numérique autour des filières industrielles, créant ainsi une communauté d'experts capable de proposer une vision prospective et d'aider les décideurs à anticiper la dimension stratégique de la transformation numérique, dans un environnement de confiance et de sécurité. Cette année, PCW a réuni 150 décideurs publics et privés en provenance de 13 pays européens.

LA SENSIBILISATION
PREMIÈRE ARME CONTRE LES CYBERMALVEILLANCES

Campagne nationale d'information et de sensibilisation « Consomag »

Afin d'améliorer la sécurité numérique des consommateurs et dans le cadre du mois européen de la cybersécurité, Cybermalveillance.gouv.fr a renouvelé son partenariat avec l'INC pour le lancement d'une campagne sur les risques numériques, composée d'une série de quatre émissions Consomag thématiques au format questions-réponses d'experts. Cette campagne a été diffusée sur les chaînes du groupe France Télévisions du 25 octobre au 13 novembre 2021, ainsi que sur les réseaux sociaux, la lettre d'information de l'INC et la plateforme de France Télévisions.

1,5 million
de téléspectateurs par programme Consomag

Comment reconnaître un message de phishing ?

Pourquoi et comment sécuriser sa messagerie ?

Pourquoi et comment sécuriser ses objets connectés ?

Comment réagir en cas d'arnaque au faux support technique ?

Les vidéos sont disponibles sur
www.cybermalveillance.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

Contenus de prévention et d'assistance publiés sur la plateforme

Pour aider les publics à assurer leur cybersécurité, savoir comment réagir en cas de cyberattaques et faire face aux escroqueries en ligne, le dispositif Cybermalveillance.gouv.fr met à disposition des particuliers et professionnels des contenus de prévention et de sensibilisation aux risques numériques.

Nouveaux supports thématiques

Dans la continuité des années précédentes, Cybermalveillance.gouv.fr a continué d'enrichir ses contenus existants et conçu de nouveaux supports originaux sur des thématiques encore non couvertes. Scindés en trois catégories pour une meilleure appropriation par les publics particuliers et professionnels, ces contenus prennent la forme d'articles thématiques :

- sur les **bonnes pratiques à adopter en matière de cybersécurité** : généralement présentés en 10 points, les conseils donnés, en termes simples et pédagogiques, offrent au lecteur les règles de base de sécurité numérique essentielles à appliquer sur le domaine abordé ;
- sur les **grandes catégories de menaces** pour les comprendre et savoir y faire face : présentés sous la forme de fiches « réflexes » ces articles et supports à vocation très opérationnelle prodiguent les conseils utiles pour s'en prémunir et les affronter en cas d'attaque. Un volet infractionnel est également indiqué pour faciliter le dépôt de plainte des victimes auprès des autorités.
- sur les **menaces d'actualités ou émergentes**, qui décrivent et illustrent les phénomènes en dispensant les conseils nécessaires pour les contenir. Dans ce cadre, un dossier complet a par exemple été réalisé en 2021 sur les principales formes d'hameçonnage (Impôts, Assurance maladie, banques, loteries, livraison de colis, fausses commandes, etc.).

98,25 %
de satisfaction en 2021

Ces différents supports visent à couvrir le plus largement possible les principaux sujets sur la cybersécurité et les cybermenaces en réponse aux préoccupations remontées par les publics du dispositif tant à titre personnel que professionnel. Ces contenus thématiques de prévention et d'assistance ont reçu un **taux de satisfaction de 98,25 %** de la part des utilisateurs de la plateforme en 2021, signe qu'ils correspondent à une réelle attente des publics.

Sept nouvelles fiches ont été publiées sur le site Internet en 2021 :

1. Les 10 mesures essentielles pour assurer votre cybersécurité
2. Les faux ordres de virement bancaire ou FOVI
3. La sécurisation des sites Internet
4. Les virus informatiques
5. Le piratage d'un système informatique
6. Les antivirus
7. L'usurpation d'identité

20 articles de prévention et d'assistance ont été publiés sur le site Internet en 2021. Quelques exemples :

- Comment trouver un professionnel qualifié ?
- L'hameçonnage aux couleurs de l'Assurance Maladie
- Les escroqueries à la livraison de colis
- Comment signaler un mail d'hameçonnage ?
- Recrudescence de l'hameçonnage bancaire (DSP2)

27 nouveaux contenus de prévention et d'assistance

L'ASSISTANCE AUX VICTIMES

UN BESOIN
UNE NÉCESSITÉ

L'ASSISTANCE AUX VICTIMES, UN BESOIN, UNE NÉCESSITÉ

AMÉLIORATION CONTINUE
DE LA PLATEFORME WWW.CYBERMALVEILLANCE.GOUV.FR

Si l'année 2020 fut portée sur la conception de nouvelles fonctionnalités pour l'utilisateur, 2021 a été davantage consacré à l'optimisation de la plateforme www.cybermalveillance.gouv.fr. Grâce à un travail d'analyse approfondi, Cybermalveillance.gouv.fr a pu améliorer le service d'assistance aux victimes, et mettre en place le parcours de mise en relation avec des prestataires labellisés pour accompagner les professionnels dans la sécurisation de leur système d'information.

Optimisation des services proposés

Grâce à l'exploitation des données et les retours d'expérience, le dispositif a pu œuvrer tout au long de l'année 2021 à l'optimisation de la plateforme www.cybermalveillance.gouv.fr, et plus particulièrement à l'amélioration de l'expérience du point de vue des professionnels référencés. Dans cette optique, Cybermalveillance.gouv.fr a réalisé fin 2020 une enquête adressée aux professionnels référencés afin de connaître leur niveau de satisfaction sur la plateforme, ses outils et ses services, et mieux identifier leurs besoins et attentes. Pour y répondre, le dispositif a mené de nombreuses évolutions de la plateforme.

Les axes de travail ont principalement porté sur **l'amélioration de la qualité de la mise en relation avec les victimes.** Parmi les actions instaurées : l'activation du compte victime rendue obligatoire, l'accès pour le professionnel référencé au suivi des actions réalisées par la victime ou encore la mise en place de relances auprès de la victime si aucune action n'est détectée de sa part. L'espace personnel des prestataires a également été optimisé pour que ces derniers puissent davantage s'approprier la plateforme. Une réflexion permettant entre autres une amélioration au niveau de l'ergonomie globale, des fonctionnalités dans le suivi et la gestion de leur intervention et dans l'accès à l'information et sa diffusion dans leur espace documentaire.

Concernant les victimes, l'expérience est également placée au cœur des préoccupations. Le dispositif a en effet mis en place différents outils de mesure, notamment de satisfaction, afin d'améliorer le service proposé et mieux appréhender leurs besoins, ce qui a entraîné une première refonte de l'ergonomie du parcours d'assistance.

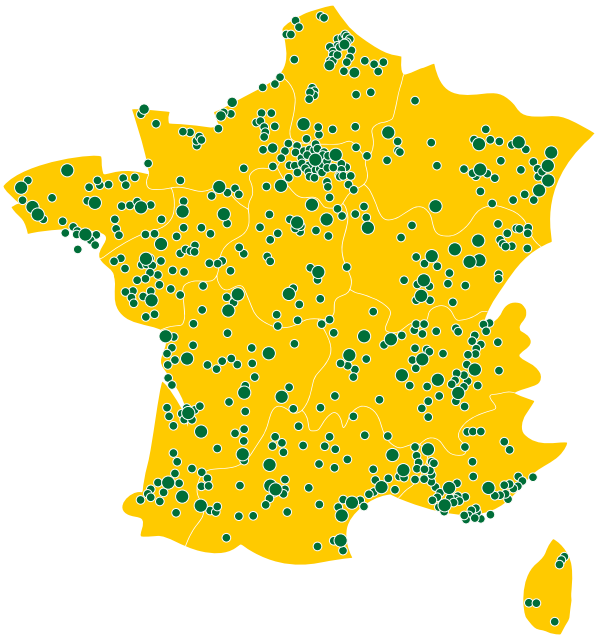
1 235
professionnels référencés **en 2021**

914
comptes rendus d'intervention

90 %
des demandes d'assistance de la part des entreprises et collectivités reçoivent une réponse d'un prestataire référencé en moins d'une heure.

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique



UN RÉSEAU DE PROFESSIONNELS D'ASSISTANCE AUX VICTIMES

Dans le cadre de sa mission d'assistance, la plateforme référençait 1 235 professionnels en cybersécurité sur le territoire national à la fin de l'année 2021. Ces prestataires, engagés à respecter une charte de bonnes pratiques, peuvent intervenir tant auprès des particuliers que des professionnels, suivant leurs champs d'action et de compétences. Ils informent, par ailleurs, le dispositif quasiment en temps réel de la menace et de ses évolutions qui pèsent sur la population. Ils sont donc un atout clé pour le GIP dans la détection de nouveaux phénomènes.

Nouveau service

63 %

des demandes de sécurisation reçoivent une réponse en moins de 3h

Avec le lancement public du label ExpertCyber le 18 février 2021 (voir page 12), la plateforme s'est dotée d'un nouveau service en ligne de mise en relation avec des prestataires labellisés pour accompagner les professionnels dans la sécurisation de leur système d'information (informatique, sites Internet, téléphonie…).

Le dispositif a ainsi agrémenté sa plateforme d'un point d'entrée spécifiquement dédié aux domaines de compétences couverts par le label, avec un **parcours inédit adapté**.

L'ASSISTANCE AUX VICTIMES, UN BESOIN, UNE NÉCESSITÉ

LA RÉPONSE À UN BESOIN
TOUJOURS PLUS FORT DES POPULATIONS

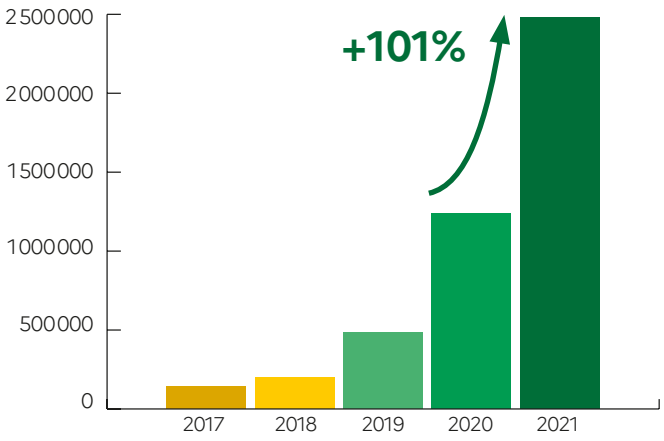
Depuis son lancement fin 2017, la fréquentation de la plateforme Cybermalveillance.gouv.fr ne cesse de croître.

Une fréquentation en hausse

En 2021, la fréquentation de la plateforme Cybermalveillance.gouv.fr a une nouvelle fois doublé par rapport à l'année précédente (**+101 %**) pour atteindre **près de 2,5 millions de visiteurs** sur l'année (2 482 788).

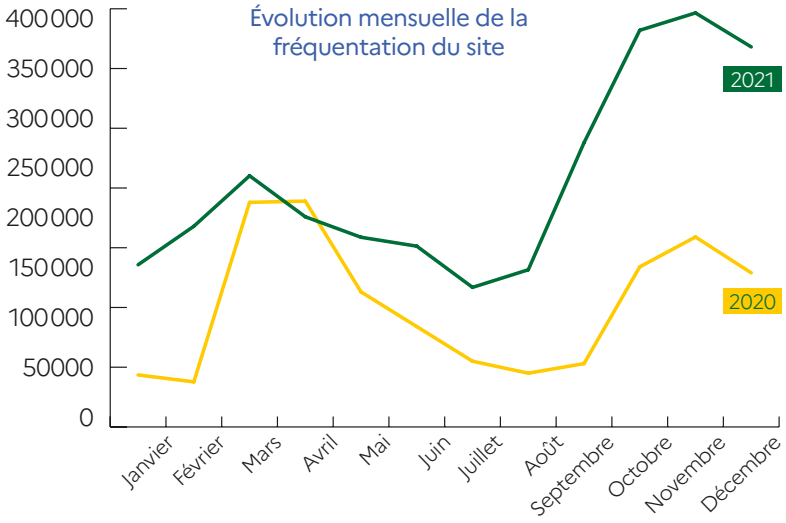
Ce nouveau record d'audience est dû en partie au développement de plus en plus important de la notoriété du dispositif auprès de ses publics, notamment du fait d'une présence accrue dans les médias, pour lesquels le dispositif est devenu en quatre ans une référence sur les sujets de cybersécurité. Cette croissance est également fortement liée à un important travail de référencement naturel sur les publications de prévention et d'assistance du dispositif, afin de les rendre toujours plus facilement accessibles via les moteurs de recherche, qui restent le premier canal de recherche d'information des victimes. Enfin, l'intérêt toujours plus important des publics, tant particuliers que professionnels, pour l'information et les services offerts par la plateforme est révélateur du besoin des populations face une cybercriminalité qui reste en forte expansion.

Fréquentation annuelle de la plateforme Cybermalveillance.gouv.fr



L'année 2020 avait connu des pics considérables de fréquentation durant les périodes de confinement en début et fin d'année. En 2021, la fréquentation mensuelle du site a presque toujours été supérieure aux mois correspondants de 2020, avec une forte croissance en fin d'année due en particulier à une recrudescence importante de différentes campagnes de messages d'hameçonnage au dernier trimestre.

Évolution mensuelle de la fréquentation du site



près de 2,5 millions de visiteurs en 2021

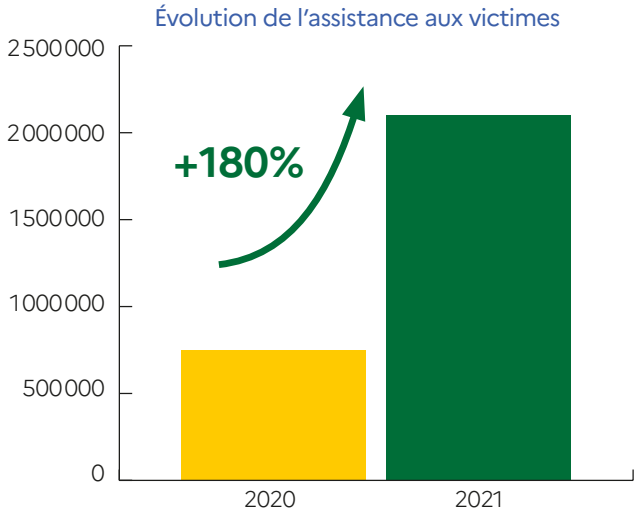
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

Une fréquentation majoritairement centrée sur l'assistance

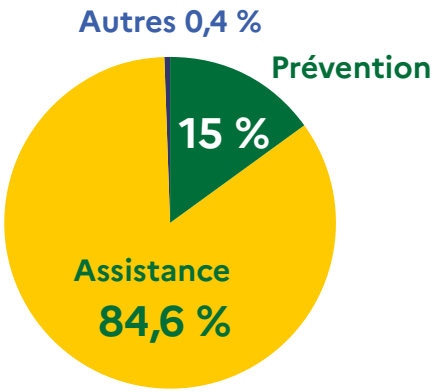
Outre l'outil d'assistance en ligne, de très nombreux contenus sur les principales menaces sont également accessibles sur Cybermalveillance.gouv.fr et dispensent tous les conseils nécessaires pour y faire face.

Sur l'année écoulée, ces articles sur les menaces ont fait l'objet de plus de 1,935 million de consultations, auxquelles s'ajoutent les 173 000 recherches d'aide en ligne, soit au total **plus de 2,1 millions de personnes assistées par Cybermalveillance.gouv.fr en 2021, en hausse de 180 % par rapport à l'année précédente**.



L'intérêt pour le curatif l'emporte toujours très largement sur le préventif

Ces chiffres mettent également en évidence que la plateforme Cybermalveillance.gouv.fr trouve l'essentiel de son public dans **sa mission première d'assistance qui représente 84,6 % de son trafic**. Bien qu'ils permettraient souvent d'empêcher, voire de contenir les cyberattaques, les contenus de prévention sur les bonnes pratiques de la sécurité numérique restent moins consultés avec environ 15 % du trafic de la plateforme.



OBSERVER LA MENACE POUR MIEUX L'ANTICIPER ET ADAPTER L'OFFRE D'ASSISTANCE

OBSERVER LA MENACE POUR MIEUX L'ANTICIPER
ET ADAPTER L'OFFRE D'ASSISTANCE

LES CHIFFRES DE LA CYBERMALVEILLANCE
EN 2021

L'analyse des demandes d'assistance en ligne sur la plateforme donne une vision plus fine des cybermalveillances rencontrées par catégorie de publics.

Cybermalveillance.gouv.fr propose un outil d'assistance en ligne qui permet, en répondant à quelques questions, d'obtenir un diagnostic du problème rencontré et de disposer des conseils permettant d'y faire face. Ces conseils peuvent être d'ordre techniques et/ou administratifs. Ce service permet également d'être au besoin mis en relation avec les plus de 1200 prestataires référencés par Cybermalveillance.gouv.fr sur l'ensemble du territoire national et en capacité d'intervenir pour apporter une assistance technique de proximité aux victimes.

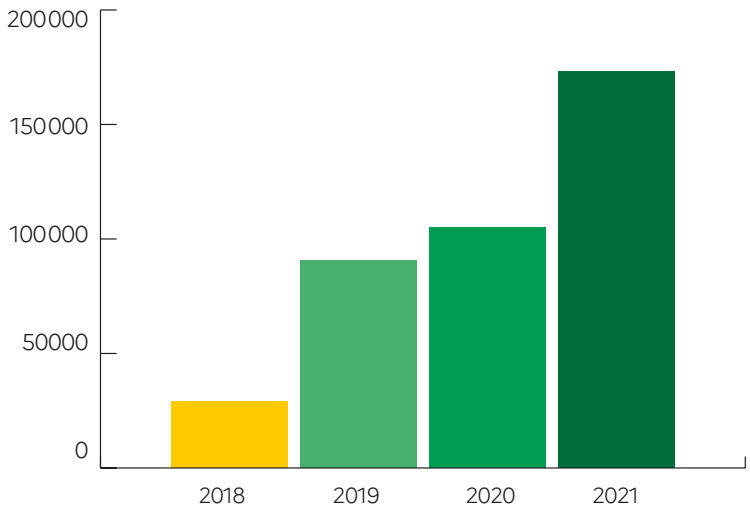
En 2021, **plus de 173000 demandes d'assistance en ligne ont été enregistrées sur Cybermalveillance.gouv.fr en augmentation de 65 %** par rapport à l'année précédente.

Le taux de satisfaction de ce service d'assistance en ligne et des plus de 420 conseils personnalisés qu'il prodigue est de 85,8 %, en progression par rapport à l'année 2020. Les 14,2 % des personnes qui se déclarent non satisfaites par cet outil sont très majoritairement en attente de services qui ne rentrent pas dans les attributions de Cybermalveillance.gouv.fr.

+173 000
demandes d'assistance sur la plateforme **en 2021**

+420
conseils personnalisés

Évolution des recherches d'assistance en ligne



RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

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

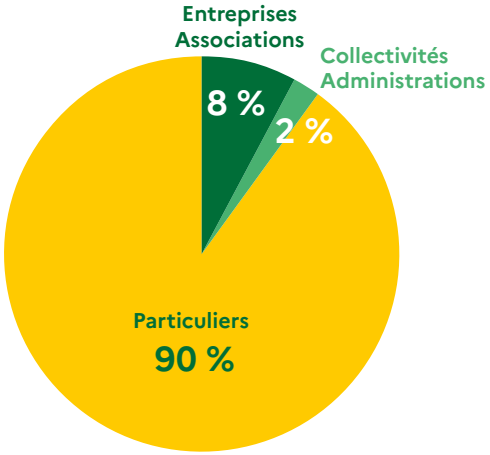
La répartition des publics de la plateforme Cybermalveillance.gouv.fr se révèle quasi stable par rapport aux années antérieures avec 90 % de particuliers, 8 % d'entreprises et 2 % de collectivités. Cet indicateur quantitatif fait apparaître que Cybermalveillance.gouv.fr est majoritairement utilisé en volume par des particuliers. Cette réalité est toutefois à rapprocher de la taille respective des populations cibles, soit 67,8 millions de particuliers, 5,6 millions d'entreprises et associations, et 36 000 collectivités et EPCI*.

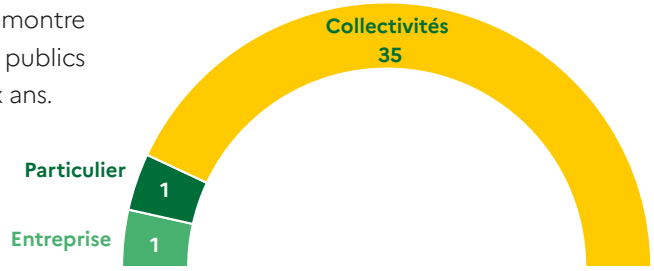
Ainsi rapporté à la proportion de ces populations, **pour 1 particulier assisté en 2021, Cybermalveillance.gouv.fr a assisté 1 entreprise et 35 collectivités.**

En 2021, avec plus de 10 300 entreprises/associations et 2 100 collectivités/administrations assistées en ligne par Cybermalveillance.gouv.fr, ce volume est globalement resté stable par rapport à l'année précédente qui avait été une année de très forte progression. Cette tendance démontre que la forte pression de la cybermalveillance sur les publics professionnels ne faiblit pas depuis maintenant deux ans.

*EPCI : Établissement public de coopération intercommunale

Proportion des publics assistés sur Cybermalveillance.gouv.fr en 2021





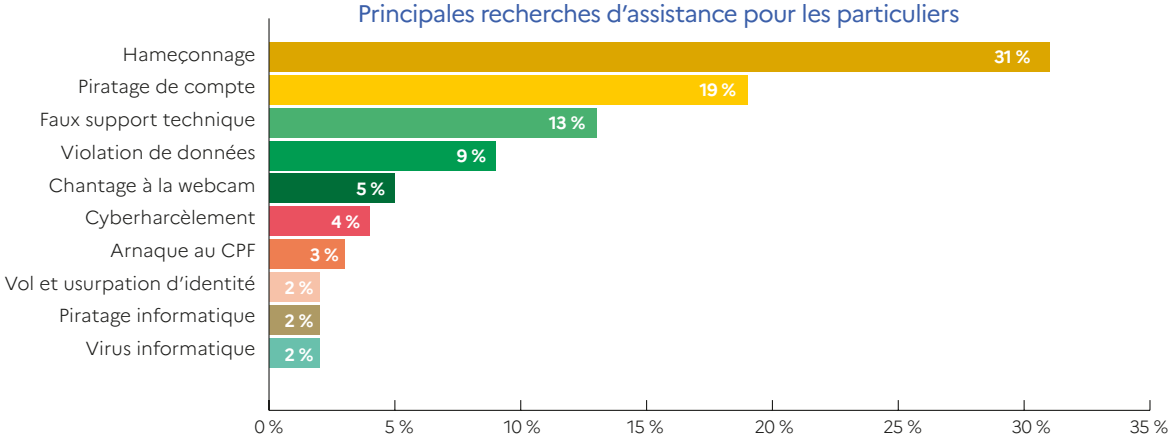
OBSERVER LA MENACE POUR MIEUX L'ANTICIPER ET ADAPTER L'OFFRE D'ASSISTANCE

Les principales menaces par catégorie de publics en 2021

Sur les 47 formes de cybermalveillance traitées par l'outil d'assistance en ligne en 2021, l'analyse des principales recherches par catégorie de publics est un indicateur fort des grandes tendances de la cybermalveillance. En effet, les classements des 10 principales cybermenaces par catégories de public décrites ci-après représentent à elles seules plus de 75 % des recherches d'assistance en ligne sur la plateforme.

À l'instar de l'année précédente, **l'hameçonnage ou phishing reste la première cybermalveillance rencontrée par les particuliers** et continue même de progresser (+82 %). L'hameçonnage reste suivi par le piratage de compte en ligne (+58 %) et les fraudes aux faux supports techniques (+18 %) qui continuent également de progresser. Une nouvelle cybermalveillance entre dans le classement de tête cette année avec les violations de données personnelles (+200 %). L'année 2021 ayant été marquée par de nombreuses fuites de données et notamment de données personnelles médicales. Les différentes formes d'escroqueries au compte personnel formation (CPF) ont également marqué l'année en hausse de +200 % par rapport à l'année précédente. Enfin pour les particuliers, on constate également une forte augmentation des faits de cyberharcèlement (+33 %).

Principales recherches d'assistance pour les particuliers

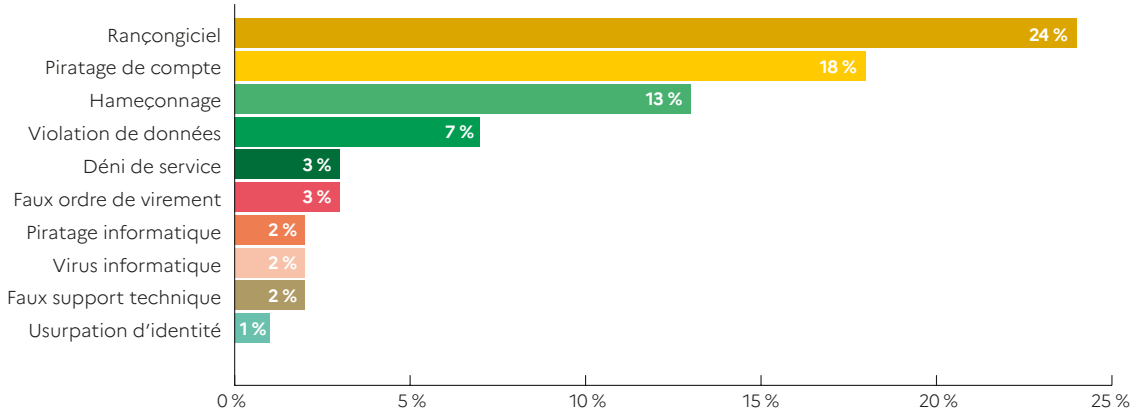


RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

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

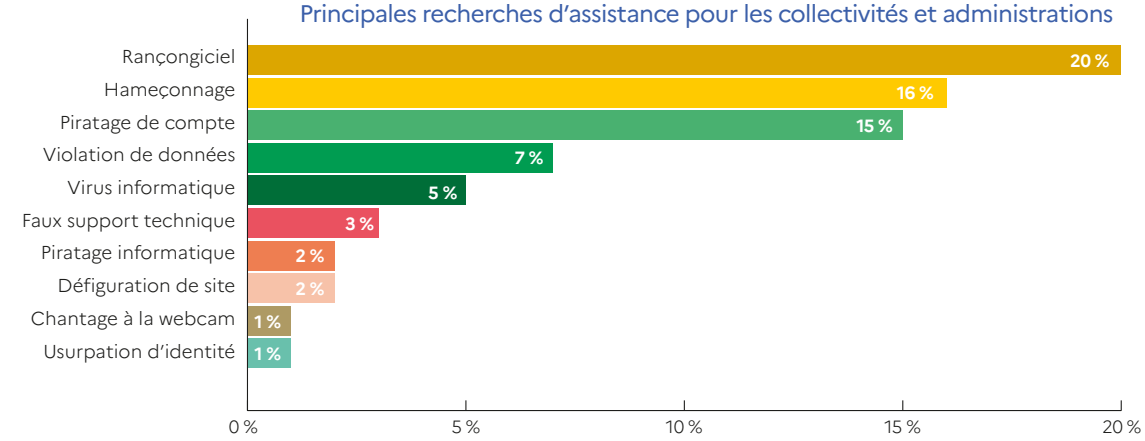
Pour les entreprises et associations, les rançongiciels ou ransomwares conservent en 2021 leur triste première place obtenue l'année précédente en continuant même de progresser fortement en proportion (+41 %). Ils restent immédiatement suivis par les piratages de compte en ligne qui progressent également considérablement (+61 %). L'hameçonnage effectue en 2021 une forte remontée dans le classement en passant de la 7e à la 3e place avec une progression de +86 %. Quant aux violations de données et fraudes aux ordres de virement, leurs proportions restent stables par rapport à l'année antérieure.

Principales recherches d'assistance pour les entreprises et associations



À l'instar des entreprises et associations, les rançongiciels conservent également leur première place dans les recherches d'assistance pour les collectivités et administrations, en légère progression (+5 %). De même, l'hameçonnage progresse considérablement pour cette population en passant de la 5e à la 2e place, en progression de +60 %. Le piratage de compte en ligne conserve sa 3e place, avec toutefois une évolution notable de +50 % par rapport à l'année précédente. Quant aux violations de données personnelles, elles progressent en 2021 et passent de la 9e à la 4e place, en hausse de +75 %.

Principales recherches d'assistance pour les collectivités et administrations



OBSERVER LA MENACE POUR MIEUX L'ANTICIPER ET ADAPTER L'OFFRE D'ASSISTANCE

LES GRANDES TENDANCES DE LA MENACE
EN 2021

L'hameçonnage, principal vecteur de cybermalveillances

L'hameçonnage, ou *phishing* en anglais, reste en 2021 la principale cybermalveillance rencontrée, tous publics confondus, en hausse de +143 % par rapport à l'année précédente.

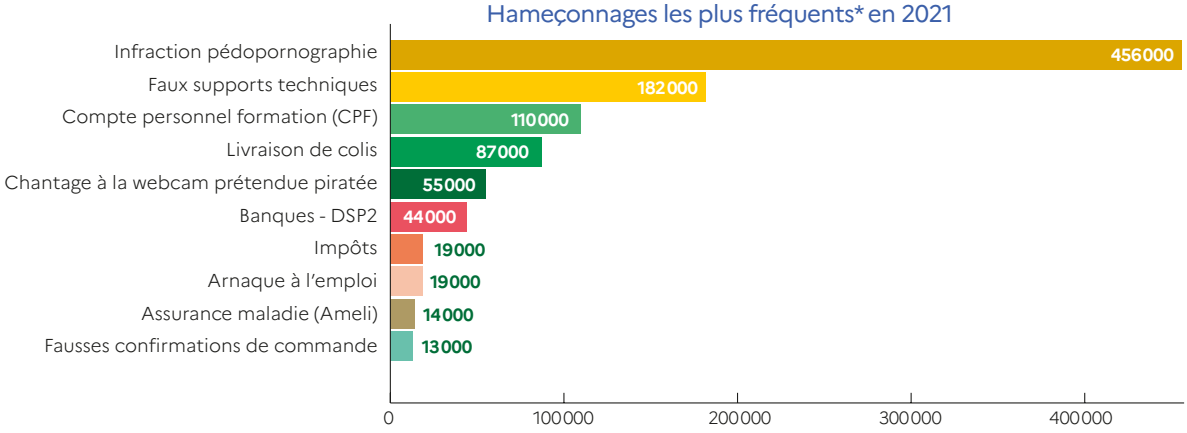
Cette technique d'attaque consiste à envoyer un message (courriel ou SMS) à la victime en usurpant une identité, pour l'inciter à communiquer des informations personnelles, des mots de passe, des coordonnées de carte bancaire, à réaliser un paiement ou même à installer un virus espion. L'hameçonnage reste très largement plébiscité par les cybercriminels, car c'est une technique d'attaque assez simple, peu onéreuse et très rentable. L'hameçonnage est ainsi devenu aujourd'hui le principal vecteur à l'origine de tout un panel de cybermalveillances qui vont du piratage de compte, en passant par des débits bancaires frauduleux, jusqu'à de l'usurpation d'identité et même les tristement célèbres attaques par rançongiciels.

Cette tendance identifiée en 2020 a amené le dispositif à développer son offre de services et de contenus pour encore mieux assister ses publics. Ainsi en 2021, un dossier a été réalisé pour permettre d'identifier tous les principaux types d'hameçonnage : faux message des impôts ou de l'assurance maladie, des forces de l'ordre, de banques, de société de livraison, de sites de vente en ligne, de loteries…

En 2021, 1,3 million de personnes sont venues chercher de l'information et de l'assistance sur Cybermalveillance.gouv.fr pour des faits apparentés à de l'hameçonnage, soit plus de 50 % du trafic global de la plateforme.

Les 10 principales formes d'hameçonnage représentent à elles seules près de 80 % des recherches d'assistance sur Cybermalveillance.gouv.fr.

Hameçonnages les plus fréquents* en 2021



*en nombre de consultations

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

Derrière les désormais traditionnels faux messages de remboursement d'impôts ou de la sécurité sociale, l'année 2021 a été plus particulièrement marquée par de nombreuses vagues de messages d'**escroquerie à la livraison de colis** qui cherchent à profiter de l'explosion du commerce en ligne depuis le début de la crise sanitaire (87 000 consultations de l'article dédié).

Les messages d'**hameçonnage visant les comptes et cartes bancaires** ont également marqué l'année passée. Les cybercriminels ont en effet essayé de mettre à profit l'actualité de la mise en place en 2021 de la directive européenne DSP2 sur la sécurité des moyens de paiement, qui impose à présent l'utilisation d'une authentification renforcée, en exploitant cette thématique pour crédibiliser leurs attaques (44 000 consultations de l'article dédié).

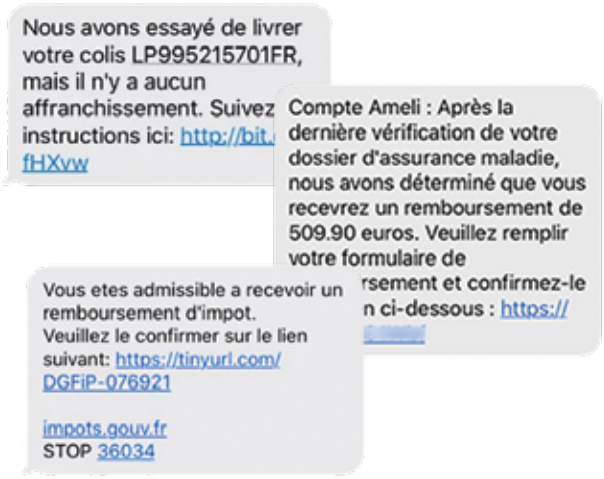
1,3 million
de recherches d'information et d'assistance
pour des faits apparentés à de l'hameçonnage

Les diverses sollicitations par courriel, SMS ou téléphone concernant le **compte personnel formation (CPF)** qui débouchent souvent sur des escroqueries, du piratage de compte, des pratiques commerciales trompeuses voire de la vente forcée n'ont pas baissé en intensité (110 000 consultations de l'article dédié).

Les **arnaques au faux support technique**, qui consistent à faire croire à la victime qu'elle doit payer un pseudo-dépannage suite à un problème de sécurité, restent à un niveau très élevé et continuent de cibler principalement les seniors les moins aguerris au numérique (182 000 consultations de l'article dédié, **en hausse de +219 %**).

Mais la première place en 2021 revient incontestablement aux **faux messages d'infraction pédopornographique**. Prétendus émaner de la police ou de la gendarmerie, voire d'Europol ou d'Interpol, ces messages accusent la victime de pédophilie ou de pédopornographie et lui demandent de payer une forte amende de plusieurs milliers d'euros pour éviter les poursuites. Identifié fin 2020 par Cybermalveillance.gouv.fr, ce nouveau type d'arnaque qui fait de nombreuses victimes, principalement par peur de l'erreur judiciaire, n'a cessé de gagner en intensité sur toute l'année 2021. L'article consacré à cette escroquerie a fait l'objet de plus de 1 250 consultations quotidiennes en moyenne sur l'année, avec une forte recrudescence de messages malveillants au dernier trimestre qui a entraîné jusqu'à plus de 4 000 consultations par jour.

Enfin, **la tendance forte du développement de l'hameçonnage par SMS (ou smishing en anglais) identifiée en 2020 s'est confirmée en 2021 et devrait encore s'accentuer**. Les cybercriminels profitent en effet du développement des services d'information réalisés par SMS des administrations, des banques ou des livreurs pour crédibiliser leurs attaques. Ils profitent également du caractère plus intrusif des SMS par rapport aux courriels et d'une moindre méfiance des victimes, ainsi que de la plus grande difficulté à identifier un SMS frauduleux sur un téléphone qu'un courriel reçu sur un ordinateur. Certains messages d'hameçonnage historiquement réalisés par courriel sont ainsi aujourd'hui massivement transposés par SMS, comme pour les faux messages des impôts, de l'assurance maladie, ou des banques.



Le piratage de compte : les messageries de plus en plus ciblées

+139 %
de piratage de compte en 2021

En 2021, **le piratage de compte en ligne conserve la seconde place des principales menaces rencontrées pour toutes les catégories de publics**, qu'il s'agisse des particuliers ou des professionnels. Avec 143 000 consultations de l'article dédié et 16 000 demandes d'assistance, ce sont près de 160 000 personnes qui sont venues chercher de l'aide sur ce phénomène sur Cybermalveillance.gouv.fr durant l'année écoulée. Soit **une hausse de +139 % par rapport à l'année 2020**.

Le **piratage des comptes bancaires en ligne** reste une cible de choix pour les cybercriminels. Mais la mise en service de la directive européenne DSP2 sur la sécurité des moyens de paiement, qui a vu les banques renforcer l'authentification aux comptes bancaires en ligne, a incité les cybercriminels à faire évoluer leurs modes opératoires. Si les comptes de réseaux sociaux apparaissent également toujours visés, la tendance à un intérêt toujours plus fort des cybercriminels pour les comptes de messagerie s'est confirmée en 2021.

Avec l'avènement des messageries en ligne et le développement des échanges électroniques, **les cybercriminels ont bien compris qu'en prenant le contrôle de la messagerie d'une victime, ils pouvaient prendre le contrôle de presque toute sa vie numérique**.

La facilité d'utilisation de ces messageries en ligne et la possibilité d'y accéder depuis de multiples appareils (ordinateur, téléphone, tablette), sans réelle limite de capacité de stockage, ont vu les utilisateurs les transformer en entrepôt numérique pour y conserver leurs documents administratifs, voire des copies de carte bancaire ou même leurs différents mots de passe. Par ailleurs, les utilisateurs y conservent tous les échanges avec leur famille, leurs amis, les administrations, les banques ou organismes de crédit. Les adresses de messagerie sont également généralement liées aux divers comptes en ligne de leurs utilisateurs (commerce, réseaux sociaux, abonnements à des services…). Les messageries contiennent donc **une grande quantité d'informations qui valent de l'or pour les cybercriminels.** En fonction de leur nature et de leur capacité à les exploiter, les cybercriminels chercheront à utiliser directe-

ment les informations dérobées ou les revendront à d'autres cybercriminels plus spécialisés. Ainsi la liste des contacts de la victime permettra de réaliser des tentatives d'arnaques vers ses proches. Les documents d'identités, fiches de paie ou avis d'imposition stockés dans la messagerie permettront de réaliser des usurpations d'identité pour, par exemple, contracter des crédits à la consommation ou encore faire réaliser des virements en écrivant au conseiller bancaire de la victime. Enfin, la messagerie est généralement le point central permettant la réinitialisation de tous ses autres comptes en ligne, notamment pour les réseaux sociaux et sites de commerce en ligne, dont les cybercriminels pourront ainsi prendre le contrôle pour passer des commandes sur le compte de la victime.

Les principales causes identifiées de ces piratages sont l'utilisation de mots de passe faciles à deviner, la réutilisation du même mot de passe sur de multiples comptes dont l'un a pu déjà être piraté, l'hameçonnage et l'absence d'authentification renforcée. Bien que souvent disponible, la double authentification est en effet jugée par les utilisateurs trop compliquée à mettre en œuvre voire contraignante à utiliser. **Au regard des gains multiples qu'ils peuvent en tirer, l'intérêt des cybercriminels pour les messageries des victimes devrait encore s'accentuer.**

FOCUS

2021, une année marquée par les fuites de données personnelles médicales

L'année 2021 a également été marquée par 2 fuites importantes de données médicales affectant 500 000 personnes en février puis 1,4 million de personnes en septembre.

Cybermalveillance.gouv.fr s'est efforcé d'accompagner au mieux les victimes en leur dispensant les conseils nécessaires pour faire face aux cybermalveillances qui peuvent être consécutives de ce type d'incident, notamment le risque d'hameçonnage et autres tentatives d'escroqueries ciblées.

En coopération avec les services du ministère de la Justice et du ministère de l'Intérieur, une lettre plainte numérique a été mise à disposition des victimes sur Cybermalveillance.gouv.fr pour les aider à faire face aux potentielles conséquences prévisibles pouvant nécessiter une judiciarisation.

OBSERVER LA MENACE POUR MIEUX L'ANTICIPER ET ADAPTER L'OFFRE D'ASSISTANCE

Les rançongiciels, principale menace pour les professionnels

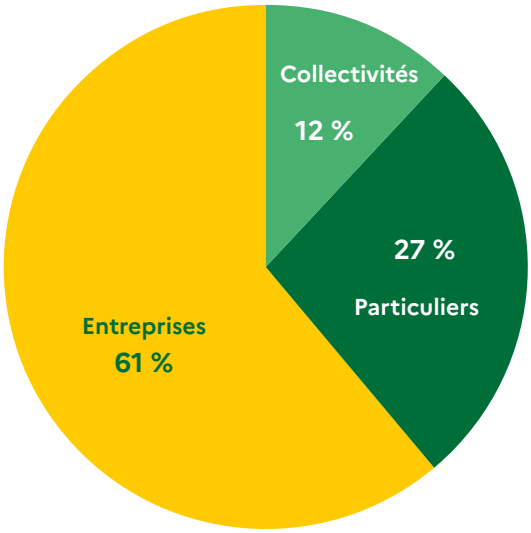
Avec plus de 60 000 consultations de l'article visant à décrire comment faire face à ce type d'attaque et 2 679 demandes d'assistance en ligne, les rançongiciels (ou *ransomwares* en anglais) demeurent en 2021 une des principales menaces traitées par la plateforme, avec toutefois de fortes variations en fonction des publics et un quasi-doublement des attaques visant les professionnels.

En hausse de +48 % tous publics confondus, **ce type d'attaque continue de cibler majoritairement les publics professionnels (73 %).**

Les demandes d'assistance des **particuliers** restent quantitativement en augmentation en 2021 (+49,5 %) avec 734 demandes d'assistance. Ces sollicitations continuent toutefois de baisser d'intensité en proportion de victimes (-5,6 %), confirmant ainsi la tendance identifiée en 2020 d'un plus faible intérêt des cybercriminels pour cette catégorie de victimes, jugées sans doute moins solvables. Pour les particuliers, les rançongiciels ne figuraient plus en 2021 qu'à la 16e place sur les 47 formes de cybermalveillance traitées par le dispositif.

Avec 1 945 demandes d'assistance par les professionnels (1 633 entreprises et 312 collectivités) **en hausse de plus de 95 %, les rançongiciels restent en 2021 la première menace qui cible les professionnels.**

La proportion des collectivités victimes reste globalement stable (+0,95 % par rapport à 2020) alors que celle des entreprises continue d'augmenter (+4,7 %). Ces chiffres tendent à démontrer que les cybercriminels n'ont pas abandonné le ciblage des collectivités mais qu'ils viseraient toujours plus prioritairement les entreprises.



Sans doute parce que ces dernières seraient plus enclines à payer les rançons demandées au regard des impacts économiques et réputationnels de ce type d'attaque pour leur activité.

Cette tendance qui fait des attaques par rançongiciels un des secteurs les plus lucratifs de l'écosystème cybercriminel devrait continuer à s'accentuer encore en 2022.

+95%
de hausse
en 2021

Les rançongiciels : première menace
pour les entreprises et les collectivités

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

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

REMERCIEMENTS

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

Ses membres publics

- Premier ministre (ANSSI);
- Ministère de l'Éducation nationale, de la Jeunesse et des Sports;
- Ministère de l'Économie, des Finances et de la Relance;
- Ministère des Armées;
- Ministère de l'Intérieur;
- Ministère de la Justice;
- Secrétariat d'État chargé de la transition numérique et des communications électroniques.

Ses membres privés

- **AFCDP** (Association française des correspondants à la protection des données à caractère personnel), **AFNIC** (Association française pour le nommage Internet en coopération), **Atempo WOOXO**, **Avicca** (Association des Villes et Collectivités pour les Communications électroniques et l'Audiovisuel), **Banque des Territoires** (groupe Caisse des Dépôts), **Bouygues Telecom**, **CCR** (Caisse centrale de réassurance), **CCI France** (Chambre de Commerce et d'Industrie), **CDSE** (Club des directeurs de sécurité des entreprises), **CESIN** (Club des Experts de la Sécurité de l'Information et du Numérique), **CINOV Numérique**, **CISCO**, **CLCV** (Association Consommation, Logement et Cadre de Vie), **Club EBIOS**, **CLUSIF** (Club de la sécurité de l'information français), **CNLL** (Union des entreprises du logiciel libre et du numérique ouvert), **CoTer Numérique**, **Covéa**, **CPME** (Confédération des Petites et Moyennes Entreprises), **e-Enfance/3018**, **ESET**, **Fédération Déclic**, **Fédération EBEN** (Fédération des Entreprises du Bureau et du Numérique), **FEVAD** (Fédération du e-commerce et de la vente à distance), **France Assureurs**, **France Victimes**, **Google France**, **INC** (Institut National de la Consommation), **Kaspersky**, **La Poste Groupe**, **MACIF** (Mutuelle assurance des commerçants et industriels de France), **MAIF** (Mutuelle assurance des instituteurs de France), **MEDEF** (Mouvement des entreprises de France), **Microsoft France**, **Neuflize OBC**, **Numeum**, **Orange Cyberdefense**, **Palo Alto Networks**, **Région Pays de la Loire**, **Régions de France**, **Signal Spam**, **SNCF**, **Stormshield**, **UFC-Que Choisir**.
- Ses nouveaux membres dont l'adhésion au GIP a été acceptée en 2021 pour rejoindre le dispositif au 1er janvier 2022 : **ANCT** (Agence Nationale de la cohésion des territoires) et **U2P** (Union des entreprises de proximité).

- **Ses professionnels référencés**, qui contribuent par leur action aux côtés du dispositif à sa mission d'assistance aux victimes sur l'ensemble du territoire.
- **Ses professionnels labellisés ExpertCyber** ainsi que l'**AFNOR** et **IT Partners** (Groupe Comexposium) pour leur soutien au label.
- Les **groupements de professionnels des technologies de l'information (IT)** qui ont accompagné le dispositif tout au long de l'élaboration du label : **Alliance du numérique**, **ESCRIM**, **EURABIS**, **FRP2i**, **Résadia**, **Séquence informatique**.
- Ses **partenaires pour les événements professionnels** liés à la cybersécurité : **Avisa Partners** (organisateur du FIC – Forum International de la cybersécurité), **Cybercercle**, **Expoprotection sécurité** (groupe Reed Exhibition), **Assises de la sécurité** (Groupe Comexposium), **IT Partners** (groupe Reed Exhibition), **Paris Cyber Week** (Garnault et Associés).
- Les **parties prenantes de son programme de sensibilisation à destination des collectivités territoriales et des élus**, qui ont relayé activement ses contenus de sensibilisation : **AdCF** (Association des communautés de France), **ADF** (Assemblée des départements de France), **ADULLACT** (Association des développeurs et utilisateurs de logiciels libres pour les administrations et les collectivités territoriales), **AMF** (Association des Maires de France), **AMIF** (Association des maires Île-de-France), **AMRF** (Association des Maires Ruraux de France), **ANSSI**, **Avicca**, **Banque des Territoires** (groupe Caisse des Dépôts), **Club des RSSI des collectivités**, **CLUSIF**, **CoTer Numérique**, **Cyber Task Force**, **Cybercercle**, **Fédération Déclic**, **FFA**, **FNCCR** (Fédération Nationale des Collectivités Concédantes et Régies), **La gazette des communes**, **Ministère de l'Intérieur**, **Mission Ecoter**, **Programme DINUM**, **Villes de France**, **Villes Internet**.
- Plus généralement, Cybermalveillance.gouv.fr remercie **l'ensemble de l'écosystème avec lequel il interagit** et qui lui permet d'assurer ses missions au quotidien.

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

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

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

Suivez-nous sur :