RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

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

# RAPPORT D'ACTIVITÉ 2020

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

www.cybermalveillance.gouv.fr

# SOMMAIRE




**Directeur de la publication :** Jérôme Notin
**Coordination éditoriale :** Pôle Communication
**Conception graphique :** Elsa Godet




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


RÉPUBLIQUE FRANÇAISE
*Liberté Égalité Fraternité*

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

# ÉDITO

## GUILLAUME **POUPARD**

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

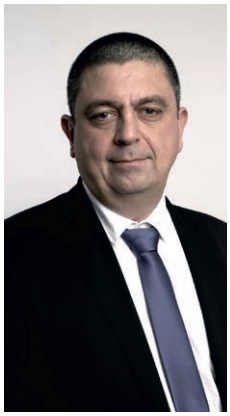
*L'année 2020 a été singulière. La crise sanitaire, que nous traversons encore aujourd'hui, a été un accélérateur de la transformation numérique des pratiques professionnelles : le télétravail s'est généralisé, les outils de visioconférence se sont multipliés, le recours à des solutions de partage de fichiers a explosé… rendant la frontière entre les usages personnels et professionnels encore plus ténue.*

*Dans ce contexte si particulier, où toute cyberattaque est susceptible d'avoir un impact exacerbé, le dispositif Cybermalveillance.gouv.fr a fait ses preuves. Grâce à la réactivité de ses membres, la plateforme a pu poursuivre ses missions de prévention et d'assistance et confirmer son statut d'acteur de référence au service de nos concitoyens, des collectivités territoriales et des petites et moyennes entreprises.*

*Alors que la menace cyber est plus importante que jamais, je suis convaincu que le dispositif Cybermalveillance.gouv.fr continuera d'apporter une réponse essentielle en venant en aide aux victimes de cybermalveillance.*

## JÉRÔME **NOTIN**

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



*L'activité de notre dispositif fut particulièrement mouvementée en 2020. Alors que nous démarrions l'année avec la mise en ligne de la nouvelle version de notre plateforme, une intensification des activités cybercriminelles, en partie liée à la crise sanitaire, a été constatée par notre dispositif.*

*Cybermalveillance.gouv.fr s'est organisé pour y faire face et accompagner ces phénomènes : développement de son réseau de professionnels en sécurité informatique pour venir en aide aux victimes, partenariats ciblés pour répondre à de nouvelles menaces et actions de sensibilisation auprès du plus large public via différents canaux (campagne télévisée, presse nationale et régionale, alertes sur les réseaux sociaux…). Cette nouvelle année a aussi vu le lancement du label ExpertCyber, dont l'objectif est notamment de mieux accompagner les publics professionnels dans la sécurisation de leurs systèmes d'information. Ce sont tous ces éléments qui confirment, une fois encore, la nécessité d'un tel dispositif pour tous les publics.*

*L'engagement au service de l'intérêt général de ses 49 membres issus des secteurs public et privé, l'investissement des professionnels référencés et la mobilisation des agents du GIP permettent à Cybermalveillance.gouv.fr de rendre ses actions plus efficaces et de relever les défis à venir.*

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


1
ASSISTANCE
AUX VICTIMES
D'ACTES DE
CYBERMALVEILLANCE
2
INFORMATION
ET SENSIBILISATION
SUR LA SÉCURITÉ
NUMÉRIQUE
ENTREPRISES

# 1 LES FAITS MARQUANTS DE L'ANNÉE 2020

# 1 LES FAITS MARQUANTS DE L'ANNÉE 2020

## JANVIER

**1er janvier :** Cybermalveillance.gouv.fr accueille 5 nouveaux membres : CCR*, CoTer Numérique, Fédération Déclic, Harmonie Technologie et MEDEF**
**9 janvier :** alerte faille critique de sécurité Firefox
**27 janvier :** alerte faille critique de sécurité Citrix
**28 au 30 janvier :** participation au Forum International de Cybersécurité (FIC) à Lille (12 500 participants)

* Caisse centrale de réassurance
** Mouvement des entreprises de France


**Janvier 2020**
Forum international de Cybersécurité à Lille.

## FÉVRIER

**4 février :** lancement de la nouvelle version de la plateforme www.cybermalveillance.gouv.fr
**4 février :** visite au sein du GIP ACYMA de Claire Landais, secrétaire générale de la Défense et de la Sécurité nationale
**4 février :** alerte sur les sites frauduleux de dédommagement du Pass Navigo
**28 février :** alerte faille critique Microsoft Exchange Server

## MARS

**4 mars :** Cybermalveillance.gouv.fr accueille 3 nouveaux membres : Afnic*, Banque Neuflize OBC, Google France
**16 mars :** appel au renforcement des mesures de vigilance en sécurité numérique dans le cadre du confinement
**18 mars :** alerte sur les sites frauduleux proposant des fausses attestations de déplacement numériques
**23 mars :** diffusion des recommandations de sécurité informatique pour le télétravail en situation de crise à destination des collaborateurs et des employeurs

* Association Française pour le Nommage Internet en Coopération

## AVRIL

**2 avril :** alerte sur une vague d'hameçonnage (*phishing*) aux couleurs des Finances Publiques
**3 avril :** alerte sur des campagnes d'arnaque au faux support technique via des newsletters sur le thème du coronavirus
**10 avril :** alerte sur le chantage à la webcam prétendue piratée
**14 avril :** alerte sur une vague d'arnaque aux couleurs de l'enseigne Leclerc
**16 avril :** alerte sur une vague d'arnaque aux collectes de dons solidaires dans le cadre de la crise du coronavirus
**18 avril :** alerte sur une vague d'arnaque aux couleurs de la marque Lancôme
**25 avril :** alerte sur les faux kits gratuits de confinement de Santé publique France dans le cadre de la crise du coronavirus
**28 avril :** alerte sur les faux messages des Impôts dans le cadre de la crise du coronavirus
**30 avril :** diffusion de recommandations de sécurité informatique pour préparer la reprise d'activité au déconfinement

## MAI

**5 mai :** accès à la BNUM* de la Gendarmerie nationale depuis la plateforme de Cybermalveillance.gouv.fr
**18 mai :** lancement de la campagne de spots TV de sensibilisation « Les réflexes essentiels pour votre sécurité numérique » en partenariat avec France Télévisions
**20 mai :** lancement du Label ExpertCyber auprès des professionnels de sécurité informatique

* Brigade numérique

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

**Mai 2020**
Lancement du label ExpertCyber.

## JUIN

**10 juin :** adoption du rapport d'information du Sénat « *Désinformation, cyberattaque et cybermalveillance : l'autre guerre du COVID-19* », par la commission des affaires étrangères et de la défense



RÉPUBLIQUE FRANÇAISE
*Liberté Égalité Fraternité*

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

# JUILLET/AOÛT

**9 juillet :** alerte à l'arnaque au chantage au site Internet prétendu piraté
**9 juillet :** lancement d'une enquête sur la notoriété du dispositif Cybermalveillance.gouv.fr et la perception du risque numérique en partenariat avec l'INC*
**19 août :** alerte d'une vague d'hameçonnage par SMS promettant aux TPE une aide financière pour la crise sanitaire
**29 août :** Cybermalveillance.gouv.fr accueille un nouveau membre : Banque des Territoires (Groupe Caisse des Dépôts)

* Institut National de la Consommation

# SEPTEMBRE

**30 septembre / 1er octobre :** partenariat Paris Cyber Week à Paris
**11 septembre :** participation aux Live Sessions de Niort Numeric
**17 septembre :** alerte faille critique Microsoft NetLogon
**30 septembre :** Cybermalveillance.gouv.fr dévoile son nouveau logo et adopte officiellement sa nouvelle identité graphique

# OCTOBRE

*Cybermalveillance.gouv.fr est partenaire du mois européen de la cybersécurité « Cybermoi/s », piloté par l'ANSSI**

**1er octobre :** Google France lance un programme de formations sur la cybersécurité pour les TPE / PME, en partenariat avec Cybermalveillance.gouv.fr et la FEVAD**
**1er octobre :** lancement de la première édition de lettre d'information destinée à tous les publics
**16 octobre :** lancement du programme de sensibilisation aux risques numériques auprès des élus
**17 octobre :** le dispositif Cybermalveillance.gouv.fr a trois ans d'existence
**21 octobre :** début de la diffusion de la campagne de sensibilisation TV Consomag réalisée en partenariat avec l'INC*** sur les chaînes du groupe France Télévisions
**25 octobre :** alerte relative à une vague de défiguration de sites Internet

* Agence Nationale de la Sécurité des Systèmes d'Information
** Fédération du e-commerce et de la vente à distance
*** Institut National de la Consommation

# NOVEMBRE

*Campagne de vidéos de sensibilisation des collectivités territoriales*

**13 novembre :** arrêté portant approbation des modifications de la convention du groupement d'intérêt public dénommé « Groupement d'intérêt public pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance ».
**18 novembre :** Cybermalveillance.gouv.fr accueille le ministère des Armées parmi les membres représentants de l'État
**26 novembre :** campagne de vidéos de sensibilisation des collectivités territoriales en partenariat avec Banque des Territoires (Groupe Caisse des Dépôts)

**Novembre 2020**
Campagne vidéos de sensibilisation des collectivités territoriales.


**Octobre 2020**
Participation à la Paris Cyber Week.

# DÉCEMBRE

**3 décembre :** résultats de l'enquête de notoriété et de la perception du risque numérique en partenariat avec l'INC*
**10 décembre :** alerte aux escroqueries au Compte Personnel de Formation (CPF) en partenariat avec la Caisse des Dépôts
**15 décembre :** alerte compromission Orion SolarWinds
**17 décembre :** conférence en ligne « Comment bâtir un environnement numérique de confiance pour les collectivités ? » organisée par Banque des Territoires (Groupe Caisse des Dépôts)
**18 décembre :** alerte de vagues de messages d'escroquerie aux couleurs de la Police et de la Gendarmerie
**24 décembre :** nouvel arrêté portant approbation des modifications de la convention du groupement d'intérêt public dénommé « Groupement d'intérêt public pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance »

* Institut National de la Consommation

# FAIRE CONNAÎTRE LE DISPOSITIF AU PLUS GRAND NOMBRE, L'UN DES ENJEUX DE CYBERMALVEILLANCE.GOUV.FR

« Devenir le premier réflexe des citoyennes et des citoyens en matière d'assistance et de prévention du risque numérique », telle est la vocation du dispositif Cybermalveillance.gouv.fr au titre de sa mission d'intérêt général. Particuliers, entreprises, associations ou collectivités : tous sont exposés quotidiennement à des cyberattaques. Afin de gagner en visibilité auprès de ces différents publics, Cybermalveillance.gouv.fr a orienté sa stratégie de communication sur la démultiplication et la diversification de ses actions et outils.

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Ancien logo

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

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

Nouveau logo

## COMMUNICATION ET VISIBILITÉ

### LA REFONTE DE L'IDENTITÉ VISUELLE

À l'occasion de ses trois ans, Cybermalveillance.gouv.fr a souhaité renforcer son identité visuelle en faisant notamment évoluer de façon significative son logo. Plus moderne, plus ancré dans l'univers numérique et plus identifiable, ce changement traduit une maturité du dispositif, qui pérennise ses missions. La signature (baseline) est réadaptée à cette identité, afin de mieux marquer le lien direct avec les actions déployées par Cybermalveillance.gouv.fr : prévenir les risques numériques, mais aussi informer sur les bonnes pratiques à adopter en sécurité numérique.

Le nouveau logo est accompagné du nouveau bloc-marque « République Française » : cette identité refondue permet de matérialiser le lien entre Cybermalveillance.gouv.fr et l'État, et accentue le rôle de service d'intérêt général que porte le dispositif.

### VIRTUALISATION DES ÉVÉNEMENTS

La crise sanitaire a bouleversé le calendrier et la tenue des événements et salons en présentiel ; si Cybermalveillance.gouv.fr a eu moins d'occasions, dans ce contexte, d'aller à la rencontre de ses publics sur le terrain, il a néanmoins poursuivi ses actions de sensibilisation dans le respect des règles sanitaires, une majeure partie de ses actions s'étant déroulée à distance (voir page 28). En 2020, Cybermalveillance.gouv.fr a pris part à **55 événements**, externes ou organisés par le dispositif (salons, conférences en ligne, tables rondes, interventions…).


Intervention de Jérôme Notin au live sur Twitter et Facebook organisé par la Commission européenne



Participation aux Live Sessions de Niort Numeric



RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

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

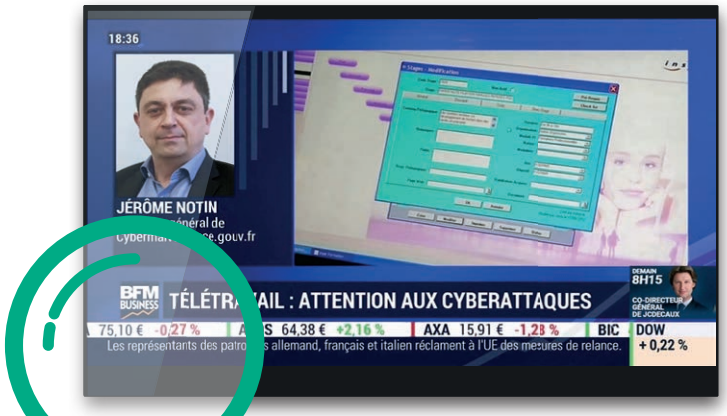
## STRATÉGIE DE CONTENUS

Tout au long de l'année, Cybermalveillance.gouv.fr a déployé et maintenu une **stratégie de publication** sur son site Internet, alternant contenus de fond, contenus d'actualité et **ressources sous différents formats** (fiches, vidéos, infographies, flyers…). Avec une recrudescence des cas de cybermalveillance observée, le dispositif a relayé **41 alertes et appels à vigilance dont 9 directement liés à la crise sanitaire**.


Cette stratégie de contenus a été enrichie par le lancement, à la veille des trois ans du dispositif et à l'occasion du Cybermoi/s (voir page 28), de **la première lettre d'information mensuelle adressée à tous les publics.** Diffusée à 25 000 abonnés, cette lettre vise à informer sur les nouvelles menaces et à dispenser les conseils pour s'en prémunir, à valoriser les actions de sensibilisation et initiatives menées avec les membres du dispositif et à relayer les alertes et actualités sur les risques numériques.


## ZOOM SUR LES RELAIS PRESSE

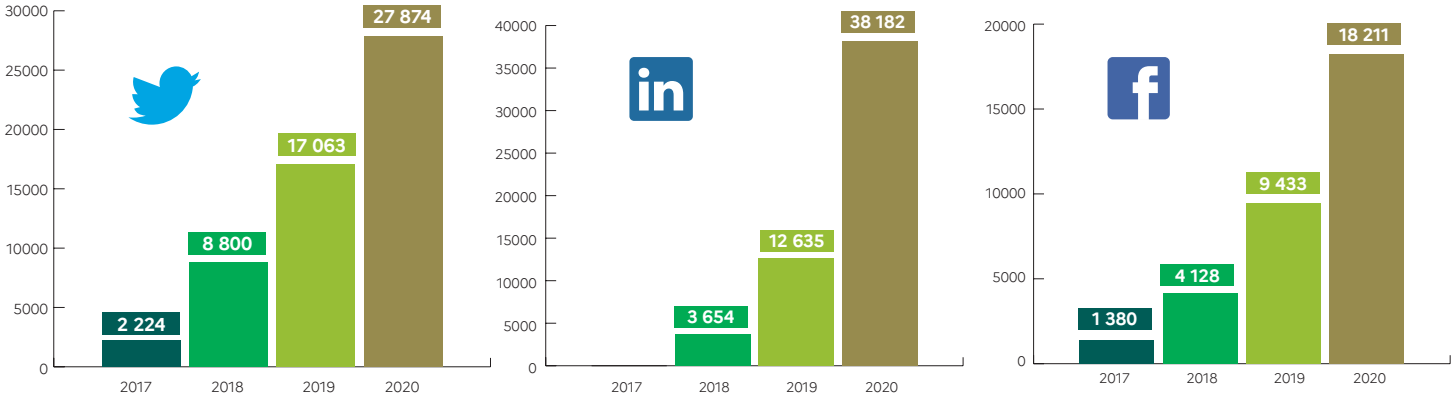
Le dispositif a fait l'objet d'une importante couverture médiatique en 2020, tant par la presse écrite et télévisée que sur les réseaux sociaux. Le lancement du label ExpertCyber et les alertes d'escroqueries et cyberattaques liées à la crise sanitaire furent notamment les temps forts de relais dans les médias.


# 1 LES FAITS MARQUANTS DE L'ANNÉE 2020

## ZOOM SUR LES 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 2020 a vu une forte croissance de son activité sur ses réseaux sociaux.




### LES PUBLICATIONS SUR LES RÉSEAUX SOCIAUX QUI ONT LE PLUS MARQUÉ L'ANNÉE 2020 PAR ORDRE D'IMPRESSIONS :

| | | |
|---|---|---|
| 1 | 25 avril | **ALERTE SUR LES FAUX KITS GRATUITS DE CONFINEMENT** DE SANTÉ PUBLIQUE FRANCE DANS LE CADRE DE LA CRISE DU CORONAVIRUS |
| 2 | 2 avril | **ALERTE SUR UNE VAGUE D'HAMEÇONNAGE** (PHISHING) AUX COULEURS DES FINANCES PUBLIQUES |
| 3 | 14 avril | **ALERTE SUR UNE VAGUE D'ARNAQUE SUR WHATSAPP** AUX COULEURS DE L'ENSEIGNE LECLERC |
| 4 | 16 mars | **APPEL AU RENFORCEMENT DES MESURES DE VIGILANCE** EN SÉCURITÉ NUMÉRIQUE DANS LE CADRE DU CONFINEMENT |
| 5 | 28 avril | **ALERTE SUR LES FAUX MESSAGES DES IMPÔTS** DANS LE CADRE DE LA CRISE DU CORONAVIRUS |

**41**
ALERTES ET APPELS À VIGILANCE PUBLIÉS SUR LES RÉSEAUX SOCIAUX

**+1 MILLION**
D'IMPRESSIONS POUR L'ALERTE SUR LES FAUX KITS GRATUITS DE CONFINEMENT


Les mois de mars et avril, soit **l'entrée en confinement**, ont été la période la plus marquante sur les réseaux sociaux : **les alertes sur les cybermenaces en cours et appels à vigilance** ont occupé une part importante des communications du dispositif.



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

# **FOCUS** SUR LA CRISE SANITAIRE

L'année 2020 aura été marquée par la crise sanitaire de la COVID-19. Cette situation exceptionnelle a vu une augmentation inédite des usages numériques liés aux confinements, tant pour des usages personnels d'information, de communication ou de commerce en ligne, que pour des usages professionnels avec un recours massif au télétravail. Comme Cybermalveillance.gouv.fr l'avait anticipé, les cybercriminels ont cherché à profiter de l'isolement et des inquiétudes des personnes pour démultiplier massivement leurs attaques. Dans le cadre de sa mission de prévention et d'information, le dispositif s'est efforcé tout au long de l'année écoulée d'accompagner au mieux ses publics face à la recrudescence induite des risques.

## ANTICIPER

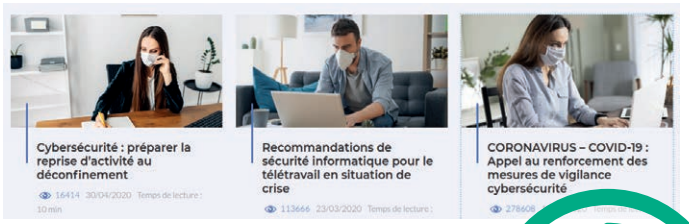
Toute situation de crise génère systématiquement une augmentation des activités cybercriminelles qui cherchent à en tirer parti. C'est partant de ce postulat que dès le 16 mars 2020, veille du premier confinement, Cybermalveillance.gouv.fr lançait un **appel à vigilance** pour exposer les risques pressentis de cybermalveillance et les moyens d'y faire face au mieux. Cet article, destiné aux particuliers et aux professionnels, **a été consulté plus de 26 000 fois en trois jours, et a cumulé au total près de 280 000 vues en 2020**, devenant ainsi l'article en ligne le plus consulté de la plateforme.

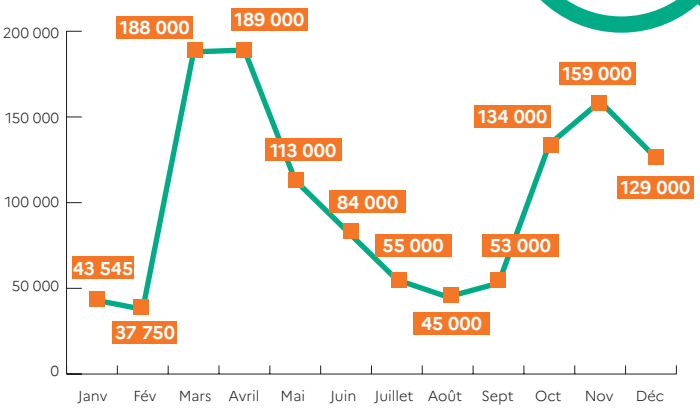
## ACCOMPAGNER

Avec cette crise, le **télétravail** s'est développé afin de préserver les activités qui le permettaient mais celui-ci a souvent été mis en place de manière improvisée, parfois même depuis les moyens personnels des collaborateurs, démultipliant de fait les risques de cybersécurité pour les organisations. Cybermalveillance.gouv.fr s'est efforcé d'accompagner au mieux les publics concernés en diffusant, une semaine après le début du premier confinement, ses conseils pour limiter les risques pressentis, tant à l'usage des collaborateurs que de leurs employeurs. Des recommandations ont également été diffusées afin de permettre aux organisations de préparer leur reprise d'activité en sortie de confinement.

## ALERTER

Lors des premières semaines de confinement, **la fréquentation de la plateforme a augmenté de près de 600 %**. Dans le même temps, **les recherches d'assistance concernant des attaques par hameçonnage liées de manière directe ou indirecte à la crise sanitaire ont augmenté de 400 %**. Cybermalveillance.gouv.fr a donc renforcé sa veille sur les phénomènes cybercriminels afin de pouvoir les détecter au plus tôt et en alerter ses publics. Faux sites d'attestation de déplacement, de ventes de masques, ou encore de « kits gratuits de confinement », messages frauduleux de toutes sortes proposant des remboursements ou des primes, appels aux dons frauduleux, faux supports techniques ou encore chantage à la webcam… ont généré autant d'alertes, principalement sur les réseaux sociaux, afin d'informer les publics.



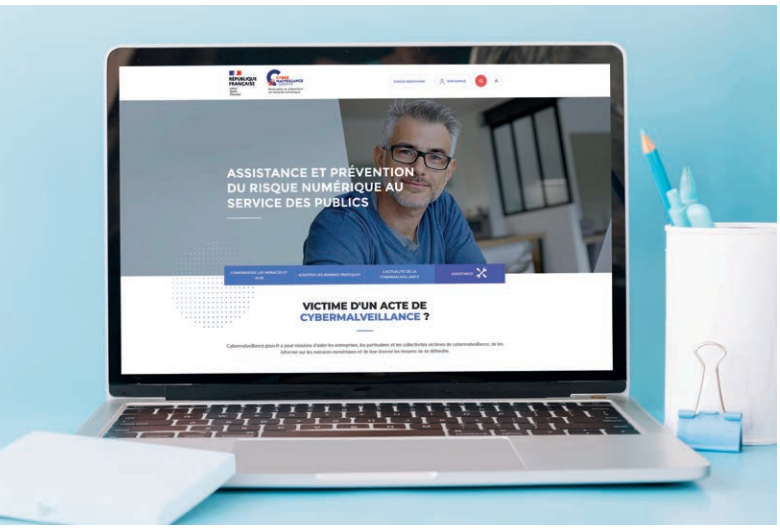

**LA FRÉQUENTATION MENSUELLE DE LA PLATEFORME EN 2020 MONTRE DES PICS IMPORTANTS SUR LES PREMIER ET SECOND CONFINEMENTS PRINCIPALEMENT LIÉS À L'ACCROISSEMENT DES ACTIVITÉS CYBERCRIMINELLES DURANT CES PÉRIODES.**

# GRANDS PROJETS
# ET PRINCIPALES RÉALISATIONS

## LA PLATEFORME WWW.CYBERMALVEILLANCE.GOUV.FR

## A FAIT PEAU NEUVE EN 2020!

Pour toujours mieux répondre à la menace qui touche les particuliers et professionnels, et grâce aux retours d'expérience, Cybermalveillance.gouv.fr a lancé le 4 février 2020 une nouvelle version de sa plateforme www.cybermalveillance.gouv.fr. Outre une ergonomie et un graphisme entièrement refondus, les principaux changements portent sur les fonctionnalités permettant de couvrir mieux encore les missions clés du dispositif.




### ASSISTANCE ET OBSERVATION

Fort des remontées et données issues de sa plateforme, le dispositif a réorganisé et réadapté ses contenus et parcours en ligne. Dans cette version, les professionnels référencés sur Cybermalveillance.gouv.fr pour assister les victimes ont pu découvrir un espace qui leur est dédié, revu en profondeur, avec un espace documentaire en lien avec l'actualité, un système de gestion avec possibilité de qualifier la demande d'une victime, un suivi étape par étape de la relation avec la victime. Un système de remontée des rapports d'interventions rendu systématique permet à Cybermalveillance.gouv.fr d'alimenter ses données d'observation et de détecter d'éventuelles nouvelles menaces.

Côté « victime », les changements sont également notables, avec le diagnostic de l'incident rencontré, la création d'un espace de suivi des interventions pour une relation optimisée avec les professionnels de proximité référencés ou encore la possibilité de noter la qualité de la prestation rendue pour une transparence et une amélioration en continu du service.

**+155%** D'AUGMENTATION DE LA FRÉQUENTATION

**+325%** DE TRAFIC PROVENANT DES MOTEURS DE RECHERCHE

**+150%** DU NOMBRE DE COMPTES-RENDUS D'INTERVENTION DES PRESTATAIRES RÉFÉRENCÉS

**98%** DES CONTENUS SONT JUGÉS UTILES



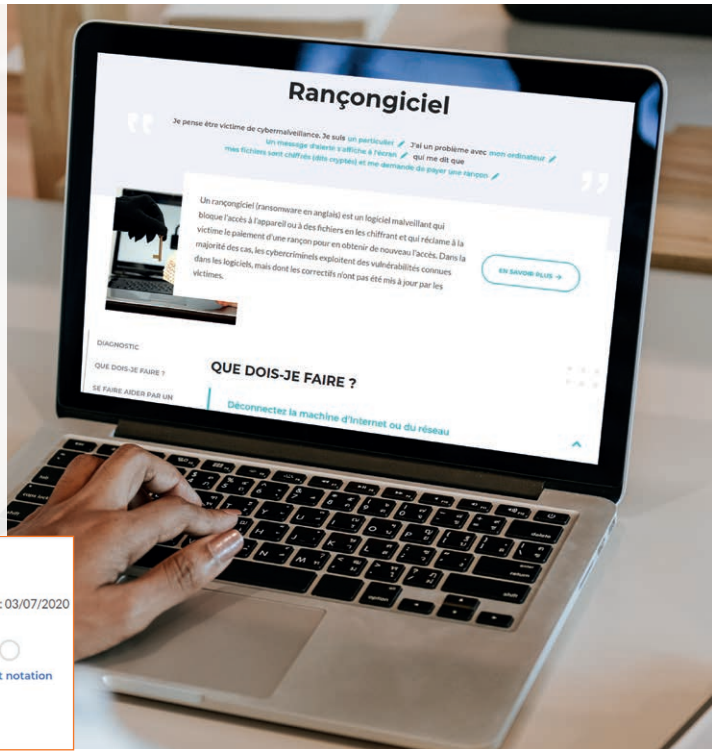
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

## PRÉVENTION ET SENSIBILISATION

Sur le volet de la sensibilisation, les contenus ont été réorganisés en rubriques distinctes : « comprendre les menaces et agir », « adopter les bonnes pratiques » et « l'actualité de la cybermalveillance ». Plus facilement accessibles et adaptées, les deux premières rubriques offrent aux internautes des conseils sur différents sujets susceptibles de les toucher ainsi que les moyens d'action lorsqu'ils sont victimes.

La rubrique « actualité de la cybermalveillance », quant à elle, a vocation à informer et alerter plus efficacement les populations et les pouvoirs publics. Des dossiers de fond thématiques en lien avec l'actualité y sont régulièrement proposés.





## AUTRES FICHES RÉFLEXES

### Le piratage de compte

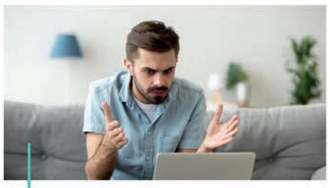
93680 15/01/2020 Temps de lecture : 16 min

Le piratage de compte désigne la prise de contrôle par un individu malveillant d'un compte (messagerie, réseau social...) au...

### L'hameçonnage (phishing)

109304 10/01/2020 Temps de lecture : 14 min

L'hameçonnage (ou phishing en anglais) est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à...



### Faire face aux arnaques au faux support technique

119096 20/12/2019 Temps de lecture : 14 min

Votre appareil semble bloqué et on vous demande de rappeler d'urgence un numéro de support technique ? L'arnaque au faux...

Nicolas **LAURENT**
Responsable des systèmes d'information
Dispositif Cybermalveillance.gouv.fr

J'ai eu le plaisir d'être nommé pilote de ce beau projet d'intérêt général, lancé il y a deux ans. Dans les nombreuses réflexions autour des fonctionnalités à déployer par rapport à la version précédente, nous avons souhaité créer plus de lien entre les victimes et nos professionnels référencés qui leur viennent en aide, ainsi qu'un accès plus optimal à nos contenus, enrichis dans cette version refondue. Pour mener à bien ce projet dans le respect du planning et du budget, j'ai eu la chance d'être entouré de passionnés et d'experts dans leur domaine, et je tiens à les remercier. Nous travaillons actuellement sur des évolutions dans une démarche d'amélioration continue des services rendus aux utilisateurs de la plateforme.

# GRANDS PROJETS ET PRINCIPALES RÉALISATIONS

## QUALITÉ / EXPERTISE / CONFIANCE : LE LABEL EXPERTCYBER

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

**Dans le cadre de sa mission d'assistance, Cybermalveillance.gouv.fr a pour objectif de mettre en relation des particuliers, des entreprises et des collectivités avec un réseau de professionnels en sécurité numérique pour les assister en cas de problème nécessitant une intervention technique.**

Face à la professionnalisation et la complexité des cyberattaques, il est apparu essentiel que les TPE, PME, collectivités et associations soient accompagnées dans leur sécurité numérique par des prestataires de confiance. Fin 2018, le dispositif a lancé un groupe de travail pour réfléchir à la reconnaissance de l'expertise des prestataires en sécurité numérique auprès des professionnels. Ce groupe a réuni CINOV Numérique, la Fédération EBEN*, la FFA** et le Syntec Numérique avec le soutien de l'AFNOR***, spécialiste de la certification, et donné naissance au label **ExpertCyber**.

Lancé officiellement le 20 mai 2020, ce label, premier dans son genre, permet de valoriser les entreprises de services informatiques justifiant d'une expertise en sécurité numérique sur les volets d'installation, de maintenance et d'assistance, et ainsi d'apporter aux bénéficiaires une meilleure lisibilité de la qualité d'offre de services pour être accompagné dans un cadre de confiance. Le processus de labellisation repose sur un questionnaire technique et un audit documentaire cadrés par un référentiel.

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

Afin de pérenniser ce projet clé du dispositif, un **comité de labellisation, constitué de membres du GIP et de l'AFNOR**, a pris la suite du groupe de travail afin d'assurer la gouvernance du label et de suivre ses évolutions futures.

**En reconnaissant l'expertise numérique des professionnels, le label ExpertCyber garantit ainsi un accompagnement de qualité et offre une meilleure lisibilité des prestations et services aux victimes.**

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

> « Le label est le fruit d'un travail collaboratif de plusieurs mois : un label créé par les prestataires, pour les prestataires, et avec comme objectif pour nos publics de pouvoir identifier facilement les spécialistes en sécurité numérique. »
>
> **Jérôme NOTIN**
> Directeur général
> de Cybermalveillance.gouv.fr.

* Fédération des Entreprises du Bureau et du Numérique
** Fédération Française de l'Assurance
*** Association française de normalisation

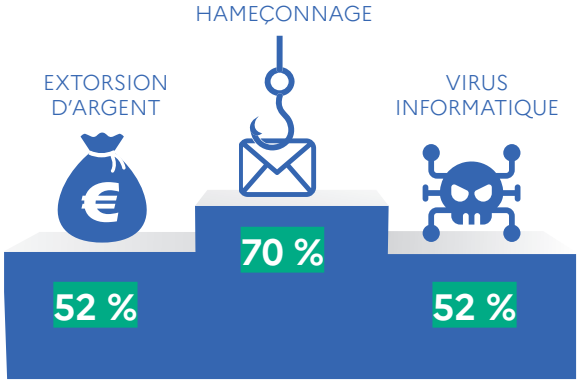
Le périmètre initialement envisagé pour ce label était l'assistance mais le groupe de travail a très vite conclu au nécessaire élargissement à la sécurisation et la maintenance. Cette approche était à la fois plus en phase avec la réalité du métier des prestataires de toutes tailles et mieux adaptée aux besoins des bénéficiaires.
Durant tout le processus de conception du label, le groupe de travail a eu à cœur de rester pragmatique face à la maturité des publics cibles (TPE/PME, collectivités et associations) sur le sujet de la sécurité numérique.
Notre volonté n'était pas de créer un label « à tiroir » ou à l'inverse un label « qui ferait absolument tout » mais de simplifier au maximum la lecture et l'accès à l'accompagnement avec un label qui couvre les besoins fondamentaux de ces publics : la sécurisation, la maintenance et l'assistance.

# **ENQUÊTE** SUR LE NIVEAU D'EXPOSITION AU RISQUE NUMÉRIQUE ET LA NOTORIÉTÉ DU DISPOSITIF

En partenariat avec l'INC, Cybermalveillance.gouv.fr a renouvelé en 2020 son étude annuelle visant à connaître l'exposition aux risques des internautes ainsi que son niveau de notoriété auprès du grand public, pour mieux adapter ses outils et messages de prévention. Cette étude, menée au mois de juillet, dévoile que plus de 90 % des internautes sondés ont déjà été victimes au moins une fois d'un acte de cybermalveillance, alors que pourtant 80 % des personnes interrogées se disent suffisamment sensibilisées et informées sur les risques liés à Internet.

## LES ACTES DE CYBERMALVEILLANCE LE PLUS SOUVENT RENCONTRÉS

À l'instar des résultats de l'étude effectuée en 2019, celle de 2020 dresse le palmarès des trois actes de cybermalveillance le plus souvent rencontrés par les internautes :




L'étude révèle également que **39 % des sondés ont indiqué avoir reçu un courriel d'un interlocuteur prétendant avoir piraté leur ordinateur** ou webcam, **25 % ont eu leur compte de messagerie ou de réseau social piraté** et utilisé à leur insu, et **10 % ont subi un cyberharcèlement**. Parmi ceux qui ont été victimes de fraude à la carte bancaire, 84 % ont contacté leur banque mais **seulement 26 % ont déposé plainte.** Dans la plupart des cas, les répondants n'ont rien fait de particulier ou se sont débrouillés seuls, sauf pour l'utilisation de la carte bancaire sur Internet à leur insu avec vol d'argent où la prise de contact auprès de la banque est courante.

## UNE NOTORIÉTÉ EN DÉVELOPPEMENT

D'après l'étude, la moitié des répondants affirme ne pas savoir à qui s'adresser en cas de problème et ne sait pas donner spontanément de nom de sites ou d'organismes pour les aider en cas de cybermalveillance. Alors que le dispositif a fêté ses 3 ans d'existence en 2020, l'étude souligne qu'en notoriété assistée, **43 % des internautes déclarent avoir entendu parler de www.cybermalveillance.gouv.fr** et 7 % d'entre eux ont utilisé le service. La première source de notoriété est la recherche sur Internet (31 %), suivie de la presse (15 %) puis le bouche-à-oreille (9 %).

## POURSUIVRE DES ACTIONS DE SENSIBILISATION, UNE NÉCESSITÉ

Comme l'année précédente, ces résultats alertent sur la nécessité de poursuivre les actions de sensibilisation sur les risques numériques auprès des publics pour leur donner les bons réflexes en cas d'attaque, et les aider à mieux comprendre les risques pour s'en prémunir.

**Enjeu de société majeur, la sécurité numérique est l'affaire de tous et Cybermalveillance.gouv.fr doit devenir le premier réflexe sécurité des citoyens connectés.**

# 2. MISSIONS ET ORGANISATION DU GIP

# 2 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 et à toutes les 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 prestataires de proximité susceptibles de les assister.

**2 LA SENSIBILISATION DES PUBLICS AUX RISQUES NUMÉRIQUES**
au travers de contenus et de campagnes de prévention à la sécurité du numérique.

**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 **49 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…

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.

# 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'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 2020

**Collège étatique :** MINISTÈRE DES ARMÉES

**Collège utilisateurs :** coTer numérique, DÉCLIC., MEDEF

**Collège offreurs de solutions et services :** afnic, Banque des Territoires, CCR Re, Google, Neuflize OBC



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

# **PAROLES** DE MEMBRES

« L'accord entre le ministère des Armées et le GIP ACYMA est en droite ligne et pleinement cohérent avec l'orientation stratégique présentée par le Président de la République, le 18 février 2021 : il s'agit bien de renforcer les synergies dans l'ensemble des régions entre petits et grands acteurs de la filière cyber et entre industriels et recherche. »

**Florence PARLY**
Ministre des Armées

« Le GIP ACYMA s'est imposé comme l'un des partenaires privilégiés de la section de lutte contre la cybercriminalité du parquet de Paris. Des réseaux de cybercriminels ont pu être démantelés cette année grâce à leur action et à leur réactivité dans le partage de l'information collectée. ACYMA nous offre également une aide précieuse pour la prise en charge efficace des victimes. »

**Johanna BROUSSE**
Vice-procureur, Chef de la section J3
Lutte contre la cybercriminalité
JUNALCO* – Tribunal judiciaire de Paris

*Juridiction nationale chargée de la lutte contre la criminalité organisée

« La Fédération EBEN qui rassemble les prestataires IT, télécoms et réseaux a rejoint Cybermalveillance.gouv.fr afin de contribuer à cette mission d'assistance et de prévention du risque numérique. Nous sommes fiers de participer à cette initiative essentielle pour accompagner la transformation numérique et instaurer un environnement de confiance pour les entreprises et les citoyens. »

**Delphine CUYNET**
Directrice générale de la Fédération EBEN

« L'explosion du numérique avec la crise de la COVID-19 occasionne par là même une recrudescence des actes d'hameçonnage et de violations des données personnelles des internautes. Déterminée à permettre à chacun de garder la main sur ses données et lutter contre les fraudes, l'UFC-Que Choisir continue son action au sein du groupement Cybermalveillance.gouv.fr. L'objectif est bien, par l'information et les outils proposés, de faire des citoyens les premiers acteurs de la cybersécurité ! »

**Alain BAZOT**
Président de l'UFC-Que Choisir

« Être membre de Cybermalveillance.gouv.fr est une évidence et s'inscrit dans la tradition de notre entreprise. De par ses missions de service public, son histoire et son ambition le Groupe La Poste est une entreprise qui s'engage et a fait de la confiance numérique un des piliers de son nouveau plan stratégique. Nous ne pouvons qu'être engagés aux côtés de Cybermalveillance.gouv.fr. »

**Gabriel DE BROSSES**
Directeur de la cybersécurité
du Groupe La Poste

« Parce que la santé numérique est un enjeu collectif, le dispositif Cybermalveillance.gouv.fr apporte au plus grand nombre une réponse concrète au besoin d'accompagnement des victimes et de sensibilisation aux cybermenaces. En tant qu'acteur de la cybersécurité, Stormshield est fier de participer à une telle initiative d'intérêt général. »

**Pierre-Yves HENTZEN**
CEO de Stormshield

# 3 UN PARTENARIAT PUBLIC – PRIVÉ AU SERVICE D'UNE MISSION D'INTÉRÊT GÉNÉRAL

# EXEMPLES DE COLLABORATIONS EN 2020

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

## FORMATION À LA CYBERSÉCURITÉ POUR LES TPE / PME, AVEC GOOGLE FRANCE ET LA FEVAD

**À l'occasion de la Paris Cyber Week et du mois européen de la cybersécurité (Cybermoi/s), Google France a lancé avec Cybermalveillance.gouv.fr et la FEVAD un nouveau programme de formations gratuites visant à sensibiliser les TPE et les PME sur les bonnes pratiques en matière de cybersécurité.**

L'objectif de ce programme est de les aider à développer leur activité en ligne en toute sécurité, un enjeu de taille notamment pour les acteurs du e-commerce.

Créé en partenariat avec les trois entités, ce programme se compose d'une initiation générale à la cybersécurité suivie de deux modules dédiés aux enjeux spécifiques de la cybersécurité pour le commerce en ligne et le télétravail.

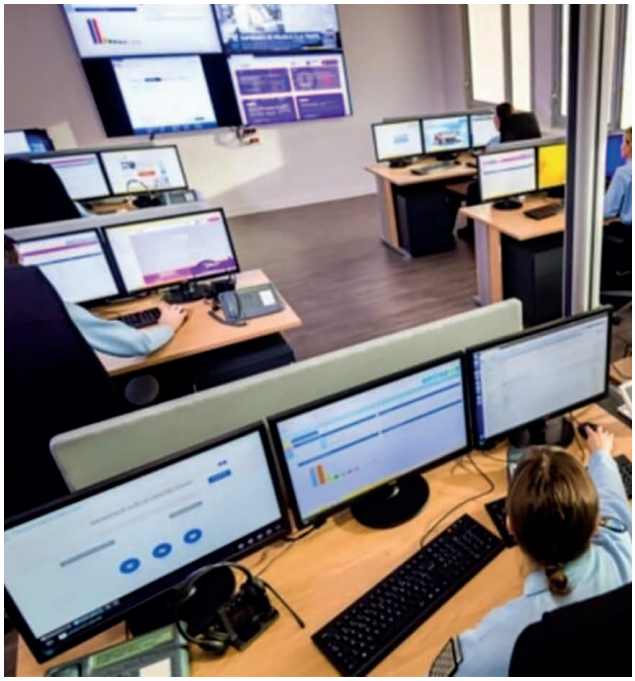
## LA BRIGADE NUMÉRIQUE BNUM

**Depuis le 20 avril 2020, Cybermalveillance.gouv.fr a complété son offre de service en permettant à ses usagers professionnels (entreprises, associations, collectivités) d'être mis directement en relation depuis sa plateforme avec la BNUM de la Gendarmerie nationale.**

Fruit d'une réflexion initiée plusieurs mois auparavant entre la Gendarmerie nationale et Cybermalveillance.gouv.fr, les travaux se sont intensifiés et accélérés en mars et avril pour pouvoir apporter au plus vite ce nouveau service aux usagers professionnels, dans un contexte particulier de confinement.

Joignables sur un service de messagerie instantanée (Tchat) 7 jours sur 7 et 24 heures sur 24, les gendarmes de la brigade numérique peuvent désormais fournir aux usagers professionnels de la plateforme Cybermalveillance.gouv.fr un conseil interactif dans leurs démarches, en particulier de dépôt de plainte, et les orienter, si nécessaire, vers les unités spécialisées compétentes.

L'accès à cette nouvelle fonctionnalité est disponible pour les usagers professionnels de la plateforme Cybermalveillance.gouv.fr depuis leur espace personnel ainsi qu'en fin des parcours de diagnostic et d'assistance de cybermalveillance qui peuvent le nécessiter.



## ESCROQUERIES AU CPF AVEC LE GROUPE CAISSE DES DÉPÔTS (CDC)

**Suite à l'identification à l'été 2020 d'une nouvelle forme d'escroquerie autour du Compte Personnel de Formation (CPF) visant à détourner les droits à la formation des salariés et demandeurs d'emploi, Cybermalveillance.gouv.fr a initié une coopération avec le groupe Caisse des Dépôts (CDC), qui gère le site Moncompteformation.gouv.fr.**

Par des échanges d'informations, cette collaboration a permis de cerner le phénomène, d'en mesurer la portée et d'envisager les actions nécessaires pour l'endiguer. Parallèlement, Cybermalveillance.gouv.fr a signalé l'ampleur des faits observés à la section J3 (cybercriminalité) du parquet de Paris qui s'est saisi du dossier. Dès début novembre, Cybermalveillance.gouv.fr a complété son **outil de diagnostic et d'assistance en ligne** pour intégrer cette menace et un article a été publié sur le site Internet du dispositif pour informer les publics sur cette menace ainsi que leur prodiguer les conseils utiles pour y faire face. Ces nouveaux service et publication ont été largement plébiscités par les utilisateurs de la plateforme.

**Cet exemple démontre tant la réactivité nécessaire pour identifier les phénomènes que le besoin de développer les synergies et partenariats pour apporter la meilleure assistance aux victimes.**

# **ZOOM** SUR LES GROUPES DE TRAVAIL AU SEIN DU GIP ACYMA

Les groupes de travail sont constitués essentiellement des membres du GIP. Ils se réunissent à plusieurs reprises tout au long de l'année pour travailler sur des sujets et projets majeurs pour le dispositif. Au nombre de trois pour l'année 2020, ils ont porté sur l'étude préalable à la création de l'observatoire du risque numérique, la sensibilisation des collectivités territoriales et la mise à disposition des outils et services techniques (préventifs et curatifs) dans un cadre de confiance.

| GROUPE DE TRAVAIL | FINALITÉ / OBJECTIF | MEMBRES CONCERNÉS |
|---|---|---|
| GT COLLECTIVITÉS | Sensibiliser les élus aux risques numériques et partager avec eux les bonnes pratiques | Ministère de l'Intérieur |
| GT OUTILS | Mettre à disposition des outils et services techniques (préventifs et curatifs) dans un cadre de confiance | Ministère de l'Intérieur<br>Services du Premier ministre |
| GT OBSERVATOIRE | Mener l'étude préalable à la création de l'observatoire du risque | Ministère de l'Économie, des Finances et de la Relance<br>Ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation<br>Ministère de la Justice<br>Ministère de l'Intérieur |

# 4 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 principales missions du dispositif Cybermalveillance.gouv.fr. Outre la production de contenus de sensibilisation et la contribution aux contenus produits par des tiers, Cybermalveillance.gouv.fr a participé ou lancé en 2020 des actions destinées à tous les publics, dans une volonté de développer sa visibilité auprès du grand public et de renforcer sa présence dans son écosystème.

## TOUS PUBLICS

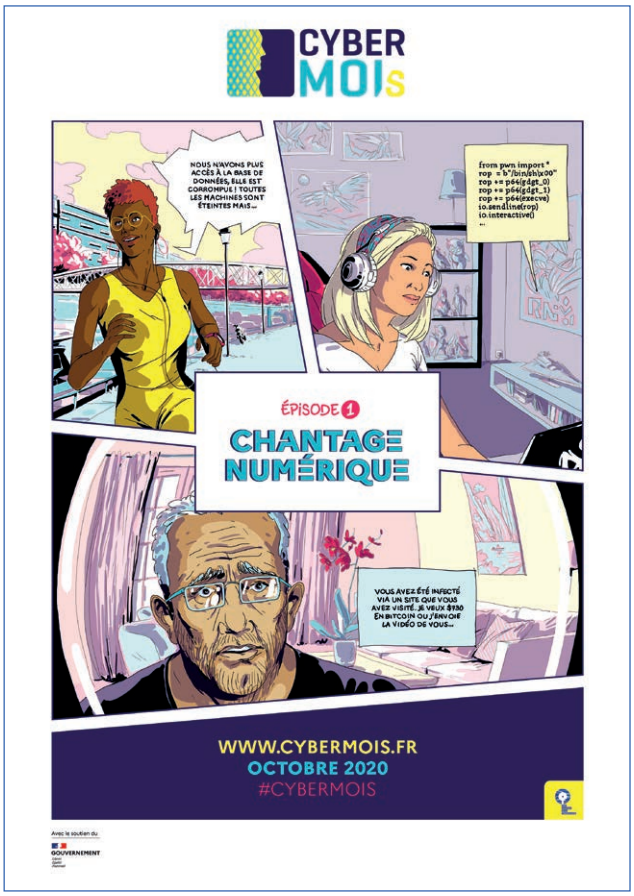
Les actions de sensibilisation ayant été impactées par la crise sanitaire, divers projets ont néanmoins pu voir le jour pour permettre à Cybermalveillance.gouv.fr de toucher ses publics, notamment à travers des campagnes médias d'information et de sensibilisation.

**Campagne télévisée « les réflexes essentiels pour votre sécurité numérique »** avec la diffusion de plus de 451 spots de sensibilisation du 18 mai au 21 juin 2020 sur les chaînes des groupes France Télévision, TF1 et Canal+ (voir page 32);

**Campagne vidéo de sensibilisation dans tous les bureaux de poste en métropole**. Du 5 au 31 octobre 2020, le Groupe La Poste, membre du dispositif, a diffusé plusieurs fois par jour sur les écrans de ses bureaux de poste des spots de sensibilisation sur les thématiques: « gestion des mots de passe » et « hameçonnage » du 5 au 17 octobre, et « mises à jour » et « sauvegardes » du 19 au 31 octobre;

> « Dans le cadre du mois européen de la cybersécurité « Cybermoi/s » en octobre 2020, le Réseau La Poste s'est associé à Cybermalveillance.gouv.fr pour relayer les campagnes de sensibilisation aux risques cyber menées par le GIP. Quatre vidéos ont été diffusées dans plus de 6 000 bureaux pour sensibiliser les clients de La Poste aux menaces auxquelles ils sont de plus en plus exposés. Ces clips ont ainsi pu être présentés à plusieurs centaines de milliers de nos clients. »
>
> **Gabriel DE BROSSES**
> Directeur de la cybersécurité
> du Groupe La Poste

**Participation au CYBERMOI/S 2020, un mois pour se protéger du chantage numérique.** Pour faire face à l'intensification des cyberattaques, la campagne de sensibilisation du Cybermoi/s pilotée par l'ANSSI en octobre 2020 a donné aux professionnels et aux particuliers les clés pour mieux comprendre et prévenir les menaces, en particulier celles liées au chantage numérique. Si le dispositif s'est appuyé sur ses membres pour démultiplier ses actions de sensibilisation, il a aussi apporté sa contribution active:






RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité 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 de bonnes pratiques et fiches réflexes pour une bonne hygiène numérique, en particulier autour du chantage numérique (webcam prétendue piratée, rançongiciels…);

- **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 22 octobre au 29 novembre (lire l'encart page 33);

- **L'exploitation des résultats de l'étude sur la perception des enjeux autour de la sécurité numérique des citoyens, pour faire évoluer les comportements.** Lancée fin 2019, avec une restitution début 2020, ses résultats ont permis d'adapter les messages et outils de sensibilisation de cette nouvelle édition du Cybermoi/s.

## PROFESSIONNELS

Durant l'année écoulée, Cybermalveillance.gouv.fr a participé à 55 événements externes ou organisés par le dispositif et ses membres. Salons, conférences en ligne ou tables rondes, ces événements s'adressaient principalement aux professionnels (FIC, Live Session de Niort Numeric, Paris Cyber Week, etc.).

### LE FORUM INTERNATIONAL DE LA CYBERSÉCURITÉ (FIC)

Le FIC s'est tenu les 28, 29 et 30 janvier 2020 à Lille. S'imposant comme un événement de référence en matière de sécurité et de confiance numérique, plus de 12 500 participants ont pris part à l'événement. À cette occasion, Cybermalveillance.gouv.fr a présenté sa nouvelle plateforme d'assistance lors d'une conférence de presse (voir page 12).


Visite de Christophe Castaner, ministre de l'Intérieur, sur le stand de Cybermalveillance.gouv.fr au FIC.

### TOUR DE FRANCE CYBER (TDFCYBER)

Cybermalveillance.gouv.fr était partenaire du TDFCyber 2020 organisé par le CyberCercle. À travers ses étapes en région, il a pour vocation de porter les sujets de sécurité et de confiance numériques au plus près des acteurs présents sur les territoires (secteurs public et privé, élus, spécialistes de la cybersécurité nationaux, européens et locaux, associations, collectivités…). En raison de la situation sanitaire, la programmation du TDFCyber s'est adaptée pour se tenir exclusivement en distanciel (Normandie et Auvergne Rhône-Alpes).

Le dispositif a également participé aux petits déjeuners débats du CyberCercle au cours de l'année pour faire découvrir ses services et son nouveau label ExpertCyber.

# 4 LA SENSIBILISATION, PREMIÈRE ARME CONTRE LES CYBERMALVEILLANCES

## PARIS CYBER WEEK (PCW)

Cybermalveillance.gouv.fr a été partenaire de l'édition 2020 de PCW, événement qui s'est déroulé les 30 septembre et 1er octobre. Celui-ci rassemble 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. Cette année, PCW a réuni 150 décideurs publics et privés en provenance de 12 pays européens.

> « La présence de Cybermalveillance.gouv.fr à nos côtés est un soutien stratégique pour Paris Cyber Week. Pierre angulaire de la sécurité numérique du quotidien, l'engagement de ce dispositif sur le terrain en fait un acteur national de proximité dont le regard est précieux pour les réflexions stratégiques des hauts décideurs qui participent à l'événement. Nous sommes donc fiers de pouvoir compter sur lui parmi nos soutiens de la première heure et reconnaissants de sa confiance, et nous espérons pouvoir nous appuyer sur cette expertise pour de nombreuses années encore. »
>
> **Sébastien GARNAULT**
> Fondateur de la Paris Cyber Week

## CONFÉRENCE EN LIGNE DE BANQUE DES TERRITOIRES

Le 17 décembre 2020 s'est tenue une conférence en ligne intitulée « Comment bâtir un environnement numérique de confiance pour les collectivités ? » organisée par Banque des Territoires (Groupe Caisse des Dépôts), nouveau membre du GIP, en partenariat avec Cybermalveillance.gouv.fr. Une table ronde centrée sur les bons réflexes à adopter en cybersécurité a permis aux experts présents d'expliquer le contexte global des cyberattaques, les enjeux et la gestion de tels incidents, ainsi que les enseignements à en tirer pour renforcer sa sécurité numérique. Cet événement fut également l'occasion pour le dispositif de présenter son programme de sensibilisation des élus aux risques numériques.

Conférence en ligne du 17 décembre 2020 organisée par Banque des Territoires.

# **ZOOM** SUR LES COLLECTIVITÉS TERRITORIALES

## PROGRAMME DE SENSIBILISATION DES ÉLUS

**Les cyberattaques envers les collectivités territoriales ne cessent de se multiplier. Si certaines communes ont pris conscience des risques, elles sont encore trop peu nombreuses à les anticiper.**

Afin d'aider les élus à mieux appréhender les risques qu'ils encourent et leur apporter des conseils pratiques en matière de sécurité numérique, Cybermalveillance.gouv.fr, avec le concours de la fédération Déclic, CoTer Numérique, l'ANSSI et le ministère de l'Intérieur, a lancé un programme de sensibilisation aux risques numériques destiné aux élus.

Interpeller ces publics sur ce sujet est un enjeu essentiel qui concerne toutes les collectivités, quelle que soit leur taille. En 2019, 1 200 d'entre elles étaient venues chercher de l'assistance sur la plateforme ; ce chiffre a augmenté de 15 % en 2020 (voir page 47). Pour la première étape de ce programme, Cybermalveillance.gouv.fr a répondu aux questions de deux maires sur les principales menaces numériques rencontrées par les collectivités et leurs conséquences, et a dispensé ses conseils sur les premiers gestes essentiels à adopter en sécurité numérique.

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

En parallèle, Cybermalveillance.gouv.fr a réalisé en partenariat avec Banque des Territoires une série de quatre vidéos de sensibilisation destinées aux collectivités. Sur le thème des rançongiciels, du piratage ou encore des fuites de données, ces vidéos ont été diffusées et reprises sur différents canaux (réseaux sociaux, sites, lettres d'information…).



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

*Quotidiennement exposées à travers leurs outils numériques (site web, messagerie, portails de paiement…), les collectivités ne réalisent pas toujours les risques qu'elles encourent : hameçonnage, rançongiciels… Afin d'aider les élus à prendre conscience de ces enjeux, Cybermalveillance.gouv.fr a lancé un programme de sensibilisation dédié. Nous remercions les membres de notre groupe de travail « Collectivités » pour leur mobilisation et leur engagement malgré le contexte sanitaire compliqué, ainsi que les nombreux relais qui ont accepté de communiquer sur ce programme.*

# LES ACTIONS DE SENSIBILISATION MARQUANTES DE L'ANNÉE

## CAMPAGNE NATIONALE TV-MÉDIAS DE SENSIBILISATION « LES RÉFLEXES ESSENTIELS POUR VOTRE SÉCURITÉ NUMÉRIQUE »

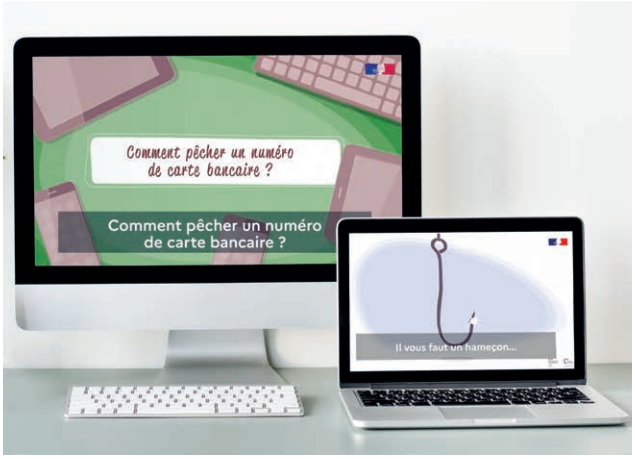
Dans un contexte de crise sanitaire, Cybermalveillance.gouv.fr a lancé en partenariat avec le groupe France Télévisions une campagne de sensibilisation aux risques numériques à destination du grand public.

Avec la recrudescence des cyberattaques et autres arnaques massives liées à l'augmentation des usages numériques et à l'intensification du recours au télétravail, Cybermalveillance.gouv.fr et le groupe France Télévisions se sont associés à travers une campagne intitulée « **Les réflexes essentiels pour votre sécurité numérique** ».

Composée d'une série de quatre spots thématiques et de supports numériques déclinés, la campagne a été diffusée sur les chaînes du groupe France Télévisions du 18 mai au 21 juin 2020. Elle a également été relayée sur les réseaux sociaux des deux institutions.

Destiné à tous les publics et ce, quel que soit leur niveau de connaissance en cybersécurité, le thème général de la campagne porte sur les principaux gestes simples à adopter pour assurer sa sécurité numérique :

- **LES MOTS DE PASSE :** « Pourquoi dit-on mot de passe et pas mot de passoire ? » (comment bien gérer ses mots de passe) ;
- **LES MISES À JOUR :** « Comment mettre en échec le piratage ? » (souvent ressenties comme une contrainte, les mises à jour des appareils numériques corrigent les failles de sécurité) ;
- **LES SAUVEGARDES :** « Comment gommer les accidents numériques ? » (pourquoi faire ses sauvegardes est indispensable ?) ;
- **L'HAMEÇONNAGE :** « Comment pêcher un numéro de carte bancaire ? » (comment reconnaître le *phishing*) ?




En contribuant à relayer gracieusement ces réflexes essentiels en matière d'hygiène numérique sur ses différents supports, le groupe France Télévisions s'est associé à la mission de prévention et d'assistance au risque numérique du dispositif dans l'intérêt des populations.

**451 SPOTS TV**
DIFFUSÉS SUR LES CHAÎNES (France Télévisions, Groupe TF1 et Canal+)

**Cette campagne a également été diffusée sur les chaînes du Groupe TF1 et Canal+ dans le cadre d'une campagne d'intérêt général, pour un nombre de diffusions total de 451 spots sur la période. Cybermalveillance.gouv.fr remercie à nouveau ces chaînes pour leurs relais.**

Retrouvez l'ensemble de ces vidéos sur : www.cybermalveillance.gouv.fr

## CAMPAGNE NATIONALE D'INFORMATION ET DE SENSIBILISATION « CONSOMAG »

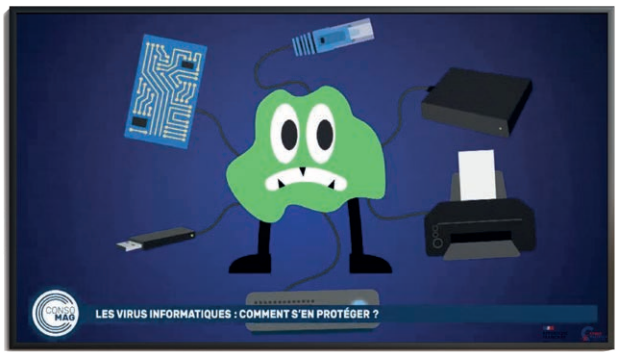
Afin d'améliorer la sécurité numérique des consommateurs et dans le cadre du mois européen de la cybersécurité, Cybermalveillance.gouv.fr a renouvelé son partenariat avec l'INC pour le lancement d'une campagne sur les risques numériques, composée d'une série de quatre émissions ConsoMag thématiques au format questions-réponses d'experts. Cette campagne a été diffusée sur les chaînes du groupe France Télévisions du 22 octobre au 13 novembre 2020.

**CONSOMAG**
**2,5 millions**
de téléspectateurs par émission

**Relais du programme de diffusion de la campagne auprès de 150 000 abonnés au magazine *60 Millions de Consommateurs* d'octobre 2020**

### QUE FAIRE EN CAS D'UTILISATION FRAUDULEUSE DE VOTRE CARTE BANCAIRE ?


### LES VIRUS INFORMATIQUES : COMMENT S'EN PROTÉGER ?




### ATTENTION AU PIRATAGE DE COMPTE EN LIGNE !

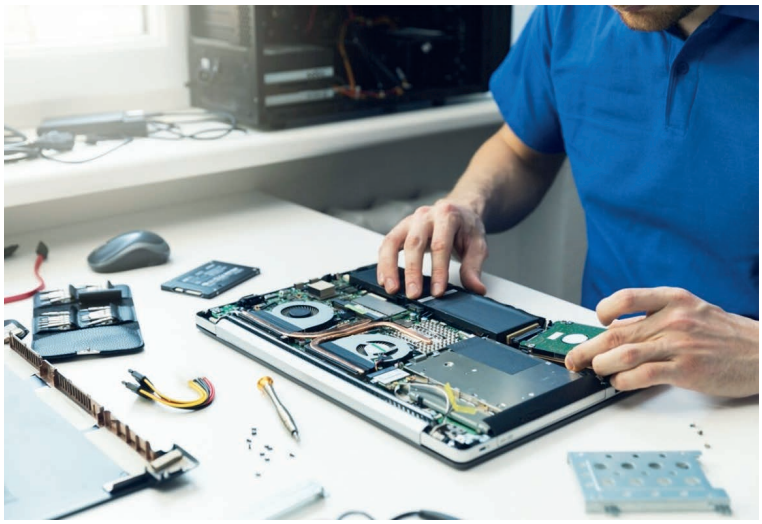

### QUE FAIRE POUR NE PAS ÊTRE VICTIME D'HAMEÇONNAGE ?


Retrouvez l'ensemble de ces vidéos sur : www.cybermalveillance.gouv.fr

# 5 L'ASSISTANCE AUX VICTIMES, UN BESOIN, UNE NÉCESSITÉ

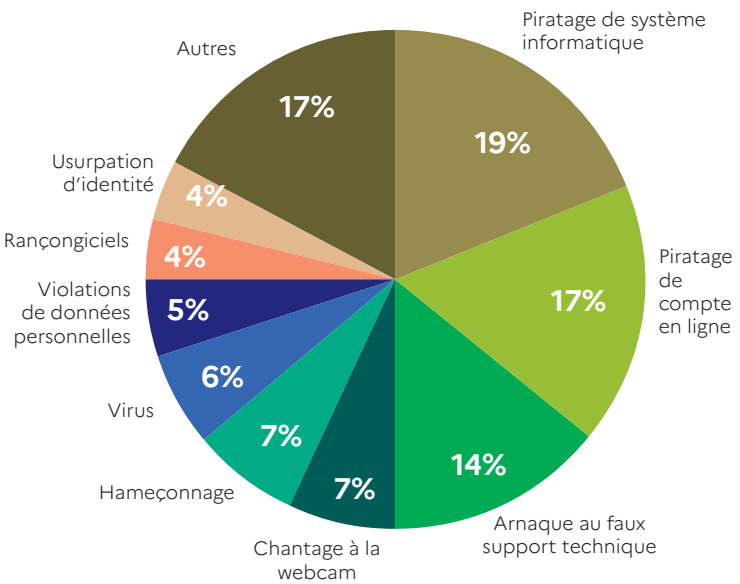
# UN RÉSEAU DE PRESTATAIRES D'ASSISTANCE AUX VICTIMES

**Parce que les victimes n'ont pas toujours la compétence technique nécessaire pour appliquer certains des conseils prodigués par la plateforme suite au diagnostic en ligne, Cybermalveillance.gouv.fr propose un réseau de professionnels en mesure de leur apporter une assistance sur la cybermalveillance qu'elles rencontrent.**



Avec la mise en place de la nouvelle version de la plateforme début 2020, une campagne de réinscription des prestataires a été lancée avec un contrôle administratif renforcé. Ce sont près de **1000 professionnels en sécurité numérique** qui ont ainsi été référencés en fin d'année. Ce **réseau unique** couvre l'ensemble du territoire national afin de pouvoir intervenir en proximité géographique et diffuser les messages de prévention du dispositif aux victimes.

Suite à une demande de mise en relation au travers de la plateforme avec ces professionnels, les victimes reçoivent des réponses en moins d'une heure dans 75 % des cas. Toutes catégories de victimes confondues, les demandes de mise en relation avec un professionnel référencé concernent principalement les cas de piratage de système informatique (19 %), de piratage de compte en ligne (17 %), d'arnaque au faux support technique (14 %), de chantage à la webcam (7 %), d'hameçonnage (7 %), de virus (6 %), de violation de données personnelles (5 %), de rançongiciels (4 %) et d'usurpation d'identité (4 %).




**CATÉGORIES CONCERNÉES PAR LES DEMANDES DE MISES EN RELATION AVEC UN PRESTATAIRE RÉFÉRENCÉ**



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

En 2020, ce réseau de professionnels a transmis au dispositif près de **900 comptes-rendus d'intervention** au travers d'une interface rénovée. Ces comptes-rendus riches d'informations permettent à Cybermalveillance.gouv.fr d'avoir la vision la plus précise possible sur l'état de la cybermalveillance et des pratiques au plus près des usagers, et de pouvoir faire évoluer son offre de services en conséquence.

## CARACTÉRISTIQUES DES PROFESSIONNELS RÉFÉRENCÉS SUR LA PLATEFORME

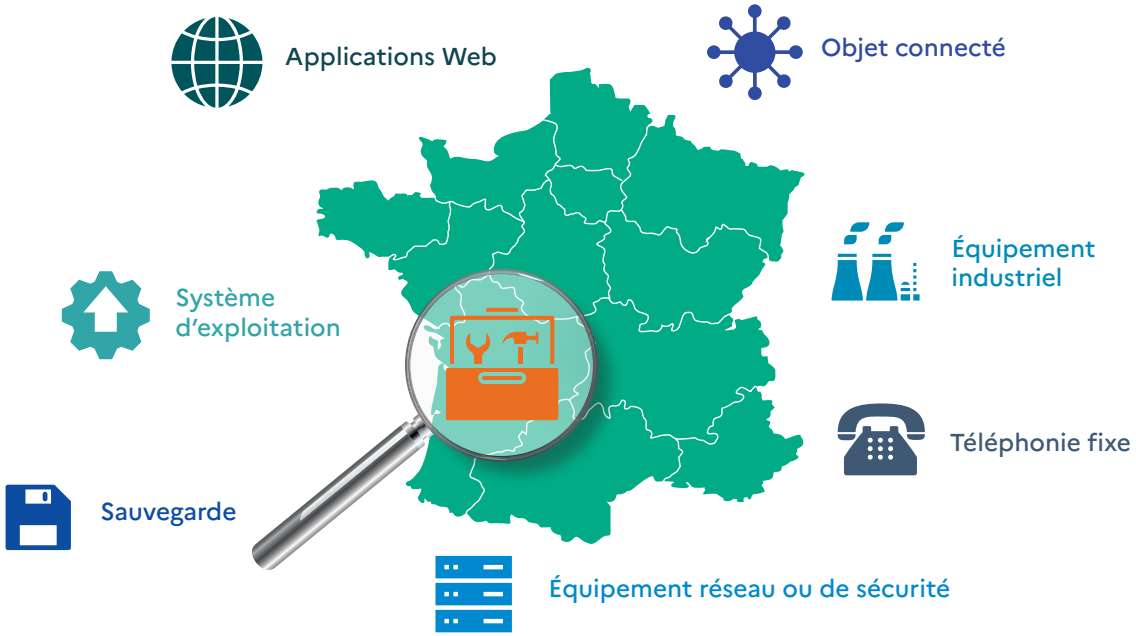
| | |
|---|---|
| CHAMPS D'ACTIONS | ASSISTANCE |
| PUBLICS CONCERNÉS | PARTICULIERS ET/OU PROFESSIONNELS (TPE, PME, COLLECTIVITÉS, ASSOCIATIONS...) |
| VALIDITÉ DU STATUT | DURÉE INDÉTERMINÉE |
| MISE EN RELATION | INTERVENTION SUR INCIDENT |

**900**
COMPTES-RENDUS D'INTERVENTION

**1000**
PROFESSIONNELS RÉFÉRENCÉS FIN 2020

**75 %**
DES DEMANDES D'ASSISTANCE REÇOIVENT UNE RÉPONSE D'UN PRESTATAIRE EN MOINS D'UNE HEURE

## LES DOMAINES DE COMPÉTENCES COUVERTS PAR LES PRESTATAIRES



# DES CONSEILS & CONTENUS ACTUALISÉS DÈS QU'UNE NOUVELLE CATÉGORIE DE MENACE EST IDENTIFIÉE

Cybermalveillance.gouv.fr a complété son outil de diagnostic et produit de nouveaux contenus au cours de l'année 2020.

## ENRICHISSEMENT DE L'OUTIL DE DIAGNOSTIC EN LIGNE

Dans la première version de la plateforme, le nombre de diagnostics traités était limité aux 23 principales catégories de cybermalveillance identifiées. Dans la nouvelle version de la plateforme livrée début 2020 et fort des retours des utilisateurs, **l'outil de diagnostic a été complètement refondu pour intégrer 12 cas de cybermalveillances supplémentaires, offrant une plus grande exhaustivité** vis-à-vis des attentes des publics. Pour recueillir plus facilement les retours des victimes, une nouvelle fonctionnalité a par ailleurs été mise en place. Au fil des mois, elle a permis d'enrichir l'outil de diagnostic et d'assistance de 9 nouvelles menaces qui n'avaient pas été jusqu'alors identifiées et pour lesquelles une attente des publics était constatée. **Fin 2020, ce sont 44 formes de cybermalveillances qui sont traitées par cet outil, avec plus de 400 conseils adaptés et déclinés selon les cas.**

**L'indice de satisfaction des utilisateurs de l'outil de diagnostic et d'assistance en ligne a été de 86,3 % en 2020.** Les travaux menés pour compléter et optimiser cet outil sont réalisés dans une démarche d'amélioration continue, en exploitant notamment les retours de motifs d'insatisfaction.

À titre d'exemple, dès l'été 2020, cette fonctionnalité a permis d'identifier un phénomène relativement important d'**arnaques sur les comptes personnels formations (CPF)** qui n'était pas traité par l'outil d'assistance en ligne et sur lesquels les particuliers demandaient de l'assistance. Après avoir analysé ce phénomène et ses modes opératoires, **un rapprochement a été réalisé avec le groupe Caisse des Dépôts**, membre du dispositif, qui opère la plateforme Moncompteformation.gouv.fr sur laquelle ces escroqueries étaient basées. L'outil d'assistance en ligne a intégré cette nouvelle menace et un article complet a été publié pour expliquer aux publics le phénomène et les mesures à prendre pour y faire face.

Sur les deux derniers mois de l'année, preuve d'une réelle attente des publics, **cette nouvelle forme de cybermalveillance s'est classée 5e (sur 44) des recherches d'assistance réalisée sur la plateforme**.

**44**
FORMES DE CYBERMALVEILLANCES TRAITÉES DANS L'OUTIL DE DIAGNOSTIC

**400**
CONSEILS




RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

## PUBLICATION D'ARTICLES SUR LE SITE CYBERMALVEILLANCE.GOUV.FR

Qu'ils soient de fond ou d'actualité, **33 articles** ont été publiés sur le site Internet en 2020.
Quelques-uns des sujets traités :

- Arnaques par message électronique : comment identifier et déjouer l'hameçonnage ?
- Recommandations de sécurité informatique pour le télétravail en situation de crise.
- Comment choisir un bon mot de passe lorsque vous créez un compte sur Internet ?
- Appareils numériques, applications, logiciels… : pourquoi est-il dangereux de négliger leurs mises à jour ?
- Campagnes de messages d'escroquerie usurpant l'identité de la Police et de la Gendarmerie.

## NOUVEAUX CONTENUS DE PRÉVENTION

Dans la continuité de l'année 2019, Cybermalveillance.gouv.fr a mis à jour ses contenus et conçu des supports de sensibilisation sur de nouvelles thématiques d'actualité. Scindés en deux catégories pour une meilleure appropriation par les publics, ceux-ci prennent la forme :

- **de conseils pour adopter les bonnes pratiques en matière de sécurité numérique** : généralement présentés en 10 points, les conseils donnés offrent au lecteur les règles de base de sécurité numérique sur le thème abordé ;
- **de fiches « réflexes » pour mieux comprendre les menaces et agir** : les sujets de ces fiches sont essentiellement issus des remontées de la plateforme d'assistance Cybermalveillance.gouv.fr et sont traités sous l'angle infractionnel.

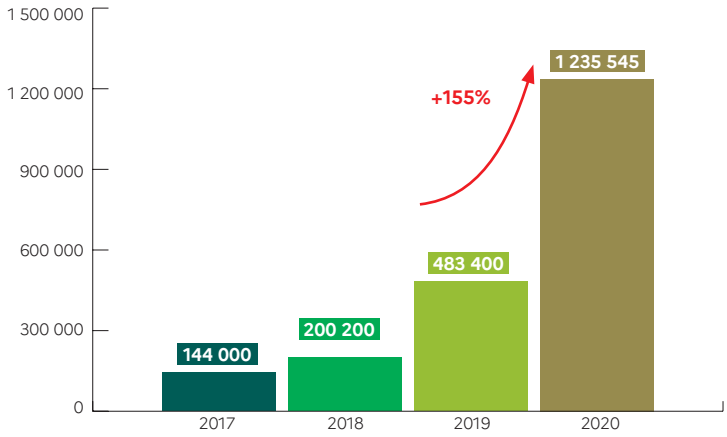
**Six nouvelles fiches ont été publiées sur le site Internet en 2020 :**

1. le spam électronique ;
2. le spam téléphonique ;
3. la sécurisation du télétravail ;
4. la sécurité des objets connectés (IoT) ;
5. le chantage à l'ordinateur ou à la webcam prétendus piratés ;
6. la fraude à la carte bancaire.

# LA RÉPONSE À UN BESOIN DES POPULATIONS : L'ASSISTANCE EN CHIFFRES

Depuis son lancement en 2017, la plateforme Cybermalveillance.gouv.fr a reçu plus de 2 millions de visiteurs et sa fréquentation ne cesse de progresser. Cette plateforme propose un service de diagnostic et d'assistance en ligne. L'utilisateur peut y décrire la situation rencontrée en fonction de son profil (particulier, entreprise, association, collectivité, administration). En répondant à une série de questions, un diagnostic de sa situation lui est proposé et les conseils adaptés pour y faire face lui sont prodigués. Au besoin, il peut même être mis en relation, quand cela apparaît pertinent, avec des professionnels spécialisés de proximité en mesure de l'assister dans la résolution de son incident.

En 2020, **plus de 1,2 million de personnes se sont rendues sur le site** pour s'informer ou rechercher de l'assistance, soit une hausse de 155 % par rapport à l'année précédente. Si cette croissance est liée au développement de la notoriété de la plateforme, elle est également le signe d'un réel intérêt des publics pour les services proposés. Le travail d'enrichissement et d'accessibilité des ressources et contenus réalisé au cours de l'année explique également cette croissance.




FRÉQUENTATION ANNUELLE DE LA PLATEFORME CYBERMALVEILLANCE.GOUV.FR

La forte augmentation de fréquentation constatée a été principalement liée à l'accroissement des actes cybercriminels avec la crise épidémique, qui a généré une forte attente des publics en information et assistance (voir page 11).

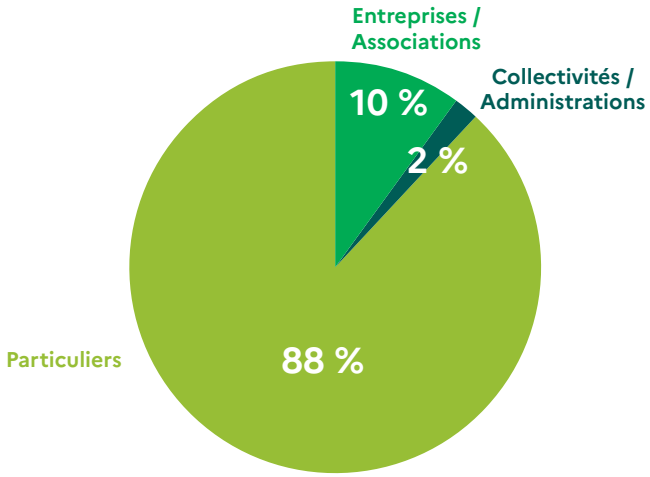
**PRÈS DE**
**225 000**
**VICTIMES**
**assistées depuis le lancement du dispositif en 2017**



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

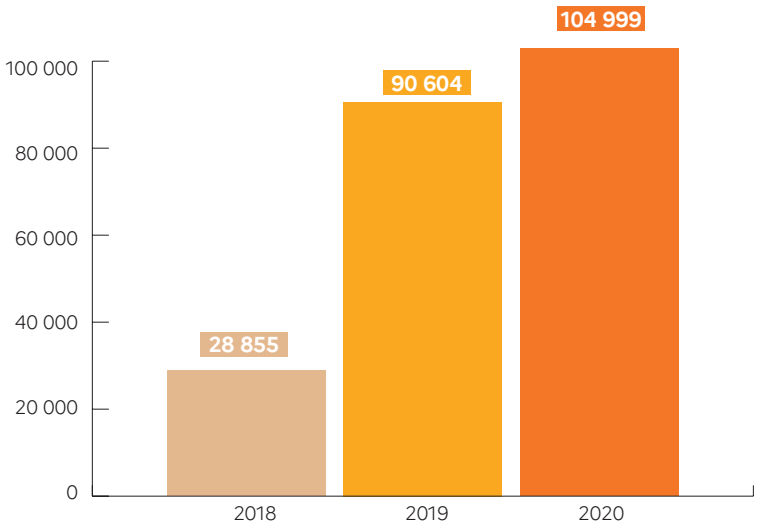
Sur les recherches d'assistance, la typologie des publics est globalement similaire aux années précédentes : les particuliers, souvent démunis face aux risques et cyberattaques, représentent toujours près de 90 % des publics de la plateforme. On note toutefois une augmentation de 20 % des recherches d'assistance provenant de publics professionnels (entreprises, associations, collectivités, administrations) sur l'année écoulée.




RÉPARTITION DES RECHERCHES D'ASSISTANCE PAR TYPE DE PUBLIC

**Le nombre de recherches de diagnostic et assistance en ligne s'élève à près de 105 000, soit une hausse de 16 % par rapport à l'année précédente.** Il convient toutefois de préciser qu'avec la mise en ligne de la nouvelle version du site en début d'année 2020, l'outil de diagnostic et d'assistance en ligne n'est plus le seul moyen de dispenser de l'assistance aux victimes. En effet, de nombreux contenus exposant les moyens de se prémunir des différentes menaces sont à présent directement accessibles dans des rubriques spécifiques de la plateforme et sont mieux référencés par les moteurs de recherche.

**Ces articles sur les différentes menaces et moyens d'y faire face ont recueilli en 2020 près de 650 000 consultations. On peut donc considérer que la plateforme a apporté une assistance à plus de 755 000 personnes durant l'année écoulée, soit une augmentation de plus de 730 % par rapport à l'année précédente.**




UTILISATION DE L'OUTIL D'ASSISTANCE EN LIGNE


CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

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

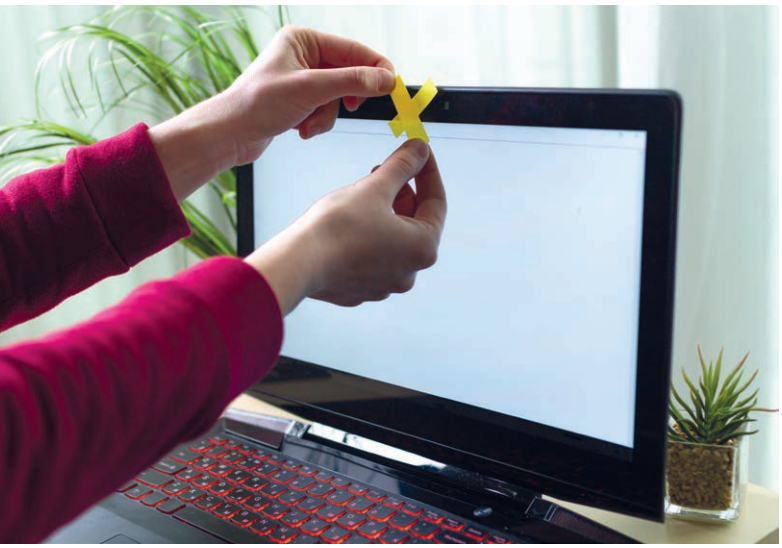
# LES CHIFFRES DE CYBERMALVEILLANCE.GOUV.FR EN 2020

L'analyse des recherches d'assistance des différentes catégories de publics apporte un éclairage sur les principaux types de cybermalveillances qui les ont touchés durant l'année écoulée.

Cette approche de catégorisation quantitative est un indicateur intéressant, qu'il convient toutefois de relativiser car elle n'intègre pas l'impact d'une cybermalveillance pour la victime. Un piratage de compte bancaire ou une usurpation d'identité peut en effet avoir des répercussions plus importantes pour un particulier qu'un spam téléphonique. De même, une arnaque au président peut avoir des conséquences bien plus dommageables pour une entreprise ou une collectivité qu'un virus informatique bénin. Par ailleurs, les impacts d'un piratage de compte en ligne peuvent être très différents d'une victime à l'autre.

## PARTICULIERS

L'**hameçonnage**, avec 17 % des recherches d'assistance des particuliers (voir graphique ci-contre), a été la malveillance prédominante rencontrée par les particuliers en 2020. Il est suivi par le **piratage de compte** en ligne avec 12 %. Ces deux menaces sont assez liées. En effet, un piratage de compte en ligne pourra souvent être permis suite à une tentative d'hameçonnage réussie. Ces deux menaces s'avèrent en outre être des vecteurs prédominants permettant de réaliser d'autres cybermalveillances.



Par exemple, un hameçonnage peut être à l'origine d'un débit de carte bancaire frauduleux, de même qu'un piratage de compte en ligne de messagerie peut donner lieu à une usurpation d'identité.

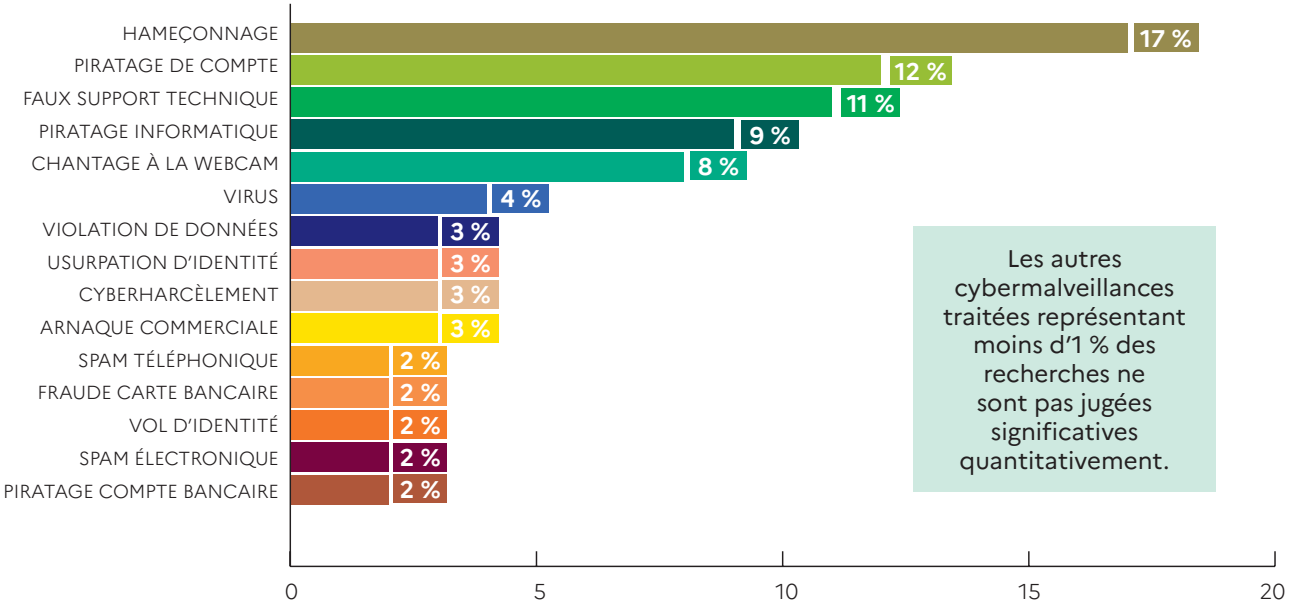

Les fraudes au **faux support technique** complètent le podium avec 11 % et continuent de faire des ravages chez les particuliers. Quant aux messages de **chantage à la webcam** prétendue piratée, phénomène majeur en 2019, ils sont restés dans le haut du classement du fait de résurgences cycliques, notamment durant les périodes de confinement.



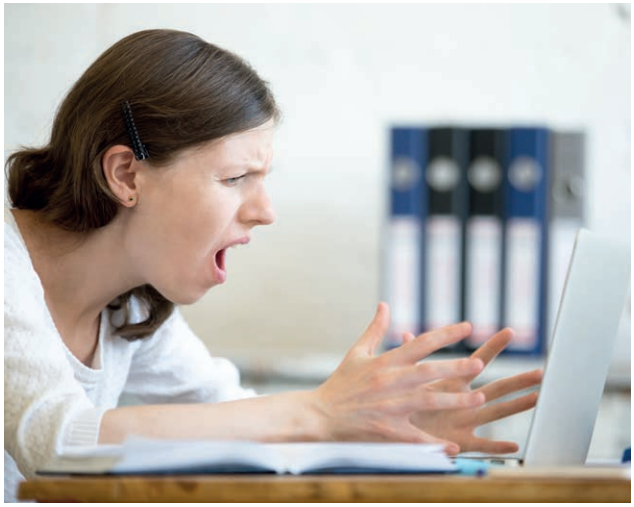
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

**LES 15 PRINCIPALES CYBERMALVEILLANCES SUR LESQUELLES ONT PORTÉ LES RECHERCHES D'ASSISTANCE DES PARTICULIERS EN 2020 PARMI LES 44 CYBERMALVEILLANCES TRAITÉES PAR LA PLATEFORME (VOIR PAGE 38)**




Le **piratage informatique** (9 %) relève de contours souvent flous pour les victimes qui ont du mal à décrire leur situation. Celle-ci va du piratage de compte en ligne aux suspicions de cyberharcèlement conjugal, ou même de messages de chantage à la webcam. Des travaux d'amélioration de l'outil de diagnostic en ligne ont été réalisés au cours de l'année pour mieux guider les victimes dans la description de leur problème, ce qui a engendré une baisse considérable des statistiques de cette catégorie de malveillance.



À noter enfin que les attaques par **rançongiciels** ont peu touché les particuliers durant l'année écoulée avec moins de 1 % des recherches d'assistance de cette catégorie de public.

# LES CHIFFRES DE CYBERMALVEILLANCE.GOUV.FR EN 2020

## PROFESSIONNELS

L'état des dix principales cybermenaces pour lesquelles des professionnels sont venus chercher de l'assistance sur la plateforme (voir graphiques ci-contre) montre de très fortes similitudes, à quelques nuances près, entre les professionnels du public et ceux du privé. Cela tend à démontrer que ces deux catégories de publics sont touchées par les mêmes phénomènes cybercriminels dans des proportions comparables.

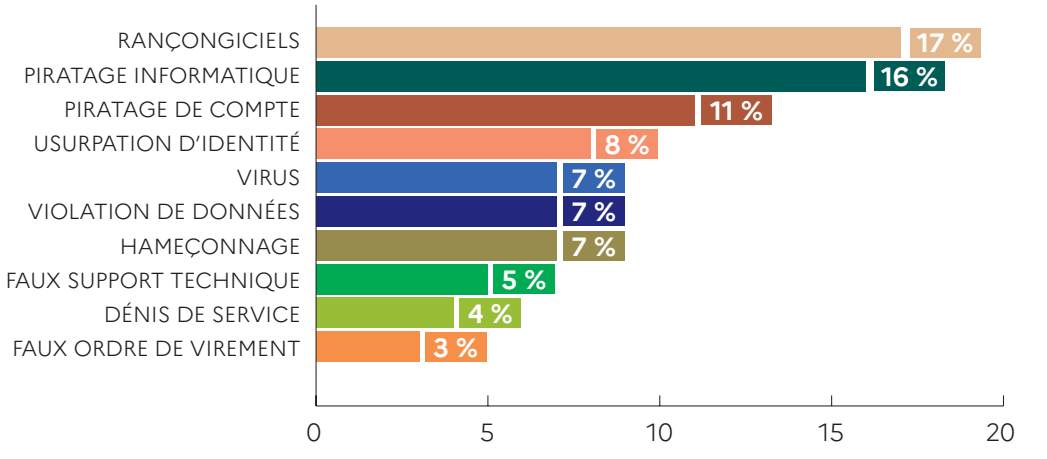
Sixième menace recensée en 2019, les attaques par **rançongiciels** ont pris une ampleur considérable durant l'année écoulée et sont devenues en un an la principale menace à laquelle les professionnels ont été confrontés, qu'ils soient du secteur privé ou du secteur public. Sur ces publics, le nombre de recherches d'assistance sur cette menace a en effet progressé de 30 % par rapport à l'année précédente.

Comme pour les particuliers, les « **piratages informatiques** » pour les professionnels regroupaient des situations particulières souvent mal cernées. Les modifications faites en 2020 sur l'outil de diagnostic en ligne ont permis de mieux orienter les victimes pour cerner cette catégorie de cybermalveillance. Bien qu'en baisse d'intensité, cette cybermalveillance continue d'être une réalité pour ces publics.

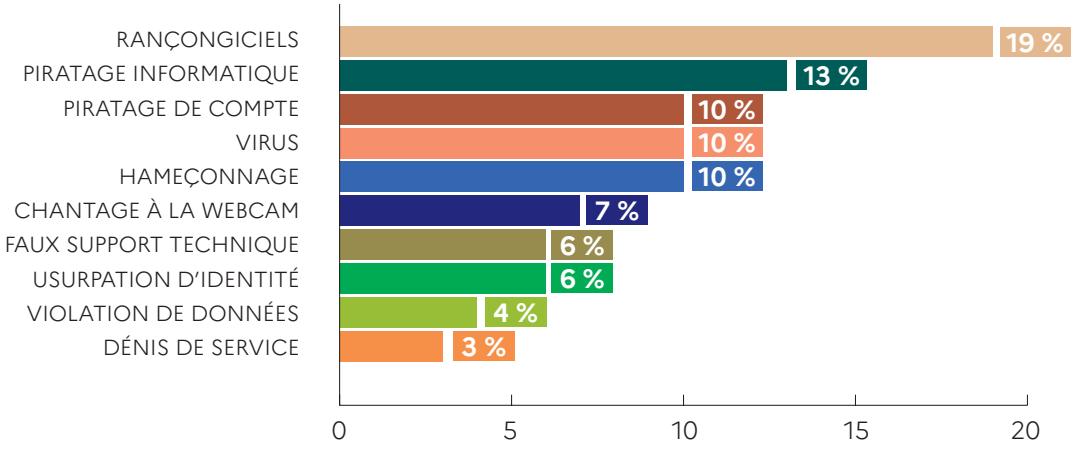
Un phénomène intéressant à observer dans ces classements est la présence des arnaques au **faux support technique** et des **chantages à la webcam** sur des publics professionnels que l'on pourrait penser plus aguerris et protégés face à ce type d'escroqueries. Ces résultats montrent qu'une partie importante des publics professionnels ayant recours à la plateforme d'assistance du dispositif a le même type d'usages que les particuliers. C'est le cas des artisans, des libéraux et TPE, voire des petites collectivités territoriales qui ne disposent pas de support informatique et qui sont rapide-




RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique



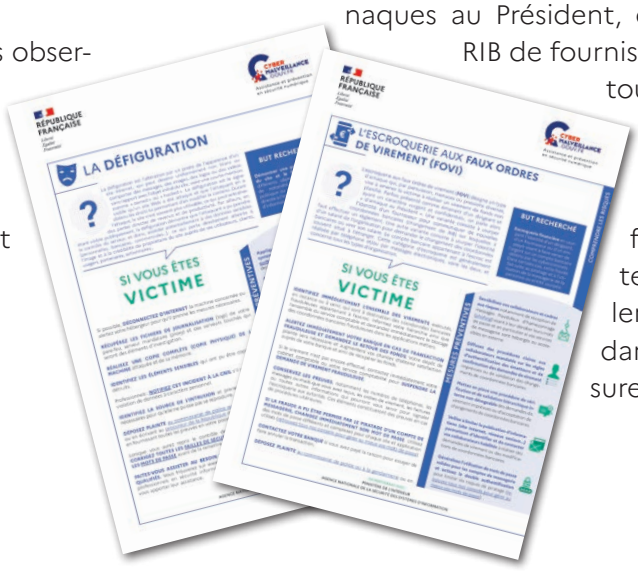

**PRINCIPALES RECHERCHES D'ASSISTANCE POUR LES ENTREPRISES ET LES ASSOCIATIONS**




**PRINCIPALES RECHERCHES D'ASSISTANCE POUR LES COLLECTIVITÉS ET LES ADMINISTRATIONS**

ment démunis quand ils sont attaqués. Pour ces catégories de victimes, l'apport d'assistance du dispositif prend tout son sens.

Par ailleurs, et comme d'autres observations tendent également à le démontrer, on constate que les opérations de **défiguration** de sites Internet semblent perdre de leur intérêt pour les cybercriminels.




Dans les différences notables entre les deux catégories de publics, on peut constater que les **fraudes au virement** (FOVI), qu'il s'agisse des arnaques au Président, de changement de RIB de fournisseurs ou de salariés, touchent principalement les professionnels du secteur privé (5 %); les professionnels du secteur public sont également touchés, mais dans une moindre mesure (1 %).

# LES GRANDES TENDANCES DE LA MENACE OBSERVÉES EN 2020

## LA CRISE SANITAIRE

### UN EFFET D'AUBAINE POUR LES CYBERCRIMINELS

**La crise sanitaire en 2020 a représenté une opportunité majeure pour les cybercriminels. Ils ont en effet cherché à jouer sur l'intensification des usages numériques et sur l'incertitude de la situation pour démultiplier leurs attaques, notamment durant les phases de confinement.**

La fréquentation de la plateforme a ainsi quadruplé durant ces périodes particulières, notamment lors des différentes campagnes d'hameçonnage qui ont pu être observées. Faux sites d'attestations de déplacement, ventes fictives de masques… si certaines d'entre elles étaient directement affichées aux couleurs de la crise, d'autres étaient plus indirectes pour ne pas dire plus insidieuses : des arnaques à la livraison de colis ont été par exemple constatées durant les périodes où de nombreuses personnes étaient susceptibles d'en recevoir, tout comme les chantages à la consultation de sites pornographiques, les cybercriminels misant sur une intensification de ces usages qui se développent inévitablement dans ce type de situation.

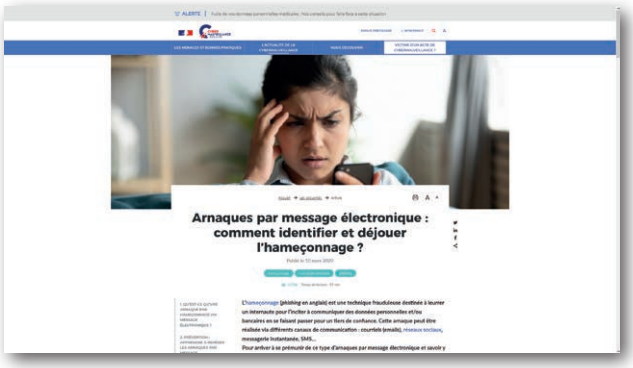
Si ces campagnes semblent viser plus particulièrement le grand public, les professionnels n'ont toutefois pas été épargnés. De nombreuses campagnes d'hameçonnage les ciblant spécifiquement ont été observées : certaines visaient à **dérober des identifiants de connexion aux réseaux d'entreprise**, tandis que d'autres lançaient **des appels frauduleux aux dons** ou proposaient **de faux remboursements ou indemnisations liés à la crise**. En parallèle, les professionnels ont été particulièrement ciblés par des attaques par rançongiciels ou des arnaques aux faux ordres de virement. En effet, la mise en place urgente et massive du télétravail conjuguée à l'intensification de la dématérialisation des procédures, ont conjoncturellement facilité le déploiement de ces attaques.

La crise sanitaire n'a provoqué aucune trêve de la part des cybercriminels qui au contraire y ont vu un moyen lucratif de commettre leurs forfaits.

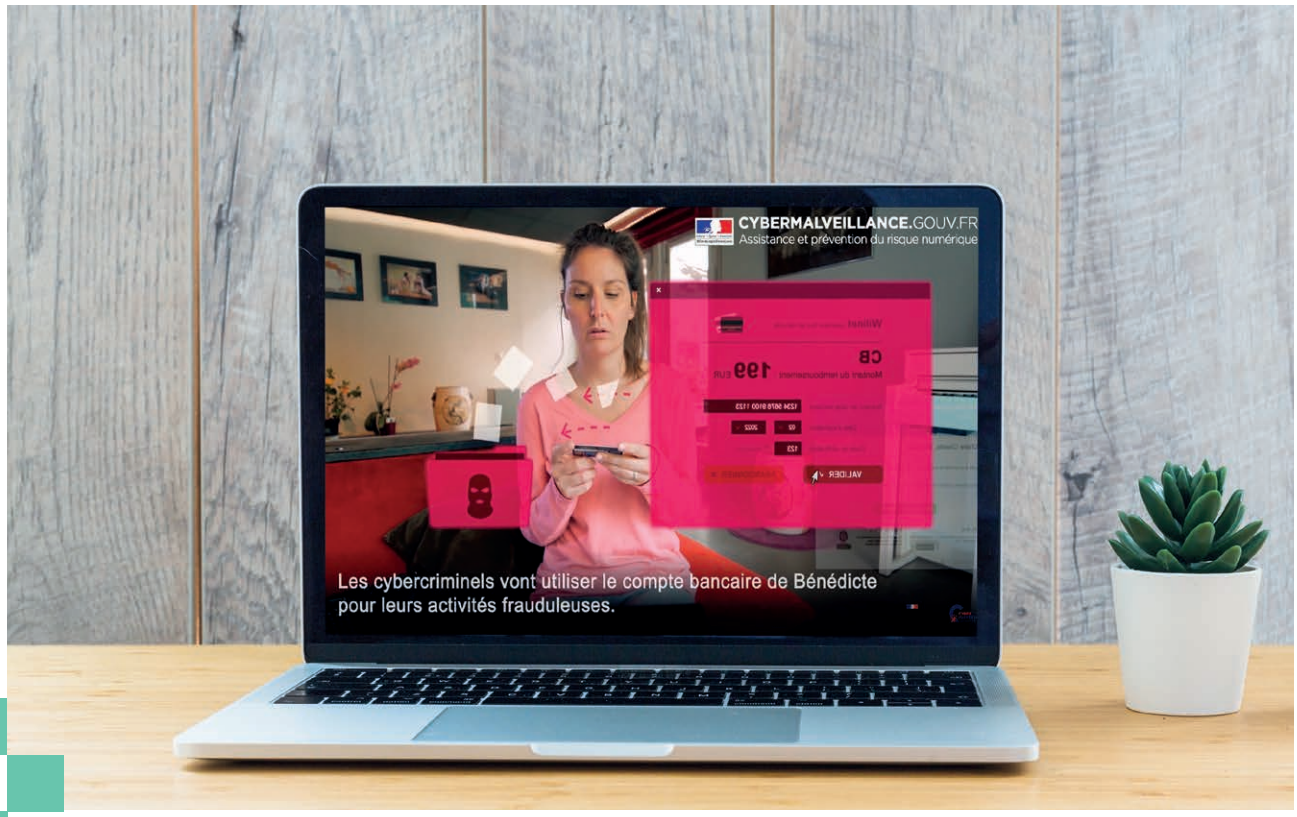
## L'HAMEÇONNAGE

### LA MÈRE DES ATTAQUES

**L'hameçonnage peut se définir comme un message usurpant une identité pour duper un internaute dans le but de l'inciter à réaliser une action. Il peut s'agir par exemple de la fourniture de données confidentielles (identité, mots de passe…), la réalisation d'un paiement (identifiants de carte bancaire…) ou encore l'ouverture d'une pièce jointe ou d'un lien qui peut contenir un virus.**




Si l'hameçonnage représente la première cause de recherche d'assistance sur la plateforme en 2020 avec **près de 30 % des recherches d'assistance et plus de 300 000 consultations des articles dédiés**, l'ampleur de ce phénomène est beaucoup plus importante que ce que les chiffres laissent envisager à première vue. En effet, lorsqu'une tentative d'hameçonnage atteint son objectif, de nombreuses autres cybermalveillances peuvent être permises : un piratage de compte en ligne, un rançongiciel, un débit bancaire frauduleux, ou encore un faux ordre de virement peuvent en être les conséquences.




Autrefois de faible intensité et facilement repérable du fait de sa réalisation par des acteurs isolés, l'hameçonnage a aujourd'hui changé d'échelle avec la structuration de l'écosystème cybercriminel. **Des bases de données de dizaines de millions d'adresses de messagerie sont disponibles pour quelques centaines d'euros, et parfois même gratuitement, sur les places de marché cybercriminelles** permettant de réaliser des campagnes massives à faible coût. De même des « kits », méthodes et tutoriels y sont également accessibles, permettant de « professionnaliser » les attaques en les rendant toujours plus difficiles à détecter pour les victimes.

**En 2020, les campagnes d'hameçonnage par SMS se sont considérablement développées.** Au même titre qu'un message électronique (e-mail), les SMS permettent aujourd'hui des interactions directes avec Internet. Ce mode de communication est de plus en plus utilisé par les différentes plateformes pour communiquer directement avec leurs usagers. Mais dans le même temps, les usagers sont beaucoup moins méfiants lorsqu'ils reçoivent un SMS, d'autant qu'il est plus difficile de repérer une usurpation d'identité ou un site frauduleux depuis un SMS sur un téléphone que dans un e-mail sur son ordinateur. L'utilisation du SMS comme support d'hameçonnage sera une tendance forte qui se confirmera et s'intensifiera certainement dans les prochaines années.

L'hameçonnage sous toutes ses formes doit donc être considéré aujourd'hui comme un des principaux vecteurs à l'origine d'une multitude d'attaques informatiques.

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

## LE PIRATAGE DE COMPTE EN LIGNE

### DES EFFETS MULTIPLES ET DÉVASTATEURS

**Le piratage de compte en ligne représente la 2e menace constatée par la plateforme en 2020 tous publics confondus, qu'il s'agisse des particuliers ou des professionnels.**


Cette catégorie de menace concerne aussi bien les comptes de réseaux sociaux que ceux des plateformes de commerce en ligne, de banques, d'opérateurs téléphoniques, de services publics ou encore les messageries.

Le dénominateur commun de l'intérêt des cybercriminels pour les comptes en ligne reste principalement le profit qu'ils pourront tirer de leur intrusion. Ainsi, **le piratage d'un compte bancaire en ligne va donner la possibilité au cybercriminel d'effectuer des virements bancaires frauduleux, tandis qu'un compte d'un site de vente en ligne lui permettra de passer des commandes.**

Dans la grande majorité des cas, **le piratage de compte en ligne est rendu possible suite à un hameçonnage ou à la réutilisation par la victime d'un même mot de passe sur plusieurs sites dont l'un a pu être compromis.**

La principale tendance observée sur cette catégorie de menace durant l'année écoulée est le très fort intérêt des cybercriminels pour les comptes de messagerie des victimes. Les services de messageries en ligne sont facilement accessibles depuis n'importe quel type d'appareil et sont devenus l'espace de stockage et d'échange d'information privilégié des internautes, ainsi que le moyen d'accès *de facto* à l'ensemble de leurs autres services en ligne.

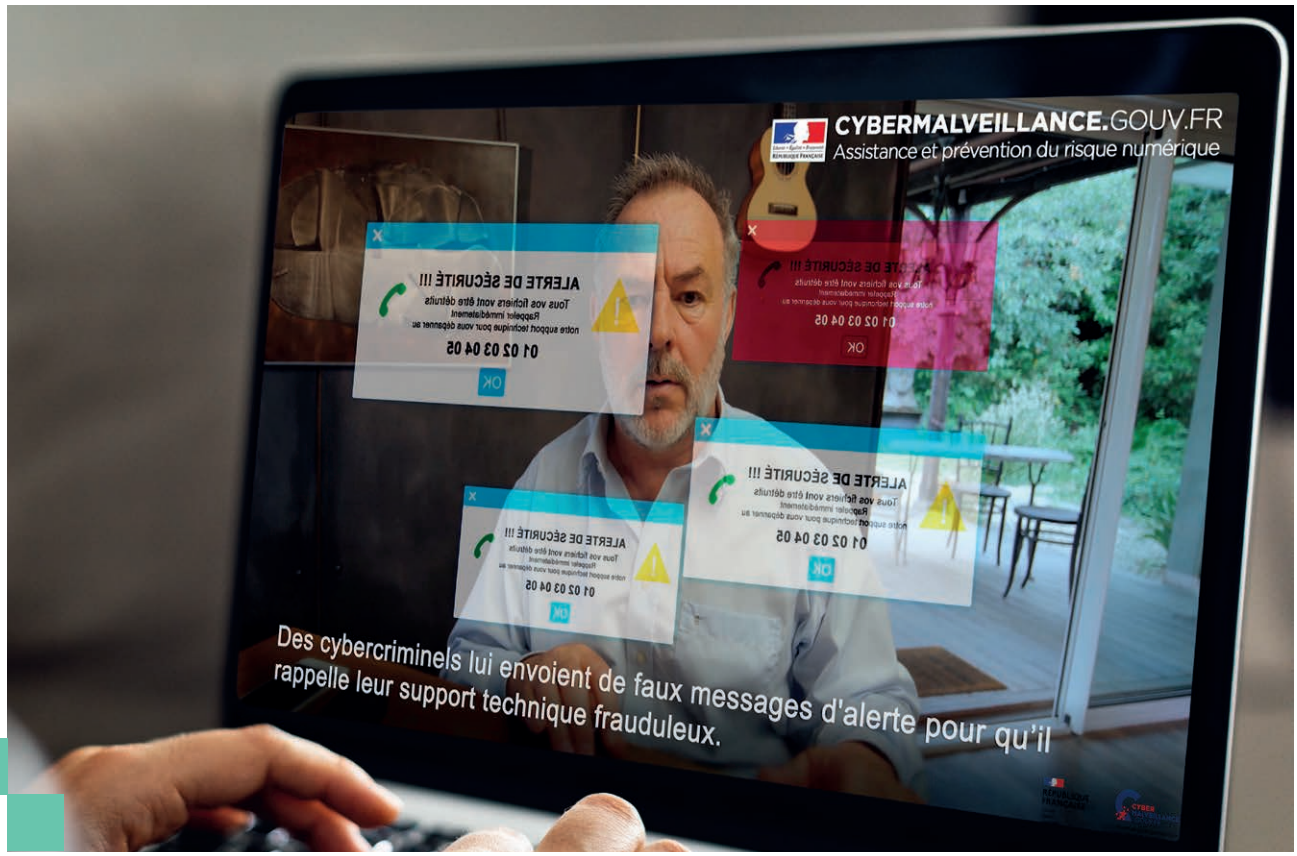
En effet, c'est aujourd'hui l'adresse de messagerie de l'internaute qui est généralement utilisée comme identifiant de connexion à la grande majorité des services en ligne et également pour réinitialiser ses mots de passe à ces différents services. De plus, les échanges administratifs de la victime avec les différents services publics et privés y sont souvent entreposés. Cela devient un véritable lieu de stockage d'une quantité importante d'informations sensibles tels que des copies de documents d'identité, de fiches de paie, d'avis d'imposition, et même malheureusement dans certains cas, ses différents mots de passe.

**En prenant le contrôle de sa messagerie, les cybercriminels mettent la main sur presque toute la vie numérique de la victime**. Ils peuvent ainsi utiliser ou revendre les informations récupérées qui permettront d'usurper son identité. Ces usurpations d'identité pourront aller de la simple tentative d'arnaque de ses proches à la réalisation de virements bancaires, et même à la souscription à des crédits à la consommation.

Dans certains cas, ces piratages pourront être le fait d'un conjoint ou ex-conjoint qui cherchera principalement à prendre connaissance des correspondances de la victime, notamment dans des situations de séparation conflictuelles.

**Les professionnels des secteurs privés et publics sont, eux aussi, particulièrement visés par ce type de cybermalveillance, qui sera souvent utilisé par les cybercriminels pour réaliser différentes formes de fraudes aux faux ordres de virement** (arnaque au président, changement de RIB de fournisseurs…).

À l'instar de l'hameçonnage, le piratage de compte en ligne, et plus particulièrement de comptes de messageries en ligne, est une attaque qui peut être la cause d'une multitude de cybermalveillances aux conséquences souvent désastreuses pour les victimes.




## LES FAUX SUPPORTS TECHNIQUES

### ILS CONTINUENT DE FAIRE DES RAVAGES

Les campagnes d'arnaques au faux support technique n'ont pas perdu en intensité en 2020 et sont la 3e cause de recherche d'assistance sur la plateforme.

**Durant leur navigation, les victimes voient apparaître un message inquiétant leur demandant de rappeler d'urgence un numéro d'un pseudo support technique**, au risque de perdre leurs données ou l'usage de leur appareil. S'en suit un dépannage factice à distance facturé plusieurs centaines d'euros.

Cette catégorie de cybermalveillance reste la **première cause d'intervention des professionnels référencés par la plateforme. Elle touche plus spécifiquement les particuliers, et notamment les populations seniors les moins informées.** Comme les statistiques de la plateforme Cybermalveillance.gouv.fr tendent à le démontrer, les professionnels ne sont pas pour autant épargnés, notamment ceux qui ne disposent pas de supports informatiques de proximité et qui sont donc plus facilement susceptibles de tomber dans ce piège.

Cette cybermenace, identifiée dans son ampleur dès la création du dispositif en 2017, a vu en 2020 ses modes opératoires continuer à évoluer dans la diversification de ses méthodes d'approche et dans ses conséquences pour les victimes. Une recrudescence d'approches téléphoniques a ainsi été observée, ainsi que de vastes campagnes d'hameçonnage usurpant des lettres d'informations de grands quotidiens, ou des notifications de réseaux sociaux contenant des liens malveillants qui déclenchent l'apparition du message d'alerte frauduleux. **Consécutivement à cette cybermalveillance, de nombreux cas de virements bancaires frauduleux ou de piratage de comptes en ligne des victimes d'arnaque au faux support technique ont, par ailleurs, été rapportés.**

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

Les cybercriminels ne semblent donc plus se contenter de faire payer un faux dépannage, ils cherchent à faire main basse sur toutes les informations de la machine de la victime dont ils prennent le contrôle, pour maximiser leur profit.

La résurgence est aussi une autre tendance observée de ce phénomène. **Les cybercriminels recontactent leurs victimes plusieurs mois après leur première attaque pour demander à reprendre le contrôle de leur machine en prétextant une « maintenance » et en profitent pour dérober toutes les informations qui ne l'auraient pas été précédemment, voire leur font payer une nouvelle prestation frauduleuse.**

Enfin, un groupe cybercriminel est même allé jusqu'à contracter une société de recouvrement française pour récupérer les impayés des victimes en jouant sur l'intimidation que ce type de procédure pouvait avoir sur les victimes.

Sous son apparence de légitimité, le faux support technique est une cybermalveillance qui ne cesse de se réinventer et de se développer en faisant toujours un nombre considérable de victimes.

## LES RANÇONGICIELS

### LE FLÉAU POUR LES PUBLICS PROFESSIONNELS

Première cause des recherches d'assistance des publics professionnels des secteurs privés et publics, les attaques par rançongiciels (*ransomware*) ont connu une intensification sans précédent en 2020.

Découverte du grand public par les attaques de masse Wanacry et NotPetya en 2017, cette catégorie de cybermalveillance n'a depuis cessé de gagner en sophistication.

À son origine au début des années 1990, le rançongiciel était basiquement un virus contenu dans la pièce jointe d'un message distribué massivement qui, en se déclenchant, chiffrait les données stockées localement par l'utilisateur et lui réclamait une rançon pour lui en redonner l'accès.


Aujourd'hui, les attaques par rançongiciels sont beaucoup plus élaborées et ciblées. Elles visent principalement les acteurs professionnels, auxquels des rançons beaucoup plus importantes peuvent être demandées qu'à des particuliers, au regard de l'impact que ces attaques peuvent avoir pour les victimes professionnelles. **Ces attaques peuvent, en effet, générer un arrêt de l'activité des victimes qui peut parfois s'étendre sur des semaines, voire des pertes de données irrémédiables**.

Elles sont commises par des groupes de cybercriminels particulièrement compétents et organisés en cartels d'équipes spécialisées dans les différentes étapes de l'attaque. **Certaines équipes de cet écosystème cybercriminel se spécialisent ainsi dans la recherche des moyens d'intrusion dans les réseaux des victimes, d'autres dans le développement des outils d'attaque et de chiffrement, d'autres encore dans le blanchiment des rançons.**

De nos jours, la pièce jointe malveillante n'est plus qu'un moyen parmi d'autres de commencer à prendre pied dans le réseau informatique de la victime. **Parmi les moyens d'intrusion les plus fréquents, on peut citer la pénétration dans le réseau de l'organisation victime par ses accès externes, suite à l'exploitation d'une faille de sécurité non corrigée, l'obtention d'un mot de passe d'accès distant trop simple qui aurait pu être forcé, ou suite à un hameçonnage.**

Une fois introduits dans le réseau de la victime, les cybercriminels y resteront plusieurs jours voire semaines, le temps de repérer les données

importantes de l'organisation et leur stratégie de sauvegarde. **Cette phase de repérage réalisée, l'attaque sera déclenchée à un moment de faible présence de l'organisation pour en garantir le succès (week-end, congés…). Les sauvegardes seront alors détruites et les données chiffrées.**

Parmi les grandes tendances d'évolution du mode opératoire de ce type d'attaque observées en 2020, on constate qu'elles sont généralement **précédées d'un vol des données de l'organisation victime et dont la menace de divulgation constitue un moyen de pression supplémentaire** pour augmenter les chances des cybercriminels d'obtenir la rançon demandée. En effet, si des victimes refusaient de payer les rançons en cherchant à restaurer leurs systèmes, les cybercriminels détenant leurs données disposent alors d'un moyen de pression contre lequel les victimes ne peuvent plus agir de manière curative. Quand elles refusent de payer la rançon, les cybercriminels n'hésitent d'ailleurs pas à publier ces données dérobées et à le faire largement savoir pour intimider d'autant plus leurs prochaines victimes.

Autre tendance majeure observée suite à ces attaques : **la simple demande de paiement à une adresse en cryptomonnaie fait place, par souci de furtivité, à une recherche de contact et de « négociation » du cybercriminel avec la victime, tant sur les montants des rançons que sur les modalités de règlement.** En 2020, les attaques par rançongiciels ont frappé des victimes de tous secteurs et de toutes tailles. **De grands groupes à des PME, de grandes métropoles à de petites collectivités et même d'associations, aucune catégorie de victime n'a été épargnée.**

Le développement considérable constaté de cette catégorie d'attaque laisse à penser qu'il s'agit d'un secteur cybercriminel très lucratif pour ses auteurs et qu'il constitue donc une tendance qui devrait continuer de perdurer, et même s'accentuer.

# 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 ;
- 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 ;
- ANSSI (Agence nationale de la sécurité des systèmes d'information).

## 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**, **Banque des Territoires** (Groupe Caisse des Dépôts), **Bitdefender**, **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**, **CLCV** (Association Consommation, Logement et Cadre de Vie), **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), **Crowdstrike**, **e-Enfance**, **ESET**, **Fédération Déclic**, **Fédération EBEN** (Fédération des Entreprises du Bureau et du Numérique), **FEVAD** (Fédération du e-commerce et de la vente à distance), **FFA** (Fédération française de l'Assurance), **France Victimes**, **Google France**, **Harmonie Technologie**, **Hub One**, **HP France**, **INC** (Institut National de la Consommation), **Kaspersky**, **Groupe La Poste**, **MAIF** (Mutuelle assurance des instituteurs de France), **MEDEF** (Mouvement des entreprises de France), **Microsoft France**, **Neuflize OBC**, **Orange Cyberdefense**, **Palo Alto Networks**, **SFR Business**, **Signal Spam**, **Stormshield**, **Syntec Numérique**, **UFC-Que Choisir ;**

ainsi que ses nouveaux membres dont l'adhésion au GIP a été acceptée en 2020 pour rejoindre le dispositif au 1er janvier 2021 : **Avicca** (Association des Villes et Collectivités pour les Communications électroniques et l'Audiovisuel), **CISCO**, **Club EBIOS**, **MACIF** (Mutuelle assurance des commerçants et industriels de France), **Ministère de l'Éducation Nationale, de la jeunesse et des Sports**, **SNCF.**



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

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 : **ESCRIM**, **EURABIS**, **FRP2i**, **Résadia**, **Séquence informatique**.

Ses **partenaires pour les événements professionnels** liés à la cybersécurité : **CEIS** (organisateur du FIC – Forum International de la cybersécurité), **Cybercercle**, **IT Partners** (Groupe Comexposium), **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**, **Collectivité de Fouras-les-Bains** (17), **Collectivité de Voreppe** (38), **Conseil Départemental 27**, **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 DCANT / 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 :