



**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*



Assistance et prévention
en sécurité numérique

Dispositif national de sensibilisation, prévention et d'assistance aux victimes



**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*



Assistance et prévention
en sécurité numérique

I- Présentation du dispositif

LES MISSIONS DU DISPOSITIF

1 **ASSISTER LES VICTIMES**
d'actes de cybermalveillance



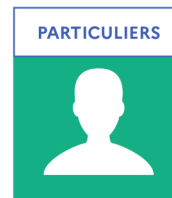
2 **INFORMER & SENSIBILISER**
à la sécurité numérique



3 **OBSERVER & ANTICIPER**
le risque numérique



QUI EST CONCERNÉ ?



CYBERMALVEILLANCE.GOUV.FR EN QUELQUES CHIFFRES



53

**organisations
membres**

(publiques et privées)
du GIP ACYMA



1200

**prestataires
référéncés**

sur l'ensemble
du territoire



350 000

**victimes
assistées**
depuis fin 2017



47

**types d'incidents
traités**

STRUCTURE : UN GROUPEMENT D'INTÉRÊT PUBLIC

53 MEMBRES PUBLICS ET PRIVÉS

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





**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*



Assistance et prévention
en sécurité numérique

II- État de la menace

PRINCIPES DE L'OBSERVATION DE LA MENACE

Capteurs :

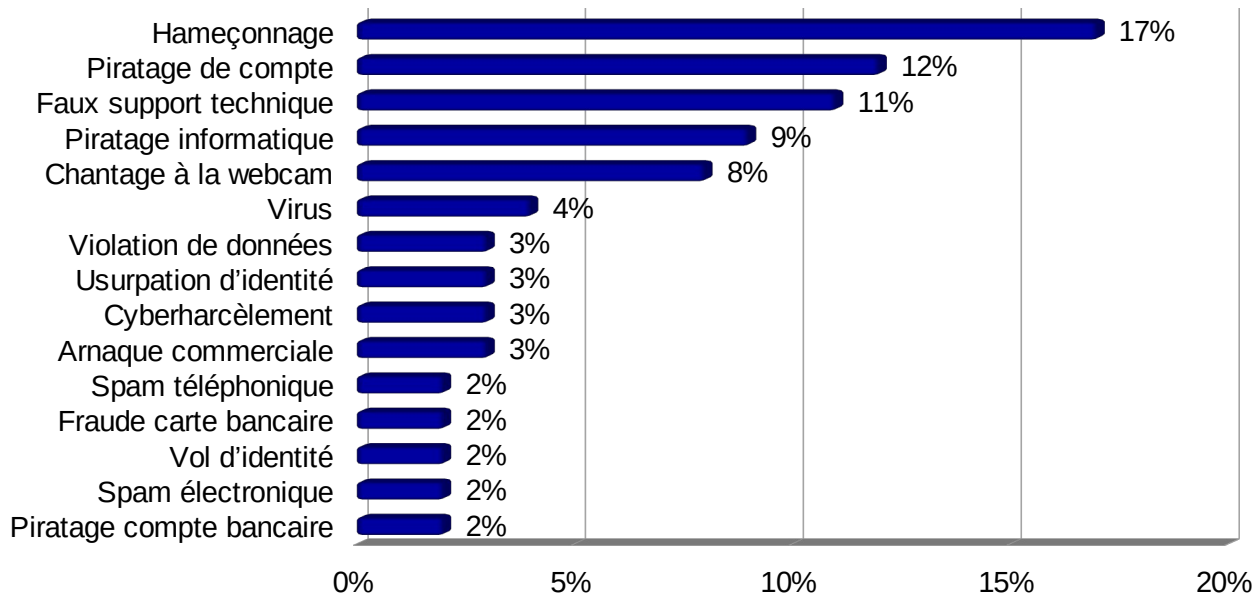
- **Parcours des victimes** sur la plateforme
- **Rapports des prestataires** référencés
- **Veille** sur la cybermenace (sources ouvertes)
- **Signalements** par des utilisateurs (réseaux sociaux, partenaires...)

Démarche :

- **Qualification** de l'information
- **Alerte** (conseils, **coopérations** au besoin/si possible)
- **Ajustement des parcours d'assistance** aux victimes
- Production de nouveaux **supports de sensibilisation** ou ajustement

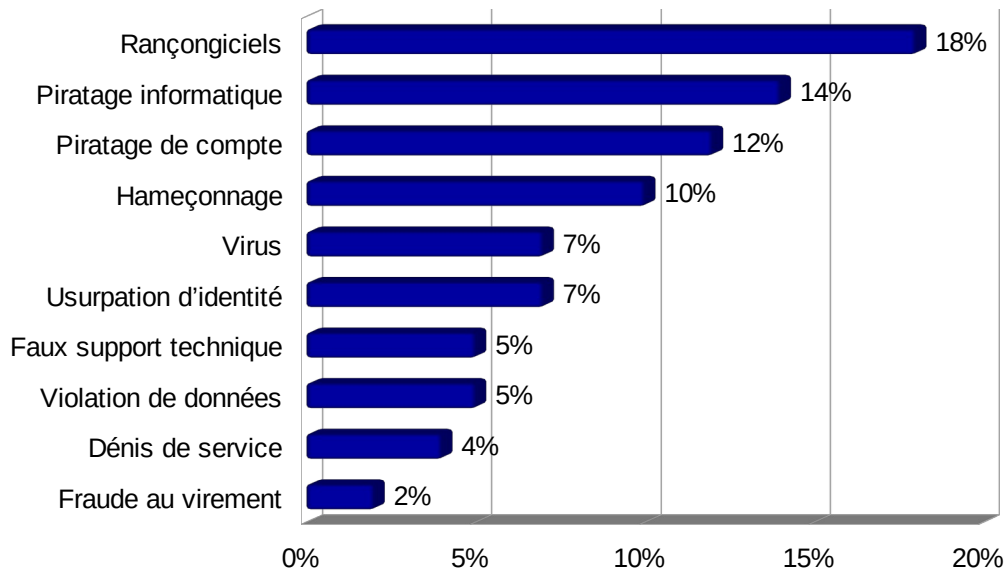
PRINCIPALES CAUSES DE RECHERCHE D'ASSISTANCE EN 2020

Particuliers :



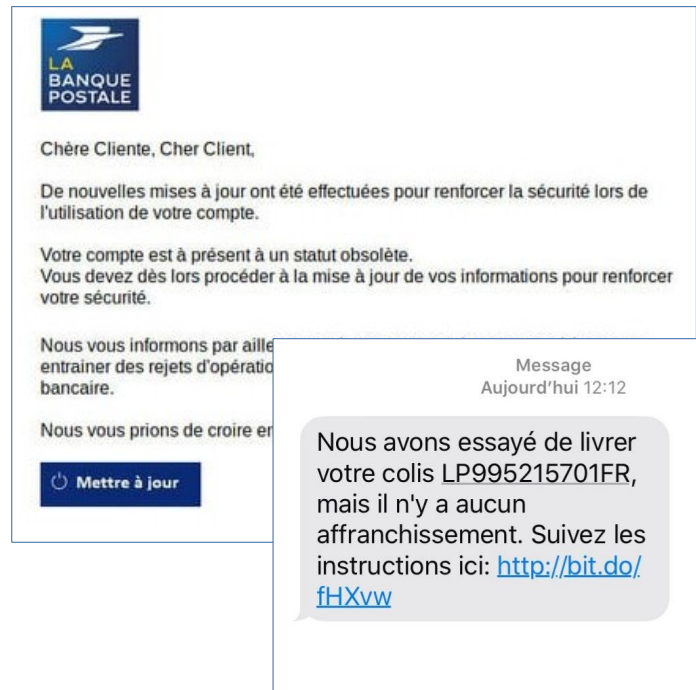
PRINCIPALES CAUSES DE RECHERCHE D'ASSISTANCE EN 2020

Professionnels (entreprises, collectivités...) :



L'HAMEÇONNAGE (PHISHING) : LA MÈRE DES ATTAQUES

- **Menace prédominante et en hausse**
(N° 1 pour les particuliers et N° 4 pour les professionnels)
- **Des attaques toujours plus sophistiquées**
(de l'artisanat à la « professionnalisation »)
- **Effet démultiplicateur avec la crise sanitaire**
(isolement numérique, télétravail...)
- **Principale cause d'autres malveillances**
(piratage de compte, rançongiciel, fraude bancaire...)
- **Développement important des attaques par SMS**
(confiance, difficulté de contrôle)



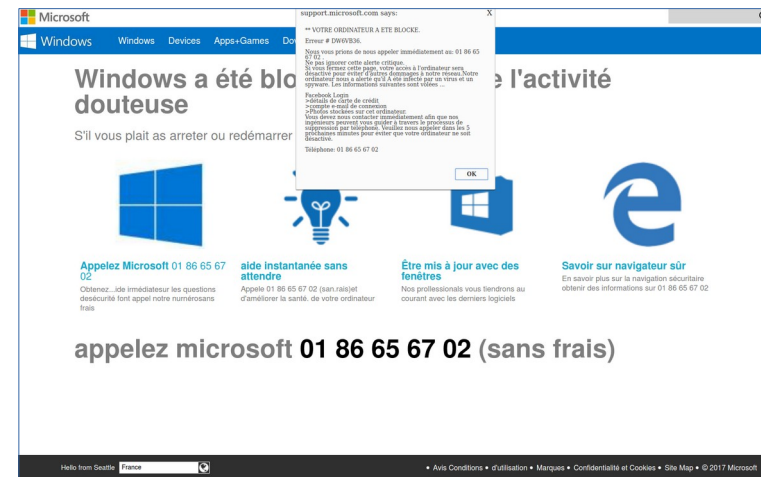
LE PIRATAGE DE COMPTE

- **Menace majeure et en expansion**
(N° 2 pour les particuliers et les professionnels)
- **Messageries, réseaux sociaux et banques visés**
(fort intérêt des cybercriminels pour les données revendues)
- **Des origines diverses**
(hameçonnage, fuite de mots de passe...)
- **Cause majeure d'autres malveillances**
(Usurpation d'identité, fraude bancaire ou au virement...)
- **Impacts de plus en plus importants pour les victimes**



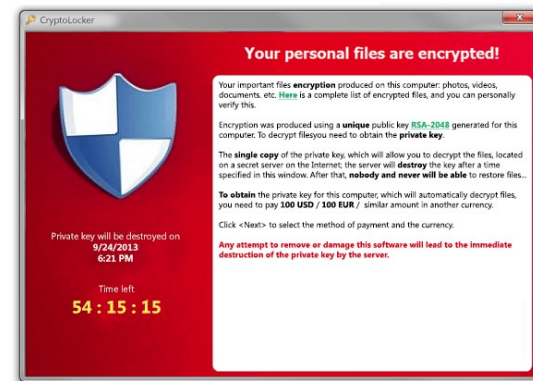
LES FAUX SUPPORTS TECHNIQUES

- **Menace détectée en 2017 et toujours en tête**
(N° 3 pour les particuliers et N° 7 pour les professionnels)
- **Concerne également les professionnels**
(en particulier les petites structures sans support)
- **Evolution des modes opératoires toujours plus agressifs**
(résurgence, piratage de données, recouvrement...)
- **1ère cause d'intervention des professionnels référencés**
- **Les seniors les moins aguerris restent en tête des victimes**



LES RANÇONGIERS

- **1ère menace pour les professionnels (entreprises, collectivités...)**
(~1 000 recherches d'assistance en 2020, +54 %)
- **Tous types et tailles d'organisations ciblées en nombre**
(PME, grands groupes, métropoles, hôpitaux, petites collectivités...)
- **Un écosystème cybercriminel redoutable qui fonctionne en cartel**
(développement, intrusion, négociation, blanchiment...)
- **L'intrusion via les accès externes 1^{er} vecteur de compromission**
(failles non corrigées, mots de passe trop simples, hameçonnage)
- **Vol de données avec menace de divulgation pour accentuer la pression depuis fin 2019**
(médiatisation, impacts RGPD et réputationnels)





**RÉPUBLIQUE
FRANÇAISE**

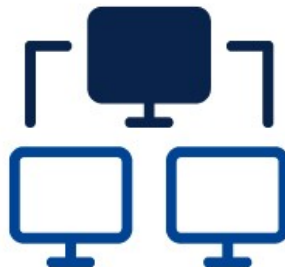
*Liberté
Égalité
Fraternité*



Assistance et prévention
en sécurité numérique

III- Comment se prémunir ?

COMMENT SE PRÉMUNIR ?

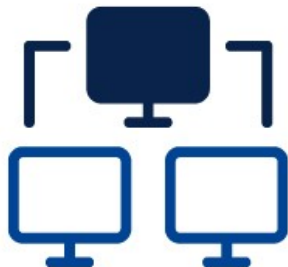


Volet technique



Volet humain

COMMENT SE PRÉMUNIR ?



Volet technique

- Mettre en place une stratégie de sécurité
- Suivre les préconisations de l'ANSSI
- Se faire accompagner par des professionnels

LE LABEL EXPERTCYBER

L'objectif :

- Reconnaître l'expertise en sécurité numérique
- Sur les activités d'installation, maintenance et assistance
- Pour les clients (TPE-PME / Associations / Collectivités)

**EXPERT
CYBER**

LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr

 **RÉPUBLIQUE FRANÇAISE**

Pensé par et pour l'écosystème :

- Avec les représentants du secteur :



- En partenariat avec : 

CAMPAGNE DE VIDÉOS DE SENSIBILISATION POUR FAIRE CONNAÎTRE LES LABELLISÉS

Conçue dans le cadre du volet cybersécurité du plan France relance

Cible : les entreprises et les collectivités

Objectif : sensibiliser à la nécessité de faire appel à de vrais experts en cybersécurité pour se protéger efficacement et être correctement assistés en cas d'incident

Thématique : Face aux risques cyber, faites confiance à un véritable expert !

- 2 vidéos dédiées aux entreprises
- 1 vidéo dédiée aux collectivités
- Des outils de sensibilisation déclinés flyers, bannières, etc...



COMMENT SE PRÉMUNIR ?



Volet humain

- Créer une charte informatique
- Organiser des sensibilisations en interne
- S'appuyer sur les conseils et ressources de [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr)

SENSIBILISATION ET PRÉVENTION

Objectifs :

- Sensibiliser aux risques
- Partager les bonnes pratiques
- Alerter

17 thématiques

6 types de contenus :

- Fiches pratiques/réflexes
- Vidéos
- Mémos et infographie
- Alertes sur les réseaux sociaux @cybervictimes
- Articles

Publics :

- Particuliers
- Entreprises
- Collectivités



ACTIONS ET OUTILS DE SENSIBILISATION RÉALISÉS EN 2021

Pour les entreprises

Interventions
dans des conférences
sur les risques liés
au télétravail

Lancement du label
ExpertCyber auprès
des TPE/PME

Dispositif d'alertes cyber
pour les TPE/PME
(diffusion par le MEDEF,
CPME, U2P)

Guide pratique
sur la cybersécurité



ACTIONS ET OUTILS DE SENSIBILISATION RÉALISÉES EN 2021

Pour les collectivités

Programme de sensibilisation
 aux risques numériques
 auprès des élus
 dont des vidéos de sensibilisation



Campagne I.M.M.U.N.I.T.É Cyber
 Actions de sensibilisation commune
 avec le Ministère de l'Intérieur, le GIP
 et l'AMF



Campagne de sensibilisation
 Inter-régions à l'occasion
 des élections régionales



Enquête à destination des
 communes de -3500 habitants





RÉPUBLIQUE
FRANÇAISE

*Liberté
Égalité
Fraternité*



www.cybermalveillance.gouv.fr



Assistance et prévention
en sécurité numérique



@cybervictimtimes



@cybervictimtimes



@cybermalveillancegouvfr