



Jérôme NOTIN
Directeur général de
[Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr)

Cybersécurité :

des solutions
pragmatiques pour les
collectivités

Colloque de printemps de l'Avicca

TRIP 2022

mercredi 1^{er} juin





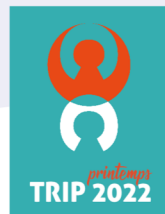
**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*



Assistance et prévention
en sécurité numérique

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



LES MISSIONS DU DISPOSITIF

- 1 ASSISTER LES VICTIMES**
d'actes de cybermalveillance 
- 2 PRÉVENIR & SENSIBILISER**
à la sécurité numérique 
- 3 OBSERVER & ANTICIPER**
le risque numérique 

QUI EST CONCERNÉ ?



PREMIER MINISTRE

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

MINISTÈRE DE L'INTÉRIEUR

MINISTÈRE DE LA JUSTICE

MINISTÈRE DE L'ÉDUCATION NATIONALE ET DE LA JEUNESSE

MINISTÈRE DES ARMÉES



CYBERMALVEILLANCE.GOUV.FR EN QUELQUES CHIFFRES



56

**organisations
membres**

(publiques et privées)
du GIP ACYMA

.....



1250

**prestataires
référéncés**

sur l'ensemble
du territoire

.....



+ 460 000

**victimes
assistées**

depuis fin 2017

.....



2 482 000

**visiteurs
uniques**

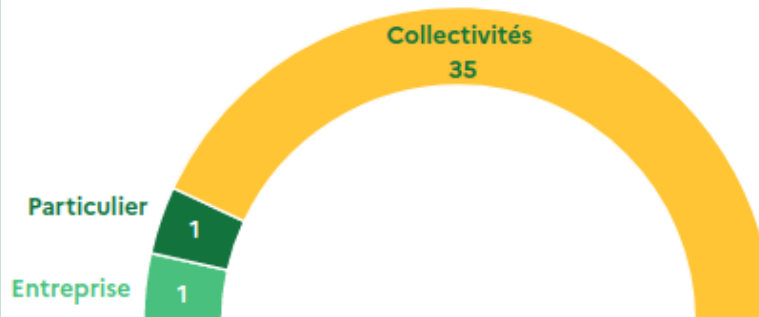
en 2021 (+101%)

L'ASSISTANCE AUX VICTIMES EN 2021

L'assistance aux victimes

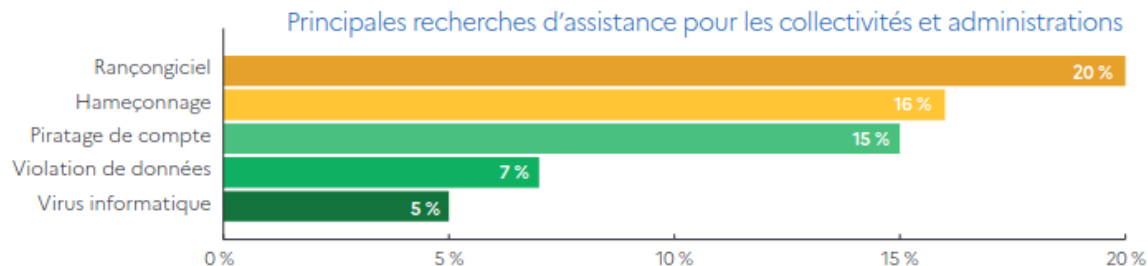


Proportion des publics assistés
sur [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) en 2021



PRINCIPALES CAUSES DE RECHERCHE D'ASSISTANCE EN 2021

Pour les collectivités et administrations :



Outils à destination des collectivités

OUTILS DE SENSIBILISATION ET DE PRÉVENTION

Objectifs :

- Sensibiliser aux risques
- Partager les bonnes pratiques
- Alerter

27 thématiques

6 types de contenus :

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

Publics :

- Particuliers
- Entreprises
- Collectivités
- Associations



Nos ressources de sensibilisation :



<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/liste-des-ressources-mises-a-disposition>

PROGRAMME DE SENSIBILISATION À DESTINATION DES ÉLUS

Objectif : sensibiliser aux risques numériques et partager avec eux les bonnes pratiques

Volet 1 : les principales **menaces** et les **réflexes essentiels** via des **questions de 2 maires**

Volet 2 : vigilance toutes les collectivités sont concernées ! via des **témoignages anonymisés**

Volet 3 : **témoignages de collectivités** ayant mis en place des **actions de sensibilisation**

Les réflexes essentiels pour la sécurité numérique des collectivités

"30%* des collectivités territoriales déclarent avoir déjà été touchées en 2020 par une cyberattaque de type rançongiciel (ransomware)."

Ce constat se vérifie à la fois sur la plateforme Cybermalveillance.gouv.fr, sur laquelle plus de 1200 collectivités sont venues chercher de l'aide en 2019, mais également avec la multiplication des attaques envers les collectivités territoriales, qui n'a cessé de croître ces dernières années et s'est largement intensifiée avec la crise de la Covid. L'actualité récente nous l'a montré :

... ignes,
y-Mory...



[Collectivités Territoriales] La recrudescence des cyberattaques envers les collectivités territoriales est une réalité : quelle que soit leur taille, toutes les collectivités sont concernées !



Vigilance face aux cyberattaques : les collectivités sont toutes concernées !
Assistance aux victimes de cybermalveillance

cybermalveillance.gouv.fr - Lecture de 3 min

x maires ont accepté de partager leurs
ujet, auxquelles Cybermalveillance.gouv.fr

ALERTES CYBER POUR LES COLLECTIVITÉS :

Conjointement avec :

- **L'ANSSI**
- **L'AMF**
- **Cybermalveillance.gouv.fr**
- **Contenu des alertes cyber :**
 - une vulnérabilité de sécurité « grand public »
 - pouvant toucher une multitude de collectivités
 - par une faille en cours d'exploitation
 - pour laquelle il existe un correctif publié par l'éditeur



ALERTE CYBERSÉCURITÉ

Faille de sécurité critique dans plusieurs produits Apple

Date de l'alerte : 17 février 2022

Risques
Espionnage, vol, voire destruction, de vos données suite à la prise de contrôle à distance de vos équipements concernés.

Description
Une faille de sécurité critique a été corrigée dans les systèmes d'exploitation d'Apple : iOS (pour téléphones iPhone et tablettes iPod touch), iPadOS (pour tablettes iPad), macOS Monterey (pour ordinateurs Mac, macOS et M1) et Safari (navigateur Internet).
L'exploitation de cette faille de sécurité peut permettre la prise de contrôle à distance des équipements concernés et le vol, voire la destruction, d'informations par des cybercriminels.
Selon Apple, des attaques en cours exploitant cette vulnérabilité auraient été constatées.

Systèmes concernés

- iOS et iPadOS, versions antérieures à 15.2.1
- macOS Monterey, versions antérieures à 12.2.1
- Safari, versions antérieures à 15.2

De nombreux appareils Apple sont concernés car la vulnérabilité affecte les modèles anciens ainsi que les plus récents.

Mesure à prendre
Mettre à jour au plus vite les équipements concernés avec les correctifs de sécurité mis à disposition par Apple.

Procédure

- Pour iOS, iPadOS : <https://support.apple.com/fr-k117204304>
- Pour macOS Monterey : <https://support.apple.com/fr-k117204304>
- Pour Safari : <https://support.apple.com/fr-k117204304>

Besoin d'assistance ?
Vous pouvez trouver sur [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) des prestataires de proximité susceptibles de vous apporter leur soutien dans la mise en œuvre de ces mesures : [ici](#)

Références
• ANSSI / CERT FR : <https://www.cert.ssi.gouv.fr/fr/CERTFR-2022-001-150/>
• CVE-2022-23029

Allez plus loin avec [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) :
Pourquoi et comment bien gérer ses alertes à jour ?

 **RÉPUBLIQUE
FRANÇAISE**
Union
Nationale

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



OUTIL AUTO-ÉVALUATION « I.M.M.U.N.I.T.É CYBER » : POUR LES COLLECTIVITÉS

Conjointement avec :

- le ministère de l'Intérieur,
- l'AMF
- [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr)


**MINISTÈRE
DE L'INTÉRIEUR**
 95000


AMF
 ASSOCIATION DES MAIRIES DE FRANCE
 ASSOCIATION DES MAIRIES DE FRANCE
 ASSOCIATION DES MAIRIES DE FRANCE

**Évaluez la sécurité numérique
de votre collectivité en 10 points**

VÉRIFIER MON IMMUNITÉ CYBER

		OUI	NON ou NE SAIS PAS
1	Avez-vous un inventaire complet de tous vos systèmes numériques ?	☐	☐
2	Utilisez-vous des mots de passe solides et différents pour chaque service ?	☐	☐
3	Vos systèmes numériques sont-ils mis à jour en temps réel et faites-vous des sauvegardes régulières de toutes vos données ?	☐	☐
4	Avez-vous sensibilisé vos agents aux risques numériques ?	☐	☐
5	Vos postes et serveurs informatiques sont-ils protégés par un antivirus ?	☐	☐
6	Êtes-vous en règle vis-à-vis du Règlement Général sur la Protection des Données (RGPD) ?	☐	☐
7	Vos agents sont-ils équipés de matériels sécurisés pour le télétravail ?	☐	☐
8	Faites-vous réaliser régulièrement des évaluations de votre sécurité numérique par des audits techniques ?	☐	☐
9	Avez-vous un plan de secours face aux cyberattaques ?	☐	☐

10 ACTION À MENER

Vous êtes dans le VERT : Bravo ! Votre collectivité met en œuvre les mesures essentielles. Pour aller encore plus loin, et vous aider à renforcer votre sécurité numérique, le réseau des cyber-gendarmes est à votre service.
 Vous êtes dans le ROUGE : Attention, votre collectivité est peut-être en danger ! La gendarmerie peut vous aider à faire un état des lieux de votre sécurité numérique et à établir un plan d'actions pour renforcer votre protection.

UNE HÉSITATION ? UN DOUTE ?
 Contactez votre GENDARMERIE pour un **ACCOMPAGNEMENT DÉTAILLÉ**

95000 Cybermalveillance.gouv.fr

FICHE ET AFFICHE « QUE FAIRE EN CAS DE CYBERATTAQUES »



CAMPAGNE DE VIDÉOS : 4 PRÉJUGÉS DES COLLECTIVITÉS SUR LA CYBERSÉCURITÉ

Cible : les collectivités

Objectifs :

- sensibiliser à la nécessité de prendre conscience des enjeux de la cybersécurité
- se sécuriser dès à présent

4 préjugés des élus mise en scène via les fables de la Fontaine :

- Le corbeau et le renard : « **Je ne suis pas concerné !** »
- La cigale et la fourmi : « **Je n'ai pas le budget !** »
- Le loup et l'agneau : « **Ce n'est pas ma priorité !** »
- Le lièvre et la tortue : « **Je n'ai pas le temps !** »


EN COURS...

- **sujet primordial à considérer**
- **orienter les collectivités vers [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr)**



GUIDE OBLIGATIONS ET RESPONSABILITÉS DES COLLECTIVITÉS EN MATIÈRE DE CYBERSÉCURITÉ

- **Objectifs :** rendre la réglementation en matière de cybersécurité plus claire
- **Contenu :**

Obligations liées à :

- la protection des données personnelles
- la mise en œuvre des téléservices locaux
- à l'hébergement des données de santé

Responsabilités auxquelles elles sont exposées:

- civile, pénale et administrative en cas de cyberattaques et/ou de dommages liés



CNIL.

ACCOMPAGNEMENT PAR DES PRESTATAIRES DE CONFIANCE

L'objectif de ce label « ExpertCyber » :

- Reconnaître l'expertise en sécurité numérique des professionnels
- Sur les activités d'installation, maintenance et assistance

Parcours dédié sur notre plateforme « Sécurisez vos systèmes numériques »

- Mise en relation avec un professionnel qualifié labellisé « ExpertCyber »
- Pour les clients (TPE-PME / Associations / Collectivités)
- www.securisation.cybermalveillance.gouv.fr



Outils d'assistance pour vos administrés

CAMPAGNE NATIONALE TV-MÉDIAS AVEC FRANCE TELEVISIONS – FÉVRIER 2022

Cible : Tous les publics

Objectif : En jouant sur l'humour et le décalage, la campagne invite les publics à s'intéresser au sujet de la cybersécurité

Thématique :

Volonté d'interpeller sur le fait que de vraies solutions existent face aux risques numériques, notamment grâce à **Cybermalveillance.gouv.fr**.



MODULE D' ASSISTANCE CYBER EN LIGNE POUR VOS ADMINISTRÉS

Proposer un outil de diagnostic cyber pour vos administrés

Une fois le diagnostic établi :

- 1) des conseils personnalisés sont proposés
- 2) la possibilité de se faire assister par un professionnel en cybersécurité référencé sur cybermalveillance.gouv.fr

Avantages :

- intégrable en moins de 10 min sur le site web de votre commune
- paramétrable totalement sur la forme
- une réponse apportée à l'utilisateur 24h/24 et 7J/7
- les données du parcours sont accessibles depuis un espace privé pour connaître l'usage de l'outil sur votre site



Exemple d'intégration du module sur le site de l'AMF
(mise en œuvre à l'étude)



MERCI



www.cybermalveillance.gouv.fr

 @cybervictimtimes

 @cybervictimtimes

 @cybermalveillancegouvfr



*Le Corbeau
et le
Renard*