



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 INFORMER & SENSIBILISER**  
à la sécurité numérique 
- 3 OBSERVER & ANTICIPER**  
le risque numérique 

## QUI EST CONCERNÉ ?



## CYBERMALVEILLANCE.GOUV.FR EN QUELQUES CHIFFRES



**56**

**organisations  
membres**

(publiques et privées)  
du GIP ACYMA



**1250**

**prestataires  
référéncés**

sur l'ensemble  
du territoire



**173 000**

**victimes  
assistées**

En 2021 (+65%)



**2 482 000**

**visiteurs  
uniques**

en 2021 (+101%)

## 56 MEMBRES RÉUNIS AUTOUR D'UN PARTENARIAT PUBLIC- PRIVÉ

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





**RÉPUBLIQUE  
FRANÇAISE**

*Liberté  
Égalité  
Fraternité*

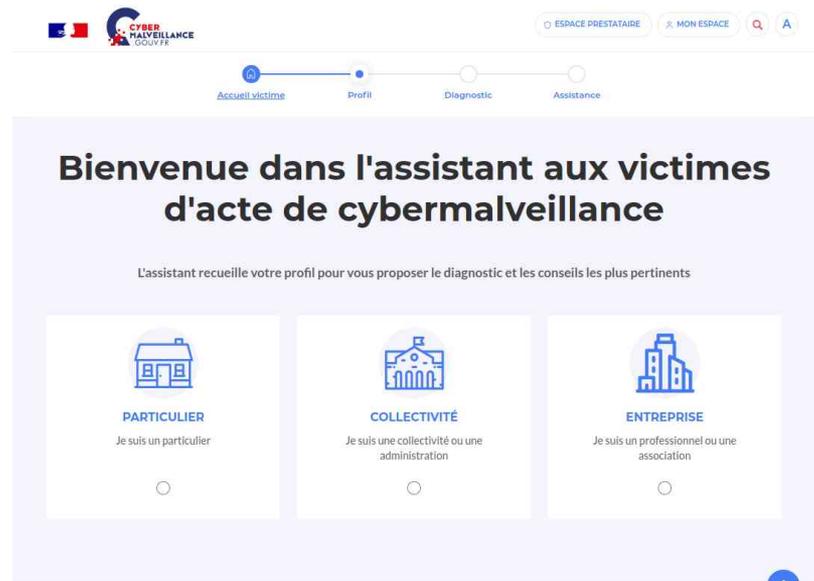


Assistance et prévention  
en sécurité numérique

# Parcours d'assistance aux victimes et tendances des menaces cyber

## LE PARCOURS VICTIME

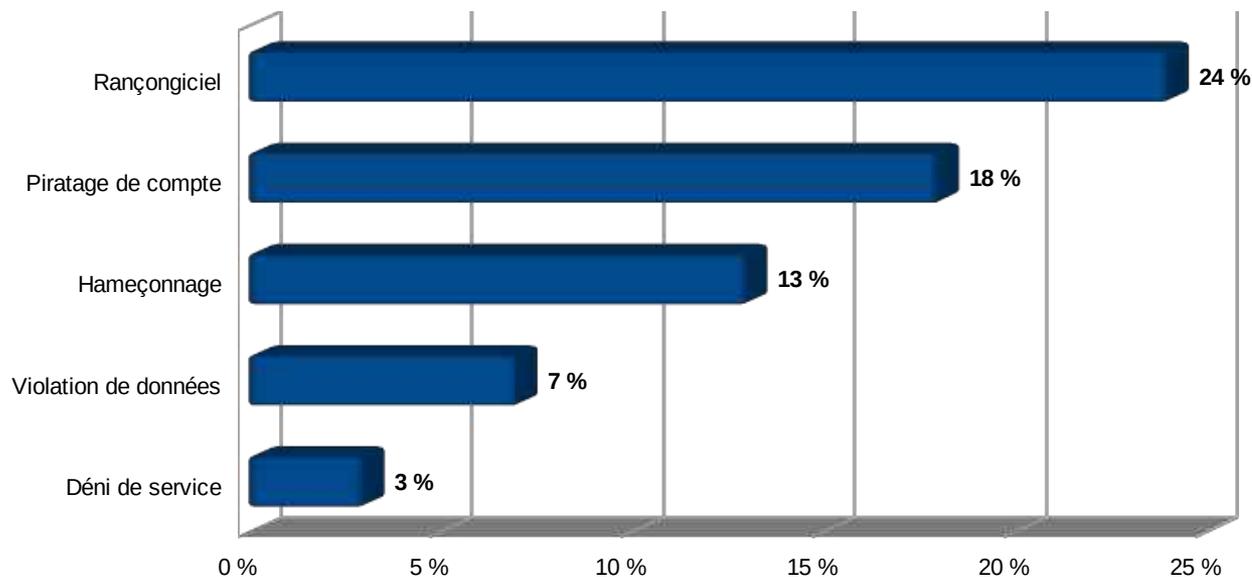
- **Un outil destiné à la remédiation**
  - Établir un diagnostic
    - Avec des questions adaptatives
    - Mettre un nom sur la cybermalveillance
  - Proposer des conseils personnalisés
    - Premières mesures
    - Identifier le bon interlocuteur
  - Mettre en relation
    - Avec un prestataire référencé (assistance)
    - Proximité géographique
- **Un outil qui évolue**
  - Traitement de la demande et satisfaction



The screenshot shows the user interface of the 'Assistant aux victimes d'acte de cybermalveillance'. At the top, there is a navigation bar with the French Republic logo and the 'CYBER MALVEILLANCE .GOUV.FR' logo. On the right, there are links for 'ESPACE PRESTATAIRE', 'MON ESPACE', and search icons. Below the navigation bar is a progress indicator with four steps: 'Accueil victime', 'Profil', 'Diagnostic', and 'Assistance'. The 'Profil' step is currently active. The main content area features a large heading: 'Bienvenue dans l'assistant aux victimes d'acte de cybermalveillance'. Below this, a sub-heading reads: 'L'assistant recueille votre profil pour vous proposer le diagnostic et les conseils les plus pertinents'. There are three selection cards: 'PARTICULIER' (Je suis un particulier), 'COLLECTIVITÉ' (Je suis une collectivité ou une administration), and 'ENTREPRISE' (Je suis un professionnel ou une association). Each card has a radio button for selection.

## PRINCIPALES RECHERCHES D'ASSISTANCE EN 2021

### Pour les entreprises et associations :



**49**  
types d'incidents  
traités

## DES CYBERMALVEILLANCES ...

- L'hameçonnage (phishing) : « la mère des attaques »
  - Menace prédominante qui s'est professionnalisée
  - Développement important des attaques par SMS
- Le piratage de compte
  - Origines diverses
  - Cause d'autres malveillances



## ... QUI S'ADAPTENT AUX CONTEXTES

- Crise sanitaire
- Évènements sportifs, conflits

Nous avons essayé de livrer votre colis LP995215701FR, mais il n'y a aucun affranchissement. Suivez les instructions ici: <http://bit.do/fHXvw>

mercredi 5 janvier 2022

Votre nouvelle carte vitale est disponible. Veuillez remplir le formulaire afin de continuer à être couvert via [ameli-vital.fr](http://ameli-vital.fr)

## LES RANÇONGIERS

- 1ère menace pour les professionnels
- Tous types et tailles d'organisations ciblées en nombre
- Un écosystème cybercriminel redoutable qui fonctionne en cartel
- Pluralité et sophistication
- Vol de données avec menace de divulgation pour accentuer la pression depuis fin 2019

Le Parisien

Hauts-de-Seine

### Les hackers de Lockbit 2.0 revendiquent la cyberattaque contre la mairie de Saint-Cloud

Les cybercriminels menacent de publier les données dérobées lors de l'attaque survenue dans la nuit du 20 au 21 janvier. La mairie assure que le rétablissement des systèmes informatiques est en bonne voie. Le groupe de hackers a aussi revendiqué, ce jeudi, une attaque contre le ministère de la Justice.





**RÉPUBLIQUE  
FRANÇAISE**

*Liberté  
Égalité  
Fraternité*



Assistance et prévention  
en sécurité numérique

# Réagir en cas de Cyber attaque

## LES PREMIERS RÉFLEXES

- **Alertez immédiatement** votre support informatique
- **Isolez** les systèmes attaqués
- **Constituez** une équipe de gestion de crise
- **Documentez** les évènements et actions réalisées



## PILOTER LA CRISE

- Mettez en place des **solutions de secours**
- **Déclarez le sinistre**
  - Assurance, banque
  - CNIL (dans les 72h si données personnelles impactées)
  - Déposez plainte
- **Identifiez** l'origine et l'étendue de l'attaque puis **corrigez**
- **Gérez votre communication** avec le juste niveau de transparence



## SORTIR DE LA CRISE

- **Faites une remise en service progressive et contrôlée**
- **En surveillant son fonctionnement**
- **Tirez les enseignements de l'attaque**
  - Définissez les plans d'action et d'investissements



## UN SUPPORT MÉTHODOLOGIQUE

- Pour les dirigeants
  - Trois étapes clés
  - Une liste de points d'attention essentiels
  - Une aide à la gestion de crise



**QUE FAIRE EN CAS DE CYBERATTAQUE ? (dirigeants)**

Méthodologie synthétique de gestion des cyberattaques pour les dirigeants des entreprises, associations, collectivités, administrations.

**1 PREMIERS RÉFLEXES**

- Alertez immédiatement votre support informatique prestataire, tel
- Isoler les systèmes attaqués, puisse se propager à d'autres les connexions à Internet et à
- Constituez une équipe de gestion des actions des différents (technique, RH, financière, etc)
- Tenez un registre des événements disposition des enquêteurs et
- Préservez les preuves de l'att

**2 PILOTER LA CRISE**

- Mettez en place des solutions d'assurer les services Indisg continuité et de reprise d'acti
- Déclarez le sinistre auprès de votre niveau de couverture ad
- Alertez votre banque ou cas auraient pu être dérobées.
- Déposez plainte avant toute possession.
- Identifiez l'origine de l'attaq un nouvel incident.
- Notifiez l'incident à la CNIL modifiées ou détruites par les
- Gérez votre communication : clients, collaborateurs, part

**3 SORTIR DE LA CRISE**

- Tirez les enseignements de l'attaque et déterminez les plans d'action
- Faites une remise en service progressive et contrôlée

**CONTACTS UTILES**

- CONSEILS ET ASSISTANCE
- NOTIFICATION DE VIOLATION DE DONNÉES PERSONNELLES
- POLICE, GENDARMERIE

Dispositif national de prévention et d'assistance aux victimes de cybermalveillance  
[www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)

Commission nationale Informatique et Liberté (CNIL)  
[www.cnil.fr/fr/notifier-une-violat-bn-ata-donnees-personnelles](http://www.cnil.fr/fr/notifier-une-violat-bn-ata-donnees-personnelles)

17

14/06/2022

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/cyberattaque-que-faire-guide-dirigeants>



# Diagnostiquer et accompagner

## LE PARCOURS DE SÉCURISATION

- **Un outil destiné à l'accompagnement**
  - Des TPE-PME / Associations / Collectivités
- Pour répondre à leurs besoins
  - Installation / maintenance / assistance
- Dans de nombreux domaines techniques
  - Serveurs, postes fixes/nomades
  - Infrastructure, sauvegarde, site web
  - Téléphonie fixe/mobile
- Être mis en relation
  - Avec un professionnel labellisé « ExpertCyber »
  - Spécialisé dans le domaine recherché
  - [www.securisation.cybermalveillance.gouv.fr](http://www.securisation.cybermalveillance.gouv.fr)



https://www.cybermalveillance.gouv.fr/accompagnement/accueil 60%

LES MENACES ET BONNES PRATIQUES L'ACTUALITÉ DE LA CYBERMALVEILLANCE NOUS DÉCOUVRIR VICTIME D'UN ACTE DE CYBERMALVEILLANCE ?

### Sécurisez vos systèmes numériques avec un professionnel qualifié

Vous souhaitez être accompagné pour sécuriser vos systèmes numériques (informatique, sites Internet, téléphonie...) ? Notre plateforme vous met en relation avec des professionnels qualifiés dans la sécurisation de nouveaux systèmes ou de systèmes existants. Ces professionnels ont reçu le label ExpertCyber qui vous garantit un niveau de compétence et d'expertise en sécurité numérique.

#### Comment cela fonctionne ?

- 01. DÉCRIVEZ**  
Répondez à quelques questions simples pour nous permettre de comprendre vos attentes.
- 02. CHOISISSEZ**  
Nous vous proposons les prestataires disposant des compétences pour répondre à votre besoin.
- 03. SÉCURISEZ**  
Le prestataire ExpertCyber que vous avez choisi vous accompagne et réalise les prestations attendues.

COMMENCER

## LES ALERTES CYBERSÉCURITÉ

- Sur les réseaux sociaux « grand public » et professionnels

**CYBERSÉCURITÉ** 

**DES CENTAINES DE FAILLES DE SÉCURITÉ  
CORRIGÉES DANS LES MISES À JOUR D'AVRIL**

Microsoft Windows, Exchange Server, Office, Edge, 365 Apps...  
Linux Red Hat, Suse, Ubuntu  
Apple iOS, iPadOS, watchOS  
Google Android, Chrome, Chrome OS  
Mozilla Firefox, Thunderbird  
GitLab - Joomla! - OpenSSH - OpenSSL - Samba - WordPress  
Cisco - Citrix - IBM - Juniper - SAP - VMware...

**Mettez à jour sans tarder !**  
[www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)

- Via des organisations et réseaux professionnels

**ALERTE  
CYBERSÉCURITÉ** 

### Failles de sécurité critiques dans les produits Apple

Date de l'alerte : 11 mai 2021

**Risque(s)**  
Vol, voire destruction, de vos données suite à la prise de contrôle à distance de vos équipements concernés.

**Description**  
Des failles de sécurité critiques ont été corrigées dans les systèmes d'exploitation d'Apple et de son navigateur Internet Safari. L'exploitation de ces failles peut permettre la prise de contrôle à distance des équipements concernés et le vol, voire la destruction, d'informations confidentielles par des cybercriminels.

Selon le constructeur, des attaques en cours exploitant ces vulnérabilités seraient constatées.

**Système(s) concerné(s)**

- macOS Big Sur : versions antérieures à 11.3.1
- iOS : versions antérieures à 14.5.1
- watchOS : versions antérieures à 7.4.1
- iPadOS : versions antérieures à 14.5.1
- Apple Safari : versions antérieures à 14.1

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

**Procédures**

- Pour iOS, iPadOS : <https://support.apple.com/fr-fr/HT204204>
- Pour macOS et Safari : <https://support.apple.com/fr-fr/HT201341>
- Pour watchOS : <https://support.apple.com/fr-fr/HT204641>

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

Référence(s)  
• ANSSI / CERT-FR : <https://www.cert.ssi.gouv.fr/fr/actualites/CERTFR-2021-04CT010/>  
• CVE-2021-30861 - CVE-2021-30863 - CVE-2021-30868 - CVE-2021-30866

Alter plus loin avec [Cybermalveillance.gouv.fr](http://Cybermalveillance.gouv.fr) :  
Pourquoi et comment bien gérer ses mises à jour ?

 **RÉPUBLIQUE  
FRANÇAISE**  
*Liberté  
Égalité  
Fraternité*

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



## 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



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



RÉPUBLIQUE  
FRANÇAISE

*Liberté  
Égalité  
Fraternité*



[www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)

Nos ressources de sensibilisation



Assistance et prévention  
en sécurité numérique



@cybervictimtimes



@cybervictimtimes



@cybermalveillancegouvfr