



**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



+ 460 000

**victimes
assistées**

depuis fin 2017



2 482 000

**visiteurs
uniques**

en 2021 (+101%)

56 MEMBRES RÉUNIS AUTOUR D'UN PARTENARIAT PUBLIC- PRIVÉ

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



1. Assister les victimes et comprendre l'évolution des menaces cyber.

LE PARCOURS VICTIME SUR CYBERMALVEILLANCE.GOUV.FR

DIAGNOSTIC

CONSEILS

MISE EN RELATION

TRAITEMENT

SATISFACTION

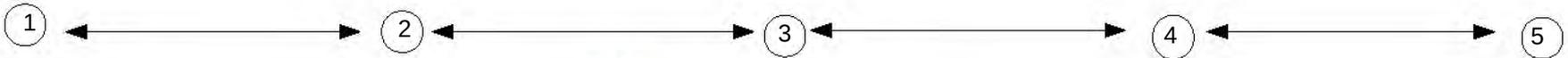
Cherche à comprendre
son problème

Applique les conseils
personnalisés proposés

Décide de se faire aider et
sélectionne un prestataire

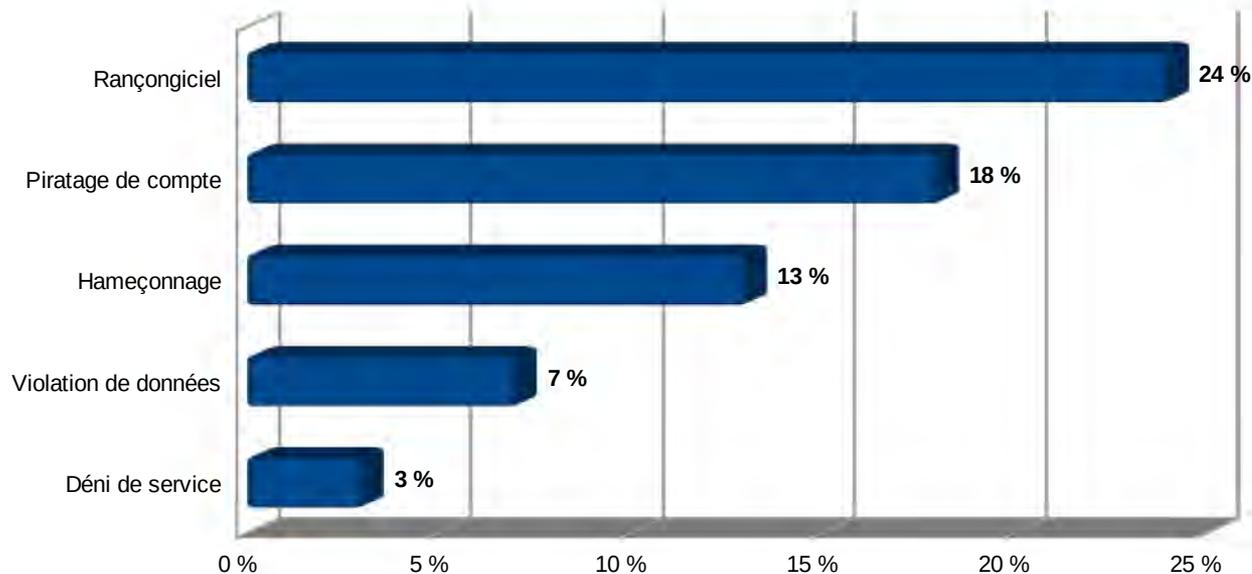
Suit la bonne exécution
de la prestation

Note la prestation et le
service



PRINCIPALES RECHERCHES D'ASSISTANCE EN 2021

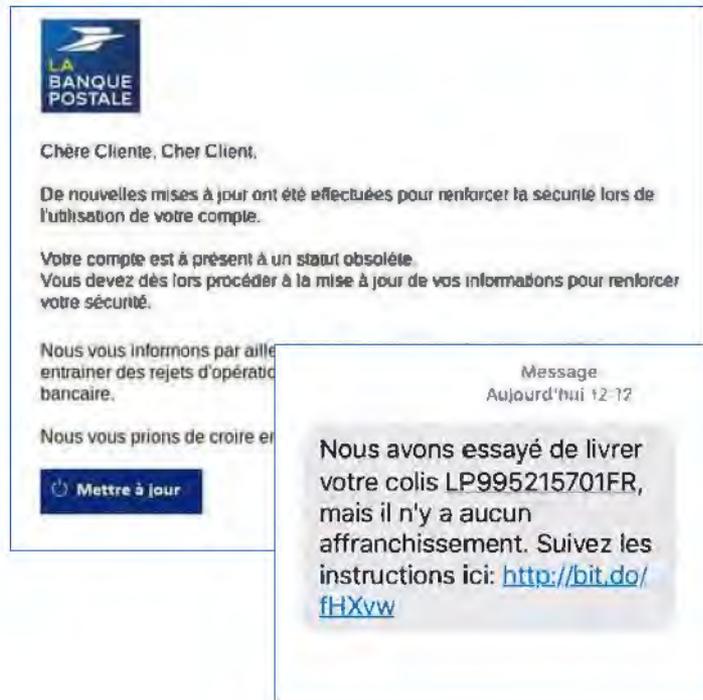
Pour les entreprises et associations :



48
types d'incidents
traités

L'HAMEÇONNAGE (PHISHING) : LA MÈRE DES ATTAQUES

- Menace prédominante et en hausse
- Des attaques toujours plus sophistiquées
- Effet démultiplicateur avec la crise sanitaire
- Principale cause d'autres malveillances
- Développement important des attaques par SMS



LE PIRATAGE DE COMPTE

- **Menace majeure et en expansion**
- **Messageries, réseaux sociaux et banques visés**
- **Cause majeure d'autres malveillances**
(Usurpation d'identité, fraude bancaire ou au virement...)
- **Impacts de plus en plus importants pour les victimes**



LES RANÇONGIELS

- 1ère menace pour les professionnels (entreprises, collectivités...)
- 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

METROPOLITAIN

Publié le 26 Nov 21 à 14:27

Une cyberattaque musclée a ciblé mercredi le groupe Orchestra, dont le siège social est implanté à Saint-Aunès, aux portes Est de Montpellier. Les hackers réclament une rançon

Cette spectaculaire attaque informatique de hackers non identifiés, a entraîné le blocage provisoire des paiements par cartes bancaires dans les terminaux des boutiques, tandis que des milliers de données de clients ont été piratés.



2. Des productions adaptées à chacun de nos publics.

DES ARTICLES ADAPTÉS AUX PARTICULIERS :

- Procédure fictive de poursuites pour infractions liées à la pédopornographie,
- Chantage de rendre ces éléments publics,
- Utilisation de noms d'organisations et de magistrats réels,
- Délais court et stressant,
- Pas de demande d'argent immédiate...

The screenshot shows a news article on the website 'CYBER MALVEILLANCE GOUV.FR'. A prominent red stamp with the text 'Attention aux ARNAQUES' is overlaid on the left side of the page. The article title is 'Campagnes de messages d'escroquerie usurpant l'identité de la Police et de la Gendarmerie', published on 18 Dec 2020. The article content begins with 'Vous avez reçu un message (mail) d'une personne prétendant appartenir à la Brigade...'. The website header includes navigation links like 'LES MENACES ET BONNES PRATIQUES' and 'L'ACTUALITÉ DE LA CYBERMALVEILLANCE'. A circular logo for 'DIRECTION CENTRALE DE LA POLICE JUDICIAIRE' is also visible.

DES ARTICLES ADAPTÉS AUX PUBLICS PRO :

- Premiers réflexes,
- Piloter la crise,
- Sortir de la crise,
- Contacts utiles,
- Des supports dédiés,

ESPACE PRESTATAIRE MONESPACE

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

Accueil → Les derniers articles → Article

Que faire en cas de cyberattaque ? (Guide pour les dirigeants)

Publié le 27 Janv. 2022

Opérations Cyber-sécurité Services professionnels

Version de l'article / 7 pages

1. PREMIERS RÉFLEXES

2. PILOTER LA CRISE

3. SORTIR DE LA CRISE

CONTACTS UTILES

NOS SUPPORTS POUR GÉRER UNE CYBERATTIQU

Pour une entreprise, une association, une administration ou une collectivité, quelle qu'en soit la taille, une cyberattaque est une situation de crise dont les conséquences ne sont pas seulement techniques, mais également financières, de réputation, voire juridiques et peuvent impacter jusqu'à la survie des plus petites structures.

Une cyberattaque est une crise de gestion majeure et implique l'ensemble de la gouvernance afin d'atténuer les impacts et permettre une reprise d'activité dans les meilleurs délais et les conditions de sécurité pour éviter une récidive.

Ces supports méthodologiques synthétisent et permettent aux dirigeants des organisations victimes

GUIDES PRATIQUES :

- **Un guide spécifiquement conçu pour les chefs d'entreprises :**
- La valeur de l'activité face aux risques,
- Les principales menaces aujourd'hui,
- Les premiers réflexes en cas d'attaque !



ALERTES POUR LES ENTREPRISES :

- **Alertes cyber relayées par le MEDEF et CPME :**
 - une vulnérabilité de sécurité « grand public »,
 - une vulnérabilité de sécurité « grand public »,
 - déjà exploitée,
 - pour laquelle il existe un correctif publié par l'éditeur,
- **4ème alerte depuis septembre 2021 !**

**ALERTE
CYBERSÉCURITÉ** 

Faillles 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/HT201541>
- Pour watchOS : <https://support.apple.com/fr-fr/HT204641>

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

Références(s)

- AMMI / CERT FR : <https://www.cert.fr/fr/actualites/actualites-cert-fr-2021-05-11-01>
- CVE-2021-30861 - CVE-2021-30863 - CVE-2021-30865 - CVE-2021-30866

Attir plus loin avec Cybermalveillance.gouv.fr
Pourquoi #SOSCERT est devenu un réflexe à avoir ?


**RÉPUBLIQUE
FRANÇAISE**
*Liberté
Égalité
Fraternité*


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



FICHES & AFFICHES POUR LES ENTREPRISES :



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 si vous en disposez afin qu'il prenne en compte l'incident (service informatique, prestataire, personne en charge).



Isolez les systèmes attaqués afin d'éviter que l'attaque ne puisse se propager à d'autres équipements en coupant toutes les connexions à Internet et au réseau local.



Constituez une équipe de gestion de crise afin de piloter les actions des différentes composantes concernées (technique, RH, financière, communication, juridique...).



Tenez un registre des événements et actions réalisées pour pouvoir en conserver la trace à disposition des enquêteurs et tirer les enseignements de l'incident a posteriori.



Préservez les preuves de l'attaque : messages reçus, machines touchées, journaux de connexions...

2 PILOTER LA CRISE



Mettez en place des solutions de secours pour pouvoir continuer

NE PAYEZ PAS DE RANÇON !

Car vous encourageriez les cybercriminels à chercher à vous attaquer à nouveau et financiez leur activité criminelle tout en n'ayant aucune garantie qu'ils tiendront leur parole.

FAITES-VOUS



QUE FAIRE EN CAS DE CYBERATTAQUE ? (dirigeants)



ALERTEZ IMMÉDIATEMENT VOTRE SUPPORT INFORMATIQUE



ISOLEZ LES SYSTÈMES ATTAQUÉS



CONSTITUEZ UNE ÉQUIPE DE GESTION DE CRISE



TENEZ UN REGISTRE DES ÉVÉNEMENTS



PRÉSERVEZ LES PREUVES DE L'ATTAQUE

METTEZ EN PLACE DES SOLUTIONS DE SECOURS

DÉCLAREZ LE SINISTRE AUPRÈS DE VOTRE ASSUREUR

ALERTEZ VOTRE BANQUE

DÉPOSEZ PLAINTÉ

IDENTIFIEZ L'ORDONNEUR DE L'ATTAQUE ET SON FINANCEUR

NOTIFIEZ L'INCIDENT À LA CNIL

ÉVALUEZ VOTRE COMMUNICATION



TIREZ LES ENSEIGNEMENTS DE L'ATTAQUE ET GÉNÉRALISEZ LES PLANS D'ACTION

FAITES UNE REVERIE EN SERVICE PROGRESSIVE ET CONTRÔLÉ

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.nadsec.malinfo.gouv.fr

Commission nationale d'enquête et d'assistance aux victimes de cybermalveillance

www.cnil.fr/fr/assistance-aux-victimes-de-cybermalveillance

17

17/03/2022 10:00:00

3. Nos recommandations et solutions pour mieux se prémunir.

TROUVER DES PRESTATAIRES DE CONFIANCE POUR SE FAIRE ACCOMPAGNER

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



LES MENACES ET BONNES PRATIQUES

L'ACTUALITÉ DE LA
CYBERMALVEILLANCE

NOUS DÉCOUVRIR

VICTIME D'UN ACTE DE
CYBERMALVEILLANCE ?

DES SERVICES POUR : TOUS PUBLICS

PROFESSIONNELS

1 - DIAGNOSTIC EN LIGNE



Victime d'acte de
cybermalveillance ?

Nous vous aidons à
qualifier votre problème



ET / OU



Des conseils et solutions vous
sont proposés pour résoudre
votre problème.

Vous pouvez faire une demande de
mise en relation avec un
professionnel spécialisé.

CLIQUER ICI

Pour commencer



En savoir plus →



SÉCURISER SON SYSTÈME D'INFORMATION

Sécurisez votre SI avec un
professionnel labellisé
ExpertCyber.

COMMENCER



SE PROTÉGER

Consultez nos bonnes
pratiques et conseils pour
vous protéger des
cybermenaces.

EN SAVOIR PLUS →



SIGNALER

Vous souhaitez signaler une
escroquerie en ligne ou un
contenu illicite sur Internet ?

EN SAVOIR PLUS →



DÉPOSER PLAINTÉ

Vous souhaitez déposer
plainte suite à une
cybermalveillance ?

EN SAVOIR PLUS →

ADOPTER LES BONNES PRATIQUES !



LES MOTS DE PASSE



Votre mot de passe doit être différent pour chaque service, suffisamment long et complexe, et impossible à deviner. Ne le communiquez jamais à un tiers. Pour votre messagerie, il doit être particulièrement robuste.



LA SÉCURITÉ SUR LES RÉSEAUX SOCIAUX



Protégez l'accès à vos comptes, vérifiez vos paramètres de confidentialité et maîtrisez vos publications. Faites attention à qui vous parlez. Vérifiez régulièrement les connexions à votre compte.



LA SÉCURITÉ DES APPAREILS MOBILES



Mettez en place les codes d'accès. Appliquez les mises à jour de sécurité et faites des sauvegardes, évitez les réseaux Wi-Fi publics ou inconnus. Ne laissez pas votre appareil sans surveillance.

C'est...

- Gérer ses mots de passe,
- Rester maître de ses réseaux sociaux,
- Sécuriser ses outils quotidiens.



SANS OUBLIER...



LES SAUVEGARDES



Pour éviter de perdre vos données, effectuez des sauvegardes régulières. Identifiez les appareils et supports qui contiennent des données et déterminez lesquelles doivent être sauvegardées. Choisissez une solution adaptée à vos besoins. Protégez et testez vos sauvegardes.



LES MISES À JOUR



Mettez à jour sans tarder l'ensemble de vos appareils et logiciels. Téléchargez les mises à jour uniquement depuis les sites officiels et activez l'option de téléchargement et d'installation automatique des mises à jour.



LES USAGES PRO-PERSO



Utilisez des mots de passe différents pour tous les services professionnels et personnels auxquels vous accédez. Ne mélangez pas votre messagerie professionnelle et personnelle et n'utilisez pas de service de stockage en ligne personnel à des fins professionnelles.



- La préservation des données,
- L'optimisation sécurisée des programmes et des plateformes,
- La différenciation des usages.



RÉPUBLIQUE
FRANÇAISE

*Liberté
Égalité
Fraternité*



Assistance et prévention
en sécurité numérique



www.cybermalveillance.gouv.fr

 @cybervictimes

 @cybervictimes

 @cybermalveillancegouvfr