RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR

Assistance et prévention en sécurité numérique

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

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

LES MISSIONS DU DISPOSITIF

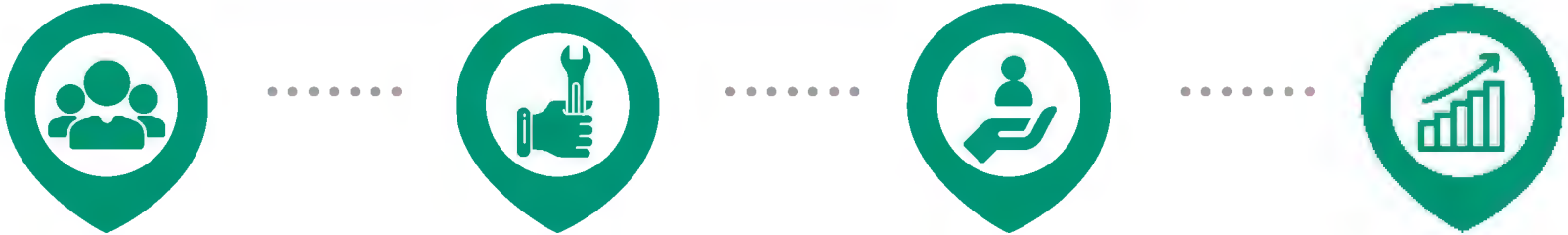
1. **ASSISTER LES VICTIMES** d'actes de cybermalveillance
2. **INFORMER & SENSIBILISER** à la sécurité numérique
3. **OBSERVER & ANTICIPER** le risque numérique

QUI EST CONCERNÉ ?

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

CYBERMALVEILLANCE.GOUV.FR EN QUELQUES CHIFFRES



56

organisations membres
(publiques et privées) du GIP ACYMA

1250

prestataires référencés
sur l'ensemble du territoire

+ 460 000

victimes assistées
depuis fin 2017

2 482 000

visiteurs uniques
en 2021 (+101%)

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

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

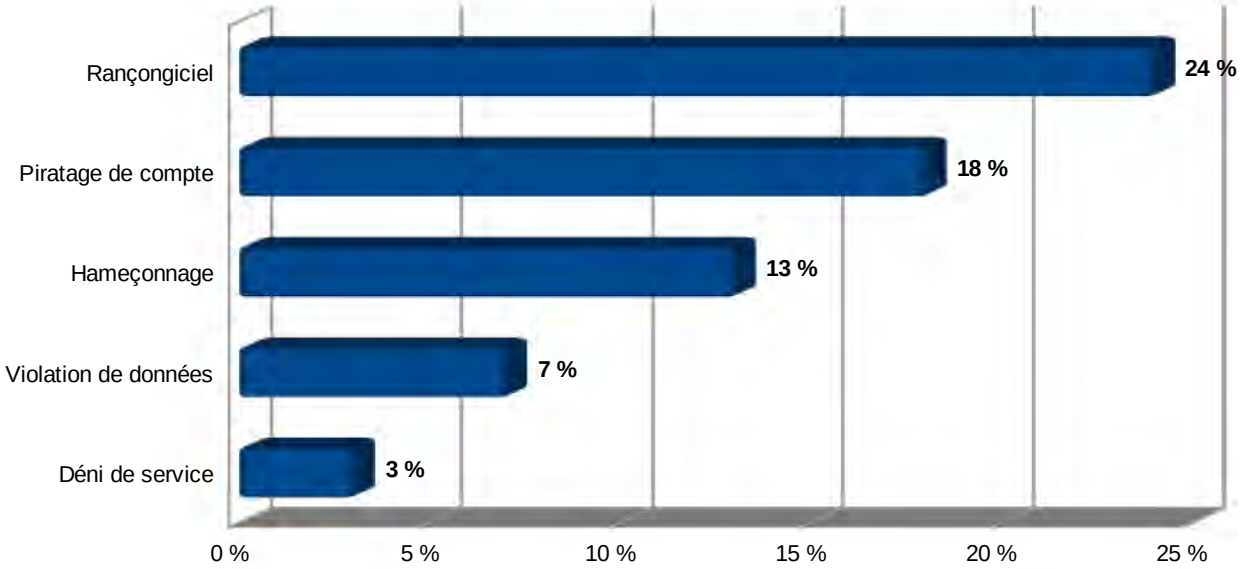
DIAGNOSTIC	CONSEILS	MISE EN RELATION	TRAITEMENT	SATISFACTION
Cherche à comprendre son problème	Applique les conseils personnalisés proposés	Décide de se faire aider et sélectionne un prestataire	Suit la bonne exécution de la prestation	Note la prestation et le service
1	2	3	4	5

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

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**

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

LES RANÇONGICIELS

- **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.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

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...**

DES ARTICLES ADAPTÉS AUX PUBLICS PRO :

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

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

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 !

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

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

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

Besoin d'assistance ?

Vous pouvez trouver sur Cybermalveillance.gouv.fr des prestataires de proximité susceptibles de vous apporter leur soutien dans la mise en œuvre de ces mesures en cliquant ici.

Référence(s)

- ANSSI / CERT-FR : https://www.cert.ssi.gouv.fr/avis/CERTFR-2021-AVI-[illegible]
- CVE-2021-30661 - CVE-2021-30663 - CVE-2021-30665 - CVE-2021-30666

Allez plus loin avec Cybermalveillance.gouv.fr
Pourquoi et comment bien gérer ses mises à jour ?

RÉPUBLIQUE FRANÇAISE

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

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

FICHES & AFFICHES POUR LES ENTREPRISES :

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

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

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

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...).

NE PAYEZ PAS DE RANÇON !

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

Tenez un registre des évènements 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

FAITES-VOUS

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

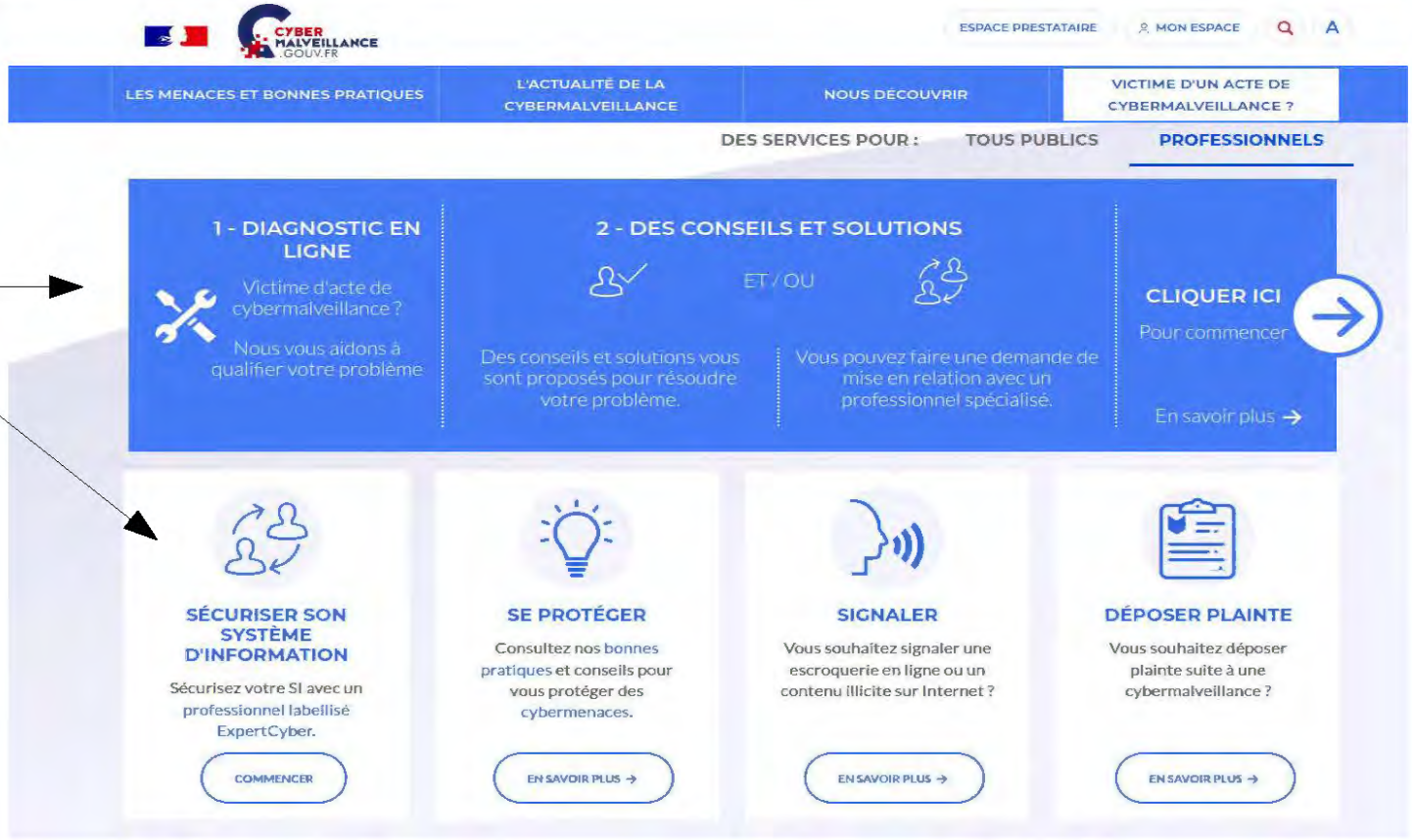
EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

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**

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique



ADOPTER LES BONNES PRATIQUES !

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 différentiation des usages.

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

Publics :

- Particuliers
- Entreprises
- Collectivités

27 thématiques

6 types de contenus :

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

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR

Assistance et prévention en sécurité numérique

www.cybermalveillance.gouv.fr

@cybervictimes

@cybervictimes

@cybermalveillancegouvfr