



**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



53

**organisations
membres**

(publiques et privées)
du GIP ACYMA



1250

**prestataires
référéncés**

sur l'ensemble
du territoire



405 000

**victimes
assistées**
depuis fin 2017



48

**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



LE PARCOURS VICTIME SUR CYBERMALVEILLANCE.GOUV.FR

DIAGNOSTIC

CONSEILS

MISE EN RELATION

TRAITEMENT

SATISFACTION

Cherche à comprendre
son problème

Applique les conseils
personnalisés proposés

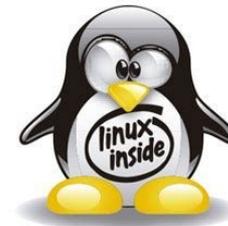
Décide de se faire aider et
sélectionne un prestataire

Suit la bonne exécution
de la prestation

Note le service

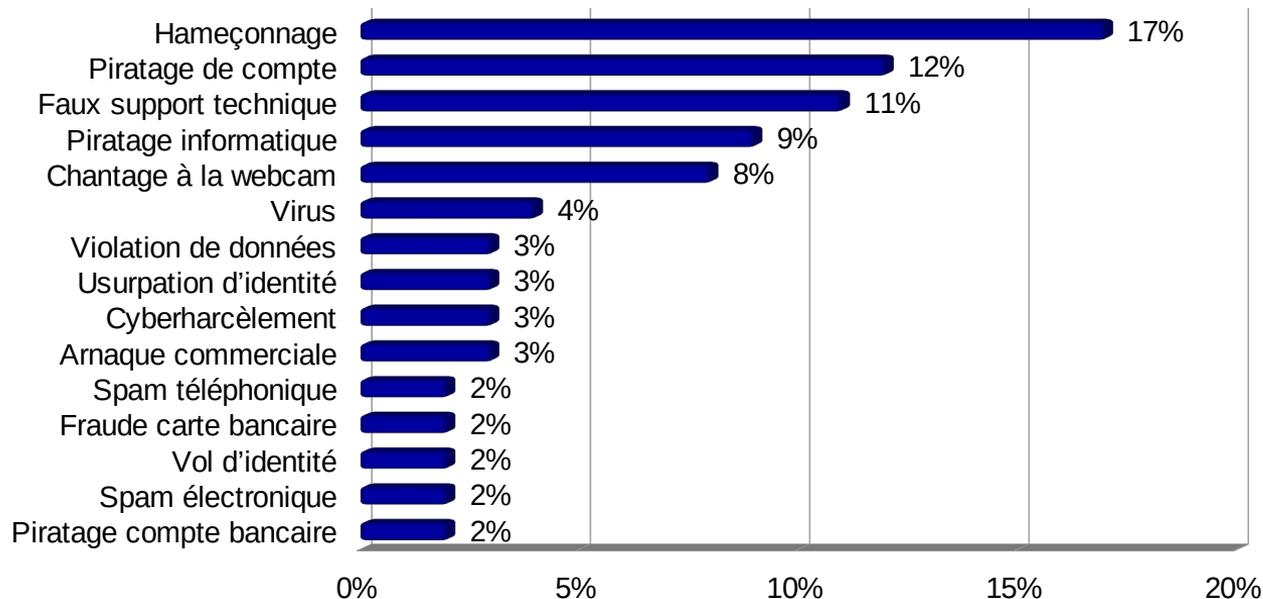
The screenshot shows the website's navigation and main content area. At the top, there are links for 'ESPACE PRESTATAIRE', 'MON ESPACE', and search/refresh icons. The main navigation bar includes 'LES MENACES ET BONNES PRATIQUES', 'L'ACTUALITÉ DE LA CYBERMALVEILLANCE', 'NOUS DÉCOUVRIR', and 'VICTIME D'UN ACTE DE CYBERMALVEILLANCE ?'. Below this, a filter for 'DES SERVICES POUR : TOUS PUBLICS' and 'PROFESSIONNELS' is visible. The main content area is divided into two columns: '1 - DIAGNOSTIC EN LIGNE' and '2 - DES CONSEILS ET SOLUTIONS'. The first column features a wrench and screwdriver icon and asks 'Victime d'acte de cybermalveillance ?' with the text 'Nous vous aidons à qualifier votre problème'. The second column features a person icon with a checkmark and asks 'ET / OU' with the text 'Des conseils et solutions vous sont proposés pour résoudre votre problème.' and 'Vous pouvez faire une demande de mise en relation avec un professionnel spécialisé.'. A 'CLIQUER ICI' button with a right arrow is positioned to the right of the second column, with the text 'Pour commencer' below it and 'En savoir plus →' at the bottom right.

CYBERMALVEILLANCES : TOUS CONCERNÉS !



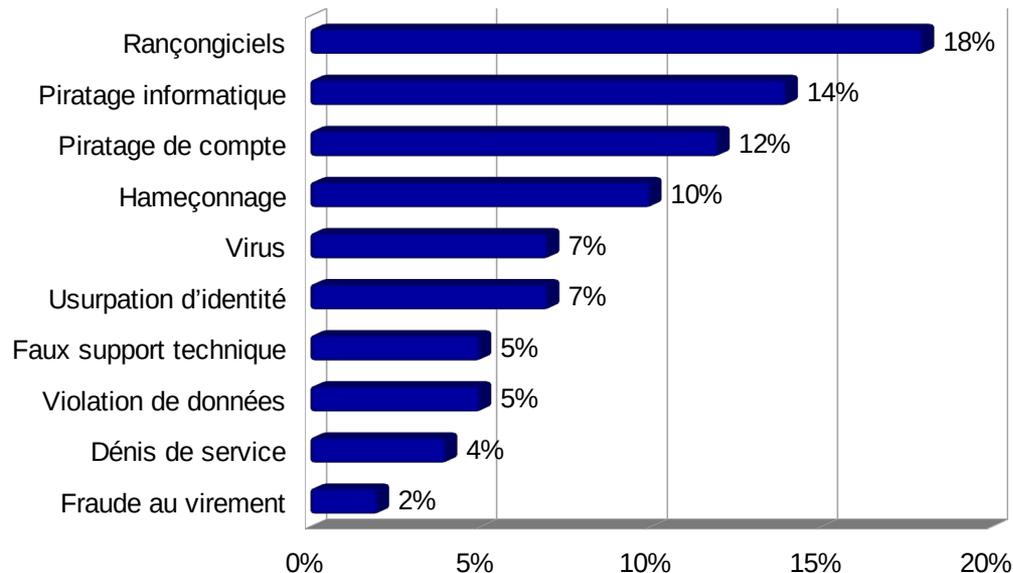
PRINCIPALES CAUSES DE RECHERCHE D'ASSISTANCE EN 2020

Particuliers :



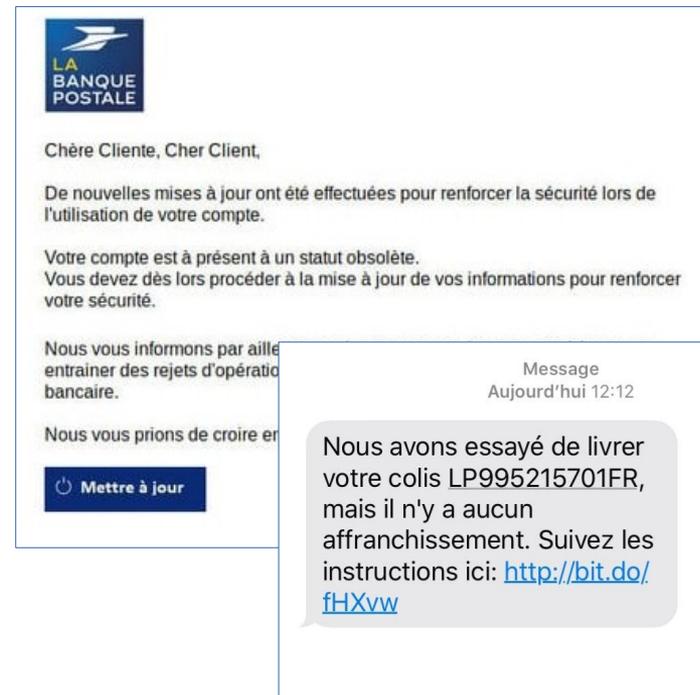
PRINCIPALES CAUSES DE RECHERCHE D'ASSISTANCE EN 2020

Professionnels (entreprises, collectivités...) :



L'HAMEÇONNAGE (PHISHING) : LA MÈRE DES ATTAQUES

- Menace prédominante et en hausse
- 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



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...



ESPACE PRESTATAIRE | MON ESPACE | A

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

Attention aux ARNAQUES

DIRECTION CENTRALE DE LA POLICE JUDICIAIRE

Accueil → Les actualités → Article

Campagnes de messages d'escroquerie usurpant l'identité de la Police et de la Gendarmerie

Publié le 18 déc. 2020

chantage par mail | message hacker boîte mail

333195 Temps de lecture : 20 min

1. DE QUOI S'AGIT-IL ? Vous avez reçu un message (mail) d'une personne prétendant appartenir à la Brigade de Protection des M...

...COMME AUX PUBLICS PROFESSIONNELS :

- Définition d'un piratage,
- Comment s'en protéger,
- Que faire si l'on est victime,
- Que dit le Code Pénal,
- Nos supports et recommandations,



The screenshot shows the website interface for Cybermalveillance.gouv.fr. At the top, there is a navigation bar with the French flag and the site logo. Below this is a menu with four items: 'LES MENACES ET BONNES PRATIQUES', 'L'ACTUALITÉ DE LA CYBERMALVEILLANCE', 'NOUS DÉCOUVRIR', and 'VICTIME D'UN ACTE DE CYBERMALVEILLANCE ?'. The main content area features a large image of a man and a woman in an office setting. Below the image, the article title 'Piratage d'un système informatique, que faire ?' is displayed in a large, bold font. The publication date 'Publié le 27 mai 2021' is shown below the title. There are three blue buttons: 'piratage informatique', 'Que faire en cas de piratage', and 'Qui contacter en cas de piratage informatique'. A small icon indicates 7724 views and a reading time of 15 minutes. On the right side, there are social media sharing icons for Twitter, LinkedIn, Facebook, and Print. At the bottom, a table of contents is visible with two items: '1. DE QUOI S'AGIT-IL ?' and '2. COMMENT S'EN PROTÉGER ?'.

ALERTES ET GUIDES PRATIQUES

- Alertes régulières sur les réseaux sociaux pour nos publics

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



- Publication d'articles et guides pratiques adaptés aux menaces et publics.

**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/HT204541>
- 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.

Références(s)
• ANSSI / CERT-FR : <https://www.cert.ssi.fr/actualites/CERT-FR-2021-02-016>
• CVE-2021-30961 - CVE-2021-30963 - CVE-2021-30965 - CVE-2021-30966

Alter plus tôt avec Cybermalveillance.gouv.fr :
#certsec et comment bien gérer ses mises à jour ?


**RÉPUBLIQUE
FRANÇAISE**
*Liberté
Égalité
Fraternité*


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



ACTIONS ET OUTILS DE SENSIBILISATION RÉALISÉES EN 2021

Pour le grand public

Campagne TV
sur les réflexes essentiels
en sécurité numérique



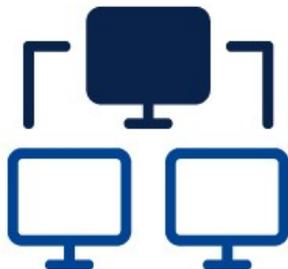
Campagne d'émissions
Consomags diffusées
sur les chaînes du groupe
France Télévisions



Les Incollables
sur les usages numériques,
lancés début septembre pour
un public entre 8 et 12 ans
et leur famille



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 des clients aux **besoins spécifiques** (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 : 

162 labellisés ExpertCyber sur l'ensemble du territoire en décembre 2021.

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 →

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)

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.

GESTES ESSENTIELS DE SÉCURITÉ NUMÉRIQUE

Utilisez des **mots de passe uniques et solides** et activez la **double authentification** chaque fois que c'est possible

Appliquez les **mise à jour de sécurité** sur vos équipements connectés (serveurs, ordinateurs, téléphones...) dès qu'elles sont disponibles



Utilisez un **antivirus** et vérifiez son bon fonctionnement

Faites régulièrement des **sauvegardes de vos données** et gardez en une copie déconnectée et **testez-les** !

SENSIBILISATION ET PRÉVENTION

Objectifs :

- Sensibiliser aux risques
- Partager les bonnes pratiques
- Alerter

Publics :

- Particuliers
- Entreprises
- Collectivités

17 thématiques

6 types de contenus :

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





RÉPUBLIQUE
FRANÇAISE

*Liberté
Égalité
Fraternité*



Assistance et prévention
en sécurité numérique



www.cybermalveillance.gouv.fr



@cybervictimes



@cybervictimes



@cybermalveillancegouvfr