Cybersécurité : mieux connaître les menaces visant les utilisateurs finaux pour adopter les cyber réflexes

Webin-aire

Nos webinaires pour construire la e-santé de demain !

Denis BOYER
Cybermalveillance.gouv.fr

Emmanuel SOHIER
CERT Santé

Thomas DAMONNEVILLE
CERT Santé

Zoom sur les menaces d'ingénierie sociale :

- Sur les 536 incidents déclarés sur les trois premiers trimestres de 2025 (576 en 2024), **307** sont d'origine malveillante (297 en 2024) soit 57% (52% en 2024).

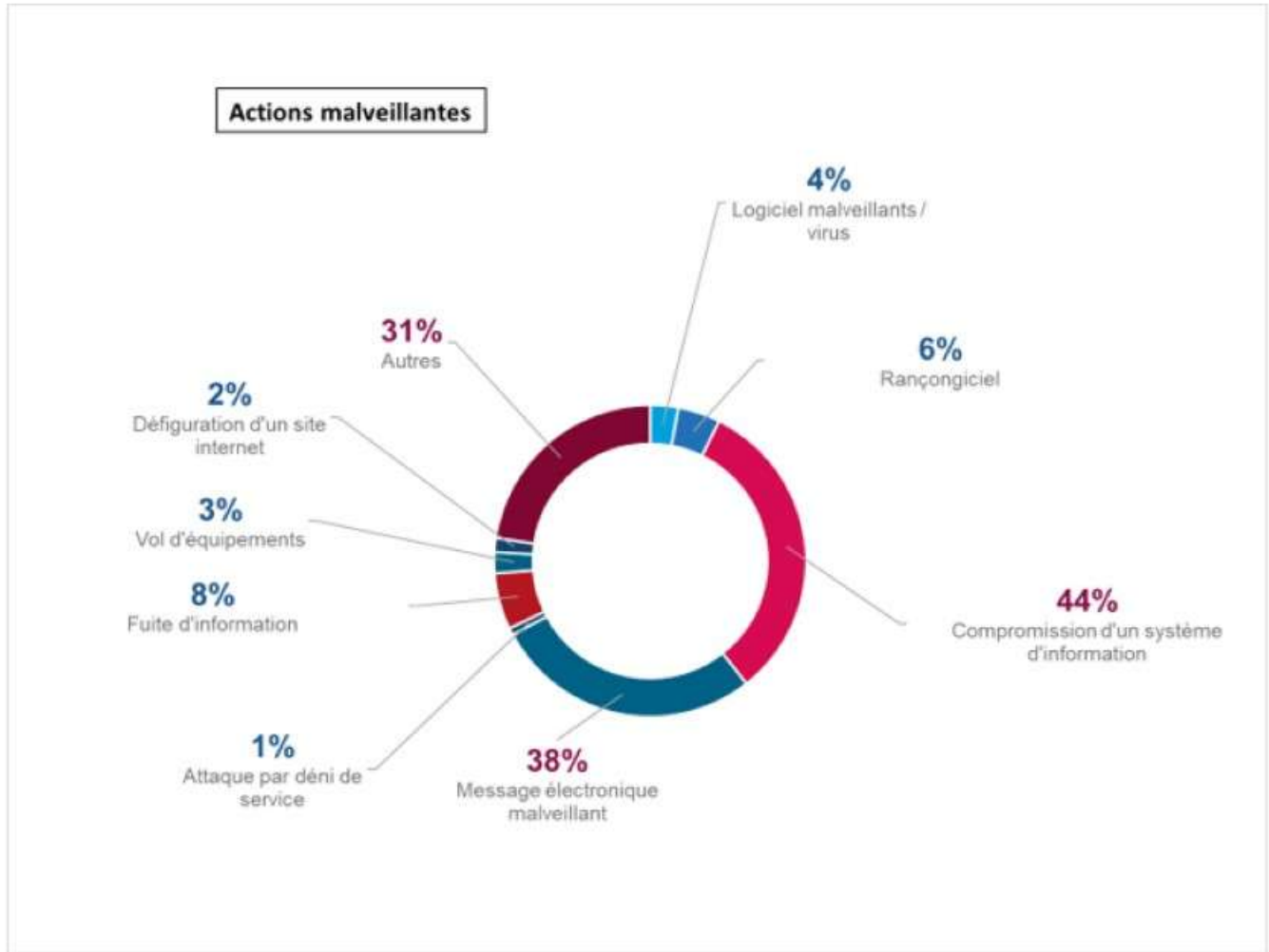
- **118** incidents sont liés à l'envoi d'un message malveillant (+39% par rapport à 2024)

  Parmi eux, on compte :

  - ❑ **56** incidents ayant entraîné la compromission d'un compte de messagerie (+75%)
  - ❑ **40** cas de phishing (x2)
  - ❑ **40** spams (x5)

- Dans la catégorie "Autres" on compte :

  - ❑ FOVI (x3)
  - ❑ Arnaques au président/usurpation d'identité (+40%)
  - ❑ Fuites/exfiltration d'informations personnelles

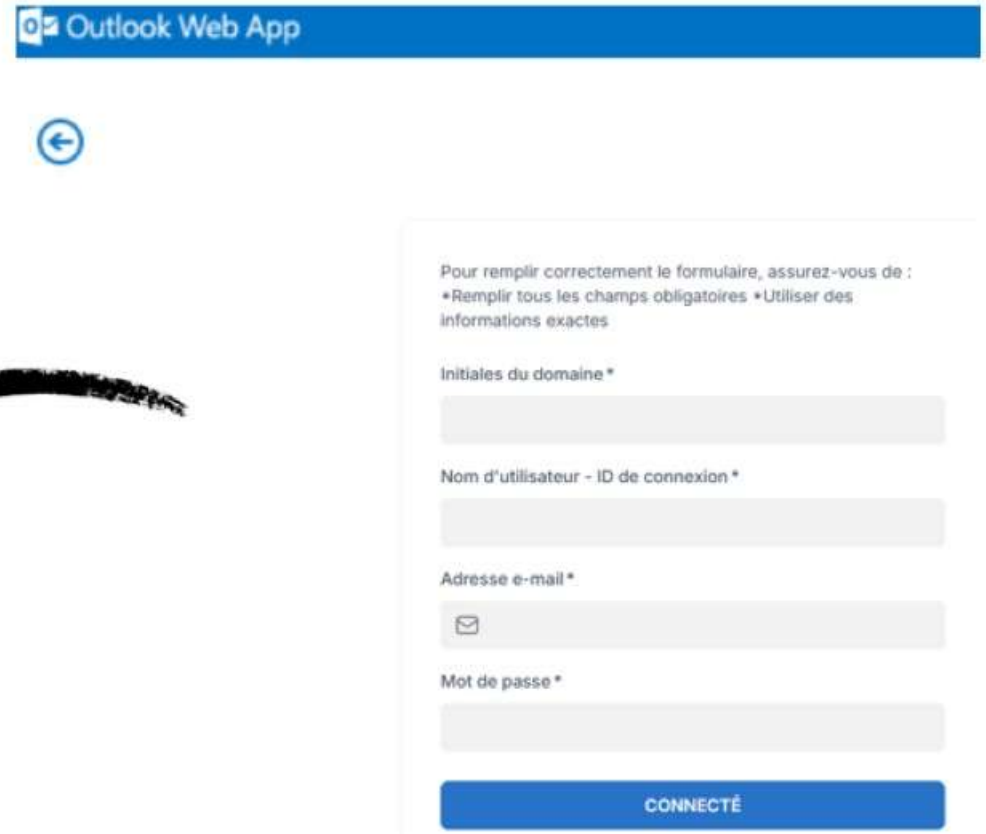


Menaces observées sur les bénéficiaires du CERT Santé

- Phishing, vol de mot de passe (messagerie, …)
- Demande de changement de RIB d'employés, virement
- Récupération d'informations personnelles de patients/individus

→ Menaces d'ingénierie sociale

Phishing, vol de mots de passe



Description

Compromission de boîte mail d'un agent hospitalier, vraisemblablement à la suite d'un phishing.Mesures prises : désactivation du compte puis changement du mot de passe. Analyse forensique sur la boîte mail.Analyse des logs d'accès Webmail.Adressage de dizaines de milliers mails à l'extérieur qui a résulté en un blocage de l'adresse IP émettrice sur plusieurs RBL.

Changement de RIB

Description

Mail reçu le 20/01/2025 pour nous communiquer le nouveau Relevé d'Identité Bancaire où les futurs virements des salaires vont être effectués; la signature du mail et le RIB sont bien au nom d'une salariée.Le 10/02/2025, appel de la salariée pour nous informer qu'elle n'a pas encore reçu son salaire de janvier 2025. En lui communiquant le contenu du mail, elle nous a confirmé que ce n'est pas son adresse mail et qu'elle n'a jamais changé de compte, or le virement de son salaire a été fait sur le nouveau RIB le 31/01/2025.

Demande de virement

Description

Tentative d'arnaque au président.Tentative de virement bancaire de 600.000€ vers notre DAF sur demande du Directeur général.Utilisation de la messagerie Whatsapp 06. [redacted] avec la voix du directeur général pour faire valider l'ordre de virement.

Récupération d'informations personnelles

Description

Une correspondante téléphonique disant s'appeler « Vanessa » a appelé à 9h29 (numéro masqué) le bureau des entrées du Centre en demandant à parler à un des salariés travaillant aux admissions en l'appelant par son prénom. Cette correspondante précise qu'elle travaille dans une clinique spécialisée en SMR, qu'un autre salarié de notre établissement lui aurait rendu plusieurs services au cours de ces derniers mois.Elle prétend qu'elle n'a pas de connexion depuis son poste de travail au service de la sécurité sociale « consultation des droits en ligne » et qu'elle souhaite être dépannée.La correspondante énonce ainsi des noms, des prénoms et des dates de naissance et demande qu'on lui transmettent oralement : le numéro d'immatriculation à la sécurité sociale, le code de gestion du centre où ces personnes adhèrent ainsi que le nom de leurs médecins traitants.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

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 ?

QUELQUES CHIFFRES CLÉS

64 MEMBRES RÉUNIS AUTOUR D'UN PARTENARIAT PUBLIC- PRIVÉ

PREMIER MINISTRE

MINISTÈRE DE L'ÉDUCATION NATIONALE,
DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

MINISTÈRE DE LA JUSTICE

MINISTÈRE DE L'INTÉRIEUR

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

MINISTÈRE DES ARMÉES

MINISTÈRE DÉLÉGUÉ CHARGÉ DE L'INTELLIGENCE ARTIFICIELLE
ET DU NUMÉRIQUE

RÉPUBLIQUE FRANÇAISE

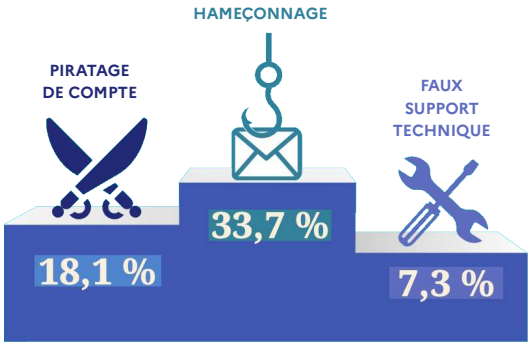
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR

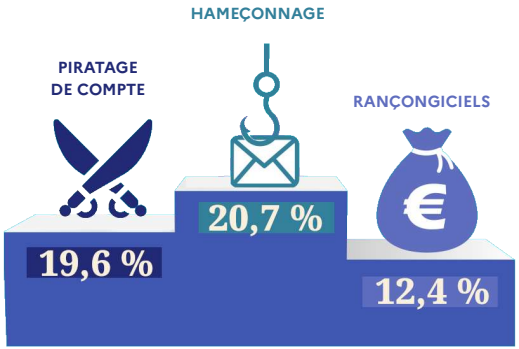
Assistance et prévention en cybersécurité

Menaces cyber : tendances et bonnes pratiques

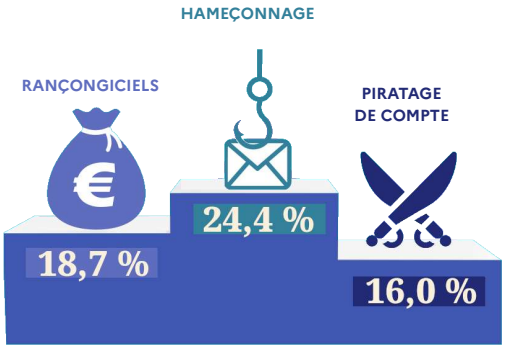
PRINCIPALES CAUSES DE RECHERCHE D'ASSISTANCE EN 2024



Particuliers



Entreprises / associations

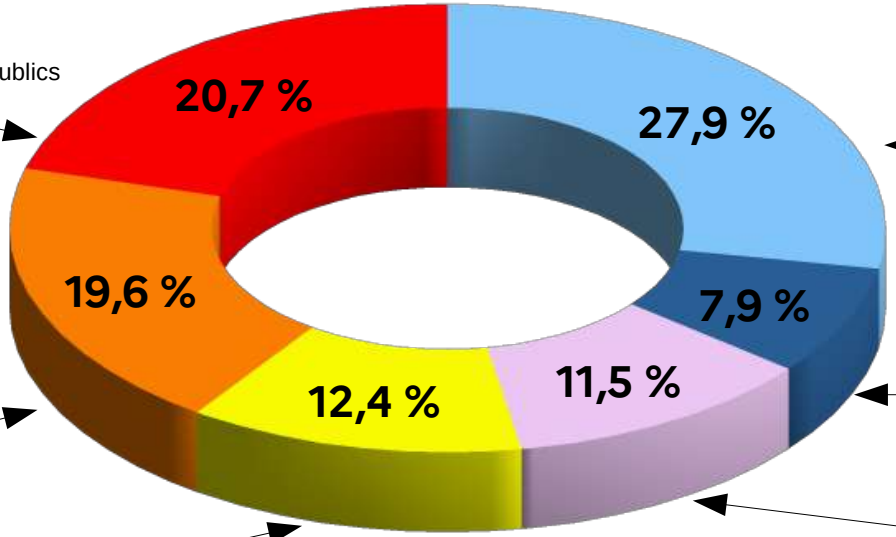


Collectivités / administrations

PRINCIPALES RECHERCHES D'ASSISTANCE EN 2024

Pour les entreprises et associations :

15 655 demandes d'assitance d'entreprises et associations



L'hameçonnage
La principale menace pour tous les publics

Autres cybermalveillances
46 catégories sur 51 recensées

Le piratage de compte
Un corollaire de l'hameçonnage

La violation de données
Une manne pour les cybercriminels

Le rançongiciel
Une menace ciblant les professionnels

Le faux ordre de virement
Une escroquerie par ingénierie sociale (+29%)

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

QUE FAIRE FACE À UN MESSAGE OU UN SMS DOUTEUX ?

Se méfier des messages alarmistes / anxiogènes / trop alléchants
- Le comportemental est la première cible des pirates !

Ne pas paniquer et garder la tête froide ! Ne pas rester seul !
- Ne pas répondre, ne pas cliquer
- En parler à un tiers de confiance

Vérifier la cohérence émetteur / message / contexte :
- Par ex. contacter l'émetteur avec ses propres coordonnées,

Si après avoir cliqué sur un lien dans un SMS, une alerte s'affiche et vous invite à mettre à jour / télécharger une application, **fermez la page**

Signaler les message frauduleux
- En interne pour les messages professionnels
- Perso : https://33700.fr ou transférez-le par SMS au 33700 (service gratuit)

1,9 M de consultations d'articles (+13 %)
•
64 000 recherches d'assistance (+22 %)

BNP PARIBAS :

Pour continuer à consulter vos comptes en ligne, merci de réactiver votre Clé Digitale en suivant les étapes ci dessous : https://compte-bnpparibas.com/clients/login.php

PROTÉGER SES « COMPTES SENSIBLES » CONTRE LE PIRATAGE

430 000 consultations d'articles (+55 %)

•

35 000 recherches d'assistance (+42 %)

Des piratages aux origines diverses

- Hameçonnage, fuite ou réutilisation de mots de passe, virus voleurs de mots de passe …

Des conséquences importantes pour les victimes

- Préjudices financiers, usurpation d'identité, fraude au virement/RIB, chantage…


ouest france Le Courrier de l'ouest

Une horticultrice du Maine-et-Loire a été victime d'une escroquerie au faux ordre de virement. Les malfaiteurs ont piraté la boîte mail de son entreprise et ont obtenu la copie d'une facture d'un vrai artisan. Ils ont réussi à lui soutirer 26 000 €.

Sécuriser les comptes « sensibles »

- Messageries, comptes bancaires, opérateurs téléphoniques, comptes administratifs, comptes à « privilèges » …

Des réflexes indispensables

- Mots de passe uniques, complexes et personnels → utiliser un gestionnaire de mots de passe
- Utiliser la double authentification dès que possible

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

RANÇONGICIELS : LES BONS RÉFLEXES À ADOPTER

2 408 recherches d'assistance (-13 %)

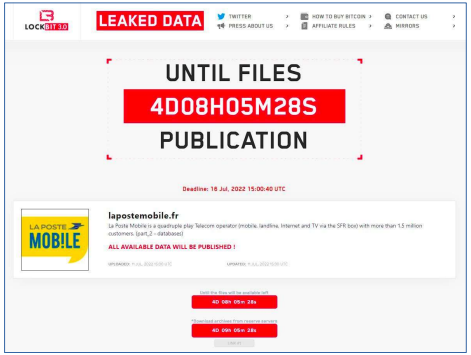
Maintenez <u>tous</u> vos systèmes et applications à jour (dont mobiles ...)

Évaluez votre niveau de protection

- Séparation pro/perso, antivirus, gestionnaire de mots de passe, double authentification, filtrage des accès externes...

Effectuez des sauvegardes fréquentes

- Règle du 3-2-1
- Restauration des données possible en cas de chiffrement



Sensibilisez vos collaborateurs

- Bonnes pratiques de cybersécurité
- Détection/réaction à une tentative de cyberattaque

Préparez-vous au pire

- Préparer des plans de secours pour affronter une crise (annuaire de crise, fonctionnement dégradé, communication...)

SE PROTÉGER CONTRE LES FAUX ORDRES DE VIREMENT (FOVI)

121 000 consultations de l'article (+33 %)

6 000 recherches d'assistance (+18 %)

Sensibilisez vos collaborateurs aux risques

- Hameçonnage, piratage de compte

Diffusez des procédures claires aux collaborateurs mandatés

- Authentification des émetteurs
  - Contre-appel avec numéro référencé (même si le mail est légitime)
- Validation hiérarchique interne non dérogeable
  - Demandes de virement imprévues
  - Changements de RIB

Limiter la publication d'informations sur internet

- Contact des collaborateurs habilités

Mots de passe solides pour les comptes de messagerie et double authentification

ouest france

L'artisan victime d'une arnaque au Rib : « 21 000 €, c'est un an de salaire »

Publié le 25/11/2024 à 06h53

Il y a quelques semaines, un carreleur de Saint-Père-en-Retz n'a jamais reçu le paiement de 21 000 € de son client, intercepté par un cybercriminel. Une attaque au Rib connue, qui peut laisser les artisans du bâtiment et leurs clients en grande difficulté.

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR

Assistance et prévention en cybersécurité

Au cœur des cybermalveillances : Le facteur humain

LES RESSORTS PSYCHOLOGIQUES DES ESCROCS …

Méconnaissance

Stress

Peur

Culpabilité

Curiosité

Envie

Profit

Passion

… POUR COMMETTRE LEURS CYBERMALVEILLANCES

Vignette Crit'air
Carte vitale
Livraison de colis
QR code frauduleux

Méconnaissance

Curiosité

Concours, loterie
Visibilité R.S.

Faux conseiller bancaire
Échéance abonnement
Avis de contravention

Stress

Envie

C.P.F.
Location immobilière

Proche en détresse
Faux support technique

Peur

Profit

Smartphone à 1€
Arnaque « Nigériane »
Placement financier

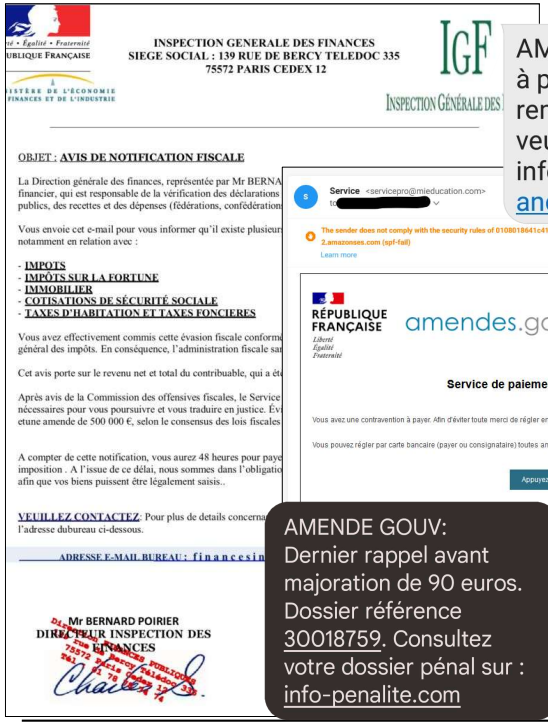
Infraction
Pédopornographique
Chantage webcam

Culpabilité

Passion

Escroquerie sentimentale

DES EXEMPLES (TROP) BIEN CONNUS



INSPECTION GENERALE DES FINANCES
SIEGE SOCIAL : 139 RUE DE BERCY TELEDOC 335
75572 PARIS CEDEX 12

IGF
INSPECTION GÉNÉRALE DES

OBJET : **AVIS DE NOTIFICATION FISCALE**

La Direction générale des finances, représentée par Mr BERNA
financier, qui est responsable de la vérification des déclarations
publics, des recettes et des dépenses (fédérations, confédération

Vous envoie cet e-mail pour vous informer qu'il existe plusieur
notamment en relation avec :

- IMPOTS
- IMPÔTS SUR LA FORTUNE
- IMMOBILIER
- COTISATIONS DE SÉCURITÉ SOCIALE
- TAXES D'HABITATION ET TAXES FONCIERES

Vous avez effectivement commis cette évasion fiscale conforme
général des impôts. En conséquence, l'administration fiscale sa

Cet avis porte sur le revenu net et total du contribuable, qui a été

Après avis de la Commission des offensives fiscales, le Service
nécessaires pour vous poursuivre et vous traduire en justice. Évi
etune amende de 500 000 €, selon le consensus des lois fiscales

A compter de cette notification, vous aurez 48 heures pour paye
imposition . A l'issue de ce délai, nous sommes dans l'obligatio
afin que vos biens puissent être légalement saisis..

VEUILLEZ CONTACTEZ: Pour plus de details concerna
l'adresse dubureau ci-dessous.

ADRESSE E-MAIL BUREAU: financesin

Mr BERNARD POIRIER
DIRECTEUR INSPECTION DES FINANCES

Service <servicepro@mieducation.com>
to [redacted]

The sender does not comply with the security rules of 0108018641c41afc-19e7daab-f2dc-4fee-86bc-2bab1b388c3d-000000@ap-southeast-2.amazonses.com (spf-fail)
Learn more

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
amendes.gouv.fr

Service de paiement en ligne des amendes

Vous avez une contravention à payer. Afin d'éviter toute merci de régler en cliquant ci-dessous

Vous pouvez régler par carte bancaire (payer ou consignataire) toutes amendes : Veuillez vous acquitter de votre amende de stationnemen

Appuyez ici pour confirmer

AMELI : Pour continuer à percevoir vos remboursements santé, veuillez actualiser vos informations www.assurancemaladie.org

Bonjour, c'est le livreur votre colis ne rentrait pas dans la boite aux lettres merci de choisir un point relais sur : https://help-mondialrelay.com

AMENDE GOUV: Dernier rappel avant majoration de 90 euros. Dossier référence 30018759. Consultez votre dossier pénal sur : info-penalite.com

CPAM: Votre carte vitale arrive à expiration, veuillez réactualiser vos informations sur le lien ci-joint: https://espace-cpam.help/
03:44

Info SFR: Merci de vous rendre sur https://compensation-sfr.info pour obtenir un remboursement de notre part de 52,63€ en raison d'une erreur de prélèvement.

Les messages et les appels sont chiffrés de bout en bout. Aucun tiers, pas même WhatsApp, ne peut les lire ou les écouter. Appuyez pour en savoir plus.

Concours Airfrance Black Friday 2022
5 000 billets aller-retour gratuits pour ...
airfrance.com

https://shortlinks.su/l015540514/ 10:05

BNP PARIBAS :

Pour continuer à consulter vos comptes en ligne, merci de réactiver votre Clé Digitale en suivant les étapes ci dessous : https://compte-bnpparibas.com/clients/login.php

A votre attention ceci est un message très urgent auquel vous devez nous répondre dans l'immédiat .

MINISTÈRE de la JUSTICE
RÉPUBLIQUE FRANÇAISE

DIRECTION GÉNÉRALE DE LA GENDARMERIE NATIONALE

Plateforme de Lutte Contre les Pédophiles sur internet (PLPN)
Brigade de protection des mineurs

MANDAT DE POURSUITE JUDICIAIRE

Pour les nécessités d'une enquête judiciaire
(Article 390-1 du Code de procédure pénale)

COPIE ORIGINALE

OBJET: POURSUITE JUDICIAIRE
Natif 7875 : PÉDOPORNOGRAPHIE
[Cyber- Espace] INTERNET
Références de la procédure 09656101560-2022

À votre attention.

Je soussigné, M. Christian RODRIGUEZ Directeur général de LA GENDARMERIE NATIONALE, en collaboration avec la Direction central de l'Office Européen de Police (EUROPOL) Vu les articles 20, 21-1, 21 1° bis, 21-1 et 75 a 78 du Code de Procédure pénal.

Nous vous adressons ce mail par voie électronique peu après une saisie informatique de la cyber-infiltration pour vous informer que vous faites l'objet de plusieurs poursuites judiciaires en vigueur.

NOUS ENGAGEONS À VOTRE ENCONTRE DES POURSUITES POUR

1)° **ATTEINTE À LA PUDEUR**
2)° **PÉDOPORNOGRAPHIQUE**
3)° **EXHIBITIONNISME**
4)° **CYBER-PORNOGRAPHIE, SITE PORNOGRAPHIE**

Pour votre information, la loi 390-1 du Code de procédure pénale de mars 2007 aggrave les peines lorsque les propositions et les agressions sexuelles ou les viols ont pu être commises.
Vous avez commis l'infraction après avoir été ciblé sur Internet (site d'annonce), visualisation de site à caractère pédopornographique, des photos/vidéos dénudée

Concours de la fête des pères Leroy Merlin
5 000 barbecue au gaz gra...
leroymerlin.fr

https://wp20.ru/t751554897/
13:01

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR

Assistance et prévention en cybersécurité

17 CYBER

Le guichet unique pour les victimes de cybermalveillances

POUR TOUTES LES VICTIMES

UN GUICHET UNIQUE

AVEC TOUS LES ACTEURS

17 CYBER

https://17cyber.gouv.fr

POLICE NATIONALE

Gendarmerie nationale

Services qualifiés / adaptés

PHAROS

PERCEV@L
FRAUDE À LA CARTE BANCAIRE SUR INTERNET

THESEE

e-Enfance 3018

France Victimes

signal spam

Et de nombreux autres...

Prestataires de confiance

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

RÉFÉRENCÉ SUR LA PLATEFORME CYBERMALVEILLANCE.GOUV.FR
RÉPUBLIQUE FRANÇAISE
CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

COMMENT ÇA MARCHE ?

VICTIMES

17cyber.gouv.fr

DIAGNOSTIC : De quoi suis-je victime ?

RECOMMANDATIONS d'urgence
ORIENTATION de la victime

Services 17Cyber

Mon assistance en ligne
24h/7j

Assistance technique
Professionnel référencé / ExpertCyber

Accompagnement F.S.I.
Police / Gendarmerie (par tchat)

Services qualifiés / adaptés
PHAROS, THESEE, PERCEVAL
France Victime, e-enfance ...

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR

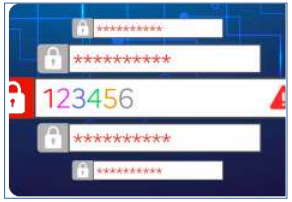
Assistance et prévention en cybersécurité

La sensibilisation : Première arme contre les cybermalveillances

LA E-SENSIBILISATION À LA CYBERSÉCURITÉ ACCESSIBLE À TOUS !

Module 1 : Comprendre *(43mn)*

- Quelles menaces aujourd'hui ?
- Quels risques pour moi et mon organisation ?
- Que faire si je suis victime d'une attaque ?



Module 2 : Agir *(33mn)*

- Quelles bonnes pratiques au quotidien ?
- Quels bons réflexes dans mes usages ?

Module 3 : Transmettre *(41mn)*

- Sensibiliser, pourquoi et comment ?
- Pour aller plus loin : Acteurs nationaux et textes de référence

SENS CYBER
E-sensibilisation à la cybersécurité pour tous

Disponible ici : **https://www.cybermalveillance.gouv.fr**/sens-cyber/apprendre

CYBER MOIS

DES ACTIONS POUR TOUS LES PUBLICS

A partir du 1er octobre :

- **Participer à une action citoyenne collective** sur les réseaux sociaux
  - En postant un conseil cyber avec le hashtag « ***#CyberEngagés*** »
  - Visuels disponibles sur le site du cybermois à partir du 1er octobre
- Participer à la **Chasse du Cybermois** (jeu-concours en ligne du 1er au 31 octobre 2025)
- Obtenir le **livret de sensibilisation destiné aux 9-12 ans** diffusé avec le numéro de septembre d'Astrapi - Bayard Éditions (12 pages de conseils et de jeux)
- **Interagir avec les publications ludiques** de Cybermalveillance.gouv.fr tout au long du mois d'octobre.

Site : **https://cybermois.gouv.fr** Adresse contact : **Cybermois@Cybermalveillance.gouv.fr**

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

SENSIBILISATION ET PRÉVENTION

Plus de 700 contenus cyber disponibles
Pour informer et sensibiliser les publics

- Kit de sensibilisation
- MOOC, e-sensibilisation
- Guides et méthodes
- Fiches pratiques / fiches réflexes
- Articles web
- Vidéos…

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

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

Nos ressources de sensibilisation

CYBER MALVEILLANCE .GOUV.FR

Assistance et prévention en cybersécurité

INSCRIVEZ-VOUS À LA NEWSLETTER

Tenez-vous informé(e) de l'actualité de la cybermalveillance et des nouvelles menaces

www.cybermalveillance.gouv.fr

OK

@cybervictimes

@cybervictimes

@cybermalveillancegouvfr

CERT Santé

Tel : 09 72 43 91 25
Mail : cyberveille@esante.gouv.fr
https://cyberveille.esante.gouv.fr/