



**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*



Assistance et prévention
en sécurité numérique

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

SOMMAIRE DU JOUR

1. Les **missions** et **publics** de [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr)
2. Quelles **menaces** ?
3. **Quels risques** ?
4. Quelles **ressources** ?,
5. **La MalletteCyber**,
6. Liens et ressources utiles.

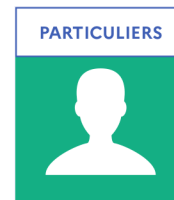
ASSISTANCE ET
PRÉVENTION DU
RISQUE
NUMÉRIQUE AU
SERVICE DES
PUBLICS



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



63

**organisations
membres**

(publiques et privées)
du GIP ACYMA



+ 1200

**prestataires
référéncés**

sur l'ensemble
du territoire



+ 200

**Experts
Cyber**

sur l'ensemble
du territoire



+ 1 000 000

**victimes
assistées**

depuis 2017



3 700 000

**visiteurs
uniques**

en 2023

63 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 ET DES OUTRE-MER

MINISTÈRE DE L'ÉDUCATION NATIONALE, DE LA JEUNESSE,
 DES SPORTS ET DES JEUX OLYMPIQUES ET PARALYMPIQUES

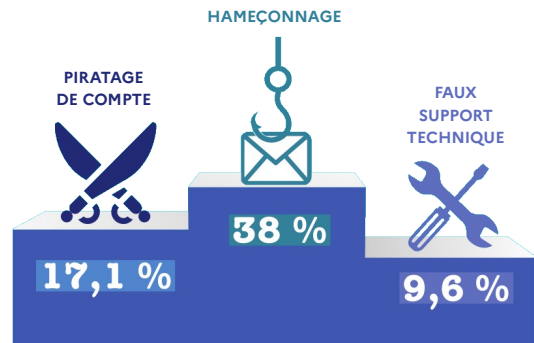
MINISTÈRE DES ARMÉES

MINISTÈRE DE LA JUSTICE

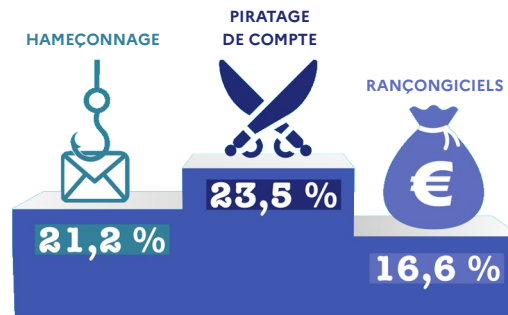
MINISTRE DÉLÉGUÉ CHARGÉ DU NUMÉRIQUE



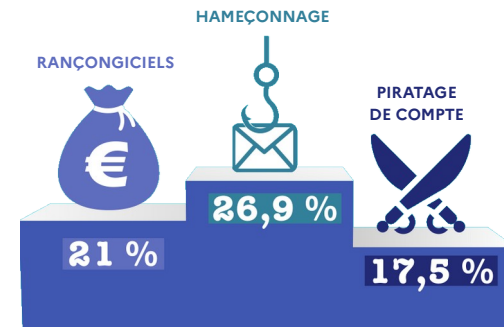
PRINCIPALES CAUSES DE RECHERCHE D'ASSISTANCE EN 2023



Particuliers



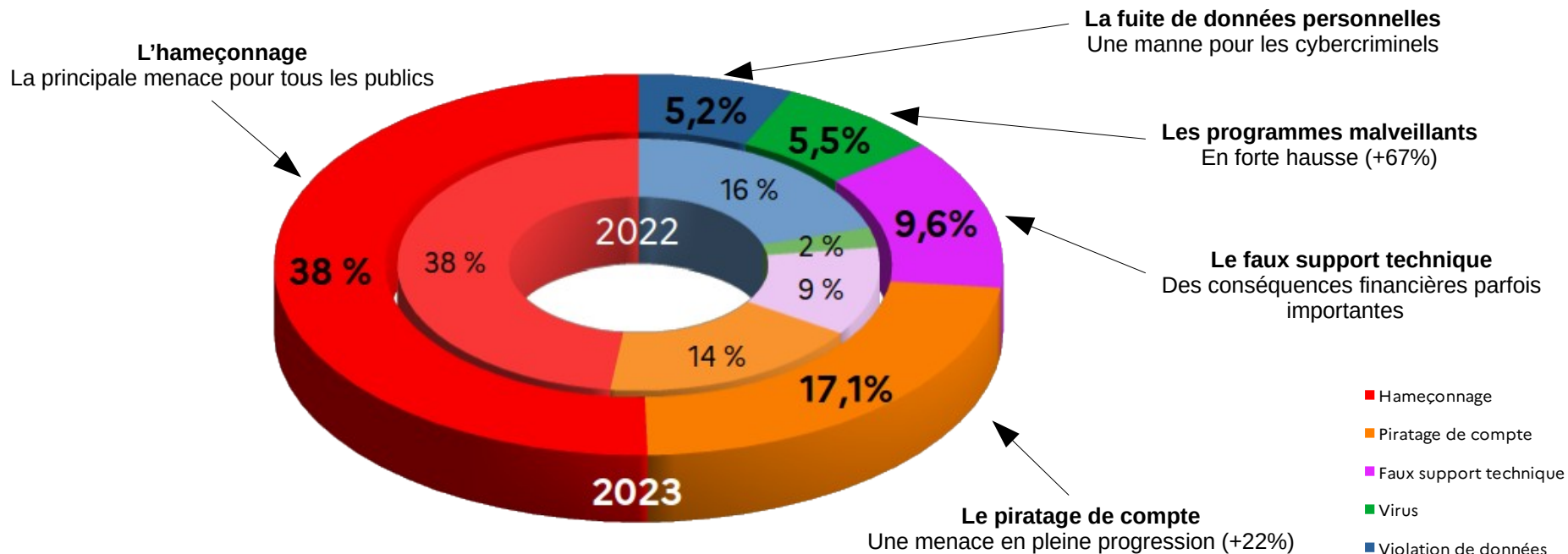
Entreprises / associations



Collectivités / administrations

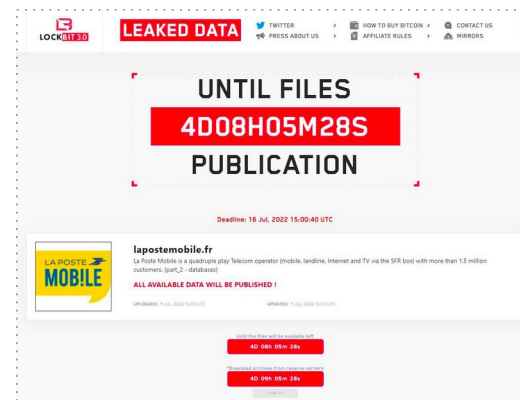
PRINCIPALES RECHERCHES D'ASSISTANCE EN 2023

Pour les particuliers :



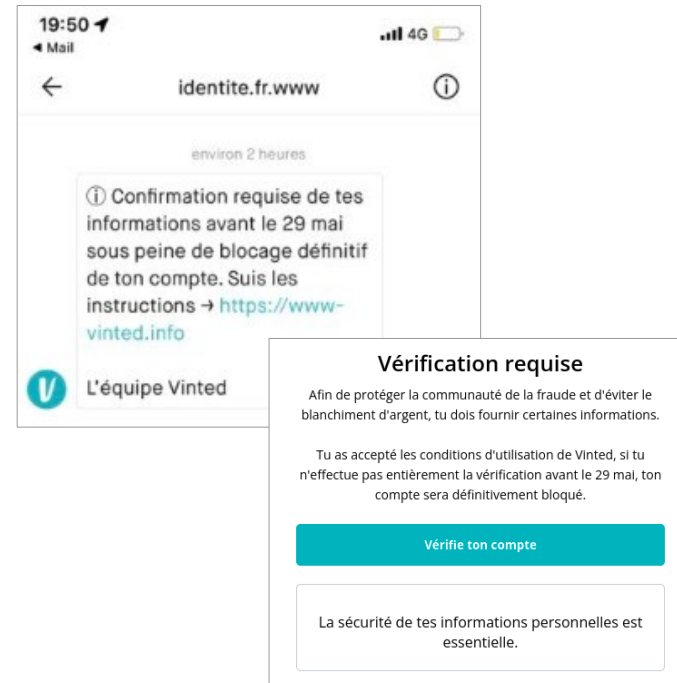
LES PRINCIPAUX RISQUES :

- **Le risque financier :**
utilisation frauduleuse des moyens de paiement,
virement frauduleux / achats non honorés...
- **La violation de données personnelles :**
identité, adresse postale, adresse mail, photo de profil,
identifiants de connexion, informations bancaires...
- **Les risques pour mon entreprise / organisation :**
compromission du système d'information,
les rançongiciels / ransomware,
l'atteinte aux données clients, partenaires, administrés...
les virements frauduleux (FOVI, RIB falsifiés...),
l'atteinte à l'image ou aux outils de production.



L'USURPATION D'IDENTITÉ

- **Corollaire d'une autre cybermalveillance**
Hameçonnage, piratage de compte/site internet...
ou récupérées physiquement : poubelles, perte/vol...
- **Utilisation d'informations personnelles à votre insu**
identité, adresse postale, adresse email, photo de profil,
identifiants de connexion, informations bancaires...
- **Conséquences importantes pour les victimes**
ouverture ligne téléphonique/compte bancaire
souscription de crédits, locations
escroquerie des proches
diffamation, chantage, cyberharcèlement ...



QUE FAIRE FACE À UN MESSAGE OU UN SMS DOUTEUX ?

Le kit d'urgence !

- **Ne pas paniquer et garder la tête froide ! Ne pas rester seul !**
 - ne pas répondre – ni cliquer / en parler à un tiers de confiance,
- **Vérifier la cohérence émetteur / message / contexte :**
 - par ex. contacter l'émetteur avec ses propres coordonnées,
- **Se méfier des messages alarmistes / anxiogènes / trop alléchants**
 - le comportemental est la première cible des pirates !
- **S'informer...ou trouver de l'assistance !**
 - sur [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr)
- **Signaler le mail ou SMS frauduleux :**
 - sur <https://33700.fr> ou transférez-le par SMS au 33700 (service gratuit) – signal-spam.fr



COMMENT PROTÉGER SES DONNÉES ?

L'importance de connaître et de protéger ses données aujourd'hui !

- **Quelles sont mes données et où sont elles situées ?**
 - quelles données ? Quelle utilisation ? Sur quels terminaux ?
- **Protéger mes données et les accès qui y mènent :**
 - adopter une gestion adaptée de ses mots de passe,
- **Sauvegarder mes données sur des supports adaptés :**
 - nature - fréquence – support ?
- **Transmission : Légitimité et sécurité !**
 - s'assurer du bien-fondé de la demande / interlocuteur,
 - sécuriser ses envois.





**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*



Assistance et prévention
en sécurité numérique

Recommandations et ressources

DES ARTICLES ADAPTÉS À NOS PUBLICS :

- [Définition simple de la menace,](#)
- [S'en prémunir en temps normal,](#)
- [Que faire si je suis victime ?](#)
- [Qu'en dit le Code Pénal ?](#)

- [Liens et ressources utiles...](#)



The screenshot shows the website interface for Cyber Malveillance Gouv.fr. At the top, there is a navigation bar with the French flag and the site logo. Below it, a blue menu bar contains the following 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 background image of hands typing on a keyboard, overlaid with social media icons for Facebook, Instagram, and Twitter. The article title is 'Que faire en cas de piratage de compte sur les réseaux sociaux ?'. Below the title, it indicates the article was published on 2 sept. 2022 and has 3379 views with a 21-minute reading time. A 'SOMMAIRE' (Table of Contents) section is visible on the left, listing: 'EN QUOI CELA CONSISTE ?', 'QUELS SONT LES SIGNAUX D'ALERTE ?', and 'POURQUOI CELA PEUT'. The main text of the article begins with: 'Facebook, Instagram, LinkedIn, Snapchat, TikTok, Twitter, WhatsApp... Vous avez remarqué une activité suspecte ou vous n'arrivez plus à vous connecter à votre compte ? Il s'agit peut-être de l'œuvre d'un pirate informatique (hacker en anglais) qui y accède à votre insu. Que faire en cas de piratage ou de suspicion de piratage de l'un de vos comptes sur les réseaux sociaux ? Réinitialiser votre mot de passe, vérifier l'historique des connexions récentes, supprimer les appareils non reconnus de votre'.

LE CYBER GUIDE FAMILLE

- **Un support pédagogique dédié aux familles**
 - 10 recommandations
- **Des contenus adaptés aux parents et enfants**
- **Des thèmes variés**
 - Mots de passe, sauvegardes, hameçonnage, réseaux sociaux, cyberharcèlement...
- **Les sensibiliser**
 - Aux risques numériques
 - Aux bonnes pratiques



10 CYBERHARCÈLEMENT, PARLEZ-EN!

Le harcèlement peut revêtir différentes formes et se reconnaître par son caractère répétitif et sa durée. Il peut être le fait d'une ou plusieurs personnes et toucher aussi bien les adultes que les plus jeunes. Avec l'avènement des nouvelles technologies et des réseaux sociaux, le harcèlement s'est également développé en ligne : intimidations, insultes, rumeurs, publication de photos ou vidéos compromettantes...

SI CERTAINS HARCELEURS L'ASSIMilent À UN JEU, LES VICTIMES QUANT À ELLES, EN SOUFFRANT ET SENSANT MOUSTRÉ PAR EN PARLANT SE RETRAIENT...

7 APPRENEZ À MAÎTRISER VOS RÉSEAUX SOCIAUX

Facebook, Instagram, LinkedIn, Snapchat, TikTok, Twitter, WhatsApp... Les réseaux sociaux sont omniprésents dans notre quotidien et celui de nos adolescents. Il ne se passe rarement un jour sans consulter ou publier des photos, vidéos, messages...

CES RÉSEAUX CONTIENNENT DE NOMBREUSES INFORMATIONS PERSONNELLES ET FAMILIALES SENSIBLES, QUI NE DOIVENT PAS TOMBER DANS DE MAUVAISES MAINS (identité, adresse postale ou de messagerie, numéro de téléphone, date de naissance, etc.).

HELP

Victime ou témoin, PARLEZ-EN!

BONNES PRATIQUES

MAUVAISES PRATIQUES!

POUR ALLER PLUS

Que faire en cas de cyberharcèlement?
www.cybermalveillance.gouv.fr/infos/les-mots-clés/les-risques-numériques/cyberharcèlement

Pour être conseillé et accompagné:
 - 116 006 : France Victimes
 - 3020 : Non au harcèlement

LES RISQUES

Les réseaux sociaux n'échappent pas aux activités malveillantes : escroqueries, usurpation d'identité, chantage, vol d'informations, cyberharcèlement, désinformation, diffamation... Les techniques frauduleuses ne manquent pas. **Certains malveillances ciblent expressément les enfants et les adolescents sur les réseaux sociaux** : les jeux morbides et dangereux déguisés en challenges, jeu-concours frauduleux, messages privés à caractère pornographique ou incitant à la prostitution...

LES CONSEILS

Pour utiliser les réseaux sociaux en toute sécurité et protéger l'accès à vos comptes, nous vous recommandons d'utiliser à la fois **des mots de passe robustes et systématiquement différents pour chaque service** mais aussi d'**activer la double authentification** lorsque cela est possible. Par ailleurs, nous vous recommandons de **vérifier régulièrement les paramètres de confidentialité de vos comptes** pour définir les options de visibilité de vos publications. Enfin, ne diffusez pas d'informations personnelles ou sensibles qui pourraient être utilisées pour vous nuire et bien sûr, **faites attention à qui vous parlez sur les réseaux**.

POUR ALLER PLUS LOIN

La sécurité sur les réseaux sociaux :
www.cybermalveillance.gouv.fr/infos/contenus/bonnes-pratiques/reseaux-sociaux

14/03/2024

14

LE KIT DE SENSIBILISATION : 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.



FICHES & MÉMOS :



10 CONSEILS POUR SÉCURISER VOS APPAREILS MOBILES

mémo

- 1 Mettez en place les codes d'accès 
- 2 Chiffrez les données de l'appareil 
- 3 Appliquez les mises à jour de sécurité 
- 4 Faites des sauvegardes 
- 5 Utilisez une solution de sécurité contre les virus et autres attaques 
- 6 N'installez des applications que depuis les sites ou magasins officiels 
- 7 Contrôlez les autorisations de vos applications 
- 8 Ne laissez pas votre appareil sans surveillance 
- 9 Évitez les réseaux Wi-Fi publics ou inconnus 
- 10 Ne stockez pas d'informations confidentielles sans protection 

ADOPTER LES BONNES PRATIQUES

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/appareils-mobiles>

CONTRE LES ARNAQUES D'ACHATS EN LIGNE

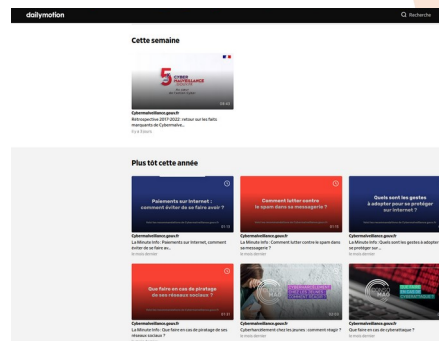
- **Les objectifs** : obtenir les coordonnées d'une carte bancaire afin de réaliser des achats frauduleux ou initier un paiement pour un produit inexistant ou non conforme
- Se méfier des offres trop alléchantes en termes de prix,
- Vérifier le sérieux et la légalité du site (FR-UE, mentions légales...),
- Mener quelques vérifications lors du paiement (https, 2 clicks...),
- Privilégier des moyens de paiement sécurisés (e-carte bleue...)

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-securiser-ses-achats-sur-internet>



JEUNES : DIVERSIFIER LES OUTILS PÉDAGOGIQUES

- S'adresser à tous les âges
- Sous toutes les formes :
 - Jeux
 - Activités
 - Vidéos
 - Livrets pratiques
 - ...
- Donner les clefs de compréhension
 - Menaces majeures
 - Exemples issus de l'actualité





**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*



Assistance et prévention
en sécurité numérique

La MalletteCyber : Du projet à la réalisation !

LA SENSIBILISATION A PORTÉE DE MAIN !

Collaboration avec l'A.N.C.T., membre du GIP,

Un outil prioritairement destiné aux professionnel.le.s de la médiation et de l'inclusion numérique

- Sensibiliser à la cybersécurité
- Fournir une ressource pédagogique et polyvalente

Au service des populations les plus éloignées du numérique

- Développé avec des acteur.rice.s de la médiation
- Permettre de mieux protéger près de **16 millions*** de nos concitoyens « éloignés du numérique » plus vulnérables aux cyberattaques...

**La société numérique française : définir et mesurer l'éloignement numérique - ANCT 2023*



La Mallette Cyber

*La sensibilisation à portée de main
pour les professionnel.le.s de la médiation*



RECUEILLIR LES BESOINS « TERRAIN » :

Objectif : recueillir les besoins opérationnels des acteurs « terrain » afin de concevoir des livrables / supports adaptés.

- Statut / degré de sensibilisation au risque cyber / gestion préalable d'une situation de cybermalveillance et rétex,
- Souhais concernant la forme et le fond en matière de contenus de sensibilisation,
- Connaissance éventuelle de nos supports et zone d'expression libre.

[Modifier](#) | [Formulaire](#) | [Résultats](#) | [Partager](#)

Quels sont les besoins en matière de sensibilisation aux menaces cyber pour les acteurs de la médiation numérique ?

 RÉPUBLIQUE
FRANÇAISE
*Liberté
Égalité
Fraternité*

 Assistance et prévention
en sécurité numérique

En 2022, l'ANCT a rejoint le dispositif national « Cybermalveillance.gouv.fr » chargé notamment de la sensibilisation des publics aux risques numériques ainsi qu'à leur assistance lors d'une cyberattaque (hameçonnage, piratage de boîte mail etc...). Dans le cadre du Plan France Relance et de son volet « sécurisation numérique des collectivités locales », nous travaillons au lancement d'une campagne nationale de sensibilisation et d'outillage des acteurs de l'inclusion / médiation numérique.

Cette enquête vous est ainsi proposée afin de recueillir vos besoins issus du terrain dans l'optique de vous fournir des supports adaptés. Elle ne prendra que quelques minutes à remplir mais nous sera d'une très grande utilité pour vous aider dans vos missions quotidiennes.



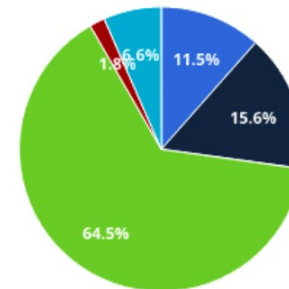
PARTICIPATIONS ET PROFILS :

Mise en ligne du **27/09** au **30/11/2022**,

684 questionnaires remplis et exploitables,

- L'ensemble des acteurs de la médiation représentés avec une nette prédominance des CNFS/CoNum (64,5%),
- Des acteurs de la médiation / inclusion pas toujours sensibilisés aux risques numériques / bonnes pratiques (52,5%),

1. Votre statut :



acteur associatif	79
agent d'une collectivité / d'un établissement public (hors Conseiller Numérique France Services)	107
conseiller Numérique France Services	441
aidant Connect	12
autre	45

AVANT-PROJET DE CAHIER DES CHARGES – AXES FORTS :

Une mallette au **format hybride**,

Des outils / ressources **pour les acteurs de la médiation**.

Une proposition **d'activité interactive / ludique / pédagogique**.

Des supports **pour les aidés**.



LA MALLETTE CYBER : UNE DÉMARCHE PÉDAGOGIQUE VERS L'AUTONOMIE

S'APPROPRIER

APPRENDRE

TRANSMETTRE

PRATIQUER

PÉRENNISER

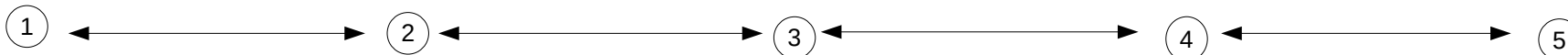
Comprendre la démarche
pédagogique

S'acculturer / actualiser
ses connaissances

Illustrer avec des
infographies adaptées

Ancrer les connaissances
en jouant

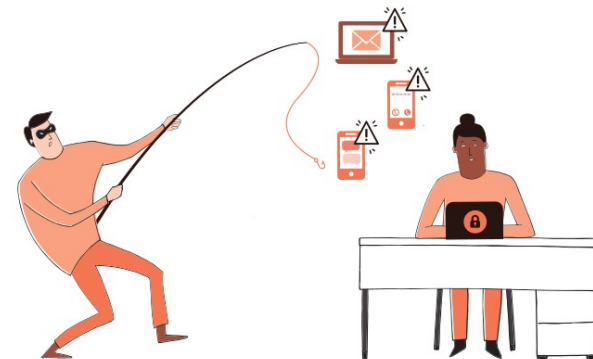
Un support laissé à
l'utilisateur – les bases



DES CONTENUS ADAPTÉS :

Pour mieux comprendre les cybermenaces les plus courantes

- L'hameçonnage (phishing)
- Le piratage de compte
- L'arnaque au faux support technique
- La fuite ou violation de données personnelles



Pour acquérir les bonnes pratiques

- Permettre aux usagers de se protéger
- Et les inciter à devenir autonomes

Pour transmettre ces connaissances aux usagers

- Et diminuer le caractère anxiogène du numérique
- Avec des illustrations simples et la ludification des apprentissages



LE LANCEMENT AU NEC 2023 à BORDEAUX

L'évènement annuel de l'écosystème de la médiation,

Un corner avec zone de présentation / démonstration

Un premier contact positif avec les acteurs du numérique inclusif !



Boîte à outils

Une Mallette Cyber pour favoriser l'inclusion numérique



À l'occasion de NEC, l'ANCT et Cybermalveillance.gouv.fr annoncent la mise à disposition de la Mallette Cyber, un ensemble de ressources dédiées au monde de la médiation numérique afin de protéger les publics les plus éloignés. Alors que 16 millions de Français restent encore « éloignés du numérique » d'après notre récente étude, les deux instances ont souhaité mettre à la disposition de tous les acteurs de la médiation numérique des contenus de sensibilisation prêts à l'emploi. Ce dispositif a ainsi vocation à familiariser les publics aux enjeux de cybersécurité et à transmettre des conseils pratiques et accessibles pour appréhender le sujet en toute sérénité. La Mallette Cyber et son contenu sont accessibles gratuitement sur Cybermalveillance.gouv.fr et sur le site de l'ANCT.

En savoir plus

LA MALLETTE CYBER: DES PLANS GRATUITS EN LICENCE OUVERTE

Où télécharger gratuitement les plans ?

- <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/outils-acteurs-mediation>
- <https://lesbases.anct.gouv.fr/ressources/la-mallette-cyber-outiller-les-professionnels-de-la-mediation>

À quel format?

- un format « prêt à l'emploi » facilement imprimable et jouable,
- un format « fabricants » (fablab / makers / imprimeurs locaux)

... en licence ouverte Etalab2.0

- <https://www.etalab.gouv.fr/licence-ouverte-open-licence/>

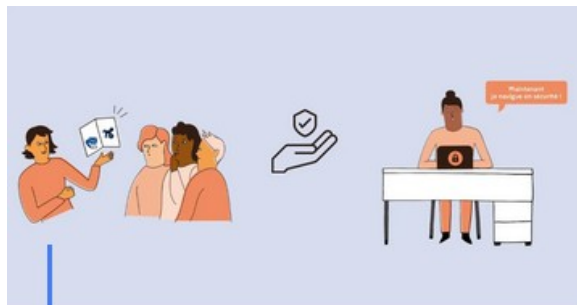


RESSOURCES COMPLÉMENTAIRES

Ce guide et les éléments qui vous ont été remis sont complétés par une page et des ressources **gratuites** dédiées aux acteurs de l'inclusion / médiation numérique en ligne sur [Cybermalveillance.gouv.fr](https://www.cybermalveillance.gouv.fr)... Allez vite les consulter !



+ UNE RUBRIQUE DÉDIÉE À LA MÉDIATION SUR CYBERMALVEILLANCE :



**Médiation et inclusion
numérique**

Nos ressources les plus utilisées par les médiateurs :

- Le kit de sensibilisation, le cyber guide famille...

Nos vidéos de sensibilisation

- Librement diffusables !

Les plans gratuits de la Mallette Cyber:

- version prêt à l'emploi,
- version fabricants,

La simulation du parcours victime :

- pour s'entraîner avec les usagers

Les liens utiles : vers nos partenaires (ANCT, PIX, CNIL...)

À venir : lien direct vers SensCyber !

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/outils-acteurs-mediation>

LA E-SENSIBILISATION « SENSCYBER »

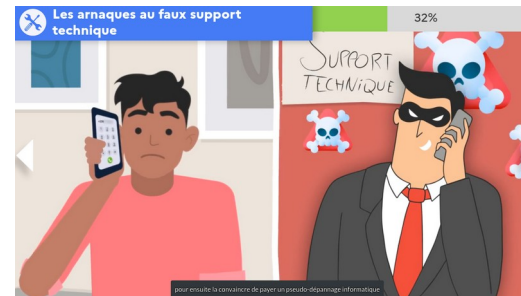
Trois modules mis à disposition gratuitement :

- Comprendre
Les menaces / les risques / Que faire en cas d'attaque
- Agir
Adopter les bonnes pratiques dans mes usages
- Transmettre
Sensibiliser

Déjà disponible sur :

- « mentor.gouv.fr » Ministère du travail et de la fonction publique
- « M@gistère » Ministère de l'Éducation Nationale
- Le catalogue de formations du CNFPT
- Le catalogue de formation de l'ANFH

Et... bientôt disponible sur « cybermalveillance.gouv.fr »





CYBERMOIS : LE MOIS EUROPÉEN DE LA CYBERSÉCURITÉ

- Événement de **sensibilisation à la cybersécurité durant le mois d'octobre**
- Une **initiative Européenne de l'ENISA***
- Volet français 2023 **piloté par Cybermalveillance.gouv.fr**
- **À destination de tous les publics** : particuliers, entreprises, collectivités, administrations et associations...
- Le thème de l'édition 2023 : **La fraude par ingénierie sociale**

**Agence de l'Union européenne pour la cybersécurité*

LIENS UTILES :

1. [Vous êtes victime](https://www.cybermalveillance.gouv.fr/diagnostic/profil), pour trouver de l'assistance : <https://www.cybermalveillance.gouv.fr/diagnostic/profil>
2. Tous nos contenus d'information et de sensibilisation :
<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/liste-des-ressources-mises-a-disposition>
3. Vidéos de sensibilisation :
<https://www.dailymotion.com/cybermalveillance>

Les nouveaux services proposés par Beta.gouv.fr & France-identité :

Ajouter un filigrane à ses documents important avant de les communiquer :

<https://filigrane.beta.gouv.fr/>



Monter un dossier de qualité en sécurisant ses documents :

<https://www.dossierfacile.fr/>

Garder la maîtrise de ses données d'identité / générer un justificatif d'identité à usage unique :

<https://france-identite.gouv.fr/>



RÉPUBLIQUE
FRANÇAISE

*Liberté
Égalité
Fraternité*



www.cybermalveillance.gouv.fr

Nos ressources de sensibilisation



Assistance et prévention
en sécurité numérique



@cybervictimtimes



@cybervictimtimes



@cybermalveillancegouvfr