



RÉPUBLIQUE
FRANÇAISE

*Liberté
Égalité
Fraternité*



Assistance et prévention
en cybersécurité

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

HubEst 

NUMÉRIQUE
EN COMMUN[S]

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

65
membres
du dispositif



Organisations
publiques et privées

plus de
1 250
prestataires
de services
référéncés



sur l'ensemble
du territoire

plus de
200
labellisés

**EXPERT
CYBER**

LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr

 **RÉPUBLIQUE FRANÇAISE**

sur l'ensemble
du territoire

plus de
280 000
demandes
d'assistance sur
la plateforme



en 2023

plus de
3 700 000
visiteurs uniques
sur la plateforme



en 2023

65 MEMBRES RÉUNIS AUTOUR D'UN PARTENARIAT PUBLIC- PRIVÉ

PREMIER MINISTRE

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

MINISTÈRE DE L'INTÉRIEUR ET DES OUTRE-MER

MINISTÈRE DE L'ÉDUCATION NATIONALE ET DE LA JEUNESSE

MINISTÈRE DES ARMÉES

MINISTÈRE DE LA JUSTICE

SECRÉTARIAT D'ÉTAT CHARGÉ DU NUMÉRIQUE





**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*



Assistance et prévention
en cybersécurité

ATELIER
—
La MalletteCyber

LA SENSIBILISATION A PORTÉE DE MAIN

Collaboration avec l'A.N.C.T.

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

- Prévention à la cybersécurité
- Ressource pédagogique et polyvalente

Au service des populations les plus éloignées du numérique

- Développé avec des acteur.rice.s de la médiation

La Mallette Cyber

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



LA DÉMARCHE PÉDAGOGIQUE

1) Apprendre ou approfondir ses connaissances

- Un livret pédagogique destiné à l'aidant.e
 - Contenus de sensibilisation à la cybersécurité

2) Transmettre

- Un support de médiation pour échanger avec l'utilisateur
 - Menaces les plus courantes et les moyens de s'en prémunir

3) Pratiquer et illustrer

- Une activité pédagogique (jeu de cartes et tapis de jeu)
 - Pour faciliter l'apprentissage des conseils et réflexes cyber

4) Pérenniser

- Une infographie remise à l'utilisateur
 - Des recommandations essentielles



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





**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*



Assistance et prévention
en cybersécurité

Démonstration ...



SITUATION

Situation

Paula reçoit un mail bancaire

boîte de réception

De : E-service Clients CG
<CG_secure4.noreply@radiopwn.com>
À : Paula@gmail.com
Sujet : Au sujet de la sécurité de votre compte !

**SÉCURITÉ RENFORCÉE POUR CONSULTER VOS
COMPTES EN LIGNE**

Chère cliente, cher client,

Conformément à la loi PSD2 pour la sécurité des paiements en ligne et afin d'arrêter l'utilisation frauduleuse des cartes bancaires sur Internet, notre équipe est dotée d'un dispositif de contrôle des transactions.

Ce service est entièrement gratuit !
Remarque : cette opération est obligatoire et à faire sous 48H sous peine de suspension de votre compte.

[ME CONNECTER](#)

- ❌ L'adresse du site ne correspond pas à l'adresse officielle du site des Impôts
- ❌ Les Impôts n'ont pas besoin de ce type d'informations : ils les ont déjà
- ❌ Un remboursement des Impôts se fait par virement automatique sur votre compte

Réponses :

Situation



SITUATION

Situation

Paula reçoit un mail bancaire

Boîte de réception

De : E-service Clients CG
<CG_secure4.noreply@radiopwn.com>
À : Paula@gmail.com
Sujet : Au sujet de la sécurité de votre compte !

**SECURITÉ RENFORCÉE POUR CONSULTER VOS
COMPTES EN LIGNE**

Chère cliente, cher client,

Conformément à la loi PSD2 pour la sécurité des paiements en ligne et afin d'arrêter l'utilisation frauduleuse des cartes bancaires sur Internet, notre équipe est dotée d'un dispositif de contrôle des transactions.

Ce service est entièrement gratuit !
Remarque : cette opération est obligatoire et à faire sous 48H sous peine de suspension de votre compte.

ME CONNECTER

ce déjà
le

UNE MENACE

Menace

Hameçonnage (phishing)

Pourquoi ?
Voler des informations sensibles (identité, adresses, comptes, mots de passe, données bancaires...) pour en faire un usage frauduleux.

Comment ?
Faux message, SMS ou appel téléphonique d'un cybercriminel qui se fait passer pour une banque, un opérateur téléphonique, un site de commerce, un réseau social, une administration...



Une personne vient sonner à la porte de la victime : elle se présente comme un agent spécialisé en placements financiers dont la société est certifiée par le ministère des Finances...

« Nous sommes mandatés pour vous proposer des investissements à hauts rendements et totalement déduits d'impôts. Si vous voulez en profiter, il faut rapidement constituer un dossier car ces mesures expirent la semaine prochaine ».

La victime fait entrer l'intéressé et après lui avoir signé un document dans lequel elle renseigne toutes ses informations bancaires, elle lui remet une grosse somme d'argent devant être placée.

Résultat : Elle a transmis tous ces éléments à un parfait inconnu qui lui a dérobé son argent et risque de réutiliser ses informations financières pour d'autres escroqueries !

Hameçonnage (phishing) dans la vraie vie

Menace



SITUATION

UNE MENACE

DES RISQUES

Situation

Paula reçoit un mail bancaire

Solite de réception

De : E-service Clients CG
<CG_secure4.noreply@radiopwn.com>
À : Paula@monmail.com
Sujet : Au sujet de la sécurité de votre compte !

SECURITE RENFORCEE POUR CONSULTER VOS COMPTES EN LIGNE

Chère cliente, cher client,

Conformément à la loi PSD2 pour la sécurité des paiements en ligne et afin d'arrêter l'utilisation frauduleuse des cartes bancaires sur Internet, notre équipe est dotée d'un dispositif de contrôle des transactions.

Ce service est entièrement gratuit !

Remarque : cette opération est obligatoire et à faire sous 48h sous peine de suspension de votre compte.

[ME CONNECTER](#)

Menace

Haçonnage (phishing)

Pourquoi ?
Voler des informations sensibles (identité, adresses, comptes, mots de passe, données bancaires...) pour en faire un usage frauduleux.

Comment ?
Faux message, SMS ou appel téléphonique d'un cybercriminel qui se fait passer pour une banque, un opérateur téléphonique, un site de commerce, un réseau social, une administration...

Risque

Vol de données bancaires

En étant trompée par haçonnage (par mail, SMS ou appel téléphonique), une personne peut être amenée à communiquer des informations bancaires (numéros de carte, code d'accès à son compte, ou encore des codes reçus par SMS de sa banque...).

Avec des données bancaires dérobées, le cybercriminel peut effectuer des virements ou réaliser des achats en ligne qui seront débités de votre compte bancaire.

Exemple de vol de données bancaires:

Risque

Risque

Vol de données d'identité

En étant trompée par haçonnage (par mail, SMS ou appel téléphonique), une personne peut être amenée à communiquer des informations ou documents d'identité (copie de la carte d'identité, bulletins de paie, avis d'imposition, justificatif de domicile...).

Avec les documents d'identité dérobés, le cybercriminel peut ouvrir un compte bancaire à votre nom qui servira à des activités frauduleuses, souscrire un crédit que vous devrez rembourser, louer une voiture...

Exemple de vol de données d'identité:

Risque

Risque

Usurpation d'identité

L'usurpation d'identité est un délit qui désigne l'utilisation d'informations personnelles permettant d'identifier une personne sans son accord pour réaliser des actions frauduleuses.

En fonction des informations recueillies, les escrocs peuvent commettre diverses infractions en se faisant passer pour la victime : escroquerie des proches, faux profil sur les réseaux sociaux, détournement d'allocations, souscription de crédit, ouverture de compte bancaire...

Exemples d'usurpation d'identité:

Risque

Risque

Escroquerie financière

L'escroquerie financière a comme objectif de tromper la victime pour lui soutirer de l'argent en utilisant différents prétextes qui peuvent jouer sur la crainte, l'urgence, l'empathie, l'attrait du gain...

- Le cybercriminel tente de se faire passer pour vous (par mail, SMS, compte de réseau social piraté) et contacte des personnes de votre entourage pour essayer de les arnaquer.
- L'escroc fait semblant de dépanner la victime à distance pour lui facturer l'intervention, des logiciels anti-virus et/ou des abonnements fictifs.
- Le cybercriminel publie une annonce frauduleuse de location pour récupérer le montant de la caution en fournissant les documents qu'il a récupérés auprès d'une autre victime.

Exemples d'escroquerie financière:

Risque

SITUATION



UNE MENACE

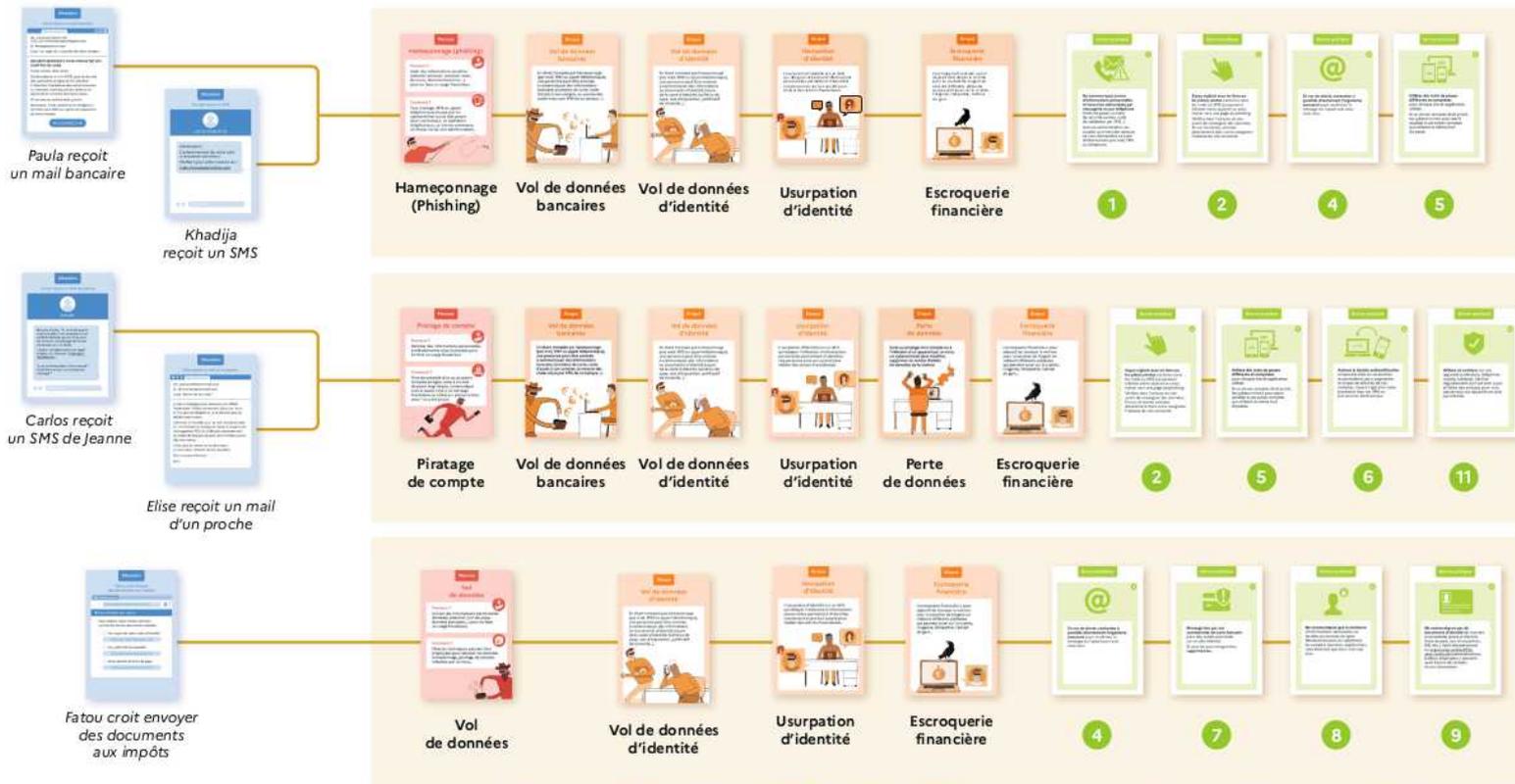


DES RISQUES



DES BONNES PRATIQUES







**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*



Assistance et prévention
en cybersécurité

Pour aller plus loin ...

LA MALLETTE CYBER EN FORMAT NUMÉRIQUE ...

Des plans en licence ouverte pour la « Mallette Cyber »

- Téléchargeables
 - Dans la rubrique « médiation » de notre site
 - Sur « **La Base** », la plateforme collaborative de l'ANCT
- Facilement façonnables
 - En version « FabLab » ou « prêt à imprimer »

... ET DE NOMBREUX OUTILS POUR LES MÉDIATEUR.ICE.S

- Une simulation de notre parcours d'assistance victime
 - pour familiariser les usagers avec l'outil.
- Des vidéos de sensibilisation et campagnes de prévention
- Des contenus à destination du jeune public

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



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

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



SENSIBILISATION ET PRÉVENTION

Des articles adaptés aux particuliers

... comme aux professionnels

- Définition de la menace
- Comment s'en protéger ?
- Que faire si vous êtes victime ?

19 grandes menaces décortiquées

- Rançongiciels, Hameçonnage, piratage de compte, usurpation d'identité ...

Diffuser les bonnes pratiques

- Sauvegardes, mises à jour, réagir en cas de cyberattaque, usages pro/perso, télétravail ...



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



RÉPUBLIQUE
FRANÇAISE

*Liberté
Égalité
Fraternité*



www.cybermalveillance.gouv.fr

Nos ressources de sensibilisation



Assistance et prévention
en cybersécurité



@cybervictimes



@cybervictimes



@cybermalveillancegouvfr