

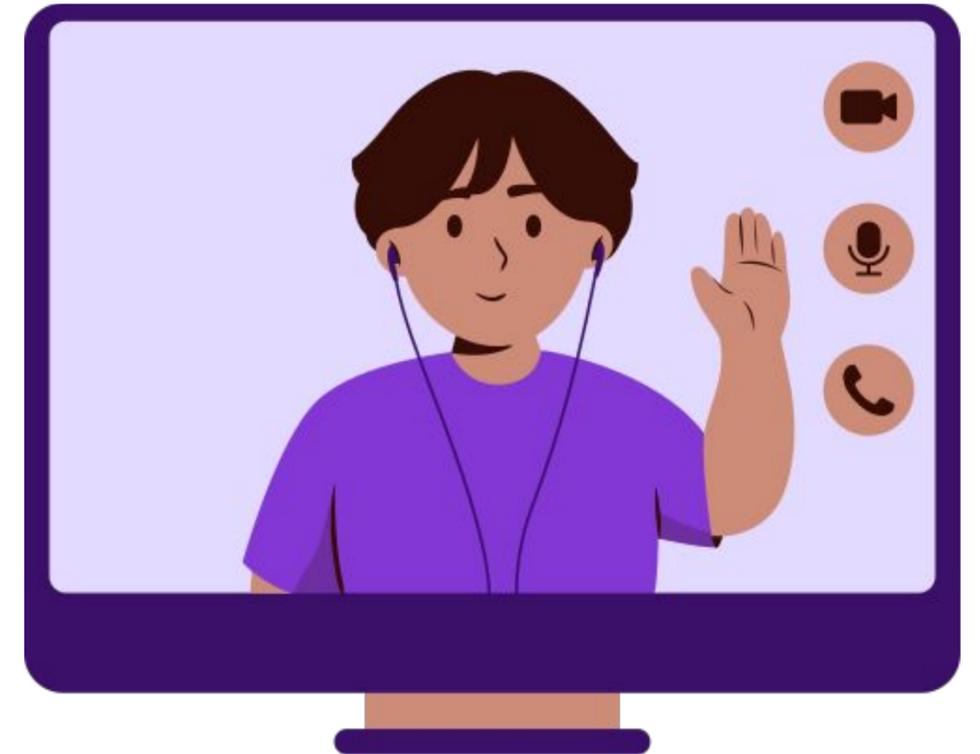
HubEst

Webinaire Présentation de la Mallette Cyber



Quelques règles communes avant de commencer

- Pour **poser des questions**, levez la main ou posez votre question dans le chat.
- Attention à bien **désactiver votre micro** lorsque vous n'êtes pas en train de parler pour éviter les bruits parasites.
- Ce **webinaire est enregistré** pour les absent·es, désactivez votre caméra si vous ne souhaitez pas être filmé·e.



Au programme de ce webinar :

- Le contexte et objectifs de la Mallette Cyber
- Le contenu pédagogique
- Obtenir sa Mallette Cyber
- La parole est à vous !

Pour plus d'info sur ce sujet, rendez vous ici :

<https://lesbases.anct.gouv.fr/ressources/la-mallette-cyber-outiller-les-professionnels-de-la-mediation>



Le contexte de création de la Mallette Cyber

Les porteurs de ce projet sont le **GIP ACYMA** (opérateur de la plateforme Cybermalveillance. gov.fr) et l'**ANCT**.

Cet outil a été développé en collaboration avec des médiateur·ices numériques afin de prendre en compte leurs besoins. Pour cela 684 d'entre elles et eux ont répondu à une enquête visant à recueillir leurs attentes concernant la création d'une mallette sur la cyber malveillance.

Les **objectifs** retenus suite à cette enquête sont :

- Renforcer les connaissances des médiateur·ices numériques sur les risques liés à la cybermalveillance.
- Sensibiliser les personnes éloignées du numérique à des pratiques en ligne sécurisées.
- S'appuyer sur un support pédagogique physique.

Le public visé par le contenu de la mallette cyber

Les médiateur·ices et conseiller·ères numériques peuvent utiliser la mallette cyber pour sensibiliser les publics éloignés du numérique.



Sensibilisation à la cybermalveillance



En accompagnement individuel
ou de groupe de 2 à 6
personnes

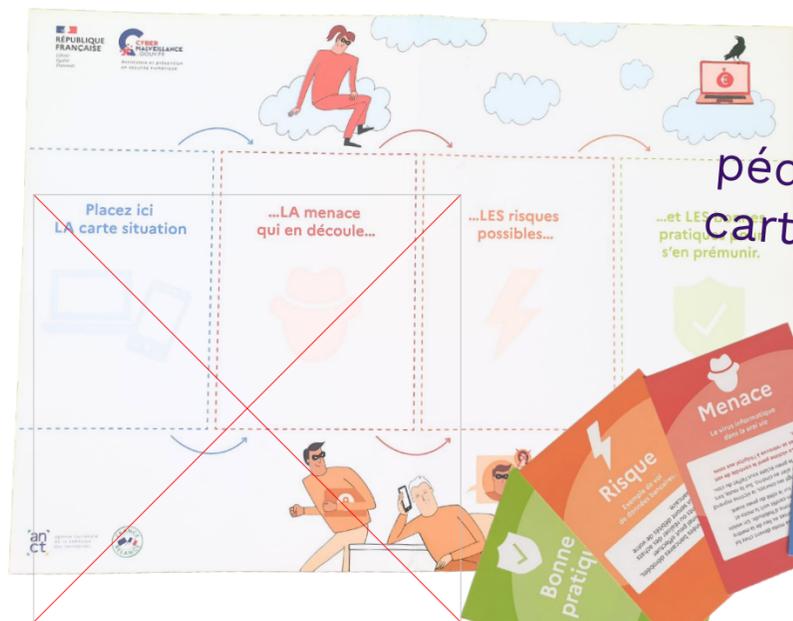


Pour des usager·ères
adultes

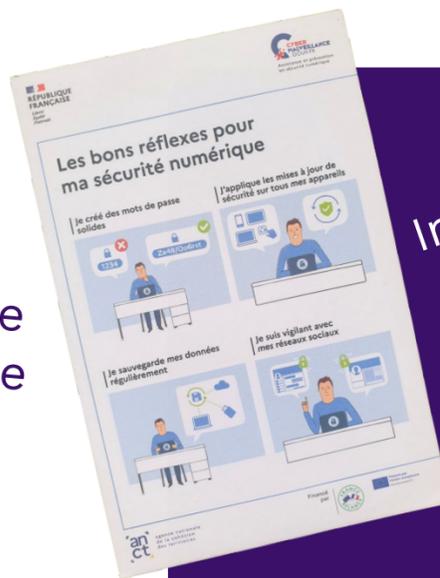
Le contenu de la mallette



Un livret pédagogique destiné aux conseiller·ères



Une activité pédagogique (jeu de cartes et un tapis de jeu).



Infographie

Affiche A2

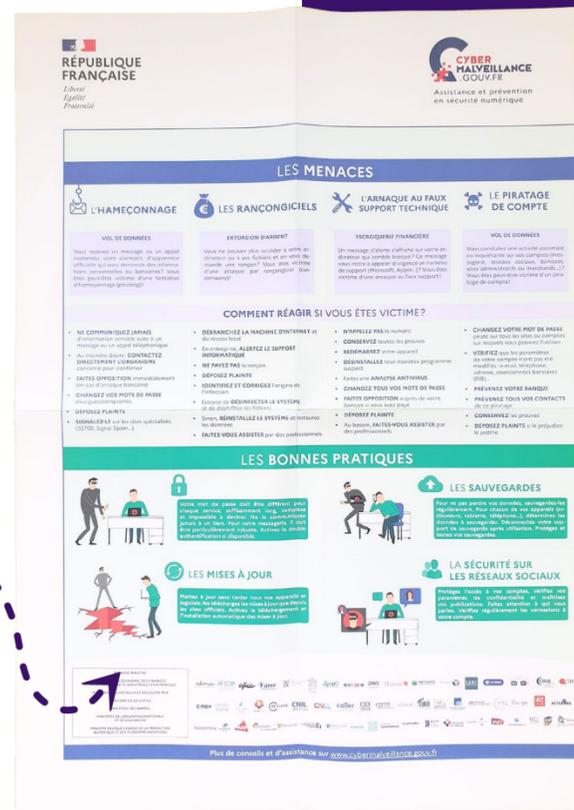


Autocollants

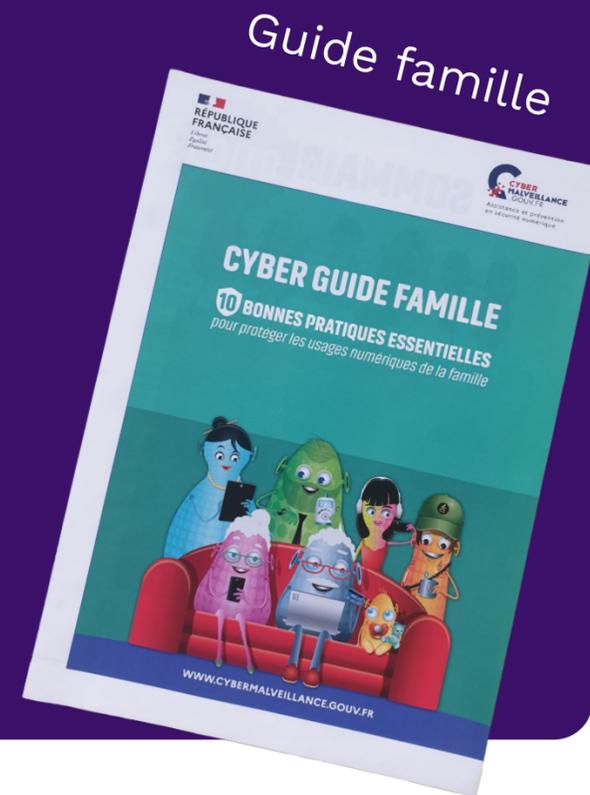
Les recommandations et bons gestes à remettre à l'utilisateur.



Un support de médiation



Flyer



Guide famille

Les ressources complémentaires

(Recommandations et bons gestes)

Le flyer cybermalveillance.gouv.fr



Un flyer présentant
cybermalveillance.gouv.fr et ses missions.

Le cyber guide famille



10 bonnes pratiques pour protéger les usages numériques d'une famille.

- Les risques des pratiques numériques.
- Les conseils pour garantir sa sécurité.
- Des ressources pour aller plus loin.

Les autocollants des mauvaises pratiques



Une plaque d'autocollants mettant en scène plusieurs situations de mauvaises pratiques.

L'affiche récapitulative

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

LES MENACES

- L'HAMEÇONNAGE**
VOL DE DONNÉES
Vous recevez un message ou un appel inattendu, voire alarmant, d'apparence officielle qui vous demande des informations personnelles ou bancaires? Vous êtes peut-être victime d'une tentative d'hameçonnage (phishing)!
- LES RANÇONGIERS**
EXTORSION D'ARGENT
Vous ne pouvez plus accéder à votre ordinateur ou à vos fichiers et on vous demande une rançon? Vous êtes victime d'une attaque par rançongiciel (ransomware)!
- L'ARNAQUE AU FAUX SUPPORT TECHNIQUE**
ESCROQUERIE FINANCIÈRE
Un message d'alerte s'affiche sur votre ordinateur qui semble bloqué? Ce message vous incite à appeler d'urgence un numéro de support (Microsoft, Apple...)? Vous êtes victime d'une arnaque au faux support!
- LE PIRATAGE DE COMPTE**
VOL DE DONNÉES
Vous constatez une activité anormale ou inquiétante sur vos comptes (messagerie, réseaux sociaux, banques, sites administratifs ou marchands...)? Vous êtes peut-être victime d'un piratage de compte!

COMMENT RÉAGIR SI VOUS ÊTES VICTIME?

- NE COMMUNIQUEZ JAMAIS** d'information sensible suite à un message ou un appel téléphonique.
- Au moindre doute, CONTACTEZ DIRECTEMENT L'ORGANISME** concerné pour confirmer.
- FAITES OPPOSITION** immédiatement (en cas d'arnaque bancaire).
- CHANGEZ VOS MOTS DE PASSE** diversifiés et complexes.
- DÉPOSEZ PLAINTE**.
- SIGNALÉZ-LE** sur les sites spécialisés (33700, Signal Spam...).
- DÉBRANCHEZ LA MACHINE D'INTERNET** et du réseau local.
- En entreprise, ALERTEZ LE SUPPORT INFORMATIQUE**.
- NE PAYEZ PAS** la rançon.
- DÉPOSEZ PLAINTE**.
- IDENTIFIEZ ET CORRIGEZ** l'origine de l'infection.
- Essayez de **DÉSINFECTER LE SYSTÈME** et de **déchiffrer les fichiers**.
- Si non, **RÉINSTALLEZ LE SYSTÈME** et restaurez les données.
- FAITES-VOUS ASSISTER** par des professionnels.
- N'APPELÉZ PAS** le numéro.
- CONSERVEZ** toutes les preuves.
- REDÉMARREZ** votre appareil.
- DÉSINSTALLEZ** tout nouveau programme suspect.
- Faites une **ANALYSE ANTIVIRUS**.
- CHANGEZ TOUS VOS MOTS DE PASSE**.
- FAITES OPPOSITION** auprès de votre banque si vous avez payé.
- DÉPOSEZ PLAINTE**.
- Au besoin, **FAITES-VOUS ASSISTER** par des professionnels.
- CHANGEZ VOTRE MOT DE PASSE** piraté sur tous les sites ou comptes sur lesquels vous pourriez l'utiliser.
- VÉRIFIEZ** que les paramètres de votre compte n'ont pas été modifiés: e-mail, téléphone, adresse, coordonnées bancaires (RIB)...
- PRÉVENEZ VOTRE BANQUE**.
- PRÉVENEZ TOUS VOS CONTACTS** de ce piratage.
- CONSERVEZ** les preuves.
- DÉPOSEZ PLAINTE** si le préjudice le justifie.

LES BONNES PRATIQUES

- LES SAUVEGARDES**
Pour ne pas perdre vos données, sauvegardez-les régulièrement. Pour chacun de vos appareils (ordinateurs, tablettes, téléphones...), déterminez les données à sauvegarder. Déconnectez votre support de sauvegarde après utilisation. Protégez et testez vos sauvegardes.
- LES MISES À JOUR**
Mettez à jour sans tarder tous vos appareils et logiciels. Ne téléchargez les mises à jour que depuis les sites officiels. Activez le téléchargement et l'installation automatique des mises à jour.
- 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.

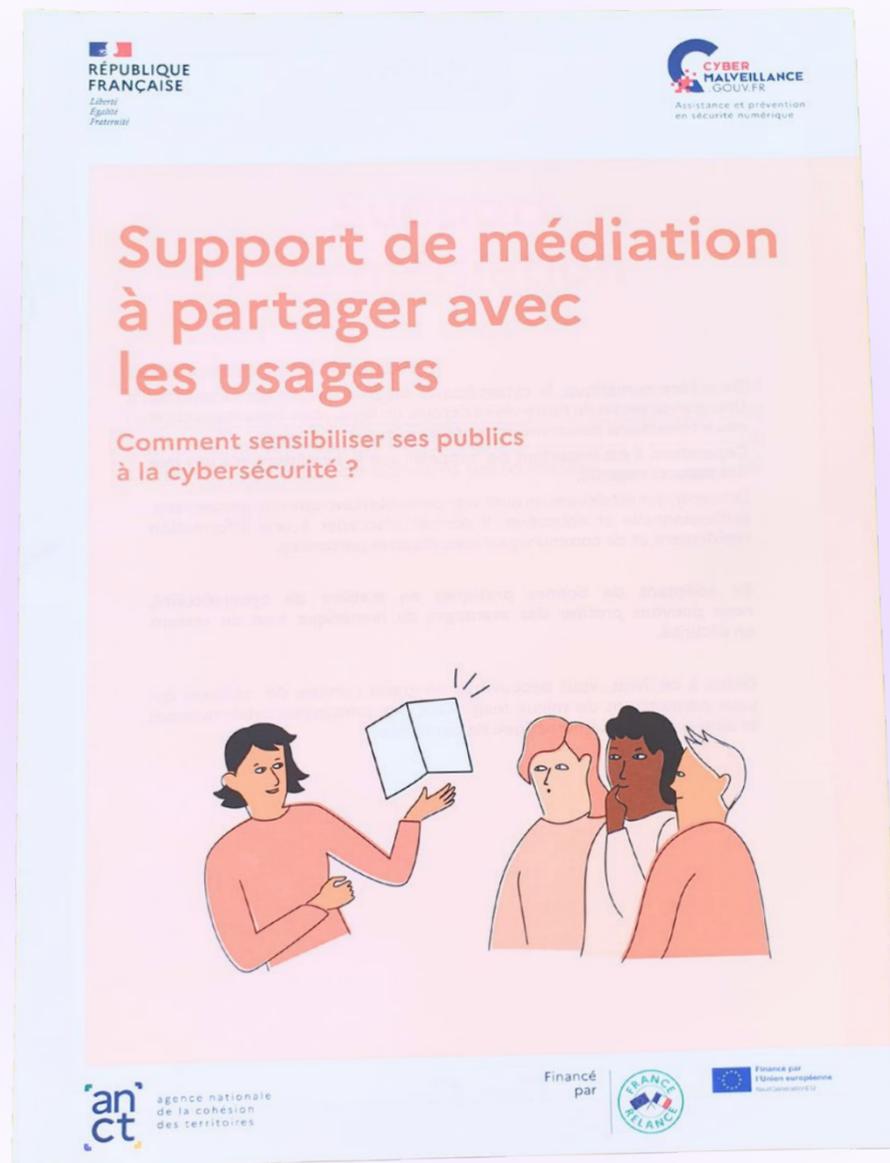
Plus de conseils et d'assistance sur www.cybermalveillance.gouv.fr

Une affiche taille A2 faisant une synthèse :

- des risques liés au hameçonnage, rançongiciel, arnaque au faux support technique et piratage de compte.
- des bonnes pratiques à toujours mettre en place.

Les ressources principales

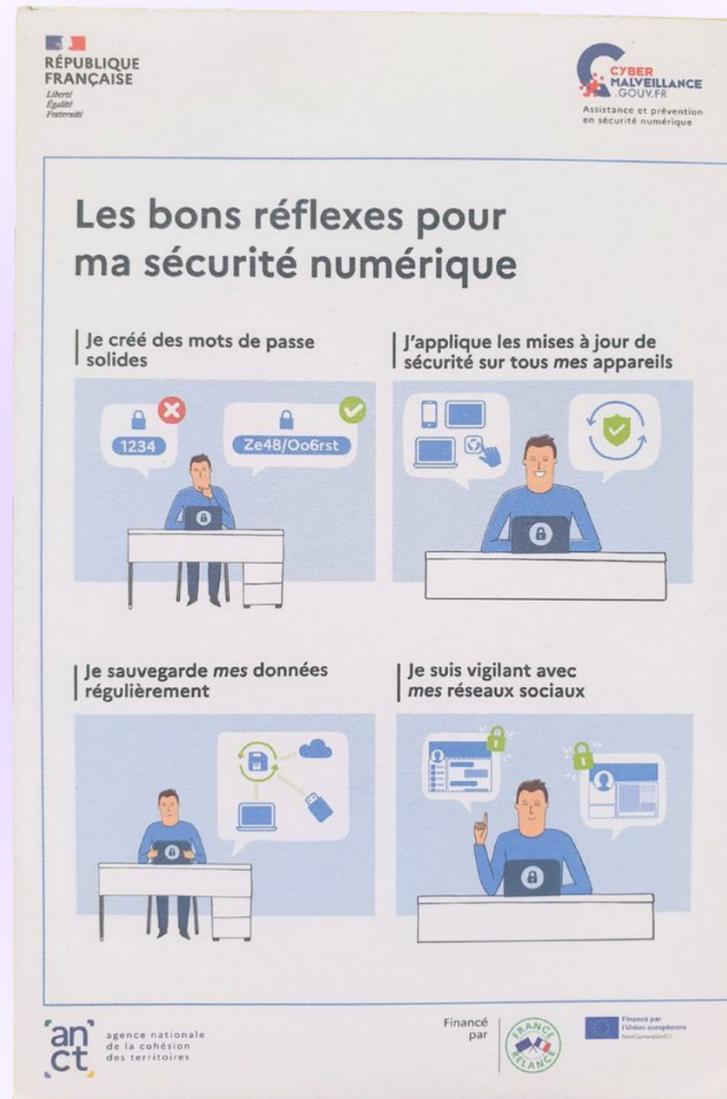
Le support de médiation à partager avec les usager·ères



Des infographies claires, expliquant les termes et les moyens de se protéger des 4 attaques les plus courantes.

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

Infographie des bons reflexes



Un bloc de 50 infographies représentant les bons réflexes pour sécuriser ses pratiques numériques.

Le livret pédagogique pour les médiateur·ices



Tout savoir sur les 4 attaques les plus courantes (hameçonnage, le piratage de compte, l'arnaque au faux support technique, la fuite ou violation de données personnelles)

- Les mesures préventives
- Les bons réflexes à avoir en cas d'attaque

La présentation du jeu de carte

- Les règles du jeu
- Les solutions
- Des conseils d'animation de groupe

Le jeu de société et son plateau



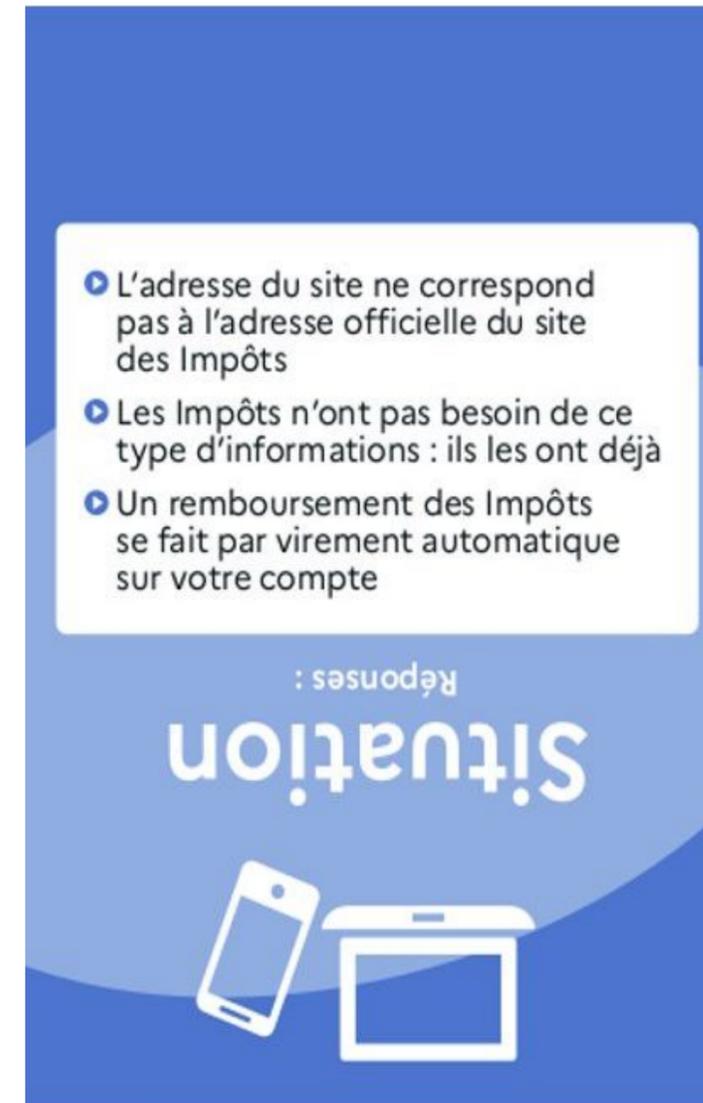
Un jeu de carte composé de quatre types de cartes :

- les cartes situations
- les cartes menaces
- les cartes risques
- les cartes bonnes pratiques

L'objectif de ce jeu de carte est de mettre en situation l'utilisateur en lui présentant une situation où il ou elle doit identifier la menace et les risques puis trouver les bonnes pratiques pour se protéger face à cette situation.

Première étape : description d'une situation

7 cartes "situation"



L'utilisateur doit trouver les indices indiquant qu'une situation est suspecte.

Les réponses sont au dos de la carte

Deuxième étape : trouver la menace

5 cartes "menace"

Réponses :

Situation

- ▶ 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

De quel type de cybermalveillance s'agit t'il ?



L'utilisateur doit trouver le type de menace qui se cache dans la situation.

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...

Menace

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 !

L'hameçonnage (phishing) dans la vraie vie

Au dos de la carte se trouve une situation similaire dans "le monde réel"

Troisième étape : comprendre les risques

5 cartes "risque"

Menace

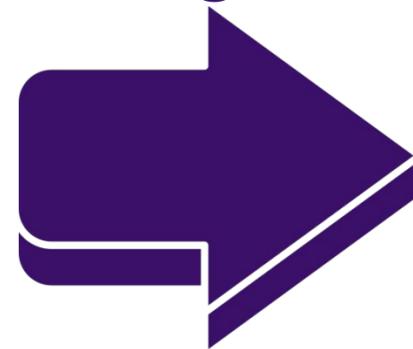
Hameçonnage (phishing)

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...



Qu'est ce que risque l'utilisateur ?



L'utilisateur doit trouver les conséquences de la menace.

Risque

Vol de données bancaires

En étant trompée par hameçonnage (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



Des exemples concrets des problèmes que posent les cyber menaces.

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



Une cyber menace peut mener à plusieurs risques.

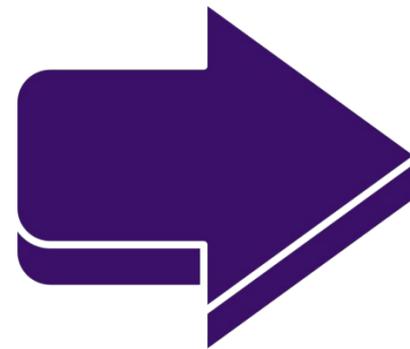
Dernière étape : éviter la situation grâce à des bonnes pratiques

13 cartes "bonnes pratiques"

Une situation peut être évitée grâce à plusieurs bonnes pratiques.



Comment éviter cette situation?



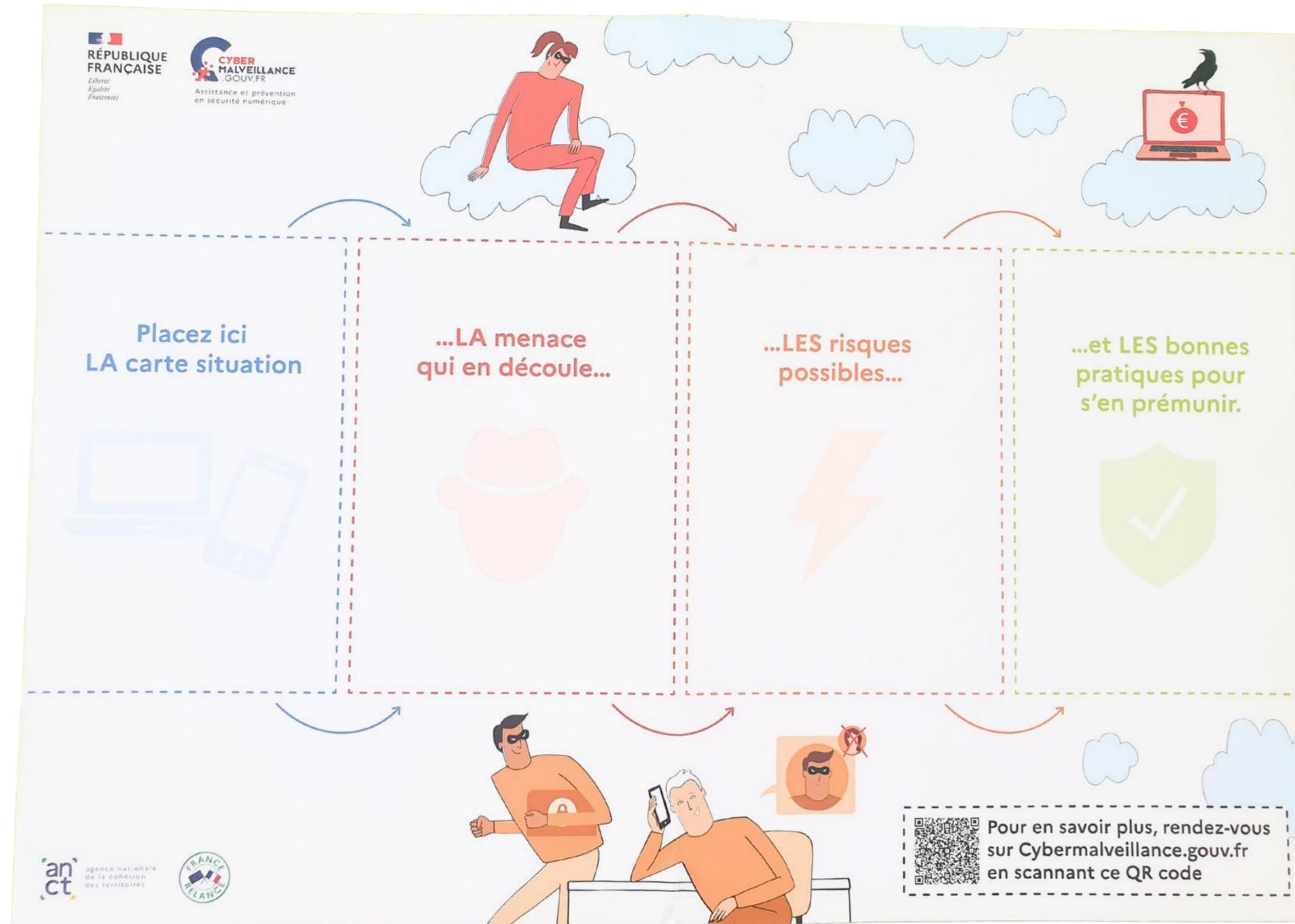
L'utilisateur doit trouver les bonnes pratiques à mettre en place pour éviter la menace et les risques.



Un tapis de jeu pour suivre le déroulement du jeu

1 - Carte situation

2 - Carte menace



3 - Une ou plusieurs cartes risques

4 - une ou plusieurs cartes bonne pratiques

Un parcours d'accompagnement graduel



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

1

2

3

4

5



Se procurer la mallette cyber



La Mallette est mise à disposition gratuitement en format numérique sous licence Etalab 2.0 (Reproduction, modification, communication, diffusion, exploitation à titre commercial...).

[Vous pouvez télécharger les plans “prêt à l’emploi” ici](#)



Les 2900 structures d’accueil des conseiller·ères numériques peuvent commander la version physique gratuitement.

[Pour commander une mallette c’est ici](#)

Participez à l'évolution de la mallette cyber



La mallette cyber qui a pour vocation d'être améliorée en fonction de vos retours de terrain. Vous pouvez donner **vos avis**, notamment sur la qualité, le contenu, et les différents contextes dans lesquels elle est utilisée par les conseiller·ères numériques (ateliers, salons, publics ciblés, etc.).

[Répondez au questionnaire ici.](#)



Vous pouvez aussi **produire des mallettes cyber** pour les diffuser aux réseaux d'acteur de l'inclusion numérique ou en les vendant. Un recensement des fabricants est fait pour permettre une production locale et à moindre coût.

[Cliquez ici pour trouver le recensement des producteurs locaux](#)

Des questions ?

