

Webinaire d'information

29 août 2024

LA MALLETTE CYBER



ELEMENTS DE CONTEXTE

Cybermalveillance.gouv.fr est le dispositif national d'assistance aux victimes d'actes de cybermalveillance, de sensibilisation aux risques numériques et d'observation de la menace sur le territoire français.

le **GIP ACYMA**, pilote du dispositif, a créé en 2023, **une boîte à outils et ressources**, autour des **risques numériques** et de la **cybermalveillance**.

- Mis à disposition aux conditions de la licence **Etalab 2.0** : (Reproduction, modification, communication, diffusion, exploitation à titre commercial...).
- Diffusion de cette mallette auprès des **2900 structures d'accueil** des conseillers numériques. en leur permettant de la commander puis la recevoir **gratuitement**.

OBJECTIFS

- Renforcer la sensibilisation et l'outillage des acteurs et professionnels de la médiation numérique.
- Proposer un outil de médiation auprès des usagers.
- Améliorer la posture du médiateur dans l'approche des risques cyber.

VISION GLOBALE

Le livret pédagogique



Le support de médiation

Le plateau de jeu



Les cartes



L'infographie



**Ensemble des ressources
disponible ici
(Site « Les bases »)**



RESSOURCES COMPLÉMENTAIRES

Le Cyber Guide Famille



Le flyer



Format spécifiques non compatibles avec une imprimante standard.

Les stickers



L'affiche



La Mallette Cyber

CONTENU PRINCIPAL

➤ Focus sur 5 menaces :

Phishing, piratage de compte, arnaque au faux support technique, violation de données, virus informatiques.

➤ Livret pédagogique :

- Dimensions préventives et curatives
- Bonnes pratiques générales : spécifique smartphone, règles et méthodes pour mots de passe, sauvegardes...
- Présentation du jeu de cartes.

➤ Support médiation :

Synthèse des bonnes pratiques pour chaque menace : comment se protéger ?

COMPOSANTS DE LA MALLETTE CYBER



UN LIVRET PÉDAGOGIQUE composé de :

- **contenus de sensibilisation** à la cybersécurité avec des fiches réflexes et des fiches pratiques
- une **présentation du jeu de cartes** pour vous permettre de l'animer



UN SUPPORT DE MÉDIATION avec :

- des **fiches sur les menaces** les plus courantes et **les bonnes pratiques** à adopter



UN JEU DE CARTES ET UN PLATEAU DE JEU

- pour mettre en pratique et ancrer les notions abordées avec les usagers



UNE INFOGRAPHIE

- à imprimer et à remettre à chaque usager pour lui laisser un résumé des bonnes pratiques essentielles

PARCOURS PÉDAGOGIQUE INTÉGRÉ



S'APPROPRIER

APPRENDRE

TRANSMETTRE

PRATIQUER

PÉRENNISER

Comprendre
la démarche
pédagogique

S'acculturer
Mettre à jour ses
connaissances

Illustrer par des
infographies
illustrées

Ancrer les
connaissances
de façon ludique

Un support
laissé à l'utilisateur



LE JEU DE CARTES



En tête à tête
ou en groupe
2 à 6 usagers

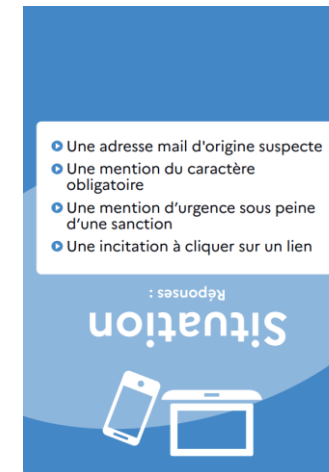
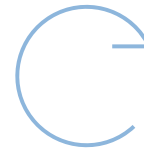


18+ ans



Prévention
uniquement

7 Cartes « situation »



Présente une situation dans laquelle une personne est confrontée à une cybermenace.

Présente les indices qui permettent d'identifier qu'il s'agit d'une cybermenace.

LE JEU DE CARTES



En tête à tête
ou en groupe
2 à 6 usagers

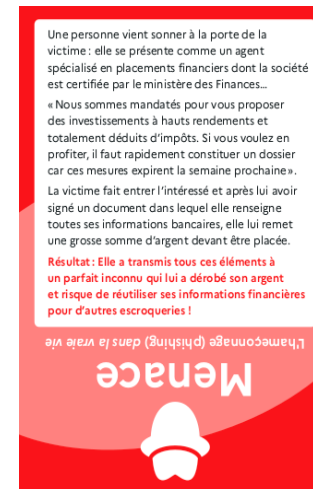
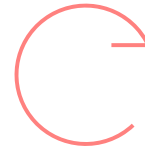


18+ ans



Prévention
uniquement

5 Cartes « menace »



Présente les principales cybermenaces auxquelles un usager peut être confronté.

Présente chaque menace sous la forme d'une situation dans la vie « réelle » et permet aux usagers moins à l'aise avec le numérique de se projeter plus concrètement.

LE JEU DE CARTES



En tête à tête
ou en groupe
2 à 6 usagers

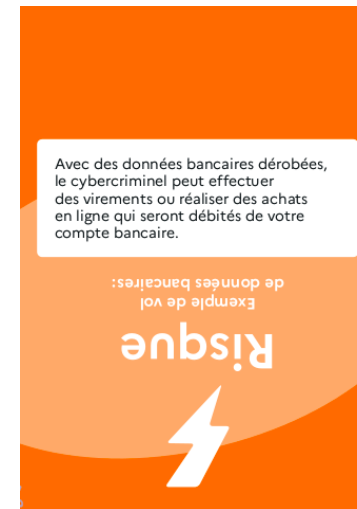


18+ ans



Prévention
uniquement

5 Cartes « risque »



Présente les principaux risques encourus lorsqu'on fait face à une cybermenace.

Présente des exemples concrets illustrant chaque risque et indiquant aux usagers ce qu'ils impliquent.

LE JEU DE CARTES



En tête à tête
ou en groupe
2 à 6 usagers



18+ ans




Prévention
uniquement

13 Cartes « bonnes pratiques »

Bonne pratique

1



Ne communiquez jamais d'informations personnelles et bancaires demandées par messagerie ou par téléphone (mots de passe, numéro de sécurité sociale, code de validation par SMS...).

Aucune administration ou société commerciale sérieuse ne vous demandera ce type d'informations par mail, SMS ou téléphone.



Présente les principales bonnes pratiques à retenir pour prévenir les cybermenaces.

LE JEU DE CARTES



En tête à tête
ou en groupe
2 à 6 usagers



18+ ans



Prévention
uniquement

Scénario d'utilisation

Situation

Paula reçoit un mail bancaire

Info de ressource

De: Espace Clients CG
<CG_secure4.noreply@radiopw.com>
À: Paula@monmail.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'améliorer 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

Hameçonnage (phishing)

Pourquoi ?
Voler des info (identité, adr de passe, don pour en faire

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 ministre 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 mesurites 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.

Comment ?
Faux message téléphonique qui se fait passer par un opérateur de commerce ou une administr

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

Le hameçonnage (phishing) dans la vraie vie

Menace



Risque

Vol de données bancaires

En étant une pe à com banca d'accè codes

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



Bonne pratique

1

Ne communiquez jamais d'informations personnelles et bancaires demandées par messagerie ou par téléphone (mots de passe, numéro de sécurité sociale, code de validation par SMS...)
Aucune administration ou société commerciale sérieuse ne vous demandera ce type d'informations par mail, SMS ou téléphone.

Bonne pratique

2

Soyez vigilant avec les liens ou les pièces jointes contenus dans les mails ou SMS qui peuvent infecter votre appareil ou vous mener vers une page de phishing. Vérifiez bien l'adresse du site avant de renseigner des données. En cas de doute, saisissez directement dans votre navigateur l'adresse du site concerné.

Bonne pratique

4

En cas de doute, contactez si possible directement l'organisme concerné pour confirmer le message ou l'appel que vous avez reçu.

Bonne pratique

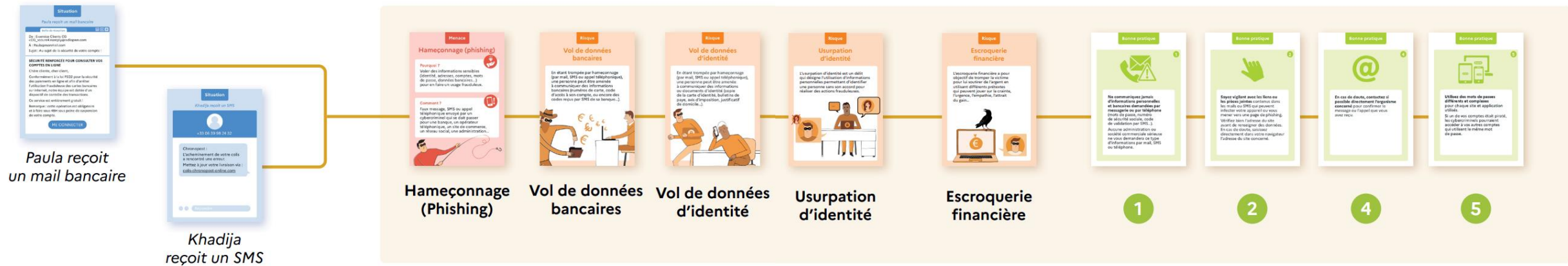
5

Utilisez des mots de passes différents et complexes pour chaque site et application utilisés.
Si un de vos comptes était piraté, les cybercriminels pourraient accéder à vos autres comptes qui utilisent le même mot de passe.

LE JEU DE CARTES



Exemple de solution



Points de vigilance



- Confusion Menace VS Risque (aléa, vulnérabilité, impacts)
- Une « menace » (« vol de données ») peut-être une conséquence (=impact) d'une autre menace (« phishing »)
- Des items tels que « vol de données » sont considérés à la fois comme « menaces » et comme « risques ».



Rôle et posture de l'animateur

- Poser et être attentif au cadre (règles du jeu, timing) - Présenter le ou les objectifs attendus.
- Rôle de sachant - expertise sur le sujet et regard extérieur.
- Faciliter, faire émerger l'intelligence collective, la bienveillance et la discussion (que chacun prenne la parole, privilégier les questions ouvertes pour développer les réponses).

EVALUATION ET PERENNISATION



Produire des données qualitatives sur l'utilisation de la mallette permettant de remonter les retours des conseillers numériques quant à la qualité de la mallette et de ses contenus, ainsi qu'aux situations dans lesquelles elle est employée (ateliers, salons, profils des publics, etc.)

Questionnaire : Retours sur l'utilisation de la mallette – (Airtable)



Identifier des « makers » locaux (FabLabs) susceptibles de produire et diffuser la mallette auprès de médiateurs ou d'aidants numériques.

→ Cartographier des structures du territoire capables de produire des Mallettes Cyber en petites ou moyennes quantités, offrant ainsi une production locale et à moindre coût.

Questionnaire : Recensement des producteurs locaux – (Airtable)

DES QUESTIONS ?

