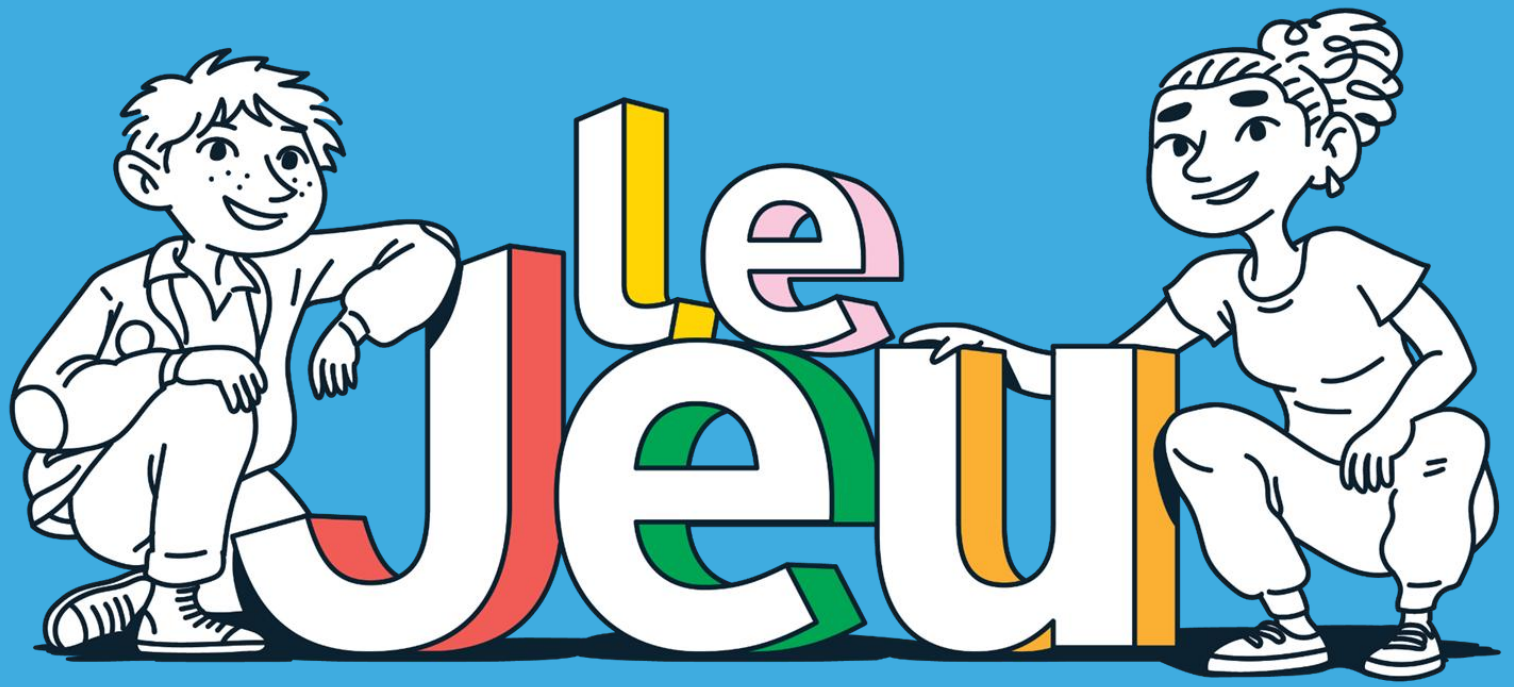


GUIDE ANIMATEUR

2023 I Par FRESQUE DES CYBERCITOYEN·NE·S

Comment utiliser ce guide animateur ?

Ce guide a été construit pour vous aider à préparer une session de sensibilisation avec le jeu « Fresque des cybercitoyen·ne·s ».

Il contient toutes les informations nécessaires à l'animation. Cependant, une séance de formation préalable à l'utilisation du jeu est fortement recommandée avant de vous lancer dans l'aventure ! Soit via les référents sur votre académie ou encore via le module de formation animé sur la plateforme magistère.

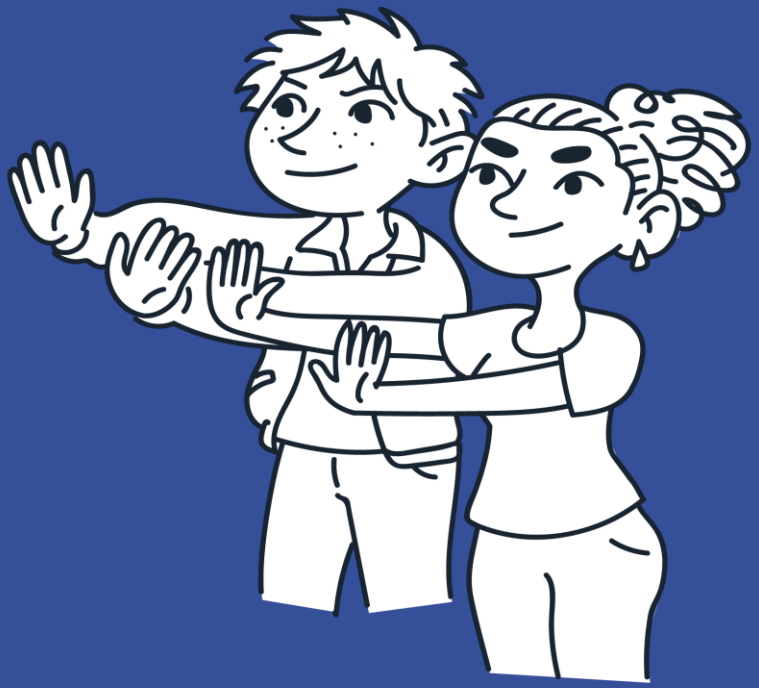
Pour naviguer dans ce guide :

1. Utiliser le sommaire pages 3 et 4 : vous pouvez cliquer sur les titres pour vous rendre directement dans une section du guide ;
2. Depuis toutes les pages du guide, vous pourrez retourner au sommaire en cliquant sur l'icône située en bas à gauche des pages.

Ce guide n'est pas fait pour être imprimé. Le jour de votre animation, munissez-vous du « Tuto Express » qui reprend toutes les informations essentielles.

SOMMAIRE

SOMMAIRE



1. INTRODUCTION

1.a Présentation générale du jeu

Le jeu "Fresque des cybercitoyen·ne·s" est une initiative éducative visant à sensibiliser les adolescents aux bonnes pratiques de sécurité numérique et à promouvoir des comportements responsables en ligne.

Conçu par Advens for People and Planet en partenariat avec l'académie de Paris et avec l'expertise en cybersécurité d'Advens, ce jeu offre une expérience ludique, collaborative et instructive pour les élèves de collège.

1.a Présentation générale du jeu

La "Fresque des Cybercitoyen·ne·s" se présente sous la forme d'un jeu de cartes élaboré pour encourager l'intelligence collective au sein d'équipes de joueurs qui rivalisent pour remporter la partie. En impliquant les élèves dans des discussions, des défis et des prises de décisions, le jeu offre une approche interactive et participative de l'apprentissage des pratiques de cybersécurité et de l'utilisation responsable d'internet.

Une session est divisée en deux parties :

- La première vise l'acquisition de connaissances sur la sécurité numérique ;
- La seconde permet la mise en pratique de celles-ci face à des scénarios d'attaque.

Les thématiques abordées sont :

- Le cyberharcèlement
- La désinformation
- La protection des équipements
- La gestion des mots de passe
- La protection de la vie privée
- Le piratage

Zoom sur les notions du jeu

À travers un quiz et des scénarios illustrés, les élèves pourront donc développer des connaissances sur les enjeux suivants :

1. Protection des données personnelles et outils de cybersécurité : Le jeu permet aux participants d'identifier et de protéger leurs données personnelles et de découvrir les équipements de cybersécurité pour renforcer leur sécurité en ligne.
2. Techniques de piratage et sécurité des comptes : Les cartes abordent les techniques de piratage courantes, tout en mettant l'accent sur la création de mots de passe solides et la protection des comptes en ligne.
3. Désinformation et vérification des informations : Les joueurs sont encouragés à développer leur esprit critique en apprenant à reconnaître et à contrer la désinformation en ligne.
4. Cyberharcèlement et respect en ligne : Le jeu aborde le cyberharcèlement, favorise des discussions sur le respect en ligne et guide les participants vers des comportements constructifs et positifs. Il indique également les moyens de réagir face à ce type de situation.

1.b Objectifs pédagogiques

Les objectifs pédagogiques du jeu "Fresque des cybercitoyen·ne·s" peuvent être classés en trois catégories principales : la connaissance, la réflexion et la collaboration. Ces objectifs pédagogiques sont traités à la fois à travers le contenu du jeu, c'est-à-dire les thématiques abordées, mais aussi à travers le fonctionnement du jeu.

1.b Objectifs pédagogiques

1. Connaissance

Compréhension du monde numérique

Les joueurs seront sensibilisés aux concepts clés du cyberespace, tels que la vie privée en ligne, la sécurité des données, la désinformation, etc.

Prise de conscience

Les joueurs prendront conscience de l'impact de leurs actions en ligne sur eux-mêmes, leur entourage et la société en général. Ils seront en mesure d'identifier les comportements non sécurisés et les manifestations de cyberharcèlement.

Connaissance des menaces

Les joueurs seront informés des risques du cyberespace et des attaques les plus courantes, tels que la cyberintimidation, le vol d'identité, vols de données personnelles, mais aussi les typologies d'attaquants dont ils pourraient être victime.

Connaissance des stratégies de prévention et d'action

Les joueurs développeront une bonne compréhension des mécanismes et des outils de prévention, ainsi que des mesures de sécurité à mettre en place. Ils sauront comment réagir de manière efficace en cas de menaces, d'attaques ou d'incidents en ligne.

2. Réflexion

Pensée éthique

Les joueurs seront encouragés à réfléchir à la dimension éthique de leurs actions en ligne et à leurs conséquences.

Prise de décisions éclairées

Les joueurs apprendront à prendre des décisions éclairées et réfléchies lorsqu'ils interagissent dans le cyberespace.

Analyse critique

Les joueurs développeront leurs compétences d'analyse en évaluant les meilleures actions à réaliser pour bloquer des attaques et relever des défis liés à la citoyenneté numérique.

3. Collaboration

Travail d'équipe

Les joueurs apprendront à collaborer au sein de leurs équipes pour échanger des idées, discuter des meilleures réponses à apporter et trouver des solutions ensemble.

Communication

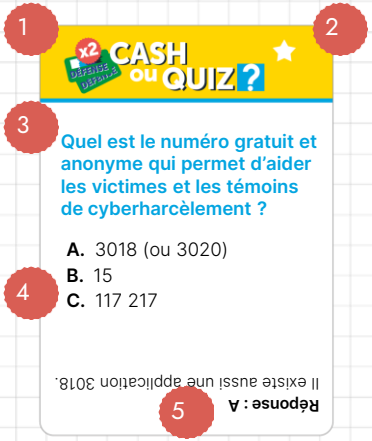
Les joueurs amélioreront leurs compétences en communication en partageant leurs opinions, en argumentant leurs points de vue et en expliquant leurs choix.

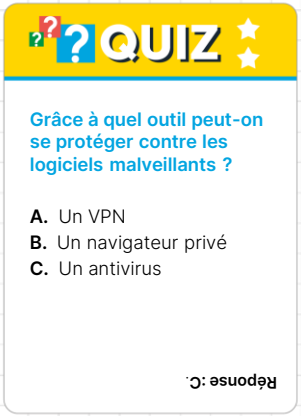
Apprentissage collectif

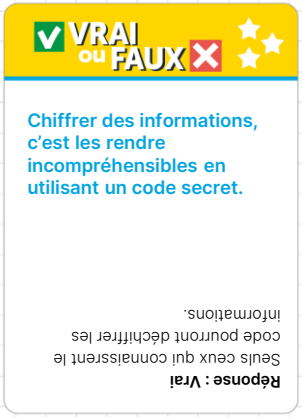
Les joueurs tireront parti des connaissances et des perspectives diverses de leurs coéquipiers pour enrichir leur compréhension globale de la citoyenneté numérique.

2. CONTENU DU JEU

2.a 90 cartes “Quiz”







1. Type de de carte : Cash ou Quiz / Quiz / Vrai ou Faux
2. Niveau de difficulté : 1, 2, 3 étoiles
3. Question
4. Propositions de réponses
5. Réponse et texte explicatif
6. Dos de la carte : identique pour toutes les cartes « Quiz »

2.b Particularités des cartes « Défense » et « Cyberattaque »

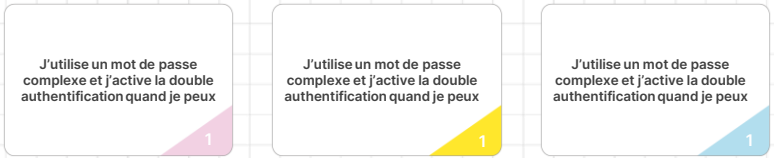
Les cartes « Défense » et les cartes « Cyberattaque » sont composées de trois lots de cartes identiques :

- 15 cartes « Défense » et 15 cartes « Cyberattaque » pour l'équipe bleue
- 15 cartes « Défense » et 15 cartes « Cyberattaque » pour l'équipe rose
- 15 cartes « Défense » et 15 cartes « Cyberattaque » pour l'équipe jaune

Tous les lots sont identiques, modulo la couleur de l'équipe. Cela permet à l'animateur de trier et ranger les cartes facilement.

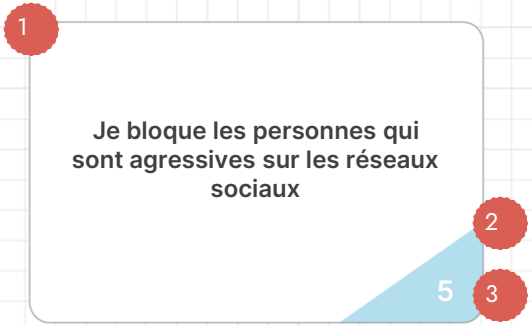
Par ailleurs, ces cartes présentent un numéro inscrit en bas à droit de la carte.

Le numéro permet à l'animateur de sélectionner ses scénarios d'attaque et d'appliquer la correction de façon simple, notamment en s'appuyant sur les propositions détaillées au Chapitre 6. Scénarios d'attaque de ce guide.
Les numéros sont identiques sur tous les lots de cartes.



Exemple pour une carte « Défense »

2.c 15 cartes “Défense” par équipe (45 cartes en tout)



1. Intitulé de la carte « Défense »
2. Couleur de l’équipe : rose, jaune ou bleu
3. Numéro de la carte
4. Dos de la carte : identique pour toutes les cartes « Défense », modulo la couleur de l’équipe

2.d 15 cartes “Cyberattaque” par équipe (45 cartes en tout)

1. Type de carte : Attaquant / Attaque / Impact
2. Intitulé de la carte « Cyberattaque »
3. Image de la carte
4. Couleur de l’équipe : rose, jaune ou bleu
5. Numéro de la carte
6. Dos de la carte : identique pour toutes les cartes « Cyberattaque » , modulo la couleur de l’équipe

3. RÈGLES DU JEU

3.a Règles du jeu

1ere partie (20 à 30 min) :

Gagner le plus de points en trouvant les bonnes réponses aux questions posées par une équipe adverse.

2ème partie (15 min) :

Gagner le plus de points en bloquant les cyberattaques avec les bonnes cartes « Défense ».

1. Première partie du jeu : Phase de « Quiz »

- Répartissez des ados en équipes de 2 à 4 personnes.

>> Maximum 3 équipes : une équipe jaune, une équipe bleue, une équipe rose (Cf Cartes défense & cyberattaques).

- Proposez-leur de choisir un nom d'équipe.
- Disposez environ 30 cartes « Quiz » sélectionnées en amont au centre de la table, face cachée.
- Chacune son tour, les équipes vont répondre à une carte « Quiz » piochée et posée par l'équipe à sa droite, en tournant dans le sens des aiguilles d'une montre. Un chrono peut être ajouté pour dynamiser le jeu.

>> L'équipe qui pose la question doit lire le type de carte, la question et les propositions de réponse (sauf pour les cartes « Cash ou Quiz »). Après concertation, l'équipe adverse répond à la question posée en choisissant aucune, une, deux ou trois bonnes réponses. L'équipe qui a posé la question doit lire la ou les bonnes réponses et le texte explicatif.

- Lorsqu'une équipe répond juste, elle gagne 1 carte « défense » piochée dans le paquet de son équipe (rose, bleu ou jaune).

>> Spécificité des cartes « Cash ou Quiz » : L'équipe qui pose la question ne lit pas les propositions de réponses et propose à l'équipe adverse de répondre « Cash ». Si l'équipe choisit le mode « Cash » et a au moins une réponse juste, elle gagne 2 cartes « défense ». Sinon, elle retombe sur un scénario classique de carte « Quiz ».

- Au bout de 30 min de jeu, la première phase s'arrête.
- Comptez les « points » - Chaque carte « Défense » gagnée rapporte 1 point.

2. Deuxième partie du jeu : Phase « Scénario d'attaque »

- Proposez aux équipes de disposer toutes les cartes « Défense » devant elles (15 cartes en tout), même celles qu'elles n'ont pas gagnées lors de la précédente phase.
- Disposez une séquence d'attaque identique devant chacune des équipes (vous pouvez vous aider du guide animateur, Chapitre 6. Scénarios d'attaque).
- Les équipes doivent réfléchir aux bonnes cartes « Défense » à utiliser pour bloquer l'attaque et les disposer sous la séquence d'attaque.

>> Seules les cartes défenses ayant un rapport direct avec l'attaque rapportent des points.

- Lorsqu'elles ont terminé (il peut être nécessaire d'utiliser un chrono d'environ 10 min), corrigez avec chacune des équipes ou faites une correction collective selon le temps dont vous disposez.
- Comptez les points - Chaque carte « Défense » correctement utilisée rapporte 1 point. Chaque carte « Défense » inutile fait perdre 1 point. Vous pouvez également vous aider de notre correction dans le Chapitre 6. Scénarios d'attaque.

- Additionnez les points des deux phases de jeu :

L'équipe qui a le plus de points a gagné !

3.b Déroulement d'une session

Vous trouverez sur le slide d'après un exemple type de déroulé d'ateliers pouvant être mené dans un contexte scolaire.

Il est cependant possible de l'adapter, par exemple :

- En passant l'intégralité de l'atelier sur la partie « Quiz » et de réserver la partie « Scénario d'attaque » pour un autre cours ;

- En passant moins de temps sur le Quiz et en traitant deux scénarios d'attaque ;

- En proposant une activité pratique type paramétrage de compte, changement de mot de passe, vérification des sources d'informations liées à un évènement… En lien avec la ou les thématiques choisies.

Nous vous recommandons de ne pas faire durer le jeu plus d'une heure pour maintenir la concentration des élèves.

Le déroulement d'une séance est détaillé dans le chapitre 5. Animer une Fresque

3.b Déroulement d'une session

Introduction
[10 min]

- Constitution des équipes et choix du nom
- Présentation de l'atelier (objectifs, thématique abordées, phases de jeux, etc…)

Explication des règles
[5 min]

- Projeter les règles du jeu au tableau avec la présentation disponible dans les ressources
  Explication des règles aux participants

Phase de jeu
[20 – 35 min]

- Quiz
- Cyberattaque
- Les deux

Fin de l'activité
[10 – 15 min]

- Annonce de l'équipe vainqueur
- Tour de table pour avoir des retours sur l'atelier
- Remplir le questionnaire

Après l'atelier
[5min]

- Tri des cartes et rangement du jeu
- Rangement de l'espace de jeu

3.c Compter les points

1. Première partie du jeu : Phase de « Quiz »

- Il y a plusieurs types de question :
  - Vrai ou faux :
    - Un point gagné par bonne réponse.
  - Quiz :
    - Zéro, une, deux ou trois bonnes réponses possibles ;
    - Toutes les bonnes réponses doivent être données pour gagner le point ;
    - Un point gagné par bonne réponse.
  - Cash ou quiz (1 ou 2 points gagnés) :
    - Une, deux ou trois bonnes réponses possibles ;
    - Un point gagné si réponse type quiz, c'est-à-dire avec les propositions de réponses ;
    - Deux points gagnés si l'équipe répond cash, c'est-à-dire sans les propositions de réponses ;
    - Une seule bonne réponse peut être donnée pour gagner les deux points si réponse cash.
- Les points gagnés peuvent être matérialisés par des cartes « Défense » que les équipes piochent au fil de la partie.

2. Deuxième partie du jeu : Phase « Cyberattaque »

- L'animateur positionne une séquence d'attaque (cf Chapitre 6. Scénarios d'attaque)
- Les équipes ont 10 minutes pour échanger et positionner les bonnes cartes « Défense » correspondant au scénario d'attaque :
  - Mauvaise carte et mauvaise justification : -1 point
  - Mauvaise carte mais justification cohérente : 0 point
  - Bonne carte et bonne justification : 1 point

4. SÉQUENCE PÉDAGOGIQUE

4. Construire une séquence pédagogique

Pour que le jeu se joue dans les meilleures conditions et pour maximiser l'atteinte de objectifs pédagogiques de la Fresque, il est fortement conseillé de sélectionner en amont les cartes Quiz et le scénario d'attaque associé en fonction du niveau des élèves et des thématiques que l'on souhaite aborder.

En effet, si vous disposez l'intégralité des 90 cartes Quiz devant les élèves, les niveaux (1, 2 ou 3 étoiles) des cartes varieront d'une équipe à l'autre et les élèves risquent de se trouver en situation d'échec face à des cartes dont ils ne maîtrisent pas les notions.

4. Construire une séquence pédagogique

1. Sélectionner les thématiques

En fonction des thématiques que vous souhaitez aborder, vous pouvez sélectionner les questions que vous placerez devant les élèves lors de la première partie du jeu et définir un scénario d'attaque associé.

Vous pourrez vous appuyer sur le document nommé « Guide animateur – Récapitulatif des cartes » pour trier les cartes en fonction de la thématique choisie et identifier le bon scénario d'attaque grâce au Chapitre 6. Scénarios d'attaque.

2. Sélectionner le niveau des cartes

Une fois la thématique choisie, vous pourrez sélectionner le niveau des cartes en fonction de la connaissance des élèves sur la thématique abordée.

De même, le niveau de chacune des cartes est indiqué dans le document « Guide animateur – Récapitulatif des cartes » fourni en annexe du guide animateur.

3. Exemple d'une séquence pédagogique

Session	Classe	Thématiques abordées	Sélection de 30 cartes Quiz	Scénario d'attaque	Cartes « Défense »
1	6e	Cyberharcèlement & mot de passe	Cartes de niveau 1 sur les thématiques abordées	3 -> 6 -> 7 -> 12	7 - 15 - 9 - 1
2	6e	Cyberharcèlement & vie privée	Cyberharcèlement : Sélection de cartes de niveau 1 & 2 Vie privée : Cartes niveau 1	2 -> 6 -> 14	7 - 8 - 9 - 10 - 13
3	5e	Piratage, mot de passe & équipement	Cartes de niveau 1 sur les thématiques abordées	1 -> 5 -> 9 -> 13	4 - 2 - 3 - 12 - 11

3. Exemple d'une séquence pédagogique

Session	Classe	Thématiques abordées	Sélection de 30 cartes Quiz	Scénario d'attaque	Cartes « Défense »
4	5e	Révision des acquis des sessions 1 à 3	Cartes de niveaux 1 & 2, sur les thématiques cyberharcèlement, piratage, mot de passe, équipement & vie privée	2 -> 5 -> 7 -> 12	4 - 11 - 15 - 1 - 7
5	4e	Désinformation, vie privée & équipement	Désinformation : Cartes de niveau 1 & 2 Vie privée et équipement : Cartes de niveau 2 & 3	1 -> 9 -> 4 -> 11	2 - 3 - 7 - 11 - 15

3. Exemple d'une séquence pédagogique

Session	Classe	Thématiques abordées	Sélection de 30 cartes Quiz	Scénario d'attaque	Cartes « Défense »
6	4e	Piratage, équipement & mot de passe	Cartes de niveaux 2 & 3 sur les thématiques abordées	1 -> 10 -> 11 -> 12	14 - 15 - 1 - 7 - 11
7	3e	Toutes les thématiques	Sélection de cartes de niveaux 2 & 3 sur l'ensemble des thématiques	Au choix	X
8	3e	Toutes les thématiques	Sélection de cartes de niveaux 2 & 3 sur l'ensemble des thématiques	Au choix	X

5.
ANIMER UNE FRESQUE

5.a Généralité sur le rôle de l'animateur

Lors de la création de cette fresque, nous avons voulu que tout le monde puisse animer une session : il suffit de lire ce guide et de suivre les cartes : aucune connaissance en cybersécurité n'est préalablement requise. En effet, l'animateur n'a pas le rôle d'enseigner dans ce cadre, mais bien de faire respecter le cadre du jeu.

5.a Généralité sur le rôle de l'animateur

L'animateur de l'atelier a un ensemble de responsabilités clés :

1. Préparer la session (Cf 5b. Avant l'Atelier)
2. Accueillir et gérer le groupe (Cf 5c. Pendant l'Atelier)
3. Guider et faciliter la session de sensibilisation :

- Répondre aux questions et définir les termes si besoin à l'aide du glossaire ;
- Assurer le respect des principes du jeu (respect mutuel, atmosphère positive...) ;
- Encourager les équipes et rester à l'écoute ;
- Assurer le bon respect du temps.

4. Conclure et réaliser le bilan de l'atelier (Cf 5c. Pendant l'atelier et 5d. Après l'Atelier)

- Conclusion à la fin de session avec les participants ;
- Rangement du jeu ;
- Déclaration de la session via le QR Code sur la boite.

5.b Avant l'atelier

Si c'est votre premier atelier, nous vous recommandons de récupérer, voire d'imprimer si vous le juger nécessaire, le Tuto Express : vous y trouverez l'ensemble des documents pour animer une séance « clef en main ». Pour rappel, ce guide n'a pas vocation à être imprimé.

En amont de l'atelier :

1. Trouvez des personnes disponibles et formées pour vous aider à encadrer : nous recommandons un animateur par jeu (soit pour 12 participants maximum).
2. Définissez votre séquence pédagogique selon les connaissances et la maturité des participants et les notions que vous souhaitez aborder. Pour cela, vous pouvez vous aider de la section 4. Séquence Pédagogique de ce guide. Pour sélectionner les cartes, vous avez également la possibilité de sélectionner directement les cartes en vous appuyant sur le document Excel fourni avec ce guide « Guide animateur – Récapitulatif des cartes ».
3. Vérifiez que vous disposez du matériel nécessaire :
   - Jeu de la fresque (1 jeu pour 12 élèves au maximum) ;
   - La version « Tuto express » du Guide animateur ;
   - Un papier et un stylo pour faire le compte des points ;
   - En option : Un chrono (montre, sablier, téléphone) pour chronométrer et dynamiser le jeu.

5.c Le jour de l'atelier

Le jour de l'atelier, voici les consignes pour préparer la salle avant le début de la séance de sensibilisation :

1. Une table dispose d'un jeu « Fresque des cybercitoyen·ne·s » et d'un animateur :
   - Si vous avez plusieurs groupes, c'est-à-dire plus de 12 jeunes en même temps, vous devrez créer plusieurs tables de jeux ;
   - Si vous avez un groupe de 12 participants ou moins, une seule table de jeu sera suffisante.

2. Configurez l'espace de jeu en créant idéalement des îlots adaptés au nombre de joueurs. Si vous êtes plusieurs animateurs, répartissez-vous dans les différents espaces de manière à ce que chacun soit responsable d'une zone de jeu. Une session peut être relativement bruyante : essayez tant que possible d'espacer les îlots les uns des autres.

3. Placez les cartes « Quiz » sélectionnées pour la séance au centre de chacun des îlots :
   - Réservez les paquets de cartes « Défense » que vous distribuerez au début de la partie ;
   - Réservez les scénarios d'attaque que vous avez préparés pour la deuxième partie de la séance.

1. Introduction

Cette première phase d'introduction peut être réalisée avec l'ensemble des groupes, par exemple en classe entière, avant de répartir les élèves par groupe de 12 maximum. Transmettez les informations essentielles aux participants :

- Présentez-vous si c'est la première fois que vous rencontrez ce public ;
- Expliquez l'objectif de cette séance de sensibilisation ;
- Décrivez brièvement le déroulé de la séance et donnez les durées des deux parties (les règles seront expliquées après) ;
- Explicitez ce que les joueurs sont autorisés à faire (parler librement, s'entraider, donner des définitions, etc…)

Afin de briser la glace, vous pouvez également poser quelques questions aux jeunes ou faire un sondage à main levée :

- Qu'est ce que c'est que pour vous la cybersécurité ?
- Qu'est ce que pour vous un hackeur ou une hackeuse ?
- Qui ici a déjà eu un virus informatique ?
- Qui a déjà eu un compte piraté ?
- Qui a déjà reçu une tentative d'escroquerie par message ?

2. Création des groupes et des équipes

Répartissez les élèves en groupe : chaque groupe sera affecté à une table de jeu avec son animateur.
Puis répartissez les élèves en équipes de 4 joueurs maximum. Ici plusieurs possibilités, à vous de déterminer le plus appréciable :

- Vous pouvez laisser les jeunes se mettre en équipes comme ils veulent ;
- Vous pouvez répartir les participants en équipes vous-même.

Dans le second cas, cela peut permettre d'homogénéiser le niveau des équipes et de briser certaines dynamiques afin de rendre le groupe plus facile à encadrer, cependant cela peut également générer de la frustration.

Afin de renforcer l'implication, vous pouvez demander à chaque équipe de se trouver un nom.

3. Explication des règles

Expliquez en premier le déroulement global du jeu :

- Le jeu se déroule en deux phases : la première c'est un Quiz, auquel ils répondront par équipe, et dans la seconde ils devront repousser une cyberattaque ;
- Durant chaque phase, les équipes pourront marquer des points ;
- L'équipe avec le plus de points à l'issue des deux phases aura gagné.

Puis expliquez les règles du Quiz plus en détail (Cf Chapitre 3.a Règles du jeu). Il n'est pas nécessaire d'expliquer dès à présent les règles du scénario car cela pourra créer de la confusion.

Vous pouvez désigner un maître du temps qui aura pour tâche de veiller au respect des différents temps de jeu ou bien le faire vous-même.

4. Mise en place du quiz

Cf Chapitre 3.a Règles du jeu

5. Conseils d'animation (1/2)

Durant la phase de Quiz, le jeu est fait pour être cogéré par les joueurs, voici cependant un ensemble de conseils pour vous permettre d'animer au mieux l'activité :

- N'hésitez pas à circuler entre les différentes équipes afin de veiller au bon déroulement du jeu ;
- Assurez-vous que les échanges se déroulent bien entre les équipes ;
- Assurez-vous que chaque équipe prend le temps de réfléchir et d'argumenter avant de donner sa réponse ;
- Après qu'ils ont répondu à une question, vous pouvez leur demander s'ils connaissaient le sujet ou bien si cela leur était déjà arrivé afin de renforcer l'implication et l'interactivité. Cependant il ne faut pas trop en abuser au risque de diminuer la prise d'autonomie et le rythme du jeu ;
- Si vous voyez qu'une question ou qu'un terme n'est pas compris, vous pouvez le reformuler ou donner la définition. Le mieux reste toutefois de demander à un volontaire d'essayer d'expliciter les notions avec ses propres mots et/ou de donner un exemple pour ses camarades ;

5. Conseils d'animation (2/2)

Durant la phase de Quiz, le jeu est fait pour être cogéré par les joueurs, voici cependant un ensemble de conseils pour vous permettre d'animer au mieux l'activité :

- En règle générale, plus vous vous appuierez sur leurs expériences personnelles plus ils seront impliqués dans l'activité ;
- Observez les équipes qui pourraient potentiellement se démotiver et n'hésitez pas à les voir pour les encourager ;
- A une minute de la fin du temps alloué à la phase de Quiz, faite une annonce pour dire que cela sera le dernier tour.

5. Fin du quiz & mise en place de l'attaque

Après avoir réclamé l'attention et mis fin à la partie « Quiz », vous pouvez faire une annonce des scores.

Puis expliquez les règles du Scénario d'attaque (Cf Partie 3.a Règles du jeu).

Demandez ensuite à chaque équipe de disposer toutes les cartes « Défense » devant eux (15 cartes par équipe). Pendant ce temps, disposez le scénario d'attaque préalablement choisi en relation avec la thématique abordée lors du « Quiz » devant chacune des équipes, et expliquez ce scénario. Pour une meilleure immersion, nous vous recommandons de présenter le scénario de façon romancée et de ne pas juste lire les cartes.

Par exemple : Une cyberharceleuse réussit à trouver ton mot de passe et elle a donc accès à tous tes comptes (Insta, Snap, ENT...). Elle va en profiter pour se faire passer pour toi, c'est-à-dire « usurper ton identité », pour envoyer des messages à tes amis ou à des profs. Qu'est-ce que vous pouvez utiliser comme carte « Défense » pour empêcher que cela se produise ? Ou pour réagir si c'est trop tard ?

Rappelez que toutes les cartes « Défense » qui n'ont pas de rapport direct avec l'attaque pourront leur faire perdre des points.

6. Correction de la deuxième partie

Pour corriger le scénario, vous pouvez :

- Faire une correction individuelle par équipe ;
- Vous appuyer sur une équipe, par exemple celle qui a posé le plus de cartes « Défense », pour faire la correction générale.

7. Fin de l'activité

La fin de l'activité doit être un moment de conclusion du jeu et d'un retour au calme mais également permettre d'avoir un retour des participants sur leur expérience. Pour cela nous vous proposons de :

1. Demander le tri et le rangement des cartes par couleur, c'est-à-dire par équipe ;
2. Faire l'annonce de l'équipe vainqueur et la féliciter ;
3. Faire un tour de table pour recueillir les impressions.

5.d Pendant l'atelier

Selon le temps disponible et le nombre de participants, vous pouvez faire un tour de table où chaque participant s'exprime à tour de rôle.

Par exemple : Chaque participant dit une notion qu'il a apprise, un élément du jeu qu'il a aimé et un élément qu'il a moins aimé.

Si le groupe est trop important ou que vous êtes à court de temps, vous pouvez faire par sondage à main levée :

- Qui va changer son mot de passe en rentrant ?
- Qui n'a pas aimé l'activité ? / Qui a bien aimé ? / Qui a beaucoup aimé l'activité ?
- Qui n'a rien appris de nouveau ? Qui a un peu appris ? Qui a beaucoup appris ?

Cette phase est très importante pour l'apprentissage : elle permet de fixer les notions apprises lors de la séance et de se questionner sur ses pratiques.

5.e Après l'atelier

Après l'atelier, chaque animateur est invité à scanner le QR Code qui se trouve sur le dos de la boite de jeu pour déclarer la session en remplissant les informations suivantes :

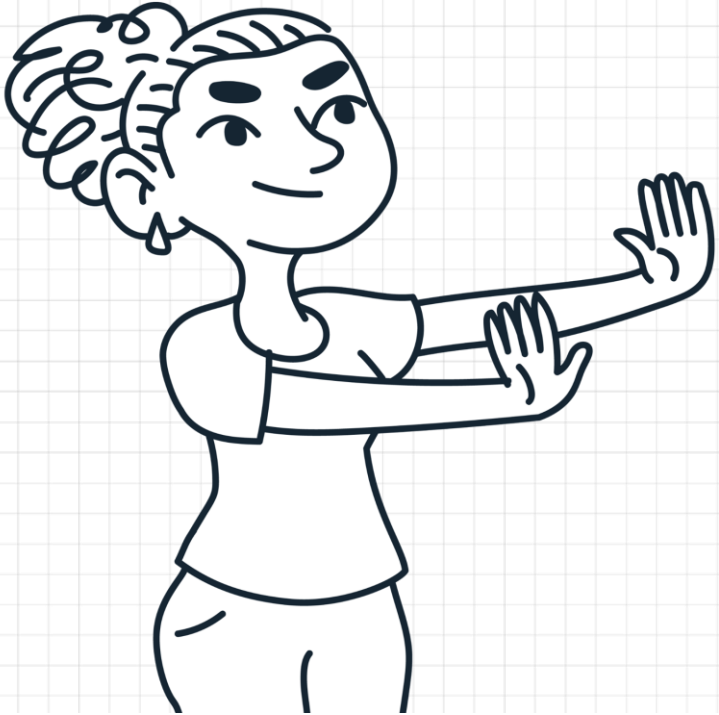
- Le nombre de participants et d'animateur ;
- Age moyen (9-10 ans ; 11-12 ans; 13-14 ans ; 15-16 ans) ;
- Le numéro de département ;
- Evaluation de la session selon l'animateur ;
- Des axes d'amélioration identifiés.

Aucune des sections n'est obligatoire. Cependant, il est dans notre intérêt à tous que vous fassiez des retours sur votre expérience et sur celle des participants.

En effet, ce jeu ne pourra continuer d'exister et de s'améliorer qu'avec votre aide.

6. SCÉNARIOS D'ATTAQUE

6. Scénarios d'attaque



Exemples de scénario clef en main

Vous trouverez ci-dessous des propositions de scénarios d'attaque classés par type d'attaquants. Vous pouvez également créer vos propres scénarios en sélectionnant des cartes « Attaquant », « Attaque » et « Impact ».

6.a Hackeur.se

Scénario	Cartes « Cyberattaque »	Cartes « Défense »
Un hackeur propage un virus sur ton téléphone qui supprime toutes les données enregistrées	1 -> 9 -> 13	2 - 3 - 12 - 11
Une hackeuse propage un virus sur ton téléphone ou ton ordinateur qui lui permet d'avoir accès à tes comptes et elle revend tes données sur le dark web.	1 -> 9 -> 4 -> 11	2 - 3 - 7 - 11 - 15
Un hackeur pirate un réseau wifi public. Comme il voit tout ce qui transite sur le réseau, il capte ton mot de passe et vole l'accès à tes comptes. Alors, il décide de revendre tes données sur le dark web.	1 -> 10 -> 4 -> 11	14 - 15 - 1 - 7 - 11
Même scénario que ci-dessus, mais cette fois-ci le hackeur décide de te faire chanter : par exemple, il te demande de l'argent pour te rendre tes accès à tes comptes sur les réseaux sociaux.	1 -> 10 -> 4 -> 14	14 - 15 - 1 - 8

6.a Hackeur.se

Scénario	Cartes « Cyberattaque »	Cartes « Défense »
Un hackeur pirate un réseau wifi public. Comme il voit tout ce qui transite sur le réseau, il peut capter le mot de passe quand tu le tapes sur internet. Avec ton mot de passe, il récupère tes accès à tes comptes et usurpe ton identité (= il se fait passer pour toi).	1 -> 10 -> 11 -> 12	14 - 15 - 1 - 7 - 11
Un hackeuse t'envoie un mail de phishing. Tu cliques le lien dans le mail et cela installe un virus sur ton appareil qui supprime tes données.	1 -> 5 -> 9 -> 13	4 - 2 - 3 - 12 - 11
Un hackeuse t'envoie un mail de phishing. Tu cliques le lien dans le mail et cela installe un virus sur ton appareil et revend tes données sur le dark net.	1 -> 5 ->9 -> 4 -> 11	4 - 2 - 3 - 7 - 11 - 15

6.b Cyberprédateur.trice

Comme vous pourrez le constater, les attaques des cyberharceleurs et cyberprédateurs sont quasiment similaires. Ce qui diffère c'est le type d'attaquant et son objectif final : le prédateur attend généralement quelque chose d'intime en échange de son « attaque ».

Choisissez l'une ou l'autre selon la thématique que vous souhaitez aborder avec votre public.

Scénario	Cartes « Cyberattaque »	Cartes « Défense »
Une cyberprédatrice se renseigne sur toi, par exemple via les réseaux sociaux et elle te fait chanter : par exemple, elle te demande de lui envoyer des photos intimes. En échange, elle te fait croire qu'elle ne va pas envoyer des informations personnelles sur toi à tes amis ou tes parents.	2 -> 6 -> 14	7 - 8 - 9 - 10 - 13

6.b Cyberprédateur.trice

Scénario	Cartes « Cyberattaque »	Cartes « Défense »
Un cyberprédateur se renseigne sur toi, par exemple sur les réseaux sociaux, et te harcèle par messages ou à l'école.	1 -> 8 -> 15	7 - 8 - 9 - 10 - 13
Un cyberprédateur t'envoie un message de phishing afin de trouver ton mot de passe. Avec tes comptes, il se fait passer pour toi (= usurpe ton identité) pour obtenir des rendez-vous avec tes amis.	2 -> 5 -> 7 -> 12	4 - 11 - 15 - 1 - 7
Une cyberprédatrice se renseigne sur toi et avec les informations qu'elle a obtenues, elle trouve ton mot de passe et usurpe ton identité. Elle contacte tes amis et tente d'obtenir des photos intimes.	2 -> 6 -> 7 -> 12	7 - 15 - 9 - 1

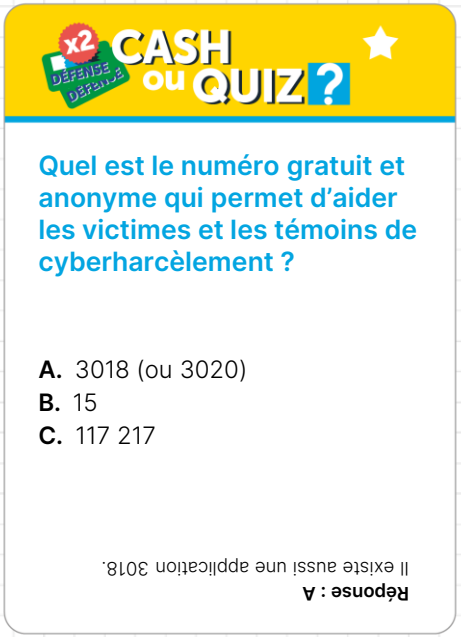
6.c Harceleur.se

Scénario	Cartes « Cyberattaque »	Cartes « Défense »
Un cyberharceleur se renseigne sur toi sur internet. Avec les infos qu'il trouve, il décide de faire chanter : par exemple, il te demande de faire ses devoirs. En échange, il te dit qu'il n'enverra pas certaines photos de toi à toute la classe.	3 -> 6 -> 14	7 - 8 - 9 - 10 - 13
Une cyberharceleuse te trouve sur les réseaux sociaux et t'envoie des messages injurieux	3 -> 8 -> 15	7 - 8 - 9 - 10 - 13
Un cyberharceleur devine ton mot de passe et se fait passer pour toi sur les réseaux sociaux ou sur l'ENT.	3 -> 7 -> 12	4 - 11 - 15 - 1 - 7
Une cyberharceleuse se renseigne sur toi, trouve ton mot de passe et te fait du chantage ou te menace de diffuser des infos persos sur toi.	3 -> 6 -> 7 -> 14	4 - 11 - 15 - 1 - 7

7.

CARTES QUIZ, SOURCES ET EXPLICATIONS

7.a
Cyberharcèlement



Explications

Lorsque l’on est victime ou témoin de harcèlement, il est important d’en parler.

Le 3018, un numéro gratuit, anonyme et confidentiel est joignable 7 jours sur 7, de 9 h à 23 h, par téléphone, sur 3018.fr par tchat en direct, sur les messageries des réseaux sociaux et via l’application 3018.

L’équipe du 3018 dispose de procédures de signalement accélérées pour faire supprimer les comptes ou les contenus préjudiciables en quelques heures auprès de plus de 20 plateformes, réseaux sociaux et messageries. Elle peut aussi conseiller les victimes dans leurs démarches.

Source : https://e-enfance.org/numero-3018/besoin-daide/

QUIZ

Si quelqu’un envoie des messages d’insultes sur les réseaux sociaux, que faut-il faire ?

A. Bloquer cette personne
B. Garder des preuves
C. Prévenir un adultes

Réponse : A, B et C

Explications

Les messages d’insultes sont considérés comme du harcèlement. On doit pouvoir en parler librement à un adulte qui prendra la situation au sérieux, sans culpabiliser la victime.

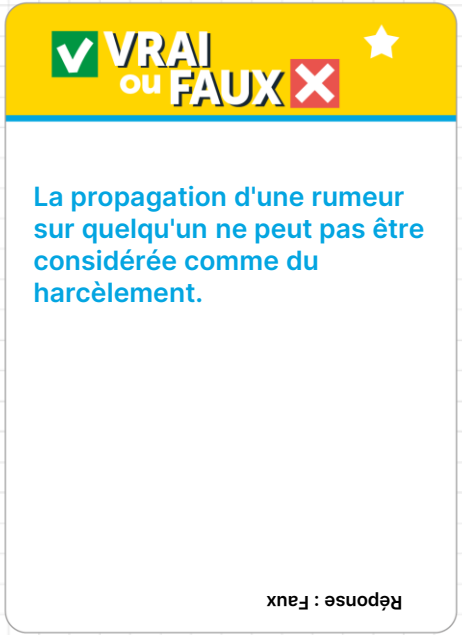
Le premier réflexe est de conserver des preuves, par exemple en prenant des captures d’écran des messages. Elles serviront au dossier judiciaire si la victime décide de porter plainte.

Ensuite, il est possible de signaler les messages, pour stopper la diffusion du contenu, et de bloquer la personne pour qu’elle ne puisse plus identifier la victime, réagir et commenter les publications.

Retrouvez d’autres conseils sur le lien source ci-dessous.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/que-faire-en-cas-de-cyberharcelement-ou-harcelement-en-ligne

7.a Thématique “Cyberharcèlement” - Niveau 1



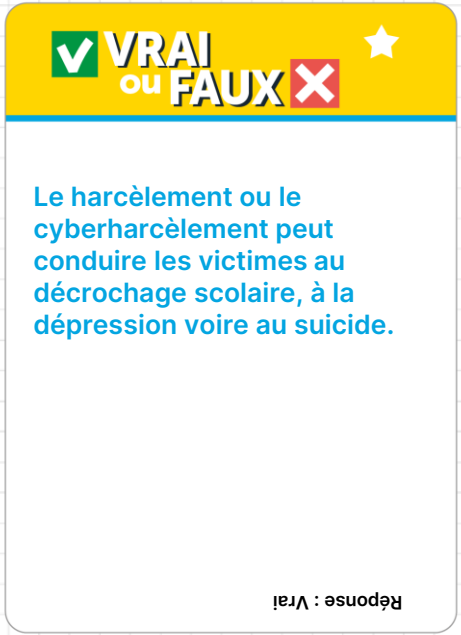
Explications

Le harcèlement peut prendre plusieurs formes :

- les intimidations, insultes, moqueries ou menaces
- la propagation de rumeurs
- le piratage de comptes et l’usurpation d’identité digitale
- la création d’un sujet de discussion, d’un groupe ou d’une page sur un réseau social à l’encontre d’un camarade de classe
- la publication d’une photo ou d’une vidéo de la victime en mauvaise posture
- Le sexting non consenti
- Le chantage à la webcam

Source : https://e-enfance.org/informer/cyber-harcelement/

7.a Thématique “Cyberharcèlement” - Niveau 1



Explications

Le harcèlement ou cyberharcèlement peut entraîner des conséquences très graves.

Il est important de rappeler que la victime n’est pas responsable de son harcèlement ou cyberharcèlement et de l’aider à s’en sortir.

Aucune tenue, aucune parole ou aucun comportement de la part de la victime ne justifie le harcèlement, qui est interdit et puni par la loi.

Source : https://www.cybermalveillance.gouv.fr/medias/2022/09/230422_FicheReflexe_Cyberharcelement.pdf

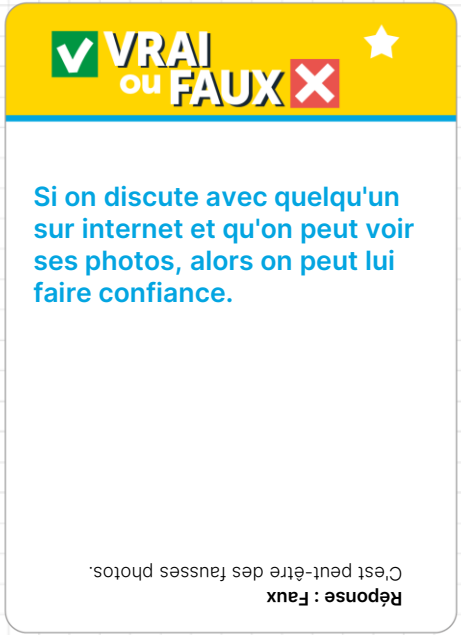
Explications

Liker un commentaire insultant c’est encourager la personne qui harcèle et valider son comportement. En réagissant ainsi ou en diffusant des propos de harceleurs, un individu tend à aggraver la situation et son impact sur la victime. Il est donc complice.

De plus, le fait de partager ou de donner de la visibilité à ce type de propos/photos est susceptible d’engager sa responsabilité devant la loi, même si on est mineur.

Même réagir à une publication dans l’intention d’aider la victime n’est pas une bonne idée, car il y a de fortes chances d’empirer la situation.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/que-faire-en-cas-de-cyberharcelement-ou-harcelement-en-ligne



Explications

Une personne malintentionnée peut facilement usurper l’identité de quelqu’un d’autre ou se créer une fausse identité sur internet.

Il est nécessaire de faire attention à qui on parle ou on se confie, d’être vigilant face aux demandes de connexion venant d’inconnus.

Une des techniques connues des cyber pédophiles, appelée grooming, consiste à mettre le jeune en confiance, souvent en se faisant passer pour quelqu’un du même âge, en lui apportant une écoute bienveillante, en le valorisant, en lui offrant des cadeaux, etc. L’objectif du prédateur est de lier un rapport intime avec le jeune pour le soumettre à des abus sexuels ou à du chantage en vue d’une exploitation sexuelle.

Source : https://www.passeportsante.net/famille/adolescence?doc=grooming-cette-pratique-dangereuse-nos-enfants

QUIZ

Les cyberharceleurs peuvent être poursuivis par la justice voire aller en prison, même si :

A. Ils utilisent un pseudo
B. Ils sont mineurs
C. Ils connaissent bien la victime

Réponse : A, B et C

Explications

Le cyberharcèlement est puni jusqu’à 2 ans d’emprisonnement et 30 000€ d’amende et ce, même si l’auteur est mineur. Si la victime est mineure, les peines peuvent même être renforcées à 5 ans d’emprisonnement et 75 000€ d’amende.

A noter : l’infraction est constituée qu’elle soit le fait d’une seule personne ou d’un groupe de personnes, même si chacune de ces personnes n’a pas agi de façon répétée.

Sources :
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/que-faire-en-cas-de-cyberharcelement-ou-harcelement-e-ligne
https://www.service-public.fr/particuliers/vosdroits/F32239

QUIZ

Que peut-on faire si une photo gênante de soi a été publiée sur un réseau social ?

A. Demander à la personne qui l’a publiée de l’effacer
B. Demander directement au réseau social de l’effacer
C. Prendre une capture d’écran pour garder une preuve

Réponse : A, B et C

Explications

Les contenus illicites peuvent être signalés auprès des plateformes sur lesquels ils sont présents afin de les faire supprimer, d’autant plus s’ils concernent une personne mineure.

Quelques exemples de liens de signalement pour les principaux réseaux sociaux : Instagram, Snapchat, Discord, TikTok, WhatsApp, YouTube, Facebook, Twitter. Dans un contexte de harcèlement, il est important de garder une preuve au cas où la victime déciderait de porter plainte.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/que-faire-en-cas-de-cyberharcelement-ou-harcelement-en-ligne#definition-cyberharcelement

QUIZ

Un élève subit des réflexions moqueuses régulièrement, et elle semble en souffrir. Que faut-il faire ?

A. L’ignorer, car ça ne me regarde pas
B. Prévenir un adulte en qui j’ai confiance
C. Appeler le 3018

Réponse : B et C
Il ne faut surtout pas rester sans réaction.

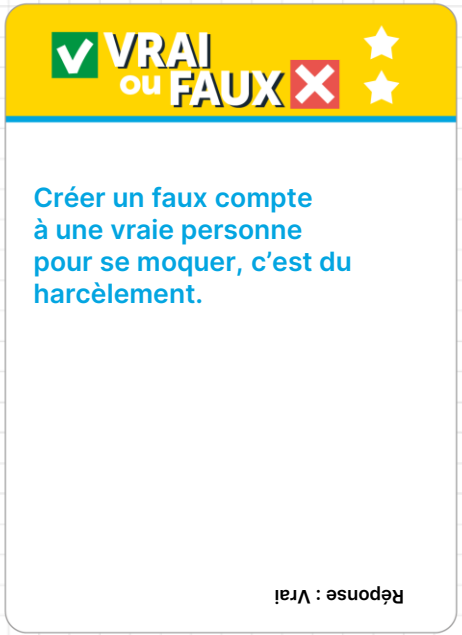
Source : https://e-enfance.org/informer/cyber-harcelement/

Explications

Lorsque l’on est victime ou témoin de harcèlement, il est important d’en parler à un adulte qui prendra la situation au sérieux et réagira.

On peut également contacter le 3018, un numéro gratuit, anonyme et confidentiel est joignable 7 jours sur 7, de 9 h à 23 h, par téléphone, sur 3018.fr par tchat en direct, sur les messageries des réseaux sociaux et via l’application 3018.

L’équipe du 3018 dispose de procédures de signalement accélérées pour faire supprimer les comptes ou les contenus préjudiciables en quelques heures auprès de plus de 20 plateformes, réseaux sociaux et messageries. Elle peut aussi conseiller les victimes dans leurs démarches.

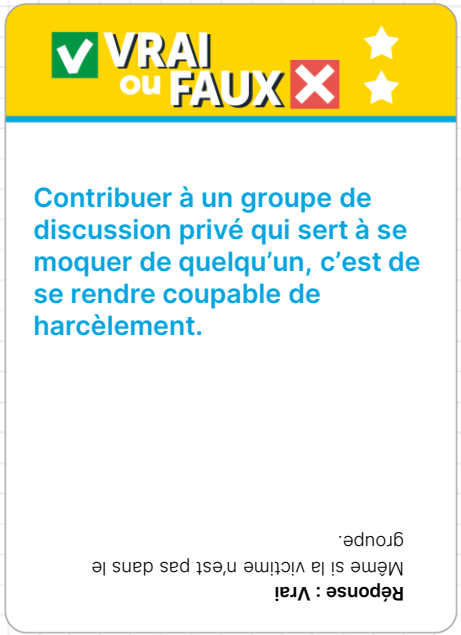


Explications

Il s’agit d’une usurpation d’identité, ce qui est considéré comme du harcèlement.

Selon le Code pénal, le fait d’usurper l’identité d’un tiers ou de faire usage d’une ou plusieurs données de toute nature permettant de l’identifier en vue de troubler sa tranquillité ou celle d’autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d’un an d’emprisonnement et de 15 000 euros d’amende.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/que-faire-en-cas-de-cyberharcelement-ou-harcelement-en-ligne#definition-cyberharcelement



Explications

La création ou la participation à un sujet de discussion, un groupe ou une page sur un réseau social à l’encontre d’un camarade de classe est considéré comme du cyberharcèlement, même si la personne concernée n’est pas dans le groupe et ne voit pas les messages.

Le fait de l’exclure et de parler de cette personne négativement de façon répétée constitue déjà du harcèlement.

Source : https://www.education.gouv.fr/non-au-harcelement/qu-est-ce-que-le-cyberharcelement-325358

QUIZ

Quel pourcentage des jeunes âgés de 6 à 18 ans ont déjà été choqués par des contenus rencontrés involontairement sur internet ?

A. 9%
B. 14%
C. 30%

Réponse : C
Les chiffres varient selon l'âge : 22% en primaire, 29% au collège et 40% au lycée.

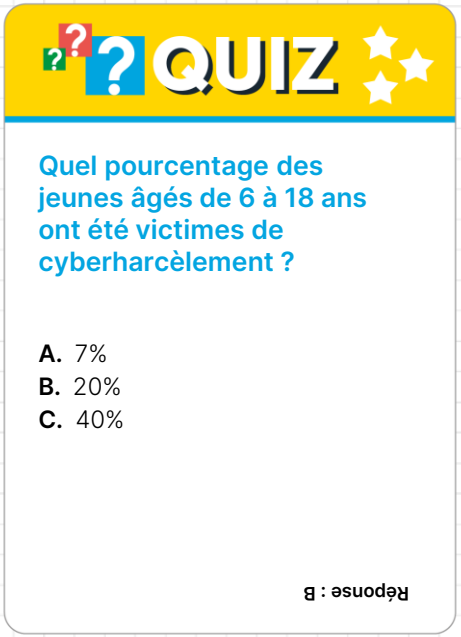
Explications

Le cyberharcèlement n’est qu’un aspect des violences numériques, qui peuvent prendre plusieurs formes :

- Exposition à des contenus choquants,
- Défis sur les réseaux,
- Cyber pédophilie,
- Arnaques en ligne…

Les contenus choquants sur internet peuvent être de nature pornographique ou d’autre nature, c’est-à-dire des contenus haineux, racistes, des violences physiques, des tortures…

Source : Étude Audirep/Association e-Enfance, Juin 2021 => https://e-enfance.org/wp-content/uploads/2021/11/Audirep-X-e-Enfance.pdf



Explications

Ce chiffre est issue d’une étude datant de 2021. Une nouvelle étude a été réalisée en 2023, et les chiffres sont éloquents : 25% des élèves de collèges ont été confrontés au cyberharcèlement (les chiffres de 2021 ne sont pas spécifiques par classe d’âge).

De plus, selon l’étude de 2021, près d’1 enfant sur 2 a été confronté de près ou de loin à au moins une expérience de cyberharcèlement, directement ou indirectement (victime, témoin, participant ou auteur).

Sources :
Étude Audirep/Association e-Enfance, Juin 2021 => https://e-enfance.org/wp-content/uploads/2021/11/Audirep-X-e-Enfance.pdf
Étude Audirep/Association e-Enfance, Juin 2023 => https://e-enfance.org/wp-content/uploads/2023/10/20231017_Infographie_Etude-Caisse-dEpargne_e_Enfance_Cyberharcelement.pdf

Pour aller plus loin - Cyberharcèlement

Des informations concernant la politique de lutte contre le harcèlement à l’école :

- Ministère de l’éducation nationale I pHARe : un programme de lutte contre le harcèlement à l’école

Des conseils pour faire face au cyberharcèlement :

CNIL I Faire face au cyberharcèlement

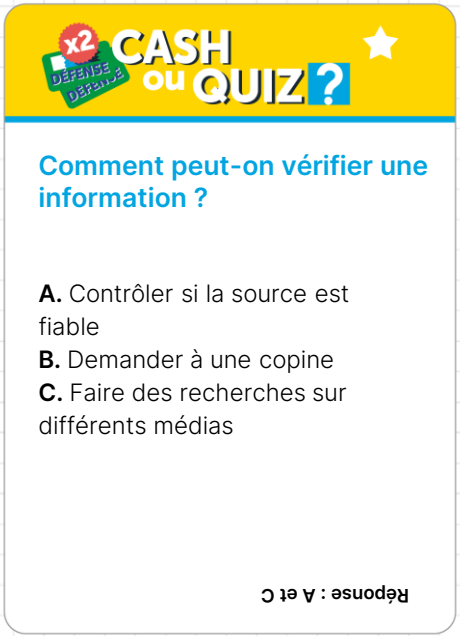
Fondation Enfance I Réagir en tant que professeur ou chef d’établissement

Pour en parler avec des jeunes :

- Pièce de théâtre de l’association pratique I Le chat
- Pièce de théâtre Cie Ariadne I Ces filles-là
- Webtoon - Cybervengers
- Webtoon Editions Dupuis I Les Combats Invisibles

7.b

Désinformation



Explications

Les sources d’une information sont primordiales pour déterminer sa crédibilité : cette information se base-t-elle sur des études ? Qui diffuse l’information ?

Il est également important de comparer et de croiser les sources. Cela permet de voir si l’information est présente sur d’autres plateformes et de voir comment elle est traitée ailleurs.

Source : Fausses nouvelles : guide des questions à se poser face à une information | Gouvernement.fr

QUIZ

Avant de repartager un contenu sur les réseaux sociaux, que doit-on vérifier ?

A. D’où vient l’information
B. Si le contenu est vrai
C. Si cela ne heurte personne en particulier

Réponse : A, B et C

Explications

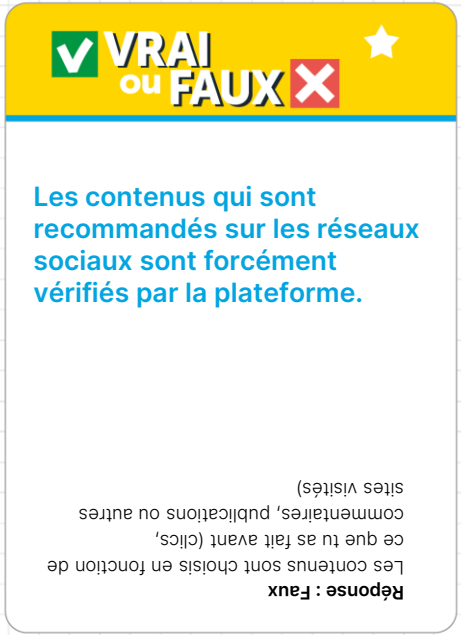
Chacun est responsable de ce qu’il publie sur les réseaux sociaux, il est donc important de réfléchir aux conséquences de ses publications :

Est-ce que je suis sûr que ce que je partage est vrai ? Est-ce que je fais confiance à la source de cette information ? Cette information risque-t-elle de blesser personnellement quelqu’un ? En cas de doute, il vaut mieux s’abstenir.

En revanche, il est important de rappeler que chacun est libre de s’exprimer librement tant que ses propos sont légaux.

Sources :
https://www.cnil.fr/fr/10-conseils-pour-rester-net-sur-le-web
https://www.service-public.fr/particuliers/vosdroits/F32075

7.b Thématique “Désinformation” - Niveau 1



Explications

La majorité des plateformes de réseaux sociaux, gratuites pour les utilisateurs, génèrent des revenus via la publicité qu’elles hébergent : plus les internautes passent de temps à utiliser leurs services, plus ils sont exposés à de la publicité et plus elles gagnent de l’argent.

Dans ce contexte, les fake news constituent des contenus particulièrement « engageants », c’est-à-dire qu’ils captent l’attention des internautes et les font réagir. Les grandes plateformes ont ainsi pu être accusées de promouvoir des fausses informations et des contenus complotistes via leurs algorithmes de recommandation, afin de générer davantage de revenus publicitaires.

Source : https://www.clemi.fr/fileadmin/user_upload/espace_familles/Guide_famille_tout_ecran_v2.pdf (page 16)

7.b Thématique “Désinformation” - Niveau 1

Explications

Wikipédia est une encyclopédie en ligne, gratuite, existante depuis 2001 et traduite dans plus de 280 langues. Sa particularité est que les articles sont rédigés par des volontaires qui écrivent gratuitement et de façon anonyme, faisant de Wikipédia une encyclopédie collaborative.

C’est très utile mais il faut garder à l’esprit que quasiment n’importe qui peut écrire ou modifier un article Wikipédia, même si le contenu est vérifié par des modérateurs. Il est donc important de croiser les informations avec d’autres sources fiables et neutres, afin de s’assurer de leur véracité.

Sources :
https://www.1jour1actu.com/culture/a-quoi-ca-sert-wikipedia
Wikipédia:Vérifiabilité — Wikipédia (wikipedia.org)

7.b Thématique “Désinformation” - Niveau 1

Explications

Selon une étude réalisée en 2018 par des chercheurs américains du MIT et publiée dans la revue scientifique *Science*, une information fausse a 70% de chances de plus d’être propagée qu’une vraie.

L’article de *Science et Avenir* explique « Selon eux, les fausses rumeurs n’agissent pas sur les mêmes leviers émotionnels que les véritables informations : ces fake news inspirent souvent la surprise, mais aussi la peur et le dégoût. Les informations exactes, elles appellent plutôt à l’anticipation des évènements à venir, la tristesse, la joie ou la confiance. Nous aurions donc plutôt tendance à faire partager la première catégorie d’émotions plutôt que la seconde. »

Source : https://www.sciencesetavenir.fr/high-tech/reseaux-et-telecoms/sur-twitter-une-fake-news-a-70-de-chances-de-plus-d-etre-diffusee-qu-une-veritable-information_121917

QUIZ

Comment peut-on identifier une fake news ?

A. Les informations ou les sources ne sont pas précises
B. Le contenu fait débat
C. Le titre est accrocheur

Réponse : A et C
Ce n'est pas parce qu'une information est polémique qu'elle est fausse.

Explications

Les fake news ressemblent parfois fortement à une information authentique et tout le monde peut être induit en erreur : 73% des Français pensent avoir déjà été confrontés à une fake news et 23% d'entre eux admettent avoir été trompés.

Sources :
Fausses nouvelles : guide des questions à se poser face à une information | Gouvernement.fr
https://e-enfance.org/informer/fake-news/

QUIZ

Pourquoi des personnes partagent des fausses informations ?

A. Parce qu’elles pensent qu’elles sont vraies
B. Parce qu’elles veulent vendre quelque chose
C. Pour faire du buzz

Réponse : A, B et C

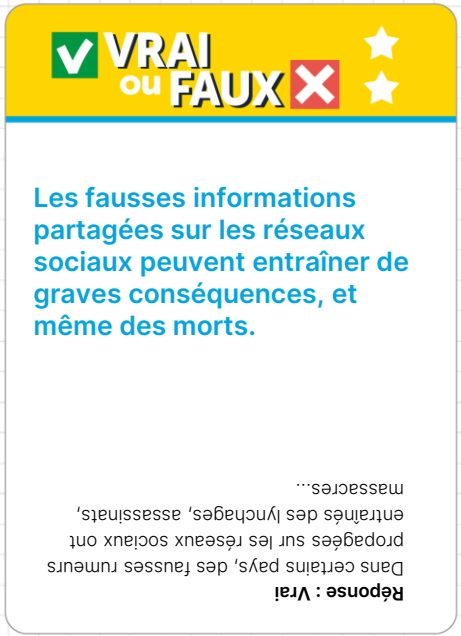
Source : https://e-enfance.org/informer/fake-news/

Explications

Les fake news peuvent être lancées pour des raisons idéologiques (campagne de désinformation), politiques (déstabiliser un adversaire lors d’une élection) ou encore financières (arnaques sur internet).

Mais beaucoup de personnes se laissent tromper et les partagent parce qu’elles y croient !

Mehdi Moussaïd, chercheur en sciences cognitives, explique très bien les phénomènes de propagation des fausses informations dans sa vidéo sur Youtube Fouloscopie I Rumeurs, fake news et téléphone arabe et dans l’article suivant : https://www.larecherche.fr/sciences-cognitives-publications/comment-se-propagent-les-rumeurs



Explications

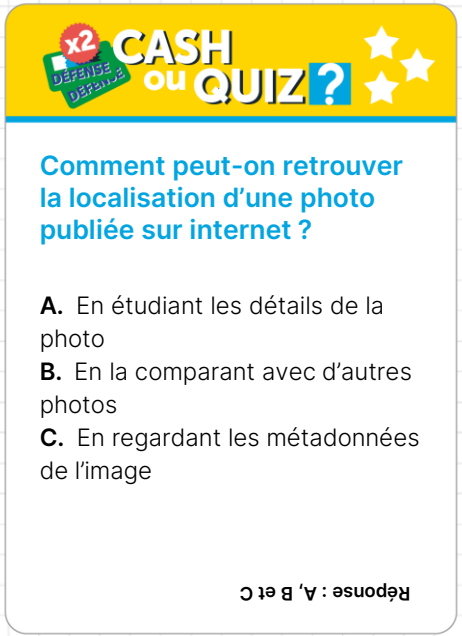
Les fausses informations partagées sur les réseaux peuvent amener ceux qui y croient à adopter des conduites à risques pouvant être dangereuses pour leur santé.

Cela peut également amener à des tensions importantes dans la population : En Inde, des rumeurs diffusées sur les réseaux sociaux concernant des enlèvements d’enfants ont conduit à des lynchages de personnes extérieures à certains villages par exemple. On dénombre plus d’une trentaine de morts.

Sources :

https://www.francetvinfo.fr/replay-radio/en-direct-du-monde/en-direct-du-monde-en-inde-des-rumeurs-diffusees-par-les-reseaux-sociaux-tuent-des-innocents_2819741.html

https://www.ouest-france.fr/leditiondusoir/2020-08-14/une-seule-fake-news-sur-le-covid19-aurait-cause-la-mort-de-800-personnes-ffc58394-9a7c-4c71-94d3-7f5700125c3e

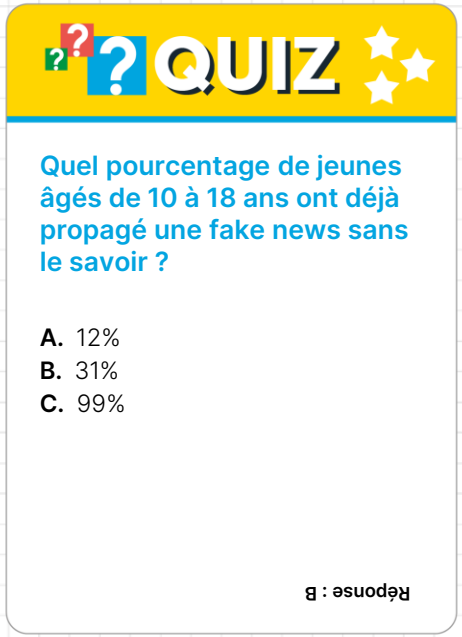


Explications

En cas de doute sur la localisation d’une photo trouvée sur internet, il peut être intéressant de la comparer à d’autres photos du même endroit, ou du même évènement. Il faut également être vigilant aux détails de la photo (météo, langue sur les panneaux, incohérences lumineuses ou déformations…)

De plus, tous les appareils photos numériques ou smartphones enregistrent des données concernant les photos qu’ils prennent (dates, réglages, coordonnées GPS). En analysant les métadonnées de l’image grâce à certains outils, il est donc possible de les retrouver.

Source : https://www.01net.com/actualites/obtenez-les-informations-de-prise-de-vue-dune-photo-504079.html



Explications

Selon une étude menée aux États-Unis par l’institut Common Sense Media, 44% des jeunes de 10 à 18 ans estiment ne pas savoir différencier une vraie info d’une fausse.

De plus, un adolescent américain sur trois a déjà partagé une information en se rendant compte plus tard qu’il s’agissait d’une "fake news".

Sources :
https://csa.eu/news/les-adolescents-et-linfo/
https://www.bva.fr/sondages/francais-fake-news/
https://www.commonsensemedia.org/research/news-and-americas-kids-infographic

QUIZ

Comment peut-on retrouver l’origine d’une image publiée sur internet ?

A. Lire la légende de l’image publiée
B. Faire une recherche d’image inversée
C. Consulter les métadonnées de l’image

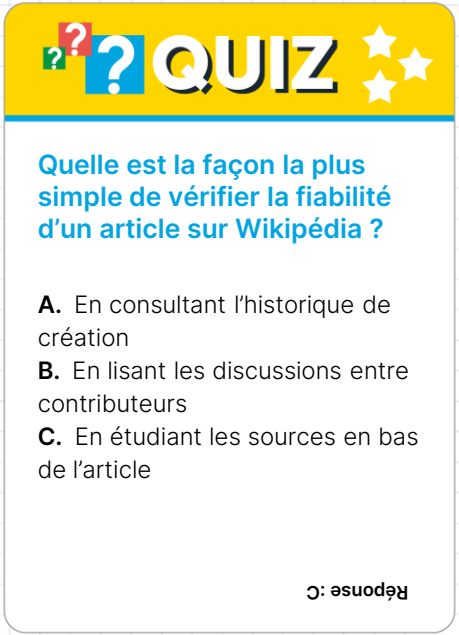
Réponse : B et C
La recherche inversée fonctionne avec Google Image ou Tineye.

Explications

Certaines images postées sur les réseaux sociaux ou en illustration d’articles sur internet peuvent avoir été détournées.

Il est possible de retrouver l’origine d’une image de plusieurs manières : en consultant les métadonnées de l’image par exemple mais aussi tout simplement en utilisant des outils dédiés, comme TinEye par exemple ou la recherche inversée de Google (Google Lens).

Sources :
https://tineye.com/
https://images.google.com/



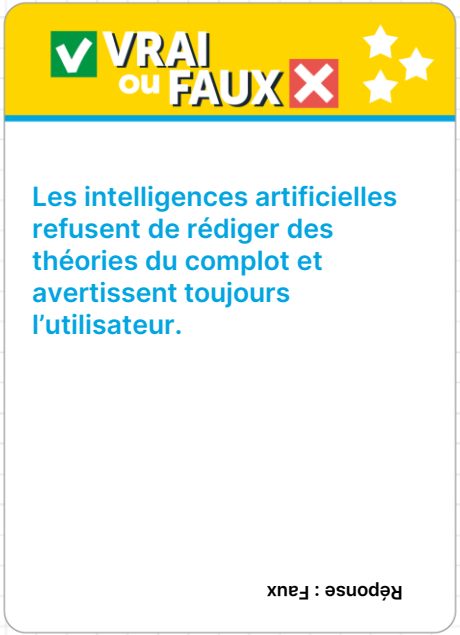
Explications

Wikipédia est une encyclopédie en ligne, gratuite, existante depuis 2001 et traduite dans plus de 280 langues. Sa particularité est que les articles sont rédigés par des volontaires qui écrivent gratuitement et de façon anonyme, faisant de Wikipédia une encyclopédie collaborative.

Afin de renforcer le contrôle des articles sur Wikipédia, les contributeurs sont obligés de citer leurs sources en bas de l’article. Ainsi, chacun peut aller vérifier par lui-même la fiabilité de ce qui est écrit.

Sources :
https://www.1jour1actu.com/culture/a-quoi-ca-sert-wikipedia
Wikipédia:Vérifiabilité — Wikipédia (wikipedia.org)

7.b Thématique “Désinformation” - Niveau 3

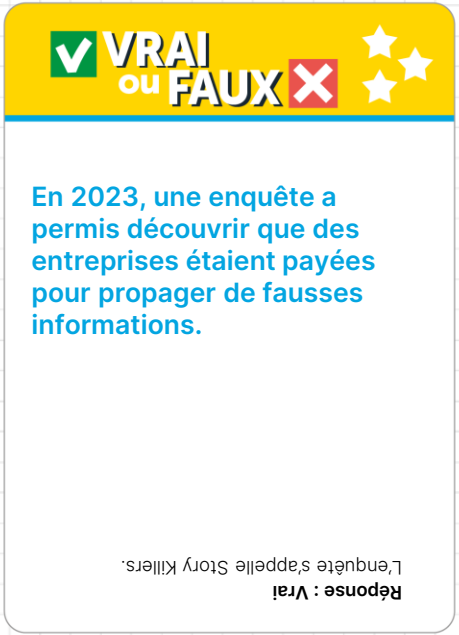


Explications

Début 2023, Newsguard, une start-up américaine spécialisée dans la lutte contre les fausses informations a soumis ChatGPT a des questions orientées sur une centaine de faux récits répandus sur Internet, concernant le COVID-19, le conflit en Ukraine ou encore les fusillades dans les écoles américaines.

Dans 80% des cas, ChatGPT a relayé des affirmations complètement fausses sur ces différents sujets. De plus, l’IA n’a indiqué que dans 23% des cas que les informations avaient fait l’objet de démentis ou provenaient de sources peu fiables.

Sources :
https://www.lesechos.fr/tech-medias/intelligence-artificielle/intelligence-artificielle-generative-la-revolution-chatgpt-en-marche-1935018
https://www.futura-sciences.com/tech/actualites/intelligence-artificielle-chatgpt-probleme-desinformation-104281/



Explications

Début 2023, une centaine de journalistes de 30 médias internationaux, réunis au sein du consortium Forbidden Stories, a publié le résultat d’une enquête de plus de 6 mois sur l’industrie de la désinformation : l’enquête s’appelle « Story Killers »

Cette enquête a révélé les ressorts utilisés par les entreprises et les mercenaires qui vendent désormais des services "clé en main" à des États ou des hommes politiques dans le but d’influencer les opinions, manipuler des élections, ou détruire des réputations au détriment de l’information et de la démocratie.

Selon un rapport du Oxford Internet Institute, en 2020, au moins 81 pays ont eu recours à des campagnes de manipulation organisées sur les réseaux sociaux.

Source : https://www.francetvinfo.fr/monde/story-killers-une-enquete-de-100-journalistes-revele-l-ampleur-de-l-industrie-de-la-desinformation_5658659.html

Pour aller plus loin - Désinformation

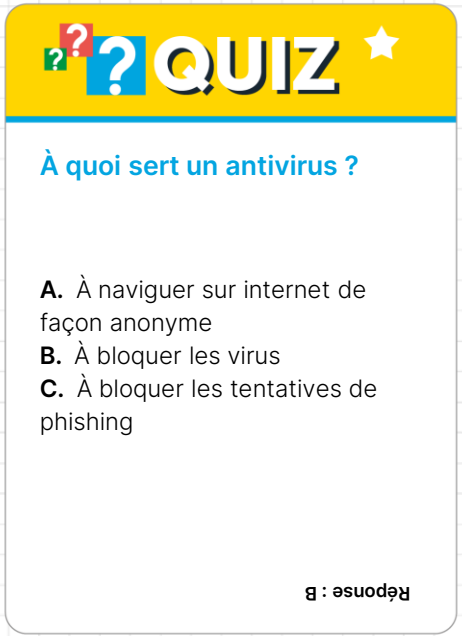
Comprendre et réagir face aux fake news :

- CLEMI I Réagir et agir face aux fakes news
- Guide pratique du CLEMI I La famille tout-écran
- Lumni I Fake news et désinformation

Des ressources pour en parler et s’informer en temps réel :

- https://www.francetvinfo.fr/vrai-ou-fake/
- https://www.hoaxbuster.com/
- https://e-enfance.org/bd-carrefour/fake-news/

7.c
Equipement



Explications

Un antivirus est un programme informatique, ou une application, qui a pour principale vocation d’identifier, de neutraliser, voire d’éliminer les virus informatiques.

Pour bien utiliser un antivirus, il faut s’assurer que :

- Il est bien installé ;
- Il est activé ;
- La protection en « temps réel » est bien configurée pour analyser ce qui entre et sort ;
- il est mis à jour régulièrement.

La fonction antivirus ne garantit pas l’anonymat sur internet et ne permet pas de lutter contre le phishing.

Sources :
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/antivirus
Cybermalveillance.gouv.fr - Comment sécuriser mes appareils pour qu’ils ne soient pas attaqués par des virus ? - Vidéo Dailymotion

QUIZ

Qu’est-ce qu’on ne doit pas faire si on se connecte à un wifi public ?

A. Visiter un site web
B. Taper ses mots de passe
C. Partager des informations privées

Réponse : B et C
Les wifis publics ont souvent une faible sécurité. Un hackeur peut facilement surveiller ce que tu fais.

Explications

Il vaut mieux privilégier la connexion 3G ou 4G que d’utiliser les réseaux wifi publics que l’on peut trouver dans les fast-foods, cafés, hôtels ou gares.

Ces wifi publics sont souvent mal sécurisés, et peuvent être contrôlés ou usurpés par des pirates qui pourraient ainsi voir passer et capturer des informations personnelles ou confidentielles (mots de passe, numéros de carte bancaire…).

Sources :

Cybermalveillance.gouv.fr - WiFi public : comment empêcher le vol de mes données ? - Vidéo Dailymotion
Cybermalveillance.gouv.fr - Quels risques prend-on en se connectant sur les réseaux #WiFi gratuits ? - Vidéo Dailymotion

QUIZ

Quand doit-on installer les mises à jour de son téléphone ?

A. Automatiquement… ou dès qu’elles sont proposées
B. Quand on a le temps pour le faire
C. Tous les 6 mois

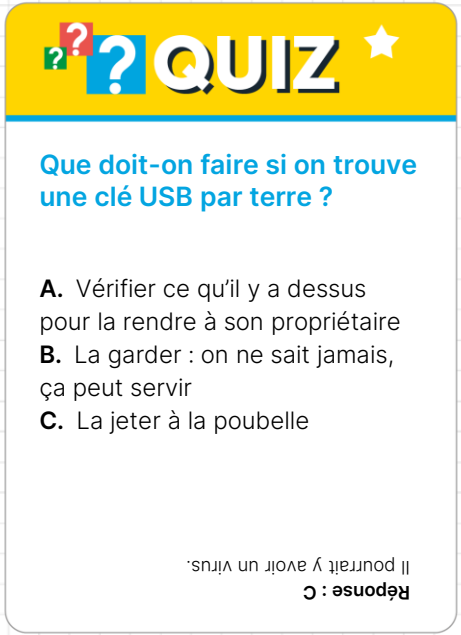
Réponse : A

Explications

Les appareils numériques et les logiciels que nous utilisons au quotidien peuvent contenir des failles de sécurité. Ces failles peuvent être utilisées par des cybercriminels pour voler des données, bloquer ou prendre le contrôle d’un ordinateur, d’un téléphone ou encore d’un objet connecté.

Face à ces risques, les éditeurs et les fabricants proposent des mises à jour (« patch » en anglais) visant à corriger ces failles. Pour ne pas faciliter la tâche des cybercriminels, il est primordial de réaliser les mises à jour de vos équipements dès qu’elles sont disponibles.

Sources :
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/10-mesures-essentielles-assurer-securite-numerique
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mises-a-jour



Explications

Lorsqu’on trouve une clé USB, la tentation est grande de regarder ce qu’il y a dessus, pour identifier son propriétaire notamment.

Pourtant on ne sait pas ce qu’elle peut contenir : certaines clés USB contenant un virus par exemple peuvent être laissées volontairement par des individus malveillants. C’est une technique de piratage.

Il faut donc, après avoir demandé oralement si elle n’appartient à personne, la jeter.

Sources :
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-usages-pro-perso
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/antivirus

QUIZ

Que risque-t-on si on télécharge une application malveillante sur son téléphone ?

A. Se faire voler toutes ses données (photos, messages, mots de passe, etc...)
B. Faire exploser son téléphone
C. Augmenter la facture de téléphone

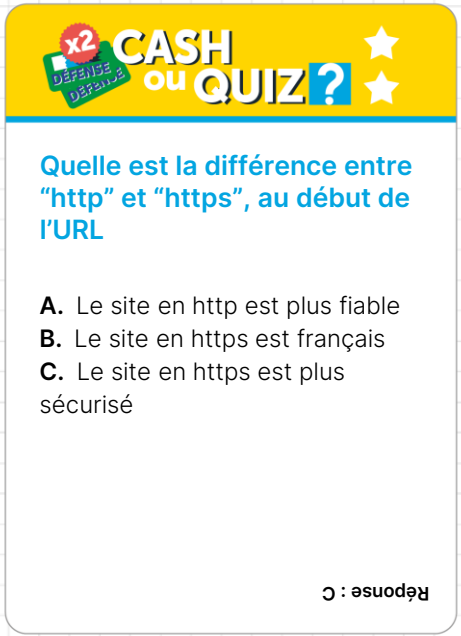
Réponse : A et C

Explications

Les applications malveillantes peuvent aspirer les données, provoquer une surconsommation de données, installer des programmes qui, en souscrivant à des services payants, augmente la facture de téléphone.

Avant de télécharger une application, on peut consulter le nombre de téléchargements et les avis des autres utilisateurs, et vérifier ce à quoi cette application va accéder dans notre téléphone (contact, photos, etc.). Au moindre doute, il vaut mieux ne pas installer l’application et/ou en choisir une autre.

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



Explications

Pour comprendre la différence entre http et https, il faut d’abord comprendre leur signification :

- Le sigle « http » signifie « HyperText Transfer Protocol »
- Le sigle « https » veut dire « HyperText Transfer Protocol Secure ».

Le protocole http permet à notre navigateur (Qwant, Google, Firefox, Edge, etc) de communiquer avec le serveur web derrière le site que nous sommes en train de consulter.

HTTPS est la variante sécurisée de ce protocole, grâce notamment au chiffrement des données qui transitent entre votre machine et le site web, ce qui signifie qu’un attaquant qui se positionnerait au milieu ne peut pas les « lire » car les échanges sont « codés ».

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

QUIZ

Comment installer de nouvelles applications sur son smartphone de façon sécurisée ?

A. Depuis des sites web qui présentent un cadenas avec l’URL
B. Depuis des plateformes de confiance (Apple Store, Google Play, etc...)
C. Depuis des sites recommandés par ses amis

Réponse : B
Il ne faut surtout pas rester sans réaction.

QUIZ

Comment peut-on s’assurer qu’une application est sécurisée avant de la télécharger ?

A. Vérifier que les autorisations demandées sont nécessaires au fonctionnement de l’app
B. Vérifier la réputation du vendeur
C. Tant qu’on a une iPhone, on ne risque rien

Réponse : A et B

Explications

Seules les plateformes officielles permettent de réduire le risque que les applications installées soient piégées, ou simplement très mal sécurisées.

Il faut également être attentif aux demandes d’autorisations des applications lors de leur première installation, mais aussi après leurs mises à jour car leurs autorisations peuvent évoluer. Certaines applications demandent parfois des droits très importants et qui peuvent être surprenants. Par exemple, un simple jeu de cartes « gratuit » qui demanderait l’autorisation d’accéder aux contacts, à la position GPS ou encore l’appareil photo est évidemment suspect.

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

QUIZ

Comment peut-on sauvegarder ses données ?

A. En les mettant sur un cloud
B. En les mettant sur un disque dur externe ou une clé USB
C. En les imprimant (exemple : un album photo)

Réponse : A, B et C

Explications

Nous utilisons tous de nombreux appareils numériques pour créer et stocker des informations. Ces appareils peuvent cependant s’user ou être endommagés, entraînant une perte, parfois irréversible, des données.

Afin de prévenir un tel risque, il est fortement conseillé d’en faire des copies pour préserver vos données à long terme.

Pour cela, il est possible d’utiliser des services en ligne (cloud), qui effectuent souvent des sauvegardes automatiques, ou bien un disque dur externe ou une clé USB qui nous est propre.

Enfin, pour certains types de données, il est possible de les imprimer, par exemple pour les photos que l’on souhaite conserver !

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes

QUIZ

Grâce à quel outil peut-on se protéger contre les logiciels malveillants ?

A. Un VPN
B. Un navigateur privé
C. Un antivirus

Réponse : C

Explications

Un antivirus est un programme informatique, ou une application, qui a pour principale vocation d’identifier, de neutraliser, voire d’éliminer les virus informatiques.

Pour bien utiliser un antivirus, il faut s’assurer qu’il est bien installé, qu’il est activé, que la protection en « temps réel » pour analyser ce qui entre et sort est bien configurée. Enfin, il est essentiel de le mettre à jour régulièrement pour s’assurer qu’il peut détecter les virus récemment découverts.

La fonction VPN et les navigateurs privés ne protègent pas contre les programmes malveillants.

Sources :
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/antivirus
Cybermalveillance.gouv.fr - Comment sécuriser mes appareils pour qu’ils ne soient pas attaqués par des virus ? - Vidéo Dailymotion

QUIZ

Quand doit-on sauvegarder ses données ?

A. Régulièrement
B. Après s’être fait pirater
C. Quand on a le temps

Réponse : A

Explications

En cas de perte, de vol, de panne, de piratage ou de destruction de tes appareils numériques, tes données enregistrées sur ces supports seront perdues.

Il est important de réaliser des sauvegardes régulièrement, pour pouvoir retrouver ses données, y compris les plus récentes (photos par exemple).

Il est important de vérifier que ses sauvegardes sont bien réalisées, notamment si vous faites des sauvegardes automatiques sur un cloud.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes

Explications

Il vaut mieux privilégier la connexion 3G ou 4G que d’utiliser les réseaux wifi publics que l’on peut trouver dans les fast-foods, cafés, hôtels ou gares.

Ces réseaux wifi sont souvent mal sécurisés, et peuvent être contrôlés ou usurpés par des pirates qui pourraient ainsi voir passer et capturer des informations personnelles ou confidentielles (mots de passe, numéros de carte bancaire…).

Quand on utilise un wifi public, il est important de s’assurer que les paramètres de partage ne sont pas ouverts, sinon n’importe qui peut récupérer les données partagées.

Sources :
Cybermalveillance.gouv.fr - WiFi public : comment empêcher le vol de mes données ? - Vidéo Dailymotion
Cybermalveillance.gouv.fr - Quels risques prend-on en se connectant sur les réseaux #WiFi gratuits ? - Vidéo Dailymotion

QUIZ

Que peut récupérer une hackeuse qui a piraté un wifi public auquel on se connecte ?

A. Les mots de passe que l’on tape sur internet
B. Les sites que l’on consulte
C. Les messages Whatsapp

Réponse : A et B
Whatsapp est chiffré, le pirate ne peut donc pas intercepter les messages.

Explications

Les réseaux wifi sont souvent mal sécurisés, et peuvent être contrôlés ou usurpés par des pirates qui pourraient ainsi voir passer et capturer des informations personnelles ou confidentielles (mots de passe, numéros de carte bancaire…) qui transitent « en clair ».

En revanche, la messagerie WhatsApp est chiffrée, ce qui signifie que les messages ne peuvent pas être lus pendant leur transmission.

Sources :
Cybermalveillance.gouv.fr - WiFi public : comment empêcher le vol de mes données ? - Vidéo Dailymotion
Cybermalveillance.gouv.fr - Quels risques prend-on en se connectant sur les réseaux #WiFi gratuits ? - Vidéo Dailymotion

QUIZ

Quelles sont les méthodes utilisées par les pirates pour détourner un wifi public ?

A. Créer un faux wifi qui a le même nom que le vrai wifi public

B. Utiliser un VPN

C. Se connecter et regarder les messages non chiffrés qui sont envoyés

Réponse : A et C
Les wifis publics ont souvent une faible sécurité. Un hackeur peut facilement surveiller ce que tu fais.

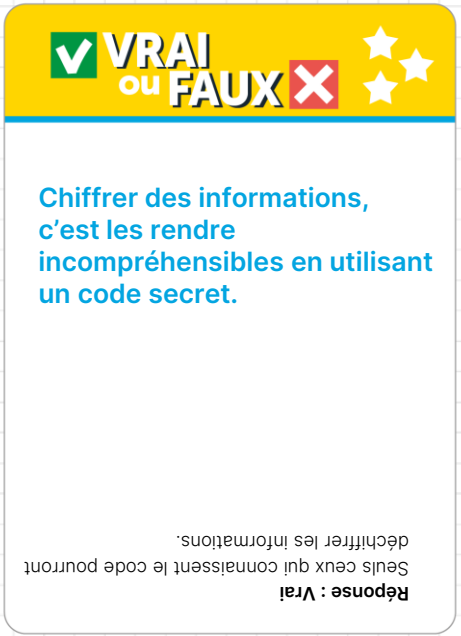
Explications

Il est facile pour un hackeur de créer un point d’accès wifi à qui il donnera le nom du restaurant, de l’hôtel, de la boutique juste à côté. Bien que se connecter au wifi public soit déconseillé, il arrive parfois qu’on en ait besoin. Dans ce cas, il faut demander au responsable le nom du réseau de l’endroit au préalable.

La sécurité des wifi publics est généralement très faible et les échanges ne sont pas chiffrés : les pirates informatiques peuvent donc facilement intercepter les données que vous taper sur internet.

C’est pourquoi, il est fortement déconseillé d’envoyer les données confidentielles (données bancaires, mots de passe, etc.) : un pirate pourrait récupérer les données qui transitent en clair par ce wifi public.

Source : https://www.cnil.fr/fr/utiliser-un-wi-fi-public-voici-4-precautions-prendre



Explications

Le chiffrement est un moyen de brouiller les données afin que seules les parties autorisées puissent comprendre les informations.

Il s’agit du processus de conversion de données lisibles par quiconque en données incompréhensibles, appelées chiffrées.

La clé permettant de passer de l’état lisible à l’état illisible, appelée clé de chiffrement, permet de reconvertir également les données dans l’autre sens. C’est pourquoi, elle ne doit être connue que des personnes autorisées.

A noter : on ne dit jamais que des données sont « cryptées ». Il s’agit d’un anglicisme qui n’a pas de sens en français.

Source : https://www.futura-sciences.com/tech/definitions/informatique-chiffrement-1722/

Pour aller plus loin - Équipements

Comprendre comment configurer et protéger ses équipements :

- Ministère de l'économie I Comment assurer sa sécurité numérique
- Cybermalveillance.gouv I 10 mesures essentielles assurer votre sécurité numérique
- Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) - Guide des bonnes pratiques de l'informatique

7.d
Mots de passe

Explications

Le code PIN est un code d’accès composé d’au moins 4 chiffres qui sert à verrouiller l’accès à la carte SIM d’un téléphone. PIN, c’est l’acronyme de l’anglais « Personal Identification Number » ou numéro d’identification personnel en français.

On le choisit généralement au moment de l’acquisition du téléphone, mais il est souvent configuré par défaut avec un code standard, par exemple « 0000 » ou « 1234 ». Il est important de le changer à la réception du téléphone.

En effet, sans ce code PIN, l’accès à la carte SIM du téléphone est bloqué. En revanche, si on garde le code par défaut, une personne qui trouve ou vole le téléphone pourra accéder aux données stockées sur la carte SIM.

Source : https://www.futura-sciences.com/tech/forfaits/guide-achat/comment-trouver-utiliser-code-pin-puk/

QUIZ

À partir de combien de caractères peut-on dire qu’un mot de passe est suffisamment long ?

A. 8
B. 12
C. 20

Réponse : B
Il doit y avoir aussi des majuscules, minuscules, chiffres et caractères spéciaux.

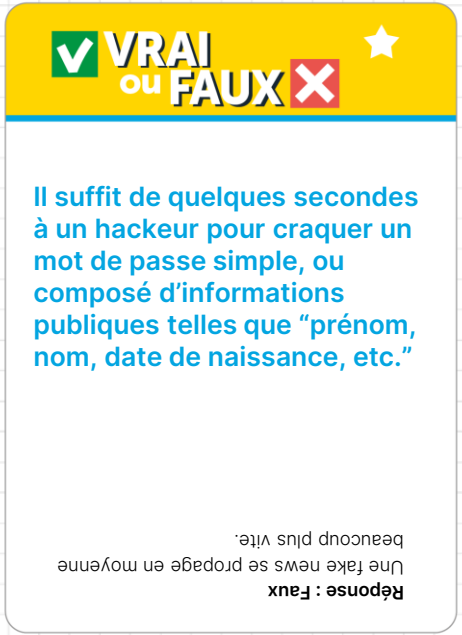
Explications

Il est admis qu’un bon mot de passe doit comporter au minimum 12 caractères mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux. C’est ce qu’on appelle un mot de passe complexe.

En effet, cela permet de réduire le risque qu’un hacker devine ou trouve un mot de passe, notamment en utilisant la technique du « brute force », une technique d’attaque répandue qui consiste à essayer toutes les combinaisons possibles de caractères jusqu’à trouver le bon mot de passe.

Outre la complexité et de la longueur, plus un mot de passe est choisi de façon aléatoire, moins il a de chance d’être craqué.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe



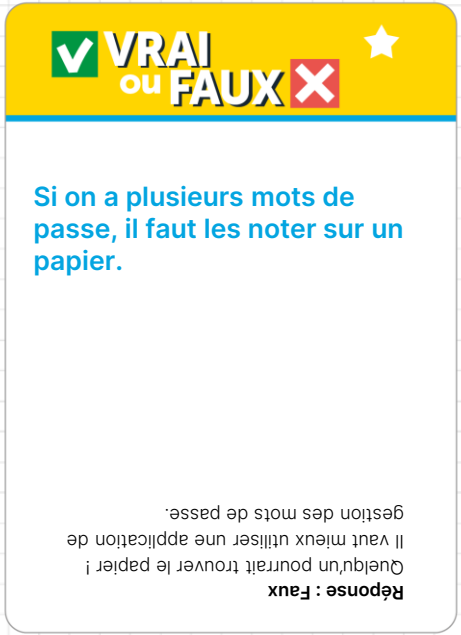
Explications

Une technique d’attaque répandue, dite par « force brute », consiste à essayer toutes les combinaisons possibles de caractères jusqu’à trouver le bon mot de passe. Réalisées par des ordinateurs, ces attaques peuvent tester des dizaines de milliers de combinaisons par seconde.

La première chose qu’un hackeur va faire, c’est de tester des combinaisons avec des mots du dictionnaire ou encore avec des informations qu’il a pu récupérer facilement sur la victime : son prénom, sa date de naissance par exemple, ou encore le nom de son chien.

C’est pourquoi il faut éviter d’utiliser ce type de mot de passe.

Source : https://www.francenum.gouv.fr/magazine-du-numerique/combien-de-temps-un-pirate-met-il-pour-trouver-votre-mot-de-passe-comment

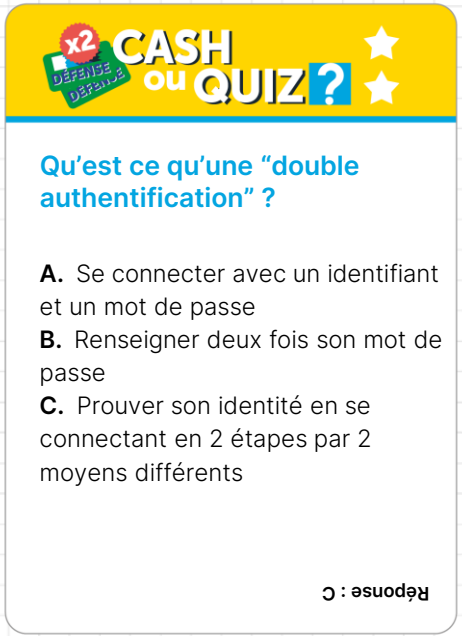


Explications

Il est humainement impossible de retenir les dizaines de mots de passe longs et complexes ! Mais il ne faut pas commettre l’erreur de les noter sur un post-it à côté de son ordinateur ou de les inscrire dans sa boite mail, dans un fichier non protégé de son ordinateur ou encore dans son portable : n’importe qui pourrait les récupérer facilement.

Il existe des gestionnaires de mots de passe sécurisés : il s’agit de coffres-forts à mots de passe, qui permettent de les stocker de façon sécurisée et de ne retenir que le mot de passe qui permet d’ouvrir le coffre-fort.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe



Explications

Pour renforcer la sécurité des accès, de plus en plus de services proposent cette option.

En plus du login et du mot de passe, le service va demander une confirmation de l’identité de la personne qui cherche à s’authentifier, sous forme de code provisoire reçu par SMS ou mail, via une autre application ou une clé spécifique, ou encore par reconnaissance biométrique.

Cela renforce considérablement la sécurité des comptes. En effet, même si un hacker réussit à trouver un mot de passe, il a peu de chances d’accéder au deuxième moyen d’authentification.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/double-authentification

QUIZ

Ton opérateur téléphonique t’appelle pour te prévenir que ton compte a été piraté. Pour pouvoir t’aider, il te demande ton mot de passe.
Que fais-tu ?

A. Si le problème est sérieux, tu lui donnes ton mot de passe
B. Tu lui demandes de t’envoyer un email
C. Tu raccroches

Réponse : C
Un mot de passe ne doit JAMAIS être transmis… Quel que soit le moyen !

Explications

Il ne faut jamais communiquer des informations sensibles par messagerie ou téléphone. Ce type de demande « urgente » doit alerter : aucune administration ou société commerciale sérieuse ne demandera un mot de passe par message électronique ou par téléphone.

Les attaquants jouent souvent sur la peur ou la surprise de leur victime. Ils peuvent utiliser des moyens convaincants, par exemple en utilisant des informations personnelles qu’ils ont trouvées sur leur victime.

En cas de doute, il faut raccrocher et recontacter l’opérateur via le numéro de téléphone habituel.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing#prevention-phishing

QUIZ

Comment faire pour inventer un mot de passe facile à retenir ?

A. Utiliser son prénom et sa date de naissance
B. Utiliser la première lettre des mots d’une phrase que l’on retient par coeur
C. Mettre le nom de son club sport favori et l’année en cours

Réponse : B

Explications

Il faut éviter d’utiliser des informations personnelles qui pourraient être faciles à retrouver (sur les réseaux sociaux par exemple), comme le prénom de son copain ou sa copine, une date anniversaire ou son groupe de musique préféré.

Il faut éviter également les suites logiques simples comme « 123456 », « azerty », « abcdef »... qui font partie des listes de mots de passe les plus courants et qui sont les premières combinaisons que testeront les hackers.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe

QUIZ

Pourquoi doit-on activer la double authentification ?

A. Pour que ses parents puissent suivre ses activités
B. Pour réduire le risque de se faire pirater ses comptes
C. Pour utiliser le même mot de passe sur tous ses comptes

Réponse : B
Exemple de double authentification : login/motdepasse + code reçu par SMS.

Explications

En plus du login et du mot de passe, le service va demander une confirmation de l’identité de la personne qui cherche à s’authentifier, sous forme de code provisoire reçu par SMS ou mail, via une autre application ou une clé spécifique, ou encore par reconnaissance biométrique.

Ainsi, cela réduit le risque de se faire pirater ses comptes : connaître ou trouver le mot de passe ne suffit pas, il faut également avoir accès au téléphone ou à la boîte mail associée.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/double-authentification

QUIZ

Qu’est ce qu’un “mot de passe complexe” ?

A. Un mot de passe avec un mot compliqué
B. Un mot de passe qui fait au moins 8 caractères
C. Un mot de passe qui avec au moins 1 majuscule, 1 minuscule, 1 chiffre et 1 caractère spécial

Réponse : C

Explications

Une technique d’attaque répandue, dite par « brute force », consiste à essayer toutes les combinaisons possibles de caractères jusqu’à trouver le bon mot de passe.

Réalisées par des ordinateurs, ces attaques peuvent tester des dizaines de milliers de combinaisons par seconde.

Pour empêcher ce type d’attaque, il est admis qu’un bon mot de passe doit comporter au minimum 12 signes : c’est le critère de longueur du mot de passe.

Un mot de passe complexe comprend également des majuscules, des minuscules, des chiffres et des caractères spéciaux.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe

QUIZ

Pourquoi doit-on verrouiller son écran avec un mot de passe ou une empreinte ?

A. Pour réduire le risque de se faire pirater ses comptes si on perd son téléphone
B. Pour protéger sa vie privée
C. Pour éviter les virus

Réponse : A et B

Explications

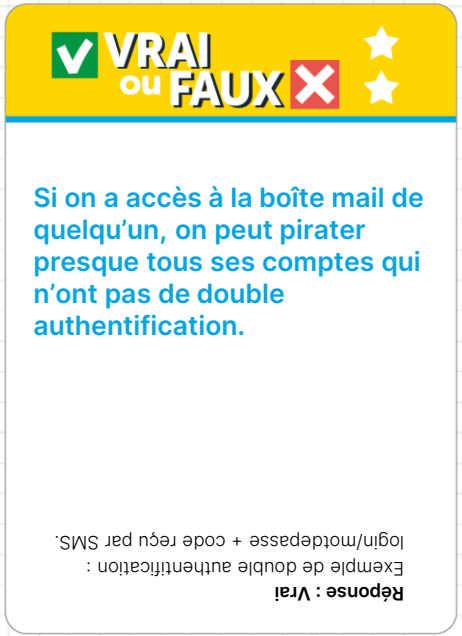
Le système de verrouillage sert à bloquer l’accès au téléphone à chaque mise en veille voire après un certain laps de temps d’inactivité.

Il peut prendre la forme d’un code à chiffres, d’un schéma à effectuer, d’une empreinte biométrique ou même d’un système de reconnaissance faciale.

Cela empêche la consultation des informations personnelles contenues dans le téléphone en cas de perte ou de vol (photos, sms) mais également d’avoir accès aux comptes sur lesquels le téléphone serait connecté.

Source : https://www.cnil.fr/fr/comment-securiser-au-maximum-lacces-votre-smartphone

7.d Thématique “Mots de passe” - Niveau 2

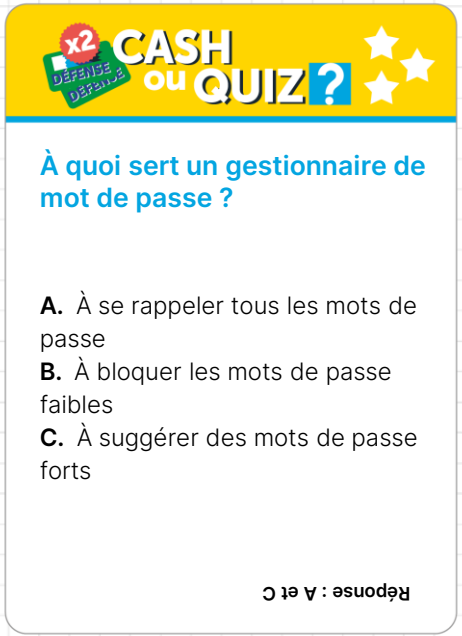


Explications

Notre boite mail est une mine d’or pour un cybercriminel : il peut y trouver plein d’informations personnelles (copie de carte d’identité par exemple) mais il peut également s’en servir pour réinitialiser les mots de passe d’autres comptes : en effet, la plupart des sites envoient un mail de réinitialisation de mot de passe sur la boîte mail qui a servi à créer le compte. Si on y a accès, il est très simple de changer les mots de passe et ensuite d’accéder aux comptes.

La double authentification permet de réduire ce risque : l’accès à la boite mail ne suffit pas. Une double vérification sera par exemple envoyée par notification ou SMS sur le téléphone.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe



Explications

Il est humainement impossible de retenir les dizaines de mots de passe longs et complexes !

Il existe des gestionnaires de mots de passe sécurisés qui permettent de générer des mots de passe complexes et de les stocker de façon sécurisée, comme dans un coffre-fort.

Ainsi, il suffit de retenir le mot de passe qui permet d’ouvrir le coffre-fort.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe

QUIZ

Choisir un bon mot de passe c’est :

A. Utiliser un mot de passe qu’on utilise déjà sur d’autres sites (pour ne pas l’oublier)
B. Utiliser des suites logiques de chiffres ou de lettres (ex: 1234 ou ABCD)
C. Combiner des informations personnelles faciles à mémoriser (ex : prénom + date de naissance)

Réponse : Aucune

Explications

Pour pirater un compte, la première chose qu’un hackeur va faire, c’est de tester des combinaisons avec des mots du dictionnaire, des suites logiques ou encore avec des informations qu’il a pu récupérer facilement sur la victime, par exemple son prénom, sa date de naissance, ou encore le nom de son chien, ou même les trois combinés.

C’est pourquoi il faut éviter d’utiliser ce type de mot de passe.

Il est également très important d’utiliser un mot de passe différent pour chaque service. Ainsi, en cas de perte ou de vol d’un des mots de passe, seul le service concerné sera vulnérable.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe

QUIZ

Que peut faire un hackeur s’il vole un téléphone et devine le code PIN ?

A. Il peut accéder aux données, même s’il y a un code pour déverrouiller l’écran
B. Il ne peut pas accéder aux données s’il y a un code pour déverrouiller l’écran
C. Il ne peut pas accéder aux données de la carte SIM si la ligne a été suspendue

Réponse : A et C

Explications

Avec simplement un code PIN, il est possible d’accéder aux réglages d’un téléphone et de tous les autres comptes qu’il contient, y compris le code de déverrouillage de l’écran, et ainsi les modifier.

C’est une faille qui existe sur les téléphones sous iOS et Android et qui a fait de nombreuses victimes.

En cas de perte ou de vol d’un téléphone, la première chose à faire est donc de suspendre la ligne. La carte SIM et le code PIN associés seront inopérants.

Source : https://www.phonandroid.com/attention-a-vos-smartphones-les-pirates-ont-trouve-un-moyen-simple-de-voler-votre-identite.html

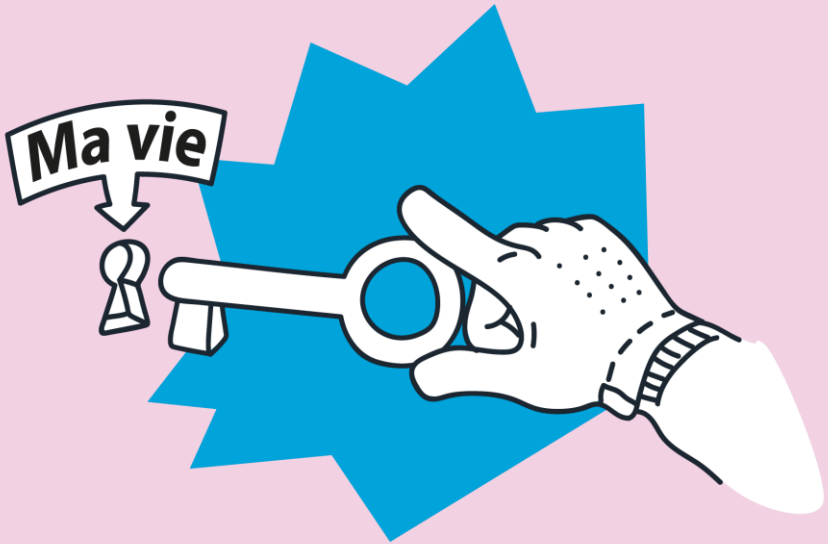
Pour aller plus loin - Mots de passe

Choisir de bons mots de passe :

- Ministère de l'économie I Comment assurer votre sécurité numérique ?
- Cybermalveillance.gouv I 10 mesures essentielles assurer votre sécurité numérique
- Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) - Guide des bonnes pratiques de l'informatique
- CNIL I Les conseils de la CNIL pour un bon mot de passe
- Cybermalveillance.gouv I Qu'est-ce que la double authentification ?

Comprendre le fonctionnement des mots de passe :

- Micode sur Youtube I Stocker son mot de passe sur son navigateur... ou pas.



7.e

Vie privée

QUIZ

Ou est-il possible de retrouver la liste des derniers sites qu’on a consultés ?

A. Dans l’historique
B. Dans les sauvegardes
C. Dans la liste des favoris

Réponse : A

Explications

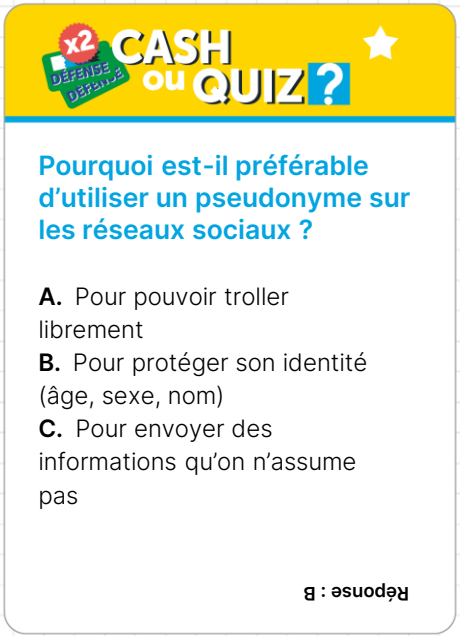
Lorsque l’on navigue sur internet, un certain nombre de traces sont conservées par les moteurs de recherche (Google Chrome, Mozilla Firefox, Safari, Microsoft Edge, etc.) dont l’historique de navigation.

Ainsi, les requêtes, les recherches effectuées, les sites web visités sont conservés dans l’historique de navigation. N’importe quelle personne ayant accès à un ordinateur peut consulter l’historique de la session ouverte.

Il existe cependant des moteurs de recherche qui ont fait le choix de ne pas conserver l’historique, par exemple Duck Duck Go ou Qwant.

Contrairement à l’historique, les favoris sont les pages web que l’on met volontairement en mémoire, comme un marque-page.

Source : https://cnil.fr/fr/faites-regulierement-le-menage-dans-lhistorique-de-navigation



Explications

L’utilisation d’un pseudonyme permet de restreindre sa visibilité sur internet, et donc de mieux protéger sa vie privée.

Cela peut également un moyen de prévention contre des prédateurs en ligne, ciblant notamment les enfants.

Cependant, l’anonymat sur internet ne doit pas laisser penser que tout est permis. Dans le cadre d’une enquête, la police peut retrouver les auteurs de menaces, de chantages ou d’insultes.

Pour certains experts, il faut même accepter que tout ce que l’on fait sur internet puisse un jour être ressorti à notre insu par des personnes plus ou moins bien intentionnées.

Sources :
https://www.cnil.fr/sites/cnil/files/atoms/files/poster_10-conseils-pour-rester-net-sur-le-web_ok.pdf
https://www.lesoir.be/280752/article/2019-11-19/identite-numerique-pouvez-vous-vraiment-la-proteger

QUIZ

Léna fait de la pâtisserie et voudrait pouvoir partager ses photos de gâteaux sur Instagram avec tous les passionnés.
Que doit-elle faire ?

A. Passer son profil privé en public
B. Accepter les invitations d’autres pâtissiers sur son compte privée
C. Créer un nouveau compte Instagram public

Réponse : C

Explications

L’utilisation d’un compte privé est essentielle lorsque l’on souhaite partager des informations personnelles en limitant l’accès aux personnes que l’on connaît personnellement et en qui on a confiance.

Cependant, si on a des centres d’intérêt ou des passions spécifiques que l’on souhaite partager en ligne, il est souvent conseillé de créer un compte dédié à ce sujet. Cela permet de développer une audience qui partage ces intérêts sans mélanger ces contenus avec sa vie et d’autant plus de protéger sa vie privée.

Ainsi, si Lena passe son profil privé en public, tous les contenus qu’elle avait publiés précédemment seront accessibles à des inconnus.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/reseaux-sociaux

QUIZ

Que peut faire un site internet lorsqu’on accepte ses “Cookies” ?

A. Enregistrer ce qu’on regarde
B. Collecter des informations pour afficher des publicités ciblées
C. M’envoyer des biscuits par la poste

Réponse : A et B

Explications

Un cookie est un petit fichier stocké par un serveur dans le terminal (ordinateur, téléphone, etc.) d’un utilisateur qui permet de collecter les données de navigation sur le web.

Certains sont nécessaires et bien utiles (pour vous rappeler par exemple le contenu de votre panier sur un site de commerce) mais d’autres ne servent qu’à collecter des informations pour faire de la publicité ciblée. Dans ce cas, ils permettent de mémoriser plein de données pour créer un profil détaillé (tranche d’âge, genre, produits regardés, liens cliqués, temps passé, etc.) et ainsi diffuser des messages publicitaires spécifiques en fonction de ces caractéristiques.

Les sites français sont désormais obligés de demander le contentement préalable au dépôt de cookies, il est conseillé de les refuser par défaut.

Sources :
https://www.cnil.fr/fr/definition/cookie
https://www.cnil.fr/fr/cookies-et-autres-traceurs/comment-se-proteger/maitriser-votre-navigateur

QUIZ

Quel serait un bon pseudo pour Sarah Martin ?

A. Sarah 2013
B. Golgotha
C. Sarah.Marin

Réponse : B

Source : https://e-enfance.org/informer/internet-les-dangers/

Explications

Il est important d’adopter de bons réflexes pour naviguer sur internet et limiter les risques, comme créer un pseudonyme pour les réseaux sociaux.

Un bon pseudo ne doit pas donner d’informations personnelles (nom, prénom, date de naissance etc.). Dans le cas présent, seul le pseudo « Golgotha » ne donne aucune information sur Sarah Martin.

Il est également important de rappeler que :

- Des personnes malveillantes peuvent se cacher derrière un pseudo, il faut rester vigilant ;
- L’utilisation d’un pseudo ne garantit pas l’anonymat complet ;
- L’utilisation d’un pseudo ne donne pas le droit à des comportements inacceptables ou illégaux.

QUIZ

Quelles sont les informations qu’on ne doit jamais révéler sur internet ?

A. Son adresse perso et son âge
B. Sa série et son jeu vidéo préférés
C. Une photo et le nom de son chien

Réponse : A

Explications

Pour limiter les risques d’internet, il est important de ne pas donner trop d’informations personnelles : son nom, son prénom, son âge mais aussi son numéro de téléphone ou son adresse.

Toutes ces informations pourraient être récupérées par des entreprises pour adresser des publicités non sollicitées mais aussi par des personnes malveillantes pour nuire directement à une personne ou les utiliser dans le cadre d’arnaques à plus grande échelle.

Source : https://e-enfance.org/informer/internet-les-dangers/

QUIZ

Sur un réseau social, quand le profil est “public”, cela veut dire que tout le monde peut :

A. Accéder aux publications, stories, etc...
B. Republier les posts
C. Commenter les publications

Réponse : A, B et C

VRAI ou FAUX

Sur certains réseaux sociaux, les contenus d’un profil public peuvent être téléchargés, modifiés et republiés.

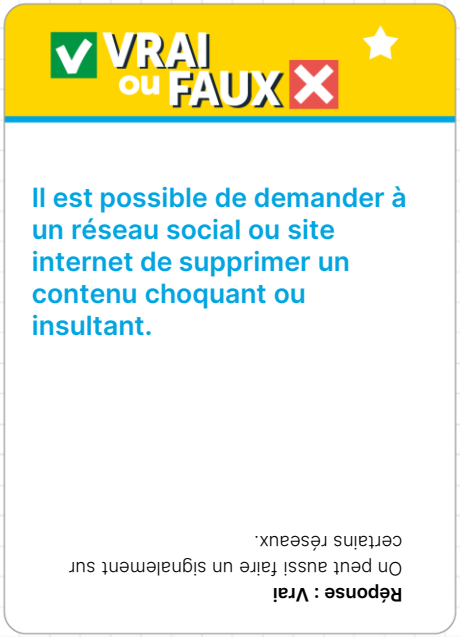
Réponse : Vrai

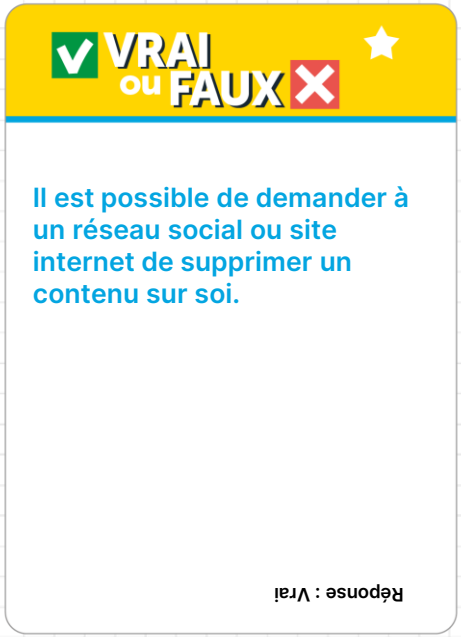
Explications

Par défaut, les paramètres de visibilité sur les réseaux sociaux sont souvent très ouverts et un profil public permet à n’importe qui de consulter les informations personnelles et les publications.

Il est généralement possible de restreindre cette visibilité en réglant la configuration du compte, afin de garder la maîtrise de ce que les autres utilisateurs voient.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/reseaux-sociaux

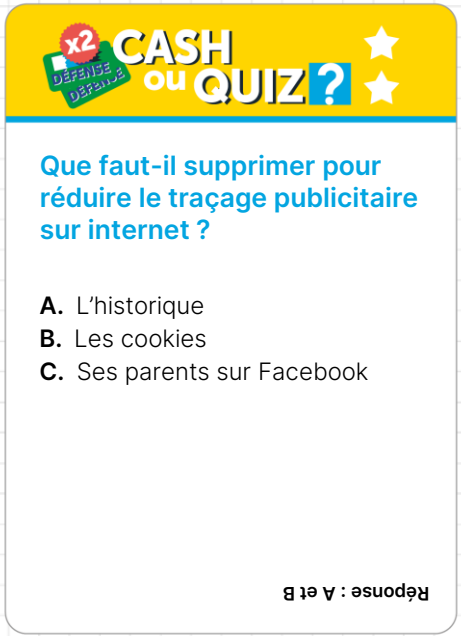




Explications

Les contenus illicites (incitation à la haine, violence contre les personnes ou les animaux, homophobie, pédophilie etc.) peuvent être signalés sur la plateforme PHAROS, qui est gérée par des policiers et des gendarmes spécialisés.
Certaines plateformes de réseaux sociaux proposent également leur propre système de signalement, en voici quelques exemples : Instagram, Snapchat, Discord, TikTok, WhatsApp, YouTube, Facebook, Twitter.

Sources :
https://www.service-public.fr/particuliers/vosdroits/F31979
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/que-faire-en-cas-de-cyberharcelement-ou-harcelement-en-ligne#definition-cyberharcelement



Explications

Pour limiter le traçage sur internet, voici trois bonnes pratiques à mettre en œuvre :

- Refuser par défaut le dépôt de cookies non essentiels à la navigation sur les sites consultés (la demande de consentement est obligatoire sur les sites français) ;
- Effacer régulièrement les cookies déposés par les sites web sur le navigateur ;
- Effacer régulièrement l’historique de navigation.

Sources :
https://www.cnil.fr/fr/faites-regulierement-le-menage-dans-lhistorique-de-navigation
https://www.cnil.fr/fr/cookies-et-autres-traceurs/comment-se-proteger/maitriser-votre-navigateur

QUIZ

À quoi sert la navigation privée ?

A. À limiter les cookies
B. À me rendre anonyme sur internet
C. À supprimer automatiquement mon historique

Réponse : A et C

Explications

L’option « navigation privée » est activable depuis n’importe quel navigateur (Qwant, Google, Firefox, Edge, etc) et permet de ne pas enregistrer certaines informations au cours de la navigation comme les mots de passe, l’historique ou encore les cookies : quand la session est coupée, ces informations ne sont pas conservées.

Cependant, cela ne rend pas anonyme sur internet : tant que le navigateur est ouvert, les cookies continuent d’être déposés. Il en est de même pour l’historique. De plus, la navigation privée n’empêche pas un site ou votre fournisseur d’accès à internet de vous identifier par d’autres biais (IP par exemple).

Source : https://www.cnil.fr/fr/la-navigation-privee-pour-limiter-les-risques-de-piratage-de-vos-comptes-en-ligne

QUIZ

Compléter la phrase suivante : “Quand un jeu est gratuit, c’est que le produit…”

A. … n’est pas top
B. … c’est toi
C. … est vieux

Réponse : B
Quand un jeu est gratuit, c’est ton “temps d’attention” qui est vendu aux entreprises qui font de la publicité.

Explications

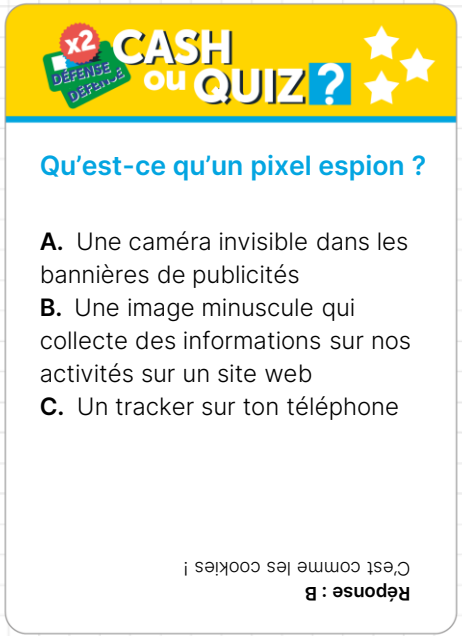
Le modèle « free-to-play » consiste à distribuer un jeu gratuitement… au moins partiellement. Le plus souvent, il est disponible en téléchargement gratuit et peut ensuite être joué sans limitation de durée.

En réalité, dans la plupart des cas, seule une portion du jeu ou certaines fonctionnalités sont accessibles gratuitement.

Il s’agit d’un réel modèle économique : les plateformes mettent le joueur dans une situation d’inconfort dans le jeu (interface peu pratique, inventaire trop petit, manque de certaines options…), le poussant ainsi à « consommer » des publicités ou acheter des crédits/jetons pour obtenir d’autres fonctionnalités.

Il est d’ailleurs prouvé que l’utilisation d’une monnaie fictive contribue à faire perdre le sens de la valeur réelle de l’achat.

Source : https://www.pedagojeux.fr/comprendre-le-jeu-video/les-modeles-economiques/



Explications

Le tracking pixel ou pixel espion est une méthode de traçage alternative aux cookies, traditionnellement mise en œuvre sous la forme d’une image de 1 pixel par 1 pixel, intégrée dans le site mais invisible pour l’utilisateur.

Le chargement de cette image, dont le nom contient un identifiant de l’utilisateur, informe le serveur sur lequel elle est hébergée que l’utilisateur tracé a visité une page ou lu un courriel.

Source : https://www.cnil.fr/fr/definition/tracking-pixelweb-beacon-ou-pixel-espion

Pour aller plus loin - Vie privée

Plus d’informations sur la protection de la vie privée et les risques associés :

- CNIL I Les droits pour maitriser vos données personnelles
- CNIL I 1 heure pour adopter de meilleurs réflexes pour votre vie privée numérique
- CNIL I La navigation privée pour limiter les risques de piratage de vos comptes en ligne
- Service de police de la Ville de Montréal (SPVM) I Informations sur les cyberprédateurs
- Cybermalveillance.gouv I 10 mesures essentielles assurer votre sécurité numérique

Jeux pour apprendre à protéger sa vie privée :

- CNIL I Découvrez le jeu immersif Les gardiens du Numérique à la cité des sciences et de l’industrie
- CNIL I Un jeu de cartes pour rester net sur internet

7.f
Piratage

QUIZ

Que doit-on faire si on reçoit le SMS suivant : "Chronopost - Votre colis n'a pas pu être livré. RDV sur le lien suivant ..." ?

A. Je ne clique pas sur le lien contenu dans le SMS
B. Je regarde l'expéditeur : si le numéro s'affiche, c'est certainement du phishing
C. Je supprime le SMS si je pense qu'il est frauduleux

Réponses : A, B et C

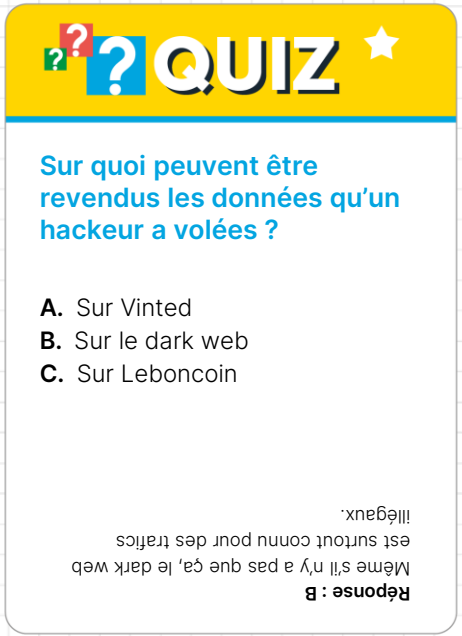
Explications

Les périodes de forte activité du commerce en ligne, comme les fêtes de fin d’année, les soldes ou bien encore le Black Friday sont très prisées des cybercriminels. Profitant du fait que de nombreuses personnes attendent ou envoient des colis, ils se font passer pour des sociétés de livraison parmi les plus connues pour piéger leurs victimes et leur voler des données personnelles ou de l’argent.

En cas de doute, il ne faut pas cliquer sur le lien, vérifier qui est l’expéditeur et enfin, il vaut mieux supprimer le SMS.

Il est également possible de signaler le SMS sur la plateforme : https://www.33700.fr/

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/escroqueries-livraison-colis



Explications

Le dark web est une zone d’Internet qui n’est pas accessible depuis votre navigateur traditionnel.

Le réseau offre un anonymat plus important que sur le web classique et c’est pourquoi il est utilisé par certains criminels pour vendre ou acheter des produits illégaux.

Cependant, cet espace n’est pas uniquement utilisé par des personnes mal intentionnées : l’anonymat permet également à des journalistes ou des opposants politiques vivant sous des dictatures d’accéder et de partager des informations.

Source : https://www.numerama.com/tech/1188862-dark-net-dark-web-de-quoi-parle-t-on.html

QUIZ

Qu’est-ce qu’un ransomware (ou rançongiciel en français) ?

A. Un logiciel malveillant qui bloque l’accès à l’ordinateur ou à des fichiers et qui réclame une rançon pour rendre l’accès
B. Un attaquant qui fait du chantage
C. Un email d’un hackeur qui demande de l’argent en échange des données qu’il a volé

Réponse : A

Explications

Le ransomware infecte un ordinateur lorsqu’il est téléchargé. Les cybercriminels vont donc redoubler d’effort pour pousser une victime à avoir confiance, par exemple :

- En le mettant en pièce jointe d’un mail de phishing ;
- En faisant croire à une mise à jour sur un téléphone portable ;
- En faisant croire que c’est une version gratuite d’un jeu ou d’un logiciel.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/ransomware-rancongiciel-definition

QUIZ

Qu'est-ce que le "phishing" ?

A. Un message envoyé par un hackeur qui cherche à tromper sa victime pour qu'elle lui donne des infos confidentielles
B. Un virus qui chiffre des données
C. Un virus qui espionne discrètement

Réponse : A

Explications

Appelé « hameçonnage » en français. On peut les répartir en plusieurs catégories :

- Phishing par mail
- Smishing par SMS
- Vishing par téléphone

A chaque fois l’objectif est le même : usurper l’identité d’une entreprise ou d’une personne de confiance afin de pousser la victime à effectuer des actions.

Le spear phishing est un type d’attaque ciblée, où l’on va se renseigner au maximum sur la victime afin de faire un message personnalisé et le plus crédible possible.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/dossier-phishing

QUIZ

Tu reçois un message d’un ami sur un réseau social. Il te dit qu’il a un problème et te demande de l’aider en urgence.
Ta première réaction est :

A. De lui passer un coup de fil
B. De faire ce qu’il te demande
C. De demander l’avis de tes followers

Réponse : A

Explications

Il existe de nombreuses variations mais les plus utilisées sont les suivantes :

- « Est-ce que ce n’est pas toi sur cette photo [URL] ? »
- « Peux-tu envoyer un SMS au numéro [NUM] ? »
- « Je suis en vacances à l’étranger, mais je me suis fait voler mon portefeuille et j’ai vraiment besoin d’argent pour rentrer, est ce que tu peux me faire un virement ?»

Avant de faire quoi que ce soit, contacte ton ami par un autre biais pour vérifier si c’est bien lui et s’il a effectivement un problème ou souhaite te montrer quelque chose.

Il ou elle s’est probablement fait pirater son compte et le cybercriminel usurpe son identité.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-savoir-si-on-est-victime-d-us

QUIZ

Tu reçois un message qui te dit que ta webcam a été piratée et qu’on a des vidéos compromettantes de toi. Que dois-tu faire ?

A. Répondre au message pour en savoir plus
B. L’ignorer et prévenir un adulte
C. Garder des preuves

Réponse : B et C

Explications

Les tentatives de chantage à la webcam sont relativement courantes. Dans la grande majorité des cas, les prétendus « hackers » n’ont pas eu accès à la caméra mais utilisent des moyens plus ou moins convaincants pour le faire croire à leur victime.

Il est effectivement possible, dans certains cas relativement rares qu’un attaquant puisse prendre le contrôle d’une webcam : soit parce que la victime a installé un logiciel malveillant ou s’est rendue sur un site internet contrôlé par un attaquant et a autorisé l’accès à la webcam.

Dans tous les cas, il est important de ne pas céder à la panique, de ne pas répondre aux sollicitations qui peuvent être très agressives et oppressantes, de garder des preuves (captures d’écrans, mails…) et, pour les jeunes, de prévenir un adulte de confiance qui réalisera les démarches nécessaires.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/campagnes-darnaques-au-chantage-a-la-webcam-pretendue-piratee

QUIZ

Un joueur sur Fortnite m’envoie un lien par message ou dans le chat pour télécharger un skin gratuit… Que faire ?

A. Génial, je clique direct
B. C’est forcément un lien approuvé par l’éditeur du jeu, je clique
C. C’est potentiellement un lien malveillant, je reste vigilant

Réponse : C

Explications

Plusieurs rapports de sociétés spécialisées mettent en évidence que les campagnes de piratage opérées dans les jeux vidéo sont en forte augmentation depuis plusieurs années.

Les principales arnaques consistent à proposer des prétendus lots de monnaies virtuelles ou encore des packs pour améliorer les caractéristiques de son personnage. Les hackers misent sur la naïveté des joueurs dans l’espoir de voler les données bancaires de leurs parents.

Il faut rester vigilant : si c’est trop beau pour être vrai, c’est probablement une arnaque.

Source : https://www.numerama.com/cyberguerre/1287618-vous-jouez-a-minecraft-ou-roblox-vous-etes-une-cible-privilegiee-des-hackers.html

QUIZ

Sur un ordinateur, positionner sa souris sur un lien permet souvent :

A. De vérifier l'émetteur
B. D'afficher l'adresse du site internet où va le lien
C. De vérifier si le lien est légal

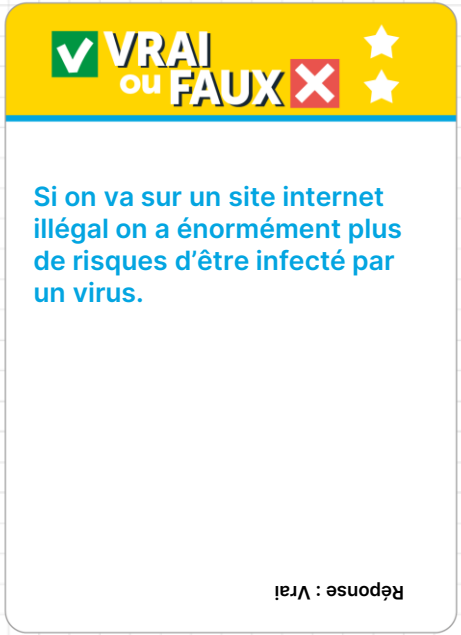
Réponse : B

Explications

Avant de cliquer sur un lien douteux, il faut prendre l'habitude de pointer le curseur de la souris sur ce lien (sans cliquer) ce qui affichera alors l'adresse vers laquelle il pointe réellement.

Si l'on est sur un site web, il faut bien regarder le coin inférieur gauche du navigateur où apparaitra l'URL du site de destination du lien. En effet le texte de substitution peut également être modifié.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing



Explications

Les adolescents peuvent être tentés de se rendre sur des sites web douteux, notamment parce qu’ils proposent des services « gratuits » comme les sites de streaming illégaux ou de téléchargements de logiciels « crackés ». Ces sites peuvent installer des logiciels malveillants ou afficher des messages alarmants pour faire télécharger des solutions payantes très chères et inutiles.

Cybermalveillance.gouv alerte sur la dangerosité des sites suivants :

- Les sites de téléchargement pirates ;
- Les sites de vidéo en ligne (streaming) ou de vidéo à la demande (VOD) pirates ;
- Les sites pornographiques pirates.

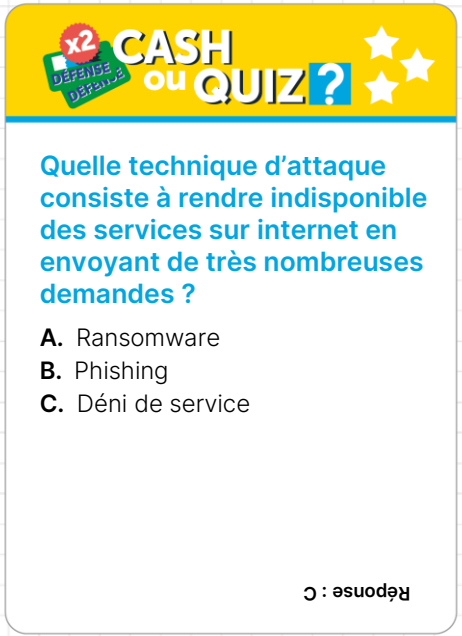
Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-se-proteger-sur-internet

Explications

Grâce à la recherche d’image inversée, une personne peut retrouver tous les sites où une image donnée apparaît.

Ainsi, si une personne utilise la même photo sur tous ses comptes, un individu mal intentionné pourra retrouver tous les comptes qui sont liés et ainsi récupérer encore plus d’informations sur elle, potentiellement pour la pirater, la harceler ou la faire chanter.

Source : https://www.quechoisir.org/actualite-photos-en-ligne-partager-n-est-pas-sans-danger-n4693/



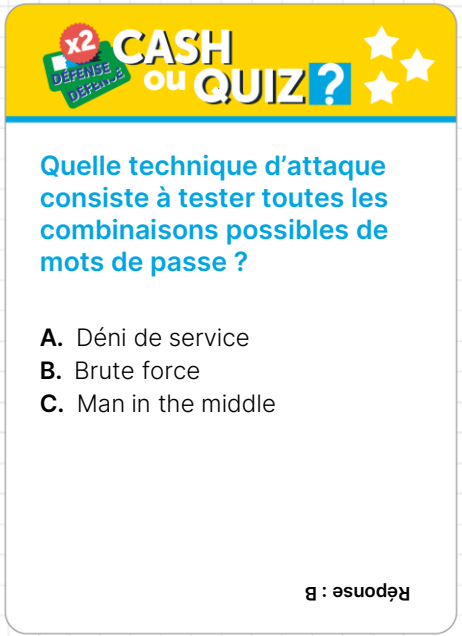
Explications

L’attaque par Déni de service (ou DOS/DDOS en anglais) a lieu lorsqu’un attaquant submerge un site internet ou une application de demandes.

Face à l’afflux de requêtes, les serveurs peuvent avoir du mal à tout traiter et dans certains cas s’effondrent (crash).

Ces attaques peuvent avoir lieu quand un groupe de personnes se coordonnent mais également grâce à l’utilisation de « botnet » : un réseau d’appareils ayant été piratés comme des caméras de surveillance.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/attaque-en-deni-de-service-ddos



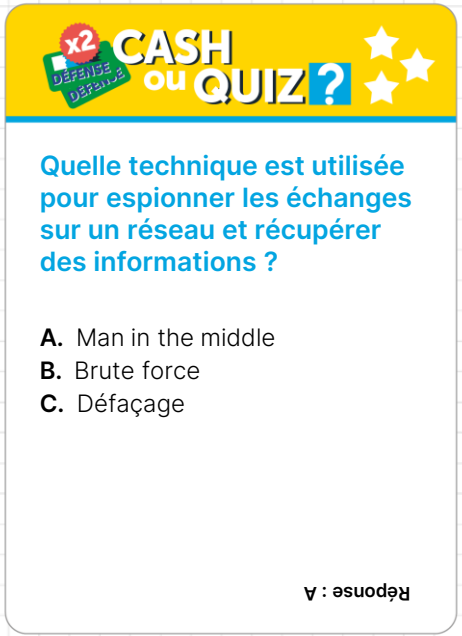
Explications

Dans le cas d’une attaque par « brute force », l’attaquant va tester toutes les combinaisons possibles : AAAA, AAAB, AAAC etc…

Actuellement, avec la puissance de calcul des ordinateurs, si le mot de passe fait moins de 6 caractères et même s’il est composé de lettres majuscules et minuscules, de chiffres et de caractères spéciaux, il est possible de le trouver presque instantanément.

Cependant dans la réalité, les attaquants vont plutôt utiliser des dictionnaires composés des mots de passe les plus probables. Par exemple : Azerty1234, Soleil, etc…

Source : https://www.francenum.gouv.fr/magazine-du-numerique/combien-de-temps-un-pirate-met-il-pour-trouver-votre-mot-de-passe-comment



Explications

Man in the Middle (ou l’homme du milieu en français) est un type d’attaque qu’un hackeur-euse peut réaliser par exemple sur un réseau public.

Il va se mettre entre sa victime et l’application qu’elle cherche à utiliser afin de récupérer les données qu’elle envoie, comme son mot de passe par exemple. C’est pour cela qu’il est recommandé de ne pas utiliser d’applications sensibles (boîte email, réseaux sociaux) sur un réseau public (gare, aéroport…)

Source : https://www.pandasecurity.com/fr/mediacenter/securite/attaque-man-in-the-middle/

QUIZ

Que signifie le cadenas devant l’URL d’un site web ?

A. Que le site est totalement sécurisé, donc tu peux renseigner ton mot de passe par exemple
B. Que les échanges entre le serveur qui héberge le site et ton mobile / ordinateur sont sécurisés
C. Que le site est légal et donc que tu peux télécharger en toute confiance

Réponse : B

Explications

Contrairement à la croyance populaire, le cadenas ne veut pas dire qu’on peut faire confiance au site internet.

Cela signifie que :

- Le site est bien ce qu’il prétend être (il n’essaye pas de se faire passer pour un autre)
- L’appareil utilisé et le site vont communiquer par messages codés (on dit que les communications sont chiffrées). Ainsi, si un hackeur se trouve sur le même réseau, il ne pourra pas récupérer les informations qui transitent sur le réseau (identifiants, messages privés ou cartes bancaires sur un site de paiement par exemple).

Source : https://numeriqueethique.fr/ressources/articles/https-5-raisons-de-sinteresser-aux-cadenas-qui-securisent-le-web

QUIZ

En 1986, un des premiers virus informatiques, nommé Brain, a massivement infecté des ordinateurs. Il n'avait pourtant pas été créé avec de mauvaises intentions. À l'origine, son but était de :

A. Une protection contre la copie illégale
B. Un jeu vidéo
C. Une application pour s'envoyer des messages

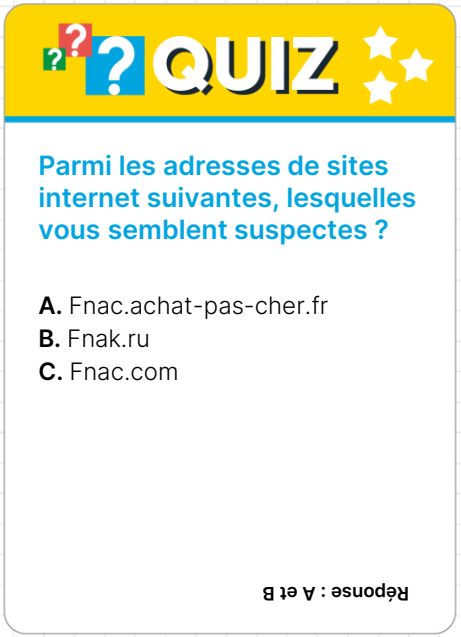
Réponse : A

Explications

"Brain" était l'un des tous premiers malwares qui a été créé en 1986 par deux frères pakistanais : Basit et Amjad Farooq Alvi. Ils l'ont développé afin d'éviter les copies illégales du programme informatique qu'ils avaient créé.

Le virus "Brain" n'avait pas été conçu dans un objectif malveillant comme les virus modernes. Il affichait simplement un message sur l'écran des ordinateurs infectés, indiquant que l'utilisateur utilisait un programme piraté et invitait celui-ci à contacter les frères Alvi pour la « vaccination ». Cependant, en propageant le virus via des disquettes (les ancêtres des clefs USB) partagées entre les ordinateurs, cela a pris beaucoup plus d'ampleur que le prévoyaient ses concepteurs.

Source : https://www.welivesecurity.com/fr/2018/11/06/logiciels-malveillants-1980-morris/



Source : https://powerdmarc.com/fr/what-is-url-phishing/

Explications

Lorsque l’on veut vérifier si une URL est valide il faut faire attention à plusieurs choses :

- L’orthographe : les attaquants vont essayer de mettre des caractères proches pour nous tromper : 1 à la place du I majuscule ou i majuscule à la place du L minuscule. Exemple : google.com (‘l’ est remplacé par ‘i’ majuscule)
- Le nom de domaine : Le domaine principal est le nom du site, suivi de l’extension (.com, .org, .net, etc.). Il convient de s’assurer qu’il correspond au site que vous souhaitez visiter. Ainsi, même s’il contient Fnac avec la bonne orthographe « Fnac.achat-pas-cher », n’est pas le site de la Fnac.

QUIZ

Comment repérer qu’on s’est fait pirater son téléphone ?

A. On ne peut pas toujours le détecter
B. La batterie peut se décharger plus vite
C. On peut avoir des pubs constantes qui popent

Réponse : A, B et C

Sources :
https://www.avg.com/fr/signal/bitcoin-miner-malware
Pegasus (logiciel espion) — Wikipédia (wikipedia.org)

Explications

Les conséquences d’un piratage dépendent du type de malware.

Certains vont ouvrir des « pop-up » de publicités pour inciter à s’inscrire sur certains sites ou télécharger certaines applications.

D’autre vont effectuer des opérations sur le téléphone, pour récupérer les données personnelles mais également forcer le téléphone à faire des opérations sans que l’on s’en aperçoive, par exemple dans l’objectif de gagner de l’argent grâce au crypto monnaies. Ces opérations étant lourdes, cela pousse ton téléphone à consommer plus de batterie.

Enfin, certains malwares très poussés comme Pegasus sont pratiquement indétectables.

QUIZ

Qu’est-ce que la technique de défaçage d’un site web ?

A. La mise hors service du site
B. La modification du site web
C. Le vol de données privées

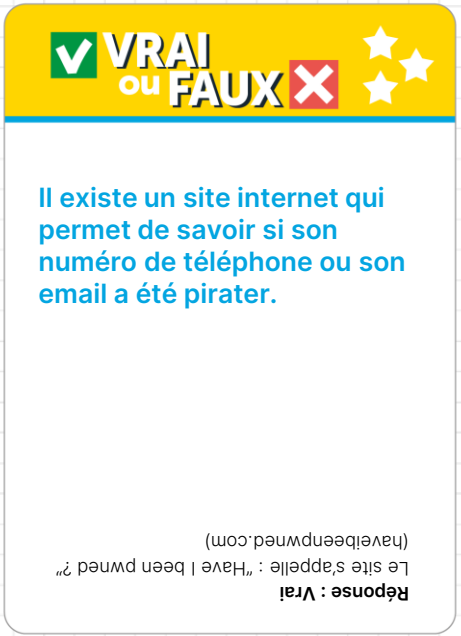
Réponse : B

Explications

Le défaçage, défacement ou défiguration d’un site correspond à la modification d’un site web, cela dans le but de nuire à l’image ou à la crédibilité du propriétaire en remplaçant ou détournant son contenu.

Cela peut également servir à faire valoir des revendications idéologiques ou politiques, notamment lorsque des sites de médias sont touchés.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/defiguration-de-site-internet



Source : https://fr.wikipedia.org/wiki/Have_I_Been_Pwned%3F

Explications

Créé en 2013 par Troy Hunt, l’application ressence les différents piratages des sites internet et permet ainsi à chacun de savoir si son adresse email ou son numéro de téléphone se trouve dans une base de données volées.

On peut également savoir à quoi les hackeurs ont accès : numéro de téléphone, adresse physique, mot de passe.

Le mieux est de tester régulièrement ses comptes et de changer tous les mots de passe qui auraient pu être récupérés.

Pour aller plus loin - Piratage

Comprendre et se protéger contre cyberattaques :

- Youtube I Le Ransomware expliqué en 5 minutes
- Youtube I Malware : comprendre l'essentiel pour se protéger
- Konbini sur Youtube I Comment ENFIN ne plus se faire piéger par du phishing ?
- Cybermalveillance.gouv I Identifier et déjouer le hameçonnage
- CNIL I Réagir en cas de chantage à la webcam
- CNIL I Comment réagir face à une usurpation d'identité ?

Réviser ses connaissances en famille :

Cybermalveillance.gouv I Cyber guide famille

Les jeux pour parler de cybersécurité :

- Cybermalveillance.gouv I Mallette cyber inclusion numerique
- Région académique Bourgogne-Franche-Comté I Le kit CyberEnJeux de l'ANSSI
- Eduscol I Education et cybersécurité
- Cyber Duel de Game Partners

Autre ressource :

Bande dessinée - Les enquêtes de Seven

7. Se former à la cybersécurité

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) propose une formation pour s'initier à la cybersécurité, approfondir vos connaissances, et ainsi agir efficacement sur la protection de vos outils numériques. Ce dispositif est accessible gratuitement. Le suivi intégral de ce dispositif vous fera bénéficier d'une attestation de réussite.

Rendez-vous sur : https://secnumacademie.gouv.fr/

8. FAQ

Comment réagir si on me pose une question dont je ne connais pas la réponse ?

Nous avons tenté de mettre le plus d'informations possibles dans ce guide pour vous permettre de répondre à la plupart des questions que pourraient avoir les participants. Cependant il est toujours possible que vous soyez confronté à une question dont vous ne trouvez pas immédiatement la réponse. Dans ce cas, nous vous recommandons d'être transparent : avouez ne pas savoir. Vous pouvez alors lui proposer de vous renseigner et de revenir vers lui ou bien lui proposer de chercher la réponse de son côté et ensuite de la transmettre à l'ensemble du groupe.

Vous pouvez également nous transmettre vos questions à l'adresse fresquedescybercitoyens@advens.fr pour que nous puissions intégrer la réponse dans le guide.

Comment réagir si un jeune vient se confier concernant une situation de harcèlement ? (1/2)

Le contexte du jeu peut amener certains jeunes à venir se confier à vous concernant des situations de harcèlement dont ils ont été ou sont toujours victimes ou témoins. D'ailleurs, nous insistons beaucoup dans le jeu pour rappeler qu'il faut en parler à un adulte de confiance.

Il est difficile d'établir une recommandation globale, mais voici quelques conseils de la fondation de France : https://www.fondation-enfance.org/jai-besoin-daide/je-suis-adulte/mon-enfant-est-temoin/suis-enseignant-directeur-decole-chef-detablissement/

Il est essentiel dans tous les cas de :

- Faire attention à ne pas minimiser la situation ou son impact sur le jeune ;
- Recueillir la parole de la personne qui se confie ;

…

Comment réagir si un jeune vient se confier concernant une situation de harcèlement ? (2/2)

Il est essentiel dans tous les cas de :

- Réagir proportionnellement à la situation décrite, mais réagir dans tous les cas ;
- S'informer : il n'est pas toujours facile d'identifier une victime de harcèlement, mais certains indices peuvent mettre sur la voie (isolement, décrochage scolaire…) ;
- Vous pouvez également appeler les numéros suivants pour obtenir des conseils :
    - 3018 (Accessible par Whatsapp, Messenger, Appel, Mail) : le numéro national pour les jeunes victimes de violences numériques et toutes les questions liées aux usages numériques. Retrouvez les infos sur https://e-enfance.org/numero-3018/besoin-daide/
    - 3020 (Appel) : Le numéro national pour les victimes de harcèlement en contexte scolaire.

Je ne suis pas un expert de la cybersécurité, comment vais-je faire pour animer ? (1/2)

Premièrement, ce n'est pas à vous qu'il incombe la charge d'apporter les connaissances sur la cybersécurité : le jeu et le guide ont été réalisés par des professionnels du domaine. Nous avons tenté de le rendre le plus « clé en main » possible pour qu'une personne sans connaissance préalable puisse l'animer après une rapide formation et la lecture de ce guide.

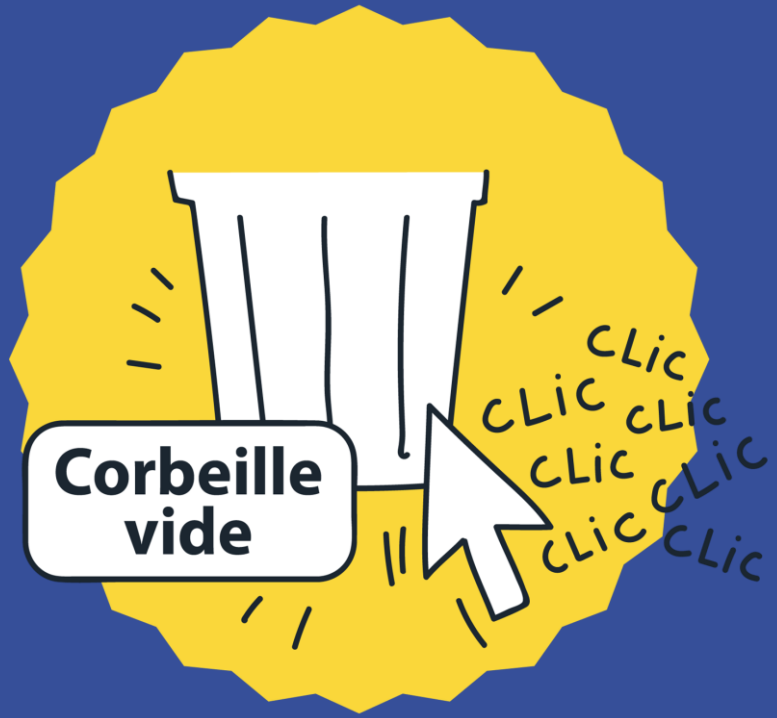
De plus, le jeu est quasiment autoporteur. Vous pouvez donc animer des ateliers, même sans compétence technique préalable.

Enfin, en admettant humblement votre propre « non-expertise » dans ce domaine, vous pouvez créer un environnement propice à l'apprentissage collaboratif. Encouragez la réflexion critique, favorisez les discussions et fournissez des ressources (définitions, scénario…) pour aider les participants à se former à être des cybercitoyens et cybercitoyennes responsables.

Je ne suis pas d'accord avec une carte, que puis-je faire ?

Il est difficile parfois de trouver l'équilibre entre être exhaustif tout en restant dans la pédagogie : des choix ont donc été faits lors de la création de ce jeu. N'hésitez donc pas à vous approprier le jeu si vous pensez que cela peut permettre de renforcer les compétences des participants. N'hésitez pas à nous envoyer toutes vos suggestions d'amélioration afin que nous puissions enrichir le jeu à l'adresse suivante : fresquedescybercitoyens@advens.fr

Retrouvez le reste de la FAQ sur le site web « www.fresquedescybercitoyens.fr »



9. GLOSSAIRE

9. Glossaire

Mot	Définition
Antivirus	Un logiciel conçu pour détecter, prévenir et éliminer les logiciels malveillants de votre système informatique.
Application	Un programme informatique conçu pour effectuer des tâches spécifiques sur un dispositif électronique, comme un smartphone ou un ordinateur.
Brute force	Une méthode d'attaque informatique où toutes les combinaisons possibles sont essayées pour trouver un mot de passe ou une clé de chiffrement.
Chiffrer	Protéger des données en les transformant en un code illisible sans la clé de déchiffrement correspondante.

9. Glossaire

Mot	Définition
ChatGPT	Un modèle de langage développé par OpenAI, capable de comprendre et de générer du texte en langage naturel.
Cloud	Un service de stockage en ligne permettant d'accéder aux données via Internet plutôt que depuis un disque dur local.
Code PIN	Un numéro confidentiel utilisé pour authentifier un utilisateur, souvent associé à des cartes bancaires ou des appareils électroniques.
Compte	Un ensemble d'informations personnelles et d'autorisations associées à un utilisateur dans un système informatique.

9. Glossaire

Mot	Définition
Cookies	De petits fichiers texte stockés sur un ordinateur par un navigateur web, contenant des informations sur les habitudes de navigation de l'utilisateur.
Cyberharcèlement	L'utilisation d'Internet et des technologies pour harceler, menacer ou intimider une personne
Cyberprédateur	Une personne utilisant Internet pour cibler et exploiter des individus vulnérables, en particulier des mineurs.
Dark web	Une partie d'Internet inaccessible aux moteurs de recherche conventionnels, souvent associée à des activités illégales.

9. Glossaire

Mot	Définition
Défaçage	Modifier le contenu d'un site web, souvent dans un but malveillant, pour afficher un message ou une image indésirable.
Déni de service	Une attaque visant à rendre un service indisponible en submergeant le serveur de requêtes.
Données	Informations stockées, traitées et utilisées par des systèmes informatiques.
Double authentification	Un mécanisme de sécurité exigeant deux formes d'identification différentes pour accéder à un compte ou un système.

9. Glossaire

Mot	Définition
Fake news	Informations fausses ou trompeuses présentées comme des faits réels, généralement diffusées sur Internet.
Faire chanter	Menacer de divulguer des informations compromettantes pour obtenir un avantage, souvent sous la forme d'argent.
Gestionnaire de mots de passe	Un outil facilitant la gestion et la sécurisation des mots de passe en les stockant de manière chiffrée.
Hackeur	Une personne utilisant ses compétences techniques pour accéder à des systèmes informatiques de manière non autorisée. Il existe cependant des hackeurs éthiques qui agissent légalement pour trouver des failles dans des systèmes d'information.

9. Glossaire

Mot	Définition
Historique	La liste des sites web visités et des actions effectuées sur un navigateur web.
Intelligence artificielle	Des systèmes informatiques conçus pour effectuer des tâches nécessitant une intelligence humaine, comme l'apprentissage et la résolution de problèmes.
Logiciel malveillant	Un programme informatique conçu pour causer des dommages, collecter des informations ou compromettre la sécurité d'un système.
Man in the middle	Une attaque où un attaquant intercepte et éventuellement modifie les communications entre deux parties sans leur consentement.

9. Glossaire

Mot	Définition
Métadonnées	Des données décrivant d'autres données, fournissant des informations contextuelles sur l'origine, le contenu, le format, etc.
Mot de passe	Une séquence de caractères utilisée pour vérifier l'identité d'un utilisateur et accéder à un compte ou un système.
Mot de passe complexe	Un mot de passe avec une combinaison de lettres, chiffres et caractères spéciaux, renforçant sa sécurité.
Navigation privée	Un mode de navigation sur Internet qui ne stocke pas l'historique de navigation ni les cookies.

9. Glossaire

Mot	Définition
Pirater	Accéder à un système informatique de manière non autorisée.
Phishing	Une technique d'escroquerie en ligne visant à tromper les gens pour obtenir leurs informations personnelles, comme les mots de passe.
Profil (réseau social)	Une page personnelle ou professionnelle créée par un utilisateur sur une plateforme de médias sociaux.
Pseudonyme	Un nom fictif utilisé pour protéger l'identité réelle d'une personne en ligne.

9. Glossaire

Mot	Définition
Rançongiciel / Ransomware	Un type de logiciel malveillant qui chiffre les données d'un utilisateur et demande une rançon en échange de leur libération.
Risque	La probabilité de subir des dommages ou des pertes liés à des menaces informatiques.
Sauvegarde	Une copie de données importantes effectuée pour prévenir la perte en cas de défaillance du système.
Source	L'origine ou la provenance d'une information, d'un fichier ou d'un programme.

9. Glossaire

Mot	Définition
Rançongiciel / Ransomware	Uniform Resource Locator, l'adresse spécifique qui identifie une ressource sur Internet.
Usurper l'identité	Faire semblant d'être quelqu'un d'autre en ligne, généralement dans le but de tromper ou de nuire.
Virus	Un programme informatique malveillant capable de se reproduire et d'infecter d'autres programmes ou fichiers.
VPN	Virtual Private Network, un réseau privé virtuel permettant de sécuriser et d'anonymiser la connexion à Internet.

Mot	Définition
Wifi public	Un réseau sans fil accessible au public, souvent disponible dans des lieux publics tels que les cafés, les aéroports, etc.