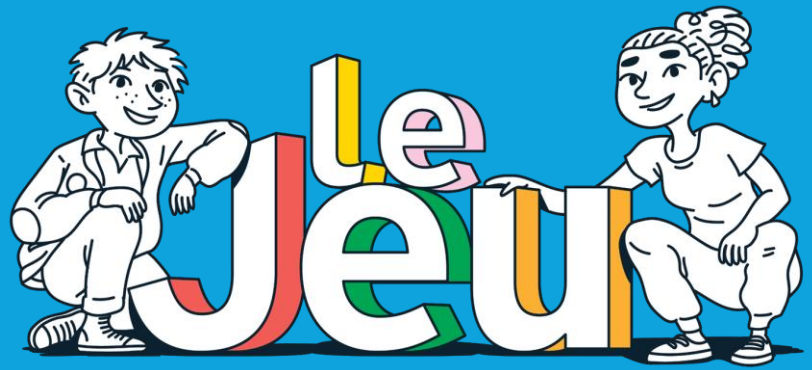
FRESQUE DES CYBERCITOYENS



Guide des cartes - v3

2025 I By aDvens
for People and Planet

Comment utiliser ce guide ?

Ce guide des cartes et sources a pour objectif de recenser toutes les cartes « Quiz », « Cyberattaques » et « Défense » du jeu, en fournissant des explications et en indiquant toutes nos sources. Vous pouvez l'utiliser dans plusieurs cadres :

- Une carte quiz pose problème ou est difficile : vous pouvez vous référer à ce guide pour donner un complément d'explication à la carte.
- Vous souhaitez approfondir un sujet lié à une séquence pédagogique : vous pouvez intégrer une ou plusieurs cartes à votre séquence puis présenter les explications au tableau ou encore approfondir la thématique avec les pages « pour aller plus loin »

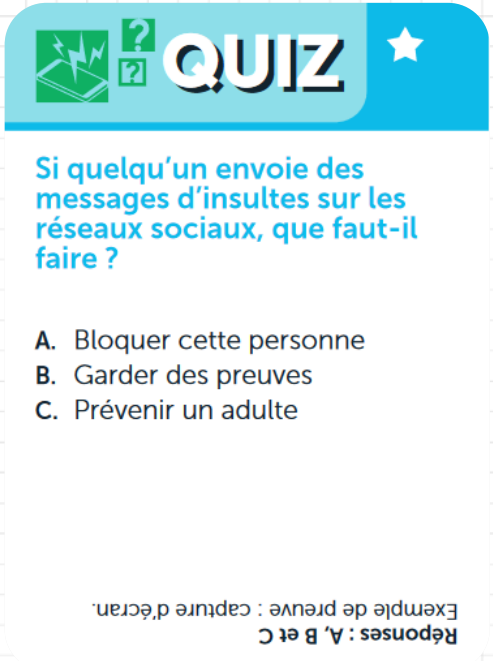
Pour naviguer dans ce guide :

1. Utiliser le sommaire page 3 : vous pouvez cliquer sur les titres pour vous rendre directement dans une section du manuel ;
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 manuel n'est pas fait pour être imprimé. Le jour de votre animation, munissez-vous du « Tuto Express » qui reprend toutes les informations essentielles, et de la présentation des règles à projet aux participants.

SOMMAIRE

1. Thématique Cyberharcèlement



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

1. Thématique “Cyberharcèlement” - Niveau 1

Explications

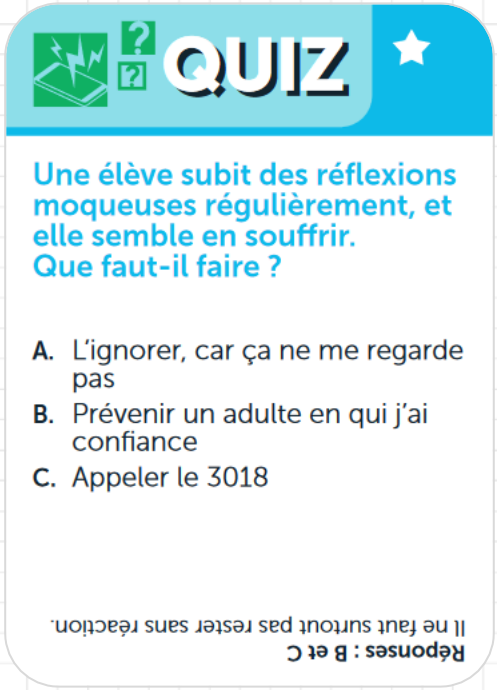
Les contenus inappropriés ou illicites, notamment les photos et vidéos humiliantes, peuvent être signalés auprès des plateformes sur lesquels ils sont présents afin de les faire supprimer, d’autant plus s’ils concernent une personne mineure.

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 des preuves au cas où la victime déciderait de porter plainte.

On peut également se faire aider en appelant le 3018, qui peut faire supprimer des contenus en quelques heures.

Source : https://www.cnil.fr/fr/publication-genante-sur-les-reseaux-sociaux-signalez-pour-supprimer

1. Thématique “Cyberharcèlement” - Niveau 1



Explications

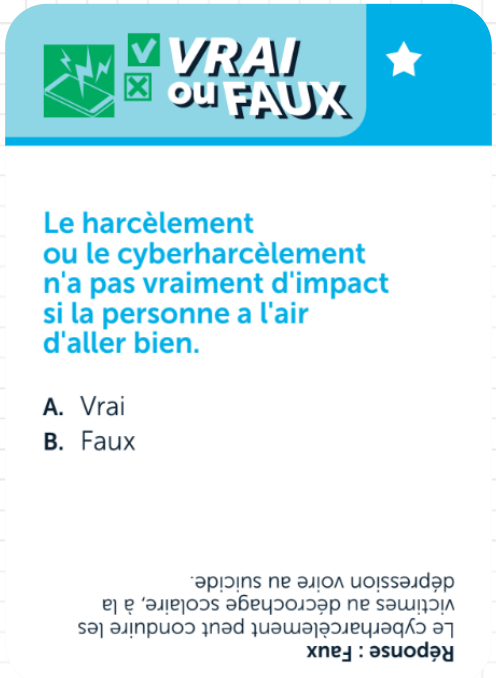
Lorsque l’on est victime ou témoin de harcèlement, il est important d’en parler à un adulte qui prendra la situation au sérieux et réagira.

On peut également contacter le 3018, un numéro gratuit, anonyme et confidentiel qui est joignable 7 jours sur 7, de 9 h à 23 h, par téléphone, sur 3018.fr par tchat en direct 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/informer/cyber-harcelement/

1. Thématique “Cyberharcèlement” - Niveau 1



Explications

Le harcèlement ou cyberharcèlement peut entraîner des conséquences très graves, comme cela a été malheureusement démontré à plusieurs reprises à travers des drames relayés par les médias.

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 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

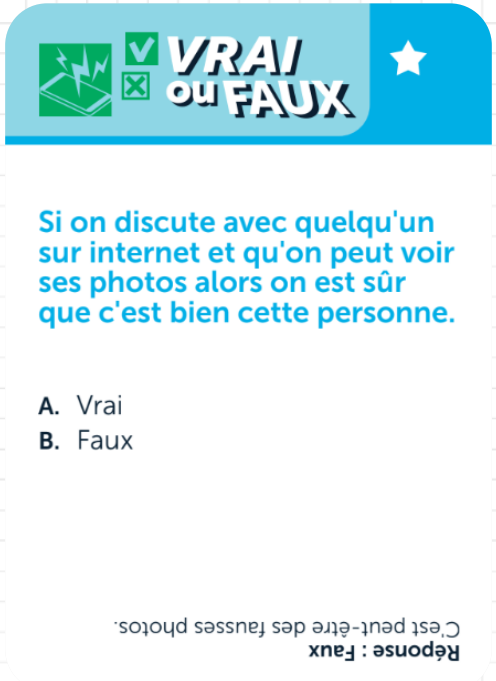
Liker un commentaire insultant c’est encourager la personne qui harcèle et valider son comportement. En réagissant ainsi ou en diffusant des propos de harceleurs, un individu tend à aggraver la situation et son impact sur la victime. Il est donc complice.

De plus, le fait de partager ou de donner de la visibilité à ce type de propos/photos/vidéos 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

1. Thématique “Cyberharcèlement” - Niveau 1



Explications

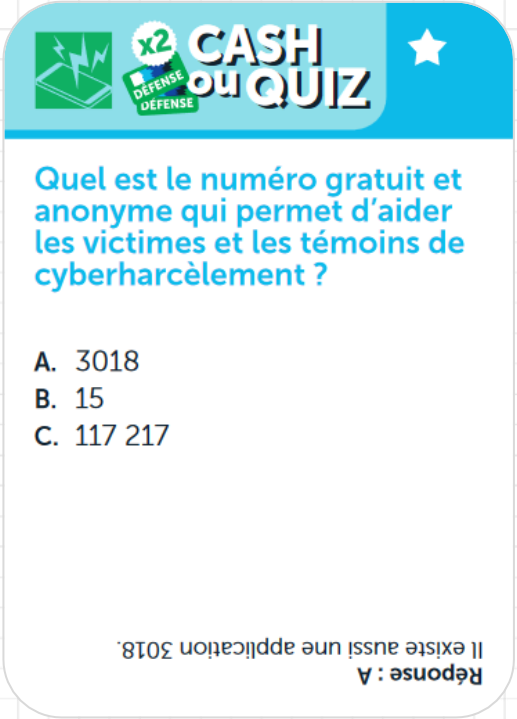
Une personne malintentionnée peut facilement usurper l’identité de quelqu’un d’autre ou se créer une fausse identité sur internet.

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 cyberprédateurs, 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

1. Thématique “Cyberharcèlement” - Niveau 1



Source : https://e-enfance.org/le3018/

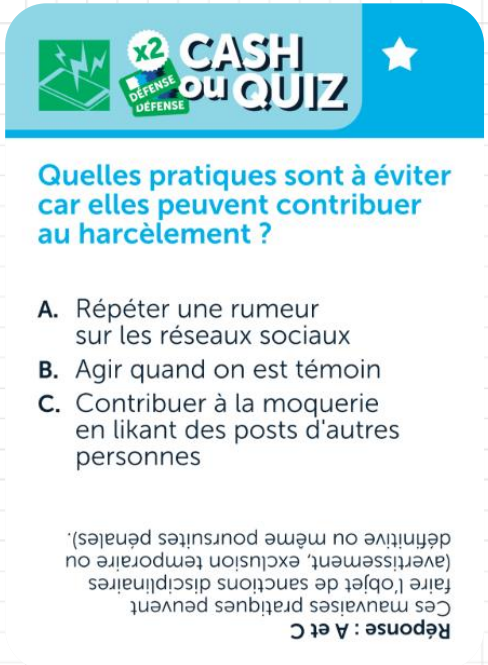
Explications

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. Cette dernière permet d’évaluer en une poignée de minutes si on est dans une situation de harcèlement.

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.

1. Thématique “Cyberharcèlement” - Niveau 1



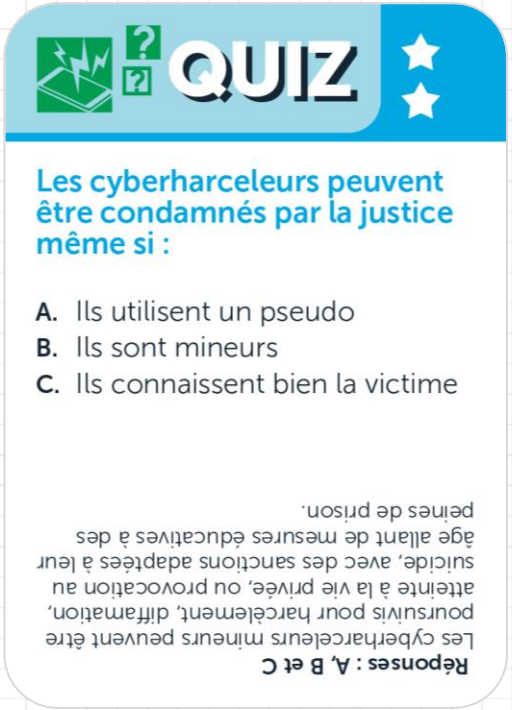
Explications

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/

1. Thématique “Cyberharcèlement” - Niveau 2



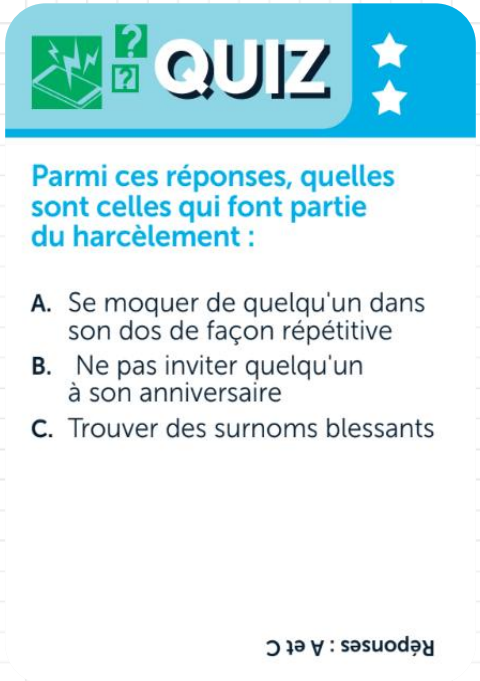
Explications

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-en-ligne
https://www.service-public.fr/particuliers/vosdroits/F32239

1. Thématique “Cyberharcèlement” - Niveau 2

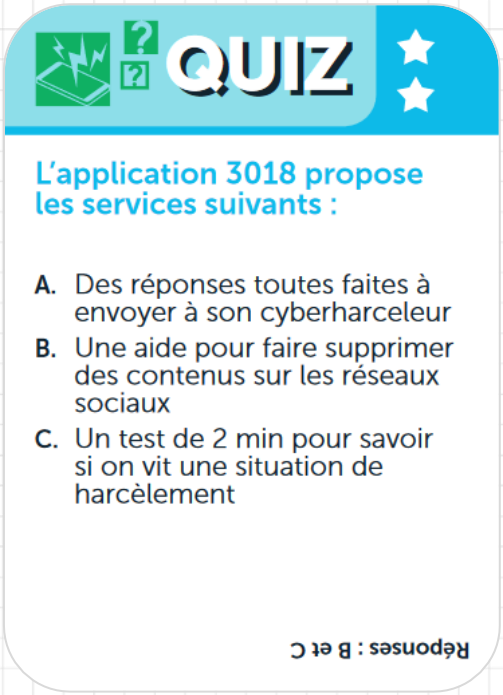


Source : https://e-enfance.org/informer/cyber-harcelement/

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



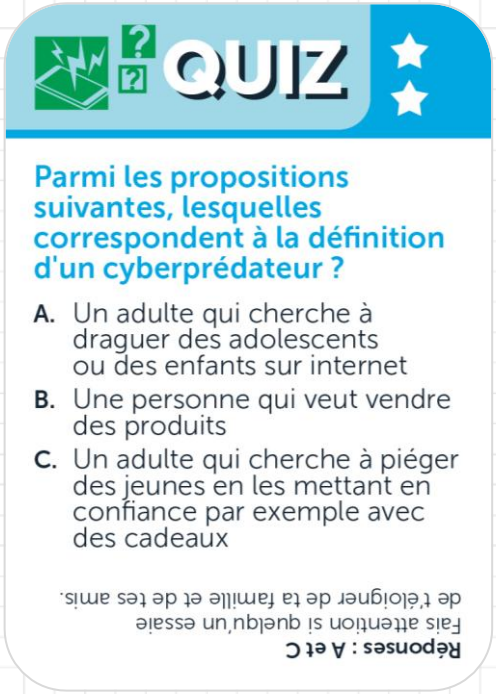
Source : https://e-enfance.org/numero-3018/besoin-daide/

Explications

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. Cette dernière permet d’évaluer en une poignée de minutes si on est dans une situation de harcèlement.

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.

1. Thématique “Cyberharcèlement” - Niveau 2

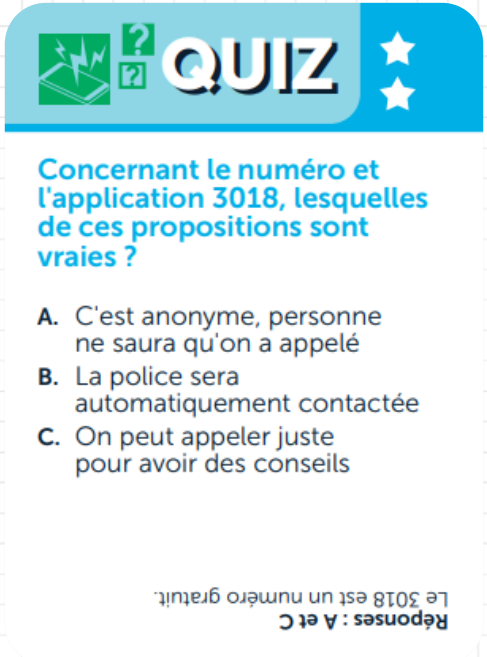


Source : https://spvm.qc.ca/fr/Jeunesse/Cyberpredateur

Explications

Un cyberprédateur cherche à manipuler des personnes vulnérables pour commettre des abus sexuels. Le cyber pédophile est un cyberprédateur qui cible des enfants.

D’après le Service de police de la Ville de Montréal (SPVM), il emploie toutes sortes de techniques pour tenter d’attirer des jeunes hors de la maison, de l’école ou d’autres endroits. Il peut faire des promesses en échange d’une rencontre, ou utiliser des cadeaux, de l’argent, comme appât.



Explications

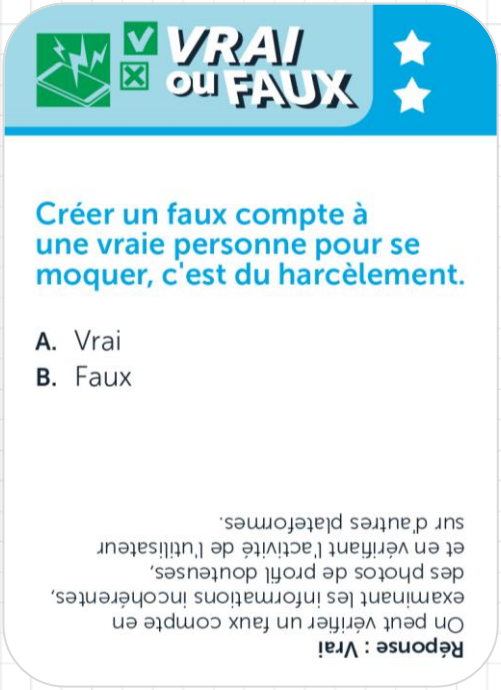
Le 3018 est un service gratuit, anonyme et confidentiel. Ni l’entourage, ni l’établissement scolaire, ni les autorités ne sont automatiquement informées de l’appel, sauf accord explicite de la personne qui contacte le service. Cette confidentialité est systématiquement mentionnée sur les sites officiels et dans la documentation du dispositif.

Si la situation l’exige, l’équipe peut conseiller de porter plainte et, avec l’accord de l’appelant, transmettre le signalement à des référents spécialisés (ex. académiques, plateforme PHAROS), mais ce n’est jamais automatique. Le choix appartient toujours à l’appelant.

Le 3018 sert aussi à conseiller et à accompagner, même sans situation d’urgence. L’appel n’est pas réservé aux victimes mais aussi aux témoins, aux proches et à toute personne ayant des questions sur les usages numériques, la sécurité sur Internet, l’exposition à certains contenus ou la prévention du harcèlement.

Sources : Victime de cyber harcèlement appeler le numéro 3018 L'application 3018 pour aider les victimes de cyberharcèlement | info.gouv.fr

1. Thématique “Cyberharcèlement” - Niveau 2



Explications

Il s’agit d’une usurpation d’identité, ce qui est déjà illégal. Par ailleurs, cela 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.

Sources : https://www.autonome-solidarite.fr/articles/lusurpation-didentite-sur-les-reseaux-sociaux-est-elle-reprehensible/

1. Thématique “Cyberharcèlement” - Niveau 3

Générer des photos, des vidéos ou des audios par l'IA de quelqu'un qu'on connait dans le but de se moquer peut être considéré comme du cyberharcèlement.

A. Vrai
B. Faux

Réponse : Vrai
Ce type de contenu manipulé, appelé généralement deepfake, est utilisé pour ridiculiser, intimider ou porter atteinte à la dignité de la victime, et peut aggraver la violence du harcèlement en ligne.

Explications

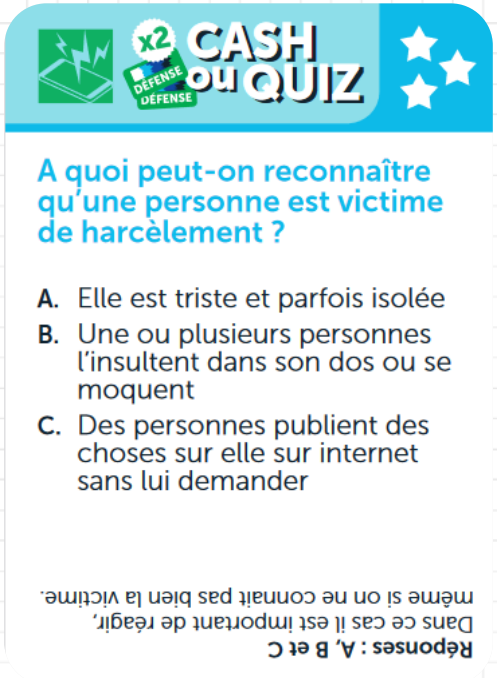
Le harcèlement numérique comprend la diffusion de contenus portant atteinte à la dignité (vidéos, photos, rumeurs...) pouvant aller jusqu’à des images ou vidéos créées ou modifiées par des outils numériques pour nuire à la victime.

Même si l’on n’est pas directement concerné, il est possible de signaler la vidéo si elle apparait sur un réseau social. En revanche, il est fortement conseillé de ne pas réagir aux posts malveillants sur les réseaux sociaux (ne pas liker ou commenter), même si l’on veut défendre la victime car cela pourrait valider le comportement du harceleur ou aggraver la situation.

Il est recommandé de se rapprocher de la victime, de lui apporter son écoute, son soutien et de l’engager à réaliser des démarches pour faire supprimer les contenus s’ils sont diffusés sur les réseaux sociaux ou pour porter plainte.

Source : https://e-enfance.org/ia-des-risques-accrus-pour-la-protection-des-mineurs-en-ligne-constates-par-lassociation-e-enfance-3018/

1. Thématique “Cyberharcèlement” - Niveau 3



Explications

Il n’est pas toujours évident de détecter une situation de harcèlement, mais il existe plusieurs signes indicateurs. Voici une liste non exhaustive de signaux qui peuvent alerter :

- Isolement soudain, ou réduction des interactions sociales
- Baisse des résultats scolaires
- Anxiété ou tristesse persistante
- Maux de tête ou de ventre fréquents
- Trouble du sommeil ou cauchemars
- Stress ou agitation à la réception de messages ou notifications

L’application 3018 propose un test réalisable et quelques minutes pour identifier si l’on vit une situation de harcèlement.

Sources : 8 signes à reconnaître pour identifier une situation de harcèlement

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

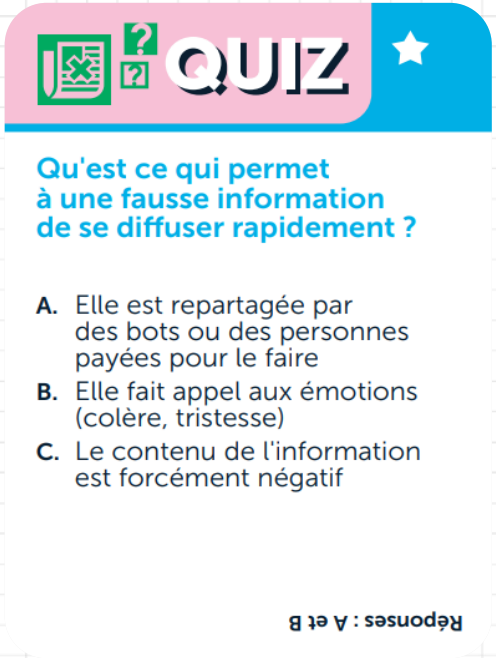
Mon enfant est victime de harcèlement | Ministère de l’Education Nationale, de l’Enseignement supérieur et de la Recherche

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

2. Thématique Désinformation

2. Thématique “Désinformation” - Niveau 1



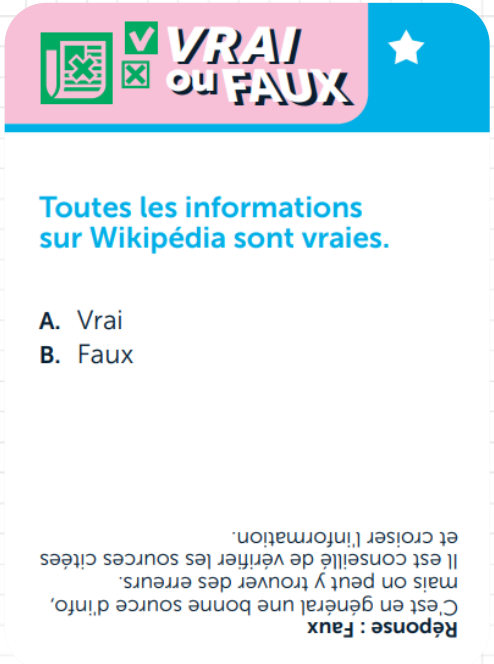
Explications

VIGINUM, c’est un service de l’Etat qui surveille ce qui se passe sur Internet pour éviter que des personnes (souvent d’autres pays) n’essaient de tromper les gens en France avec de fausses informations, surtout quand elles se mettent à circuler partout en même temps grâce à des faux comptes ou des robots.

VIGINUM observe si ces messages veulent manipuler nos émotions, que ce soit pour nous mettre en colère, tristes, ou même contents, selon le but de ceux qui les envoient.

Source : https://www.sciencedirect.com/science/article/abs/pii/S1169833022001934

2. Thématique “Désinformation” - Niveau 1



Sources :
Wikipédia:Vérifiabilité — Wikipédia (wikipedia.org)

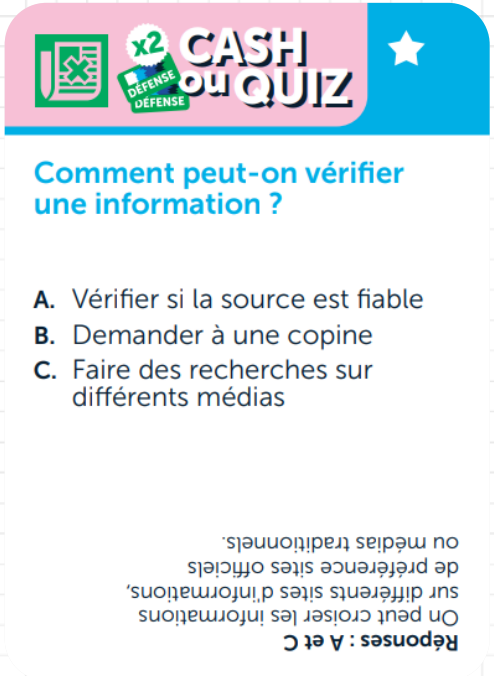
Explications

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 majoritairement anonyme, faisant de Wikipédia une encyclopédie collaborative. L’anonymat permet de respecter leur vie privée et de protéger leur liberté d’expression.

Il faut cependant garder à l’esprit que tout visiteur peut écrire ou modifier un article Wikipédia. Le contenu sera vérifié a posteriori par la communauté de Wikipediens.

De manière générale, il est important de vérifier les sources de l’article et de croiser les informations avec d’autres sources fiables et neutres, afin de s’assurer de leur véracité.

2. Thématique “Désinformation” - Niveau 1



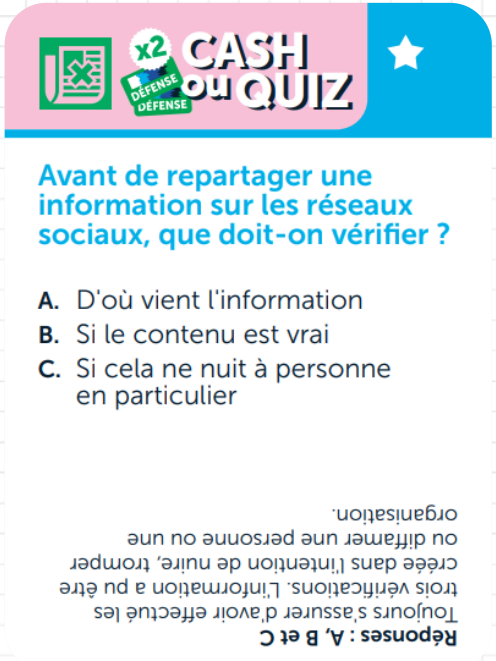
Explications

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

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, si elle n’a pas été manipulée, transformée, sortie de son contexte, ré-écrite dans le but de tromper son auditoire.

Source : https://www.clemi.fr/sites/default/files/clemi/RepereEMI/fausses_infos_poster.pdf

2. Thématique “Désinformation” - Niveau 1



Explications

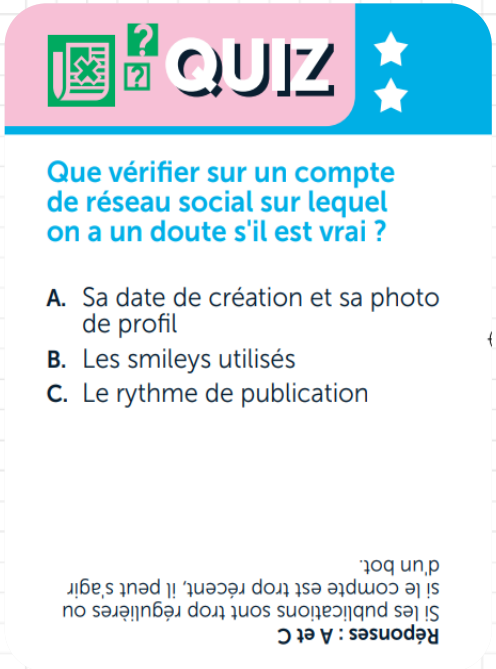
Chacun est responsable de ce qu’il publie sur les réseaux sociaux, il est donc important de réfléchir aux conséquences de ses publications :

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 nuire 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 (attention notamment à ne pas repartager des contenus diffamants, négationnistes ou qui incitent à la haine, violence ou discrimination).

Sources : https://www.service-public.fr/particuliers/vosdroits/F32075

2. Thématique “Désinformation” - Niveau 2



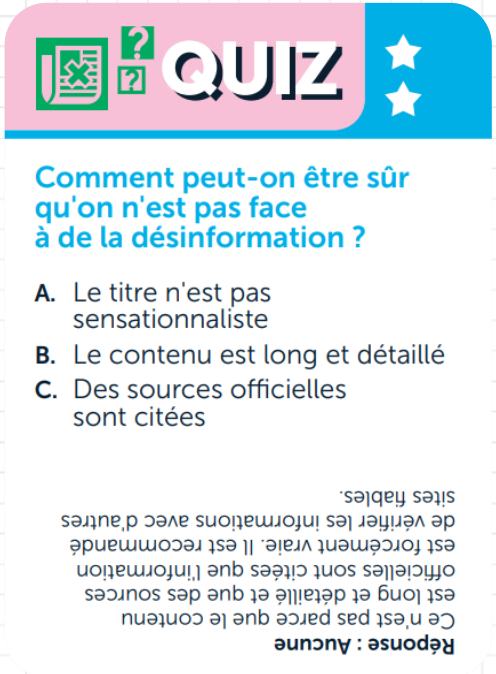
Explications

Un compte récemment créé (date de création très récente) est un indice classique d’un compte potentiellement faux ou automatisé, surtout si le nombre de publications ou d’amis/abonnés est inhabituellement bas ou incohérent avec la prétendue identité. L’absence de photo de profil, la présence d’une image générique, floue ou volée (image retrouvée ailleurs sur Internet) sont également des signaux révélateurs.

Un rythme de publication très régulier et automatisé (publications à intervalles fixes ou répétition massive) est fréquemment observé chez les comptes bots. Une activité intense ou trop régulière (beaucoup de posts identiques, retweets automatiques, commentaires systématiques) est un fort indice d’automatisation.

Source : Comment repérer les faux comptes et les bots sur Facebook, Instagram et Twitter

2. Thématique “Désinformation” - Niveau 2

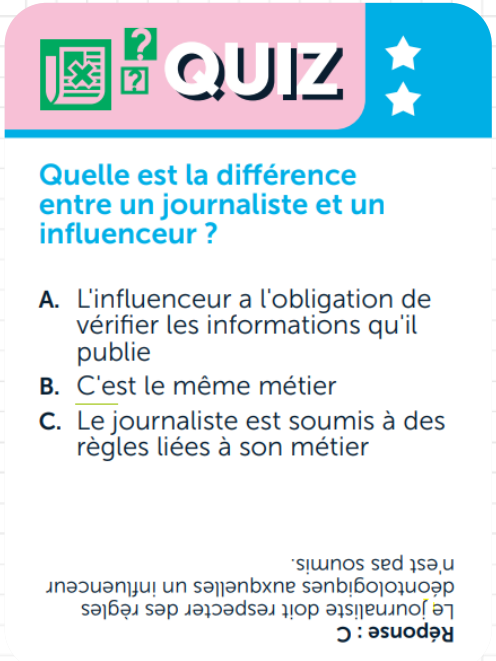


Explications

Le fait qu’un titre ne soit pas sensationnaliste n’est pas suffisant pour garantir la véracité d’une information. Les fake news peuvent aussi utiliser des titres neutres ou sobres pour tromper. La longueur n’est pas non plus liée à la justesse de l’information. Les producteurs de désinformation peuvent multiplier les détails pour renforcer l’apparence de crédibilité, même dans un contenu trompeur.

La simple présence de sources officielles citées ne garantit pas non plus que l’information est juste, car il est possible de sortir des citations de leur contexte ou de les falsifier. Il est recommandé « de varier les sources et de toujours aller vérifier par soi-même les informations avancées sur différents sites fiables ».

Source : Déterminer la fiabilité des sources : Un guide pour évaluer la qualité de l'information - Lycée - Collège Ipécom Paris



Explications

Un journaliste et un influenceur occupent des rôles distincts dans le paysage médiatique.

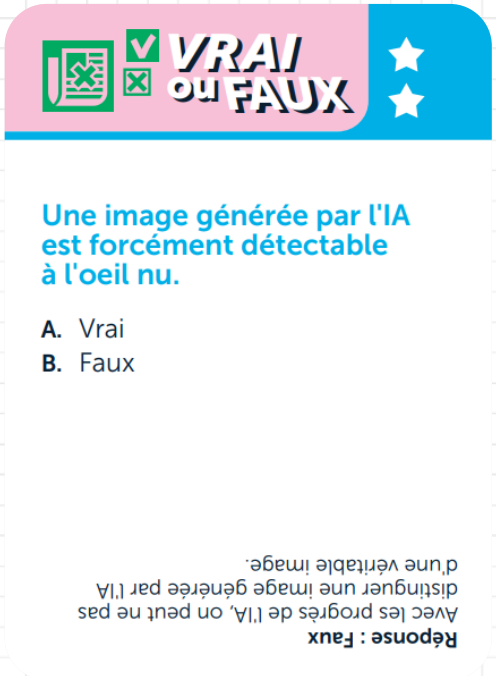
Le journaliste a pour mission de rechercher, vérifier et rapporter des informations de manière objective et rigoureuse, en respectant des normes déontologiques strictes et en visant à informer le public de manière précise et impartiale.

En revanche, un influenceur utilise principalement les réseaux sociaux pour partager des contenus personnels ou sponsorisés, souvent dans le but de promouvoir des produits, des marques ou des modes de vie.

Tandis que le journaliste sert avant tout l'intérêt public, l'influenceur se concentre généralement sur l'engagement et la monétisation de son audience.

Source : https://www.maisondesjournalistes.org/deontologie-journalistique-en-france/

2. Thématique “Désinformation” - Niveau 2



Explications

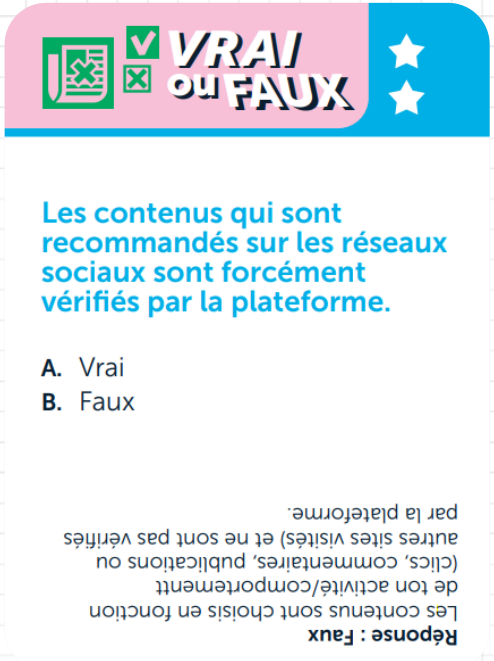
Avec les progrès de l’IA, il n’est quasiment plus possible de distinguer une image générée par l’IA d’une image réelle.

Les logiciels qui permettaient jusqu’ici de repérer un photomontage en pointant des différences de pixels ne sont pas fiables pour détecter les images générées par IA.

Ces dernières sont en effet constituées de milliers voire millions d’images, qui sont déconstruites pixel par pixel pour recréer une nouvelle image. Et pour le moment, aucun logiciel n’est capable de détecter correctement une image générée par intelligence artificielle.

Source : Vidéos générées par IA : êtes-vous encore capable de faire la différence ?
Libération Lecture d'image : repérer les créations de l'intelligence artificielle | Documentation

2. Thématique “Désinformation” - Niveau 2



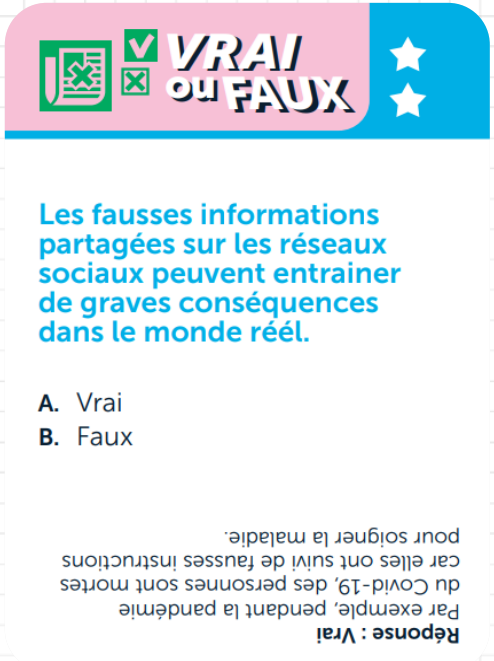
Explications

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)

2. Thématique “Désinformation” - Niveau 2



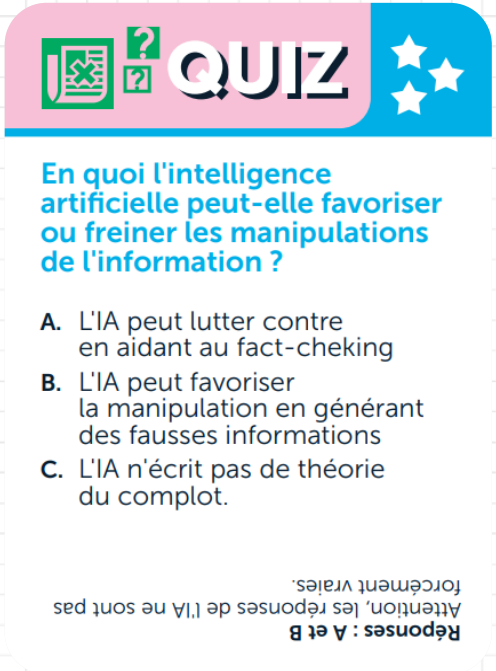
Explications

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 (exemple rumeurs pendant l’épidémie de Covid 19).

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 a dénombré plus d’une trentaine de morts.

Sources : 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
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

2. Thématique “Désinformation” - Niveau 3



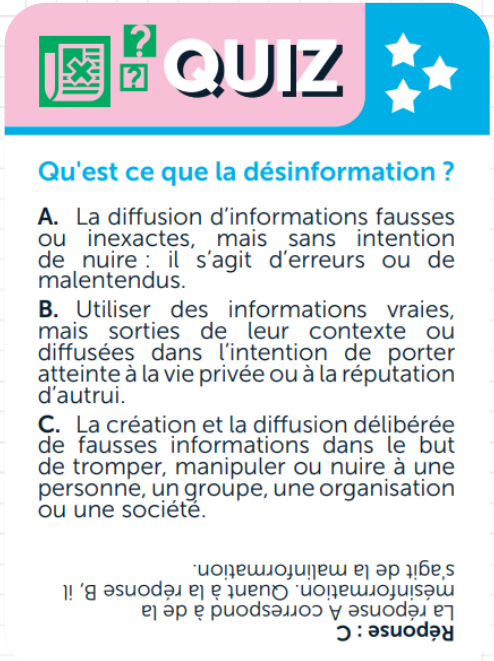
Explications

Le CLEMI promeut l’usage d’outils IA pour aider à la vérification des faits, citant notamment la plateforme vera.ai ou la création d’assistants journalistiques automatisés permettant de lutter contre la désinformation, notamment dans l’éducation aux médias.

VIGINUM alerte cependant : l’IA générative (textes, images, deepfakes, profils fictifs) est massivement utilisée pour produire et diffuser de la désinformation, tromper le public, amplifier des campagnes de manipulation et rendre plus difficile la détection manuelle ou automatique des faussetés.

Sources :
L’intelligence artificielle générative : quelle révolution et quels enjeux pour les médias ? | CLEMI 20250207_NP_SGDSN_VIGINUM_Rapport menace informationnelle IA_VF.pdf

2. Thématique “Désinformation” - Niveau 3



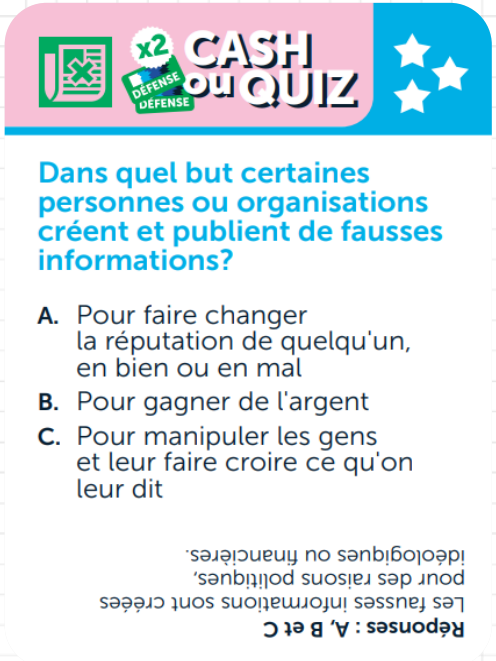
Explications

Le Conseil de l’Europe précise ainsi qu’on distingue trois utilisations bien différentes de l’information :

- La mésinformation : information fausse qui n’est pas partagée dans l’intention de nuire
- La désinformation : information fausse qui est délibérément partagée pour porter préjudice
- L’information malveillante : information fondée sur des faits réels, utilisée pour porter préjudice.

Sources :https://www.isfj.fr/actualites/28122023-desinformation-mesinformation-malinformation-decryptage-des-nuances-cruciales/

2. Thématique “Désinformation” - Niveau 3



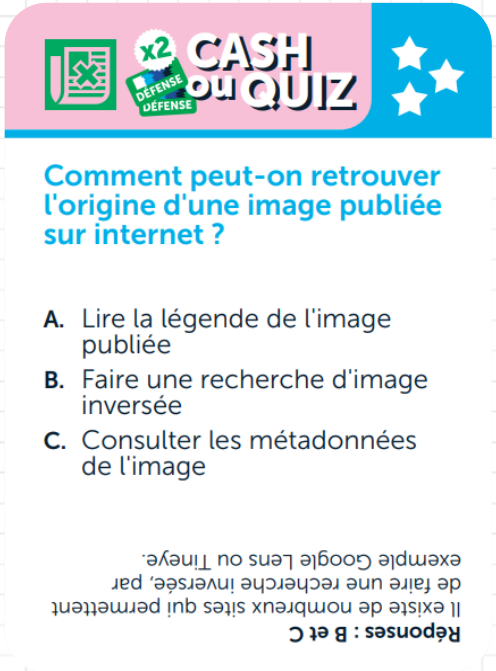
Source : https://e-enfance.org/informer/fake-news/

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). Début 2023, une centaine de journalistes de 30 médias internationaux, réunis au sein du consortium Forbidden Stories, a publié le résultat d’une enquête qui 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.

2. Thématique “Désinformation” - Niveau 3



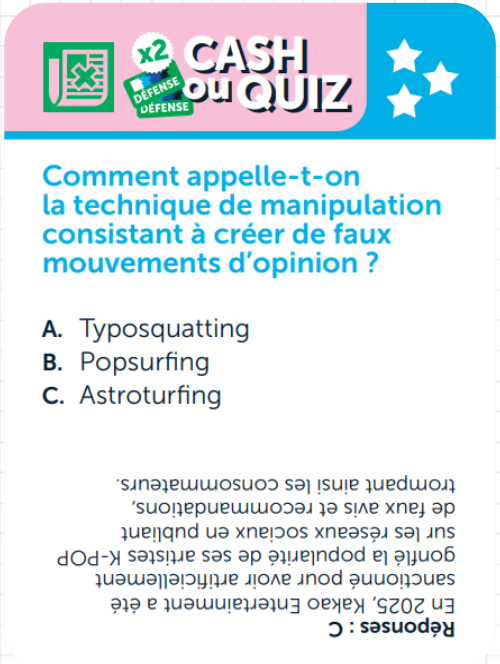
Sources : https://the-osint-project.fr/

Explications

On appelle cette recherche de l’OSINT. Cet acronyme signifie « Open Source Intelligence », ou en français « renseignement de source ouverte ». Il s’agit de la collecte et de l’analyse d’informations accessibles publiquement (sites web, réseaux sociaux, journaux, bases de données publiques, etc.) afin d’en tirer des renseignements exploitables. Ces informations doivent être accessibles librement, obtenues légalement et collectées gratuitement. L’OSINT joue un rôle crucial dans différents domaines : cybersécurité, enquête journalistique, veille concurrentielle, lutte contre la criminalité, etc. Contrairement au renseignement secret, les données OSINT ne nécessitent aucun accès privilégié ou piratage : tout le monde peut théoriquement y accéder.

The OSINT Project (TOP) est une initiative pédagogique française qui propose des outils, des défis et des missions pour apprendre à utiliser l’OSINT, à s’entraîner à l’investigation sur les données publiques, et à vérifier l’authenticité d’informations ou d’images.

2. Thématique “Désinformation” - Niveau 3



Explications

L’astroturfing désigne une pratique de manipulation visant à faire croire à un mouvement populaire spontané alors qu’il s’agit en réalité d’une opération orchestrée par un groupe, une organisation ou une entreprise pour influencer l’opinion publique à des fins politiques, économiques ou commerciales.

Kakao Entertainment, géant du divertissement sud-coréen, a récemment été sanctionné pour astroturfing sur les réseaux sociaux durant huit ans : entre 2016 et 2024, la société a promu ses chansons et artistes via des comptes de réseaux sociaux dont elle cachait le contrôle, publiant plus de 2,350 messages faussement présentés comme des avis spontanés de fans. D’autres publications ont été faites sur des forums majeurs en se faisant passer pour des utilisateurs ordinaires, sans révéler qu’il s’agissait de campagnes dirigées par des employés ou des agences rémunérées. Au total, Kakao Entertainment a versé environ 860 millions de wons à 35 agences pour poster de tels contenus « anonymes ».

Sources :

Séminaire ACCS : "Astroturfing, de l'usurpation à la manipulation du débat public ?" | Crem
Kakao Entertainment gets fined a pittance by FTC for astroturfing social media for ~8 years – Asian Junkie

2. Thématique « Désinformation »

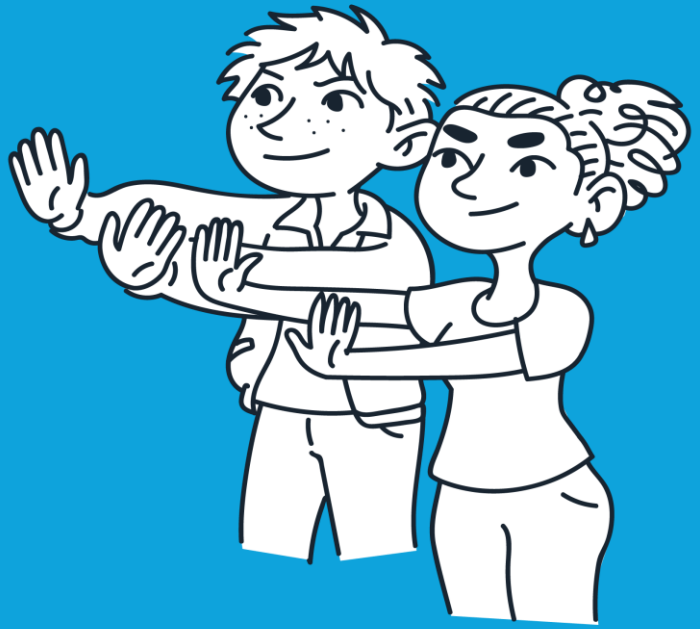
Pour aller plus loin - Désinformation

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
- Le débrief de Clara et Raphaël : Comment débusquer les manipulations de l'information – DE FACTO – Des clés pour mieux s'informer
- https://www.wikimedia.fr/wikeys
- Educ'ARTE

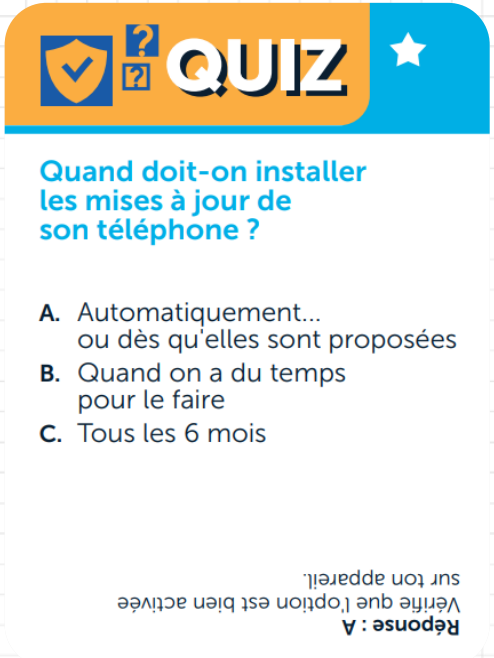
Des ressources pour en parler et s'informer en temps réel :

- https://www.francetvinfo.fr/vrai-ou-fake/
- https://www.hoaxbuster.com/
- https://e-enfance.org/bd-carrefour/fake-news/
- Rapports de VIGINUM : Publications - Page 1 sur 2 - SGDSN | SGDSN



3. Thématique Cyberdéfense

3. Thématique « Cyberdéfense » - Niveau 1



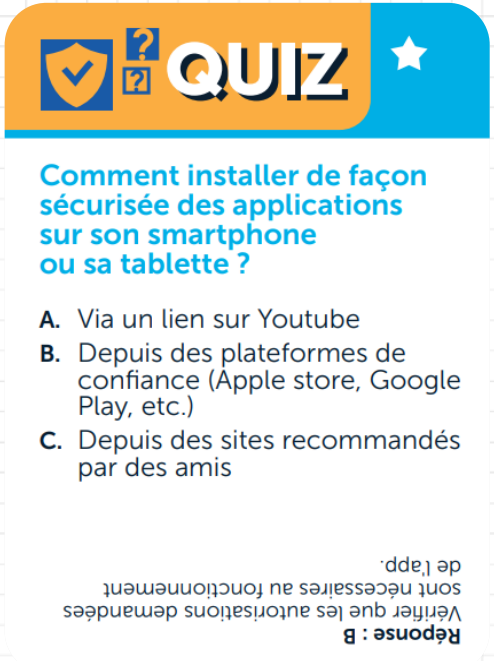
Explications

Les appareils numériques et les logiciels que nous utilisons au quotidien peuvent contenir des failles de sécurité. Ces vulnérabilités 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/mises-a-jour

3. Thématique « Cyberdéfense » - Niveau 1



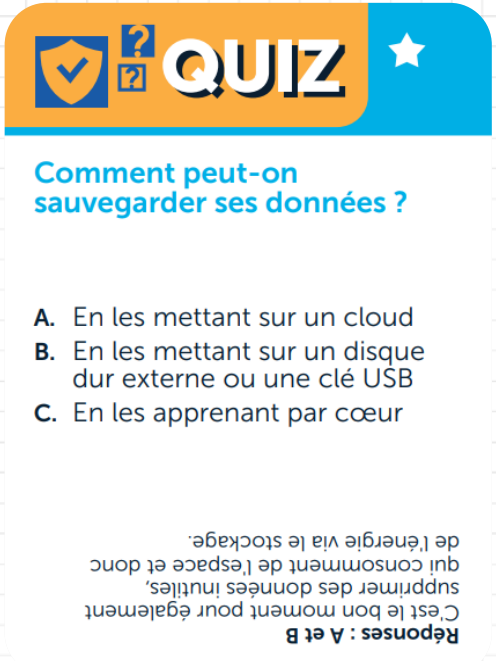
Explications

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

3. Thématique « Cyberdéfense » - Niveau 1



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.

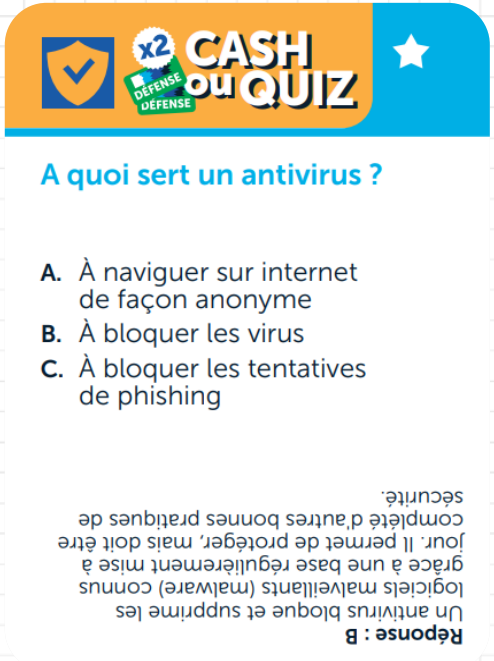
Afin de prévenir un tel risque, il est fortement conseillé d'en faire des copies pour préserver vos données à long terme.

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

3. Thématique « Cyberdéfense » - Niveau 1



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.

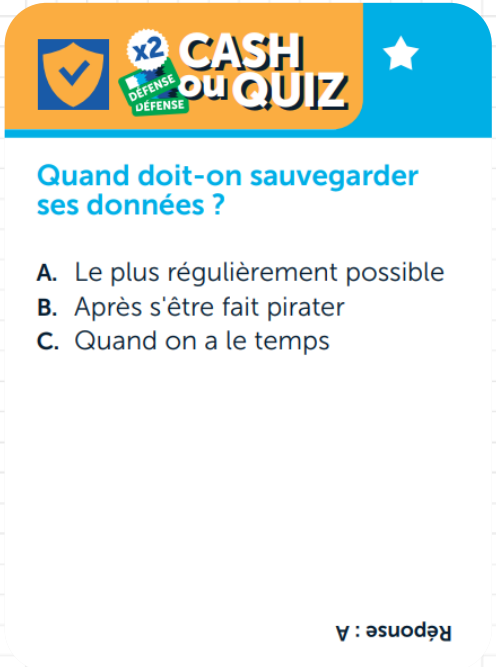
Pour bien utiliser un antivirus, il faut s'assurer que :

- 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

3. Thématique « Cyberdéfense » - Niveau 1



Explications

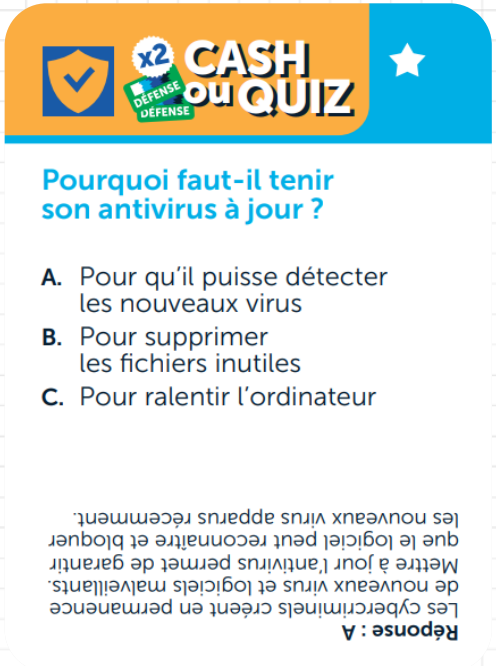
En cas de perte, de vol, de panne, de piratage ou de destruction de tes appareils numériques, tes données enregistrées sur ces supports seront perdues.

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

3. Thématique « Cyberdéfense » - Niveau 1



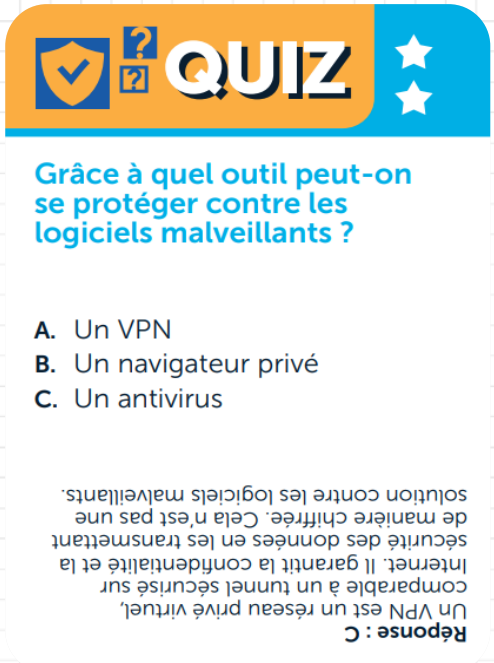
Explications

Des milliers de nouveaux virus et malwares sont créés chaque jour. La mise à jour régulière de l'antivirus permet d'intégrer les signatures et techniques nécessaires pour détecter et bloquer ces nouvelles menaces.

Un antivirus non mis à jour devient rapidement inefficace face aux virus récents.

Source : Les antivirus - Assistance aux victimes de cybermalveillance

3. Thématique « Cyberdéfense » - Niveau 2



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

3. Thématique « Cyberdéfense » - Niveau 2

Explications

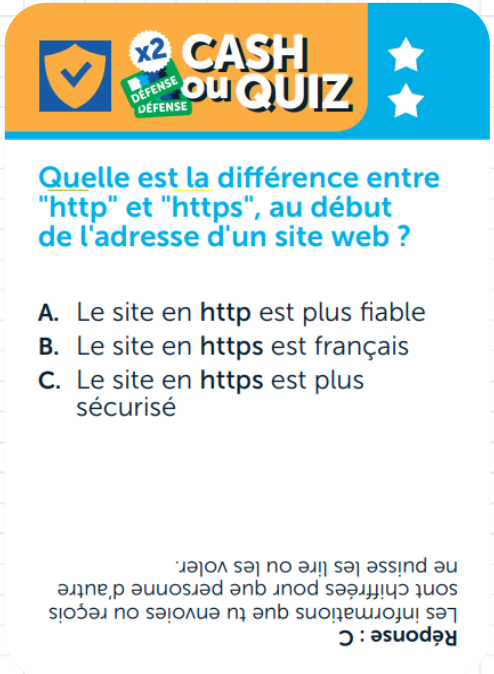
Il vaut mieux privilégier la connexion 4G ou 5G que d'utiliser les réseaux wifi publics que l'on peut trouver dans les fast-foods, cafés, hôtels ou gares.

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.

Source : https://www.numerama.com/tech/1053366-wi-fi-public-quels-sont-les-risques-pour-vos-donnees.html

3. Thématique « Cyberdéfense » - Niveau 2



Explications

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

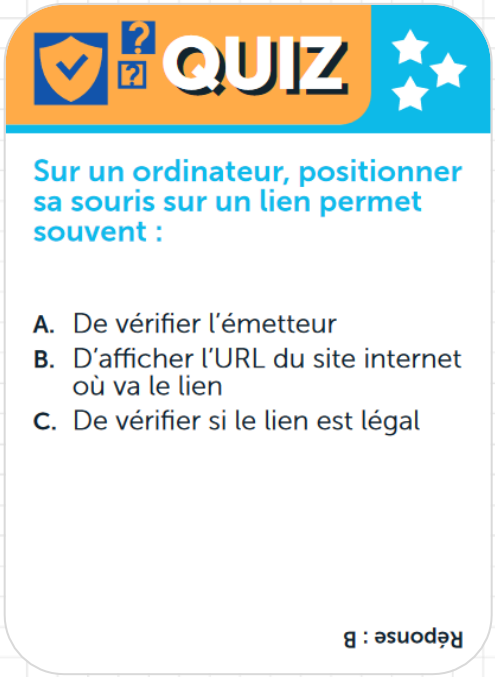
- Le sigle « http » signifie « HyperText Transfer Protocol »
- Le sigle « https » veut dire « HyperText Transfer Protocol Secure ».

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

3. Thématique « Cyberdéfense » - Niveau 3



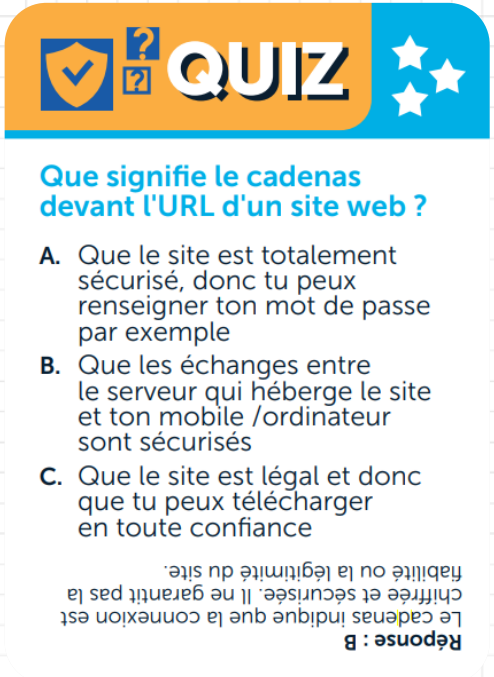
Explications

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

3. Thématique « Cyberdéfense » - Niveau 3



Explications

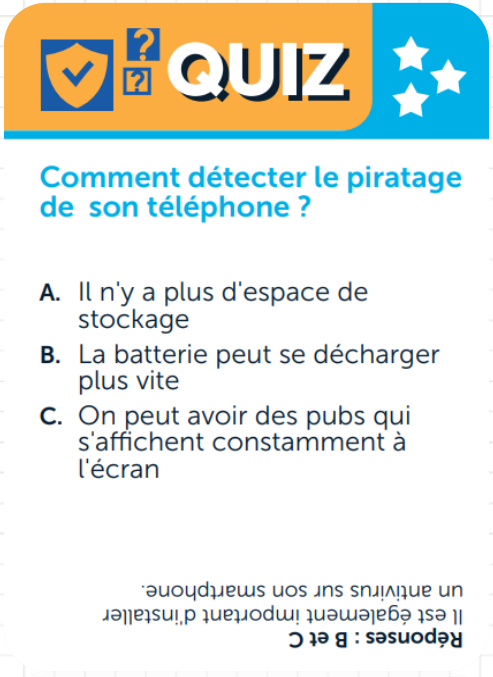
Contrairement à une croyance répandue, le cadenas ne veut pas dire qu'on peut faire confiance au site internet.

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

3. Thématique « Cyberdéfense » - Niveau 3



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.

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

3. Thématique « Cyberdéfense » - Niveau 3

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.

Une clé permettant de passer de l'état lisible à l'état illisible. Appelée clé de chiffrement, elle 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/

3. Thématique « Cyberdéfense » - Niveau 3

Explications

Créé en 2013 par Troy Hunt, le Directeur Régional de Microsoft en Australie, 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.

Source : https://haveibeenpwned.com/

3. Thématique « Cyberdéfense »

Pour aller plus loin - Cyberdéfense

Comprendre comment se protéger contre les cyberattaques :

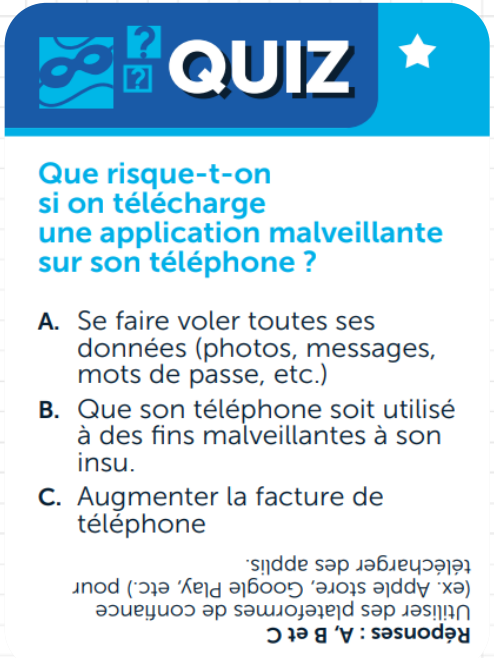
- Cybermalveillance.gouv | Cyberguide famille
- Ministère de l'économie I Comment assurer sa sécurité numérique
- Cybermalveillance.gouv I 10 mesures essentielles assurer votre sécurité numérique
- Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) - Guide des bonnes pratiques de l'informatique

Pour aller plus loin dans la formation à la cybersécurité :

- Cybermalveillance.gouv | MOOC sens-cyber
- ANSSI | MOOC secnumacademie

4. Thématique Cyberattaque

4. Thématique « Cyberattaque » - Niveau 1



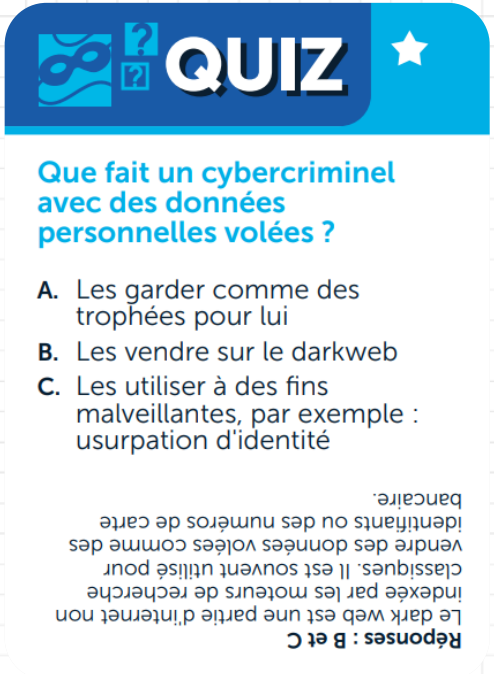
Explications

Les applications malveillantes peuvent aspirer les données, provoquer une surconsommation de données, installer des programmes qui, en souscrivant à des services payants, augmenter 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

4. Thématique « Cyberattaque » - Niveau 1



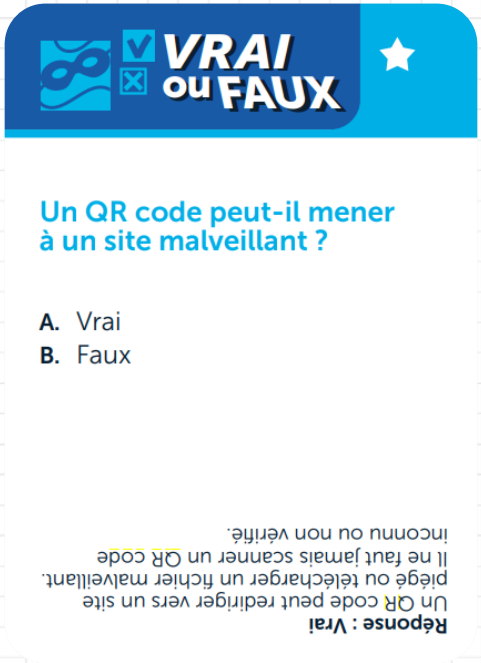
Explications

Les cybercriminels peuvent utiliser les données volées pour ouvrir des comptes bancaires, souscrire des crédits, percevoir des aides sociales ou réaliser des achats au nom de la victime. Cela peut entraîner des conséquences graves comme fichage bancaire, poursuites de créanciers ou atteinte à la réputation. Il s'agit de l'usurpation d'identité à des fins malveillantes.

Le dark web est une partie d'internet non indexée par les moteurs de recherche classiques. C'est ici que des cybercriminels vendent des données personnelles volées, comme des identifiants de connexion, des numéros de carte bancaire ou des « fullz » (ensembles complets d'identité comprenant : nom, adresse, numéro de sécurité sociale, etc.).

Source : L'usurpation d'identité | Ma Sécurité

4. Thématique « Cyberattaque » - Niveau 1



Explications

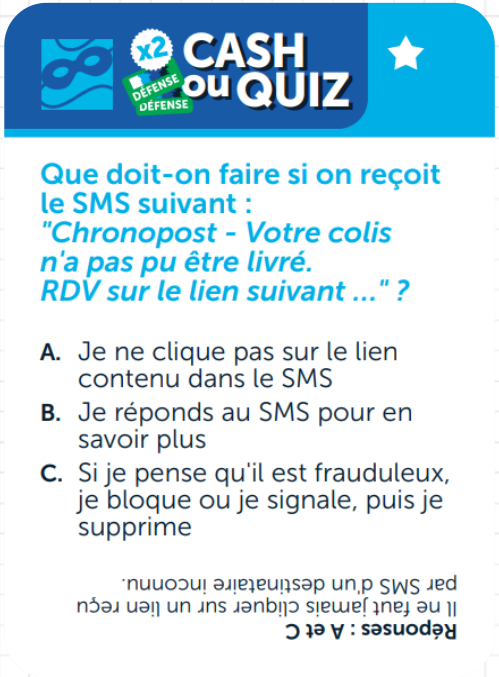
De nombreux organismes officiels mettent en garde contre les faux QR codes qui renvoient vers des sites piégés cherchant à voler des informations ou à infecter les smartphones. Cette technique d'attaque appelée le « quishing ». permet via des faux QR codes de renvoyer vers des sites piégés afin de voler des informations ou à infecter les smartphones.

Le simple scan d'un QR code peut initier le téléchargement d'un logiciel malveillant sans que l'utilisateur ne s'en rende compte, ce qui peut mettre en danger les données personnelles ou l'appareil entier.

Ainsi, il faut toujours se poser la question du contexte dans lequel le scan du QR code est demandé, et vérifier, sur des supports physiques qu'aucun QR code n'a été collé par-dessus le support original.

Source : Le « quishing » : l'hameçonnage par QR code - Assistance aux victimes de cybermalveillance

4. Thématique « Cyberattaque » - Niveau 1



Explications

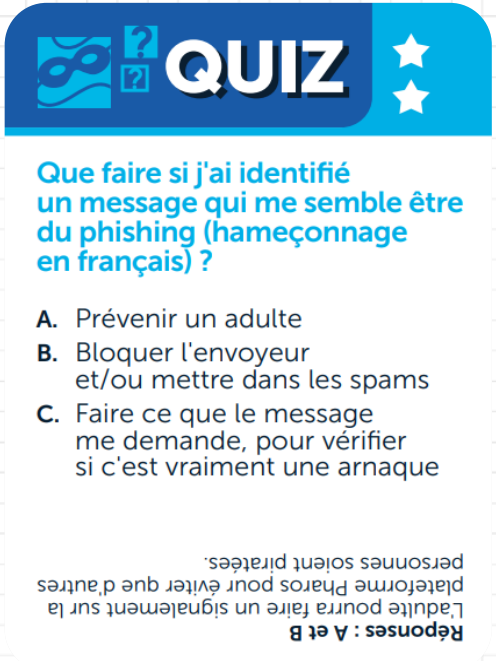
Les périodes de forte activité du commerce en ligne, comme les fêtes de fin d'année, les soldes ou bien encore le Black Friday sont très prisées des cybercriminels. Profitant du fait que de nombreuses personnes attendent ou envoient des colis, ils se font passer pour des sociétés de livraison parmi les 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

4. Thématique « Cyberattaque » - Niveau 2



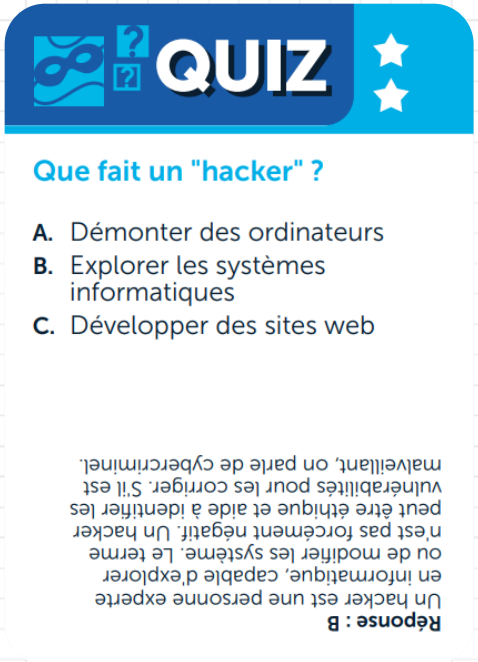
Explications

Si on repère une tentative de phishing avant de cliquer sur le lien, il est recommandé de garder des preuves (par exemple une capture d'écran), prévenir un adulte puis supprimer le message.

L'adulte pourra ensuite signaler le message sur la plateforme Pharos (https://www.internet-signalement.gouv.fr/PharosS1/) ou sur Signal Spam (https://www.signal-spam.fr/) pour éviter que d'autres personnes se fassent avoir.

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

4. Thématique « Cyberattaque » - Niveau 2

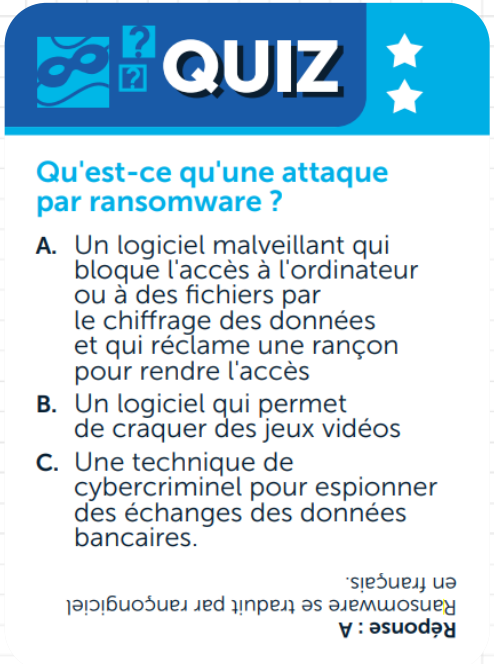


Explications

Un hacker est une personne experte en informatique capable d'explorer et modifier des systèmes. Le terme n'est pas forcément négatif : un hacker éthique (« white hat») utilise ses compétences pour identifier et corriger des vulnérabilités afin de renforcer la sécurité. En revanche, un hacker malveillant est un cybercriminel qui exploite ces failles à des fins frauduleuses.

Source : Quels sont les différents types de piratage informatique ? - Assistance aux victimes de cybermalveillance

4. Thématique « Cyberattaque » - Niveau 2



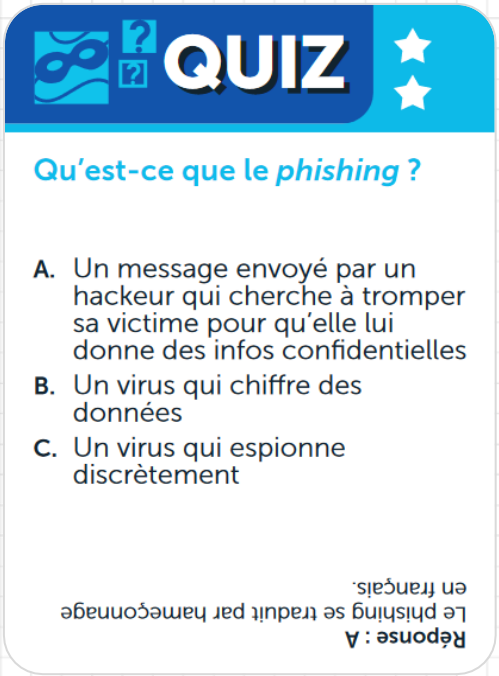
Explications

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

4. Thématique « Cyberattaque » - Niveau 2



Explications

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

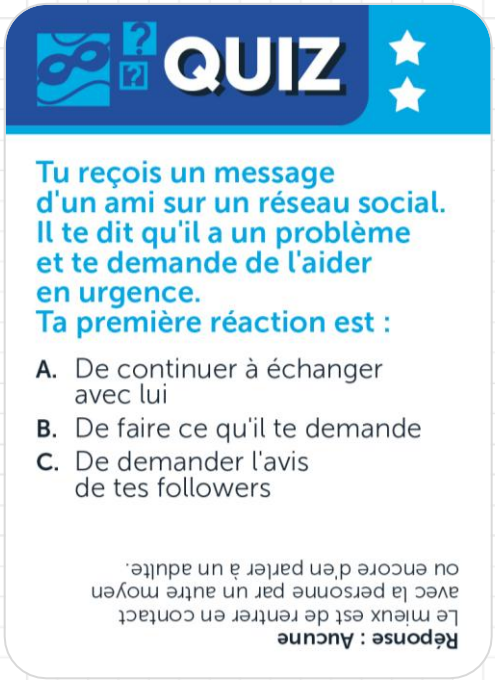
- Phishing par mail
- Smishing par SMS
- Vishing par appel téléphonique
- Quishing par QR Code

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 spearphishing 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

4. Thématique « Cyberattaque » - Niveau 2



Explications

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

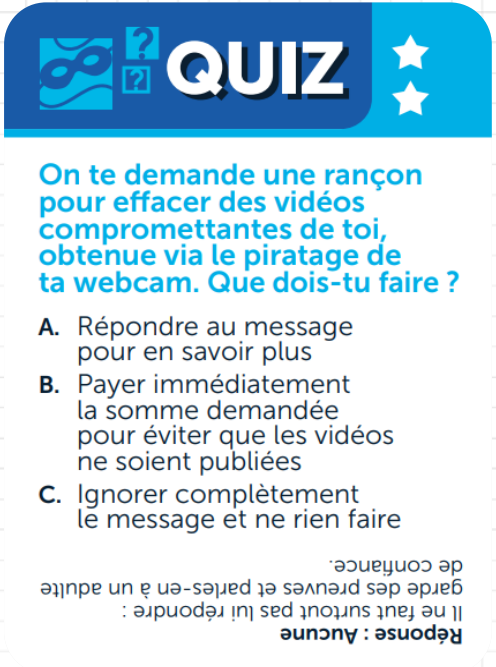
- « Est-ce que ce n'est pas toi sur cette photo [URL] ? »
- « Peux-tu envoyer un SMS au numéro [NUM] ? »
- « Je suis en vacances à l'étranger, mais je me suis fait voler mon portefeuille et j'ai vraiment besoin d'argent pour rentrer, est ce que tu peux me faire un virement ?»

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-usurpation-d-identite

4. Thématique « Cyberattaque » - Niveau 2



Explications

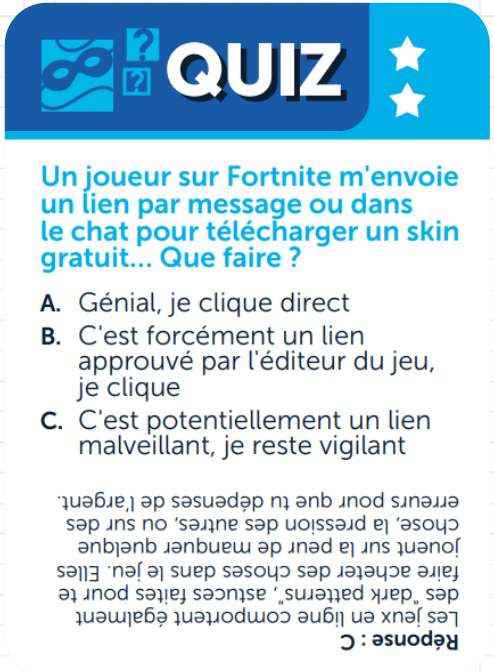
Les tentatives de chantage à la webcam sont relativement courantes. Dans la grande majorité des cas, les prétendus « hackers » n'ont pas eu accès à la caméra mais utilisent des moyens plus ou moins convaincants pour le faire croire à leur victime.

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

3. Thématique « Cyberdéfense » - Niveau 2



Explications

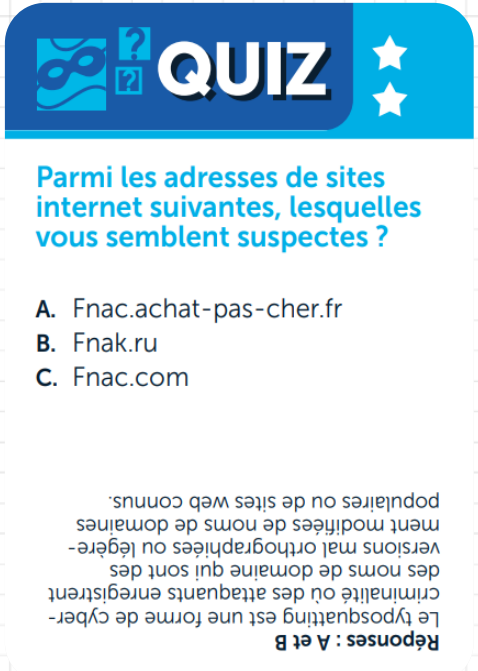
Plusieurs rapports de sociétés spécialisées mettent en évidence que les campagnes de piratage opérées dans les jeux vidéo sont en forte augmentation depuis plusieurs années.

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

4. Thématique « Cyberattaque » - Niveau 2



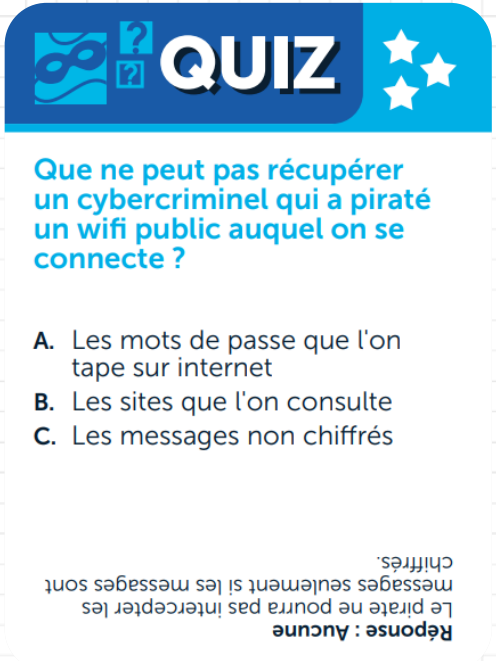
Explications

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.

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

4. Thématique « Cyberattaque » - Niveau 3



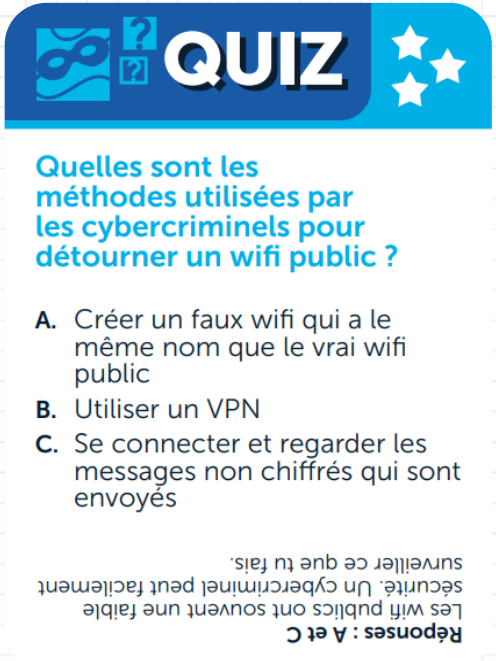
Explications

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 :
https://www.kaspersky.fr/resource-center/preemptive-safety/public-wifi-risks

4. Thématique « Cyberattaque » - Niveau 3



Explications

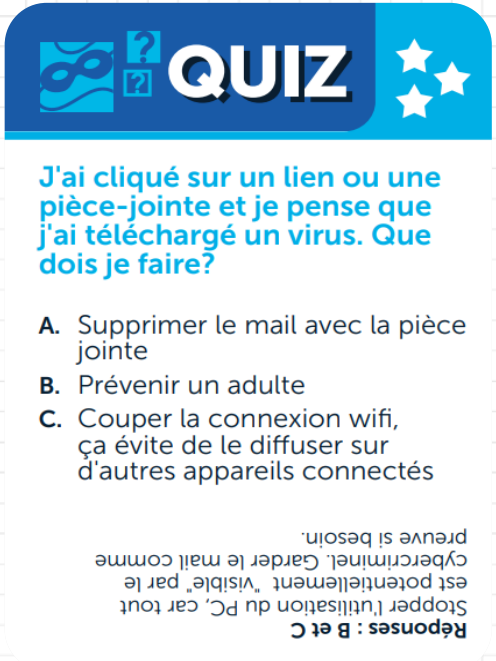
Il est facile pour un hackeur de créer un point d'accès wifi à qui il donnera le nom du restaurant, de l'hôtel, de la boutique juste à côté. Bien que se connecter au wifi public soit déconseillé, il arrive parfois qu'on en ait besoin. Dans ce cas, il faut demander au responsable le nom du réseau de l'endroit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

4. Thématique « Cyberattaque » - Niveau 3



Explications

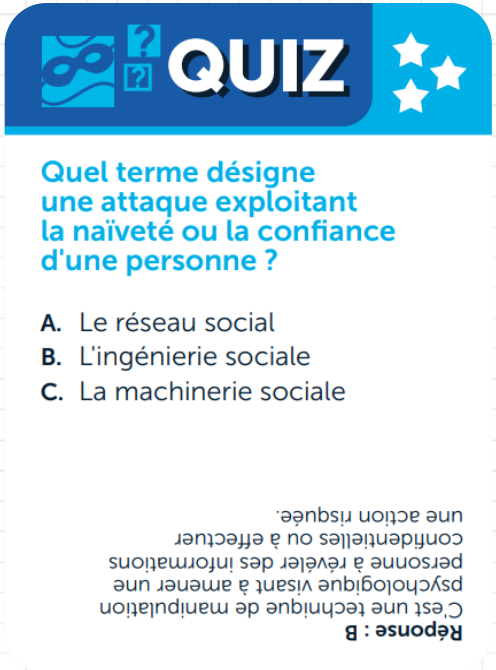
Si on pense avoir téléchargé un virus, le premier reflexe à avoir est de prévenir un adulte et de couper internet, pour éviter tout connexion entre le hackeur et l'appareil qui a été piraté. Si on est connecté à un Wifi, il est très important de se déconnecter afin de prévenir la diffusion du virus sur d'autres appareils.

Ensuite, il est fortement conseillé de réaliser une analyse antivirus pour supprimer tout fichier ou logiciel malveillant. Il convient également de vérifier si vos données sont bien sauvegardées sur un autre support ou un cloud.

Enfin, il est important de changer tous vos mots de passe pour renforcer la sécurité de vos comptes qui auraient pu être touchés.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/piratage-systeme-informatique-particuliers

4. Thématique « Cyberattaque » - Niveau 3



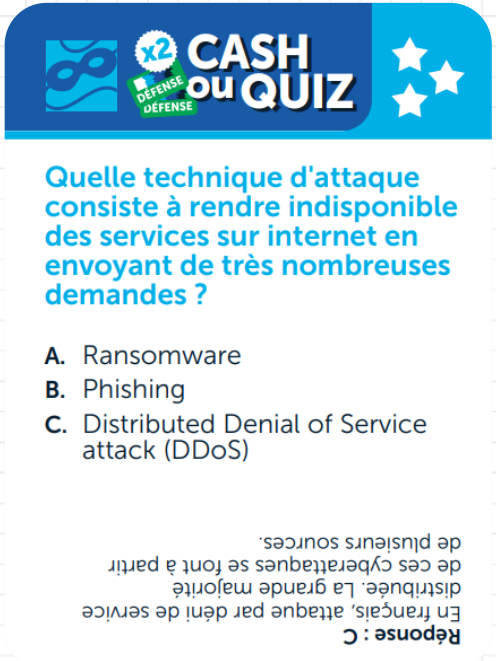
Explications

L'ANSSI (Agence nationale de la sécurité des systèmes d'information) définit l'ingénierie sociale comme une « manipulation consistant à obtenir un bien ou une information, en exploitant la confiance, l'ignorance ou la crédulité de tierces personnes ». Il s'agit d'une technique psychologique et systémique qui vise à manipuler un individu pour obtenir des informations stratégiques ou des comportements inadaptés, souvent utilisée dans des escroqueries économiques et financières.

L'ingénierie sociale exploite les faiblesses humaines et organisationnelles, s'appuyant généralement sur une relation de confiance établie par contact direct, téléphone, courrier électronique ou réseaux sociaux.

Source : https://cyber.gouv.fr/le-cyberdico#:~:text=de%20la%20Nation.-,Ing%C3%A9nierie%20sociale,-EN%20%3A%20Social

4. Thématique « Cyberattaque » - Niveau 3



Explications

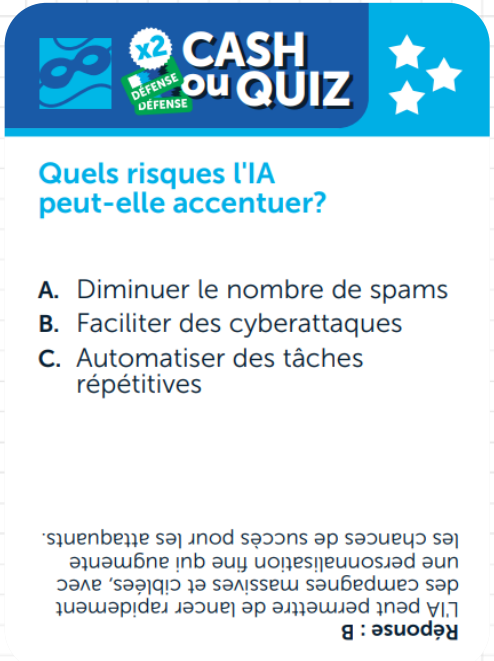
L'attaque par Déni de service (ou DOS/DDOS en anglais) a lieu lorsqu'un attaquant submerge un site internet ou une application de demandes.

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

4. Thématique « Cyberattaque » - Niveau 3



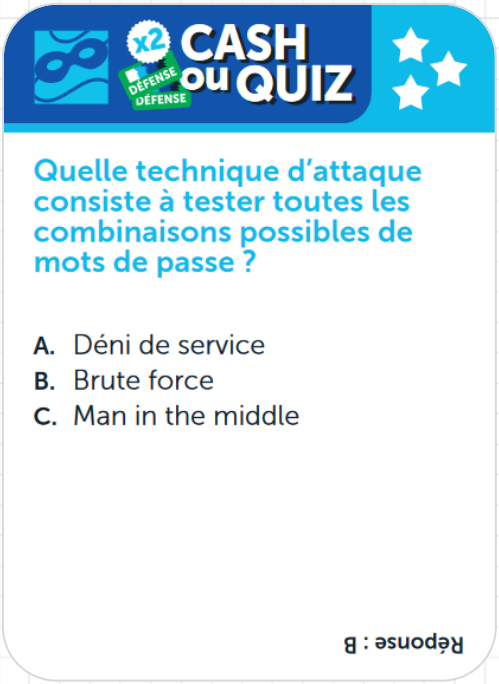
Explications

L'intelligence artificielle (IA) facilite les cyberattaques principalement en permettant aux attaquants d'automatiser et d'accélérer leurs actions, comme la détection rapide de vulnérabilités, la génération de contenus frauduleux (ex. phishing), ou l'automatisation de campagnes malveillantes.

L'IA générative, en particulier, peut aider à créer des scripts d'attaque, des messages d'hameçonnage très réalistes ou à exploiter plus facilement des failles, rendant les attaques plus sophistiquées et difficiles à détecter.

Source : Recommandations de sécurité pour un système d'IA générative | ANSSI

4. Thématique « Cyberattaque » - Niveau 3



Explications

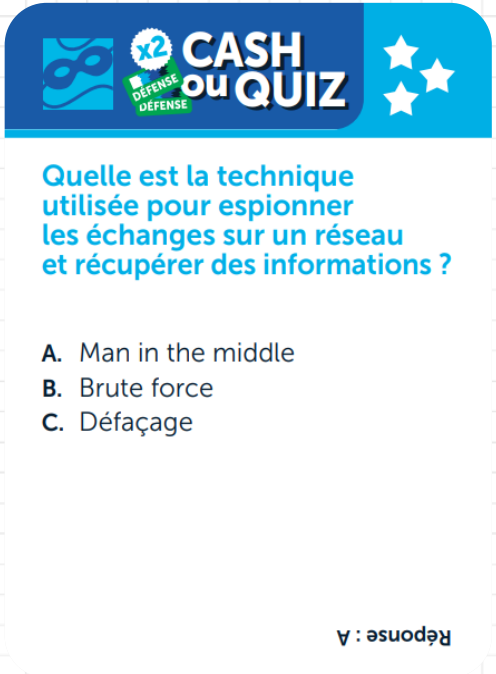
Dans le cas d'une attaque par « brute force », l'attaquant va tester toutes les combinaisons possibles : AAAA, AAAB, AAAC etc…

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

4. Thématique « Cyberattaque » - Niveau 3



Explications

Le Man In The Middle est une technique d'attaque informatique définie comme une interception et une modification clandestine des communications entre deux parties sans leur consentement.

L'attaquant se place « au milieu » de la communication pour écouter, espionner, détourner ou altérer les échanges (messages, données, identifiants) en temps réel, souvent sans que les victimes s'en aperçoivent. Cette attaque vise à compromettre la confidentialité et l'intégrité des échanges, par exemple lors de connexions non sécurisées (Wi-Fi public, protocoles non chiffrés).

Source : https://cyber.gouv.fr/le-cyberdico#:~:text=des%20commandes%20arbitraires.-,Man%2Din%2Dthe%2Dmiddle,-FR%20%3A%20Homme%2Ddu

4. Thématique « Cyberattaque »

Pour aller plus loin - Cyberattaque

Comprendre et réagir face aux 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 ?

Les jeux pour parler de cybersécurité :

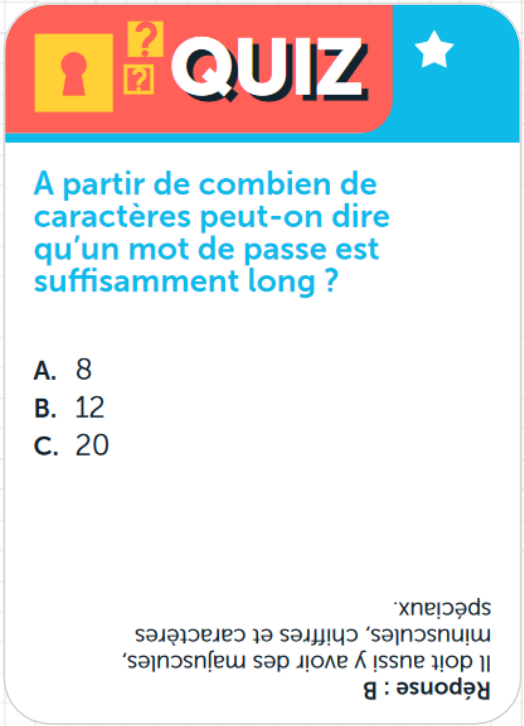
- Cybermalveillance.gouv I Mallette cyber inclusion numerique
- Région académique Bourgogne-Franche-Comté I Le kit CyberEnJeux de l'ANSSI
- Eduscol I Education et cybersécurité
- Cyber Duel de Game Partners

Autre ressource :

Bande dessinée - Les enquêtes de Seven

5. Thématique
Mots de passe

5. Thématique « Mot de passe » - Niveau 1



Explications

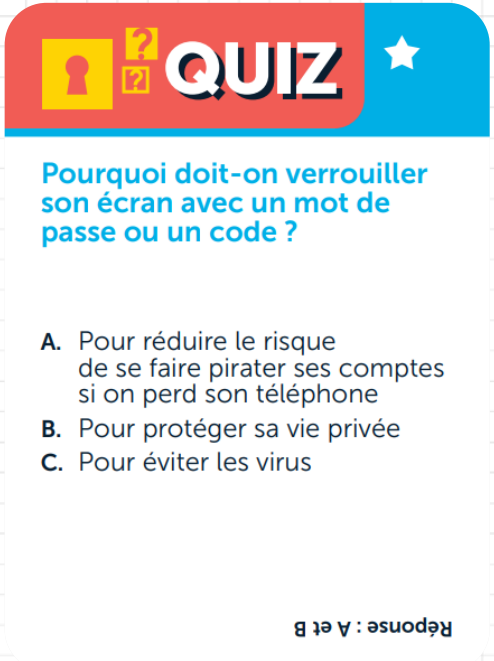
Il est admis qu'un bon mot de passe doit comporter au minimum 12 caractères mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux. C'est ce qu'on appelle un mot de passe complexe.

En effet, cela permet de réduire le risque qu'un cybercriminel devine ou trouve un mot de passe, notamment en utilisant la technique du « brute force », une technique d'attaque automatisée 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

5. Thématique « Mot de passe » - Niveau 1



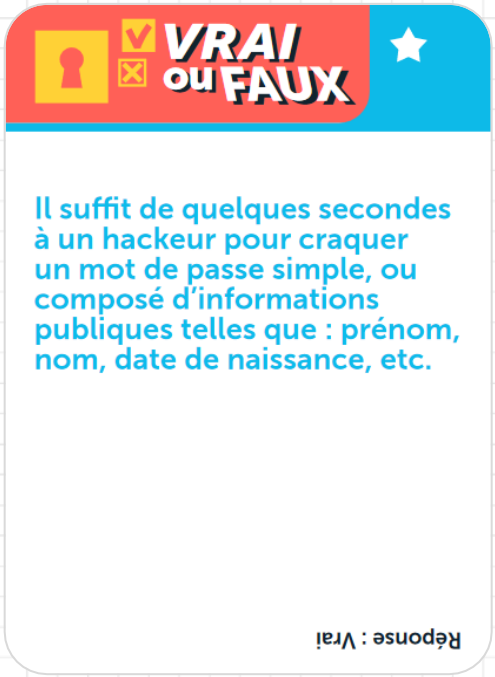
Explications

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. Cependant, une personne mal intentionnée avec des compétences en informatique pourrait récupérer des informations sur votre téléphone, malgré le système de verrouillage.

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

5. Thématique « Mot de passe » - Niveau 1



Explications

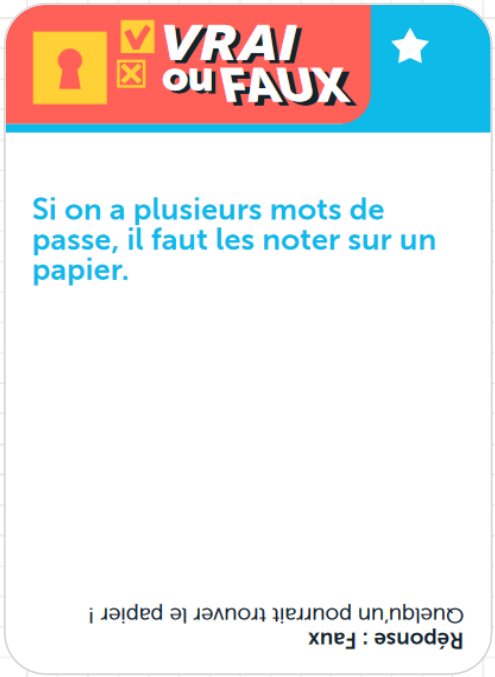
Une technique automatisée, dite par «brute force », consiste à essayer toutes les combinaisons possibles de caractères jusqu'à trouver le bon mot de passe. Réalisées par des programmes spécifiques qui se basent sur des librairies de mots, ces attaques peuvent tester des dizaines de milliers de combinaisons par seconde.

La première chose qu'un cybercriminel 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 ou son club de sport préféré.

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

5. Thématique « Mot de passe » - Niveau 1



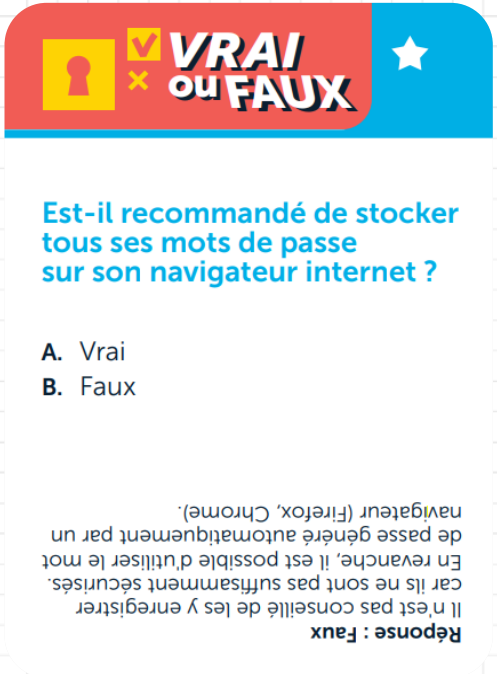
Explications

Il est quasiment impossible de retenir des 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 : cela pourrait être récupéré 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

5. Thématique « Mot de passe » - Niveau 1



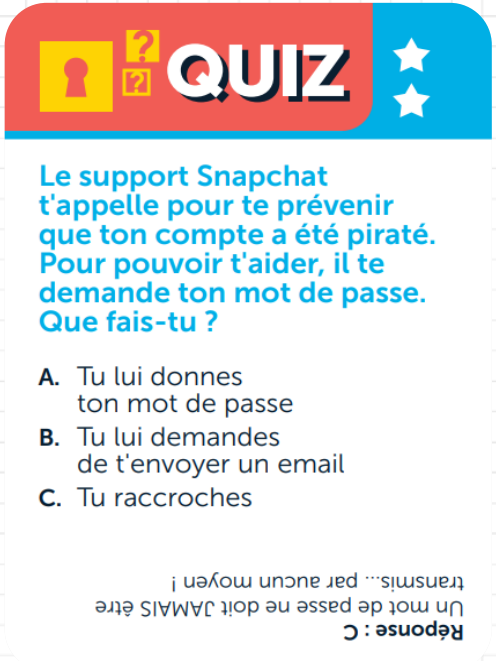
Explications

Même si les navigateurs chiffrent les mots de passe, la clé de chiffrement est souvent stockée à proximité et facilement accessible, ce qui facilite le déchiffrement par des malwares ou des attaquants disposant d'un accès à l'ordinateur.

De plus, tout logiciel malveillant ou personne ayant accès physiquement à votre appareil peut extraire ces mots de passe sans difficulté, d'autant plus que les protections comme un mot de passe principal sur le navigateur sont souvent désactivées par défaut. En cas de piratage du compte de synchronisation du navigateur, un cybercriminel peut aussi récupérer à distance tous vos mots de passe stockés dans le cloud. C'est pourquoi les experts et sources officielles recommandent plutôt d'utiliser un gestionnaire de mots de passe dédié, plus sécurisé, avec un chiffrement renforcé et un mot de passe maître unique.

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

5. Thématique « Mot de passe » - Niveau 2



Explications

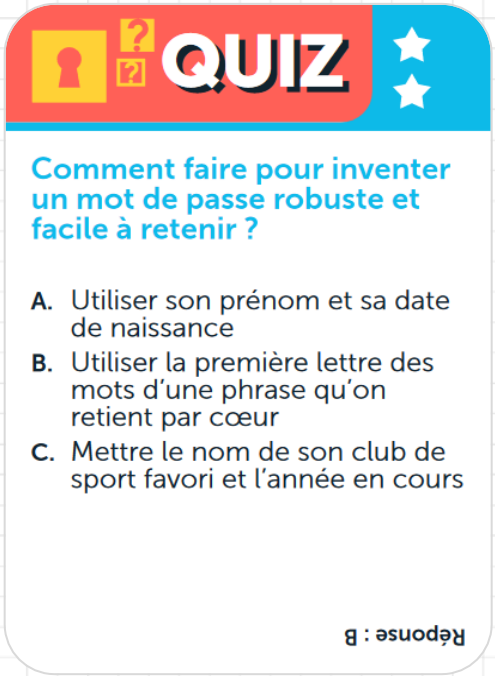
Il ne faut jamais communiquer des informations sensibles par messagerie ou téléphone. Ce type de demande « urgente » doit alerter : aucune administration ou société commerciale sérieuse ne demandera un mot de passe par message électronique ou par téléphone.

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

5. Thématique « Mot de passe » - Niveau 2



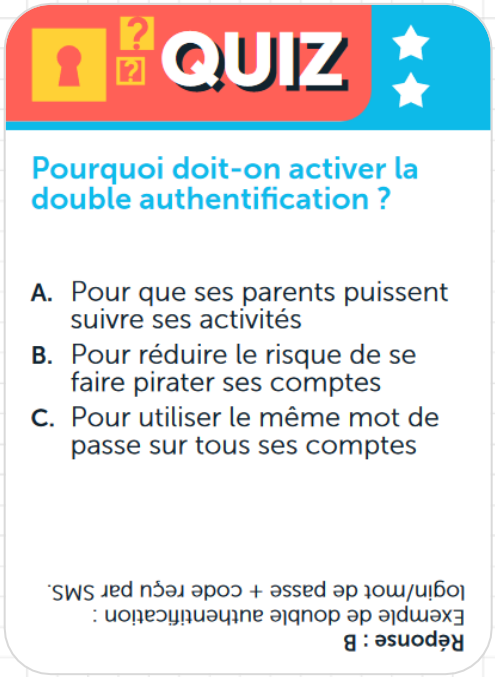
Explications

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 hackeurs.

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

5. Thématique « Mot de passe » - Niveau 2



Explications

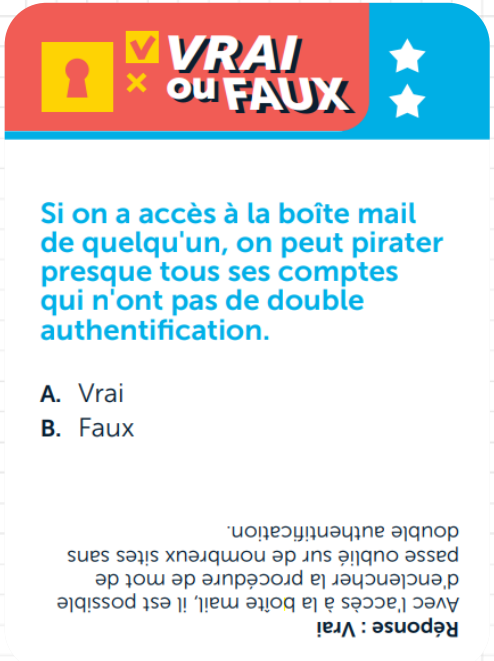
Pour renforcer la sécurité des accès, de plus en plus de services proposent cette option.

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 cybercriminel 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/bonnes-pratiques/mots-de-passe

5. Thématique « Mot de passe » - Niveau 2



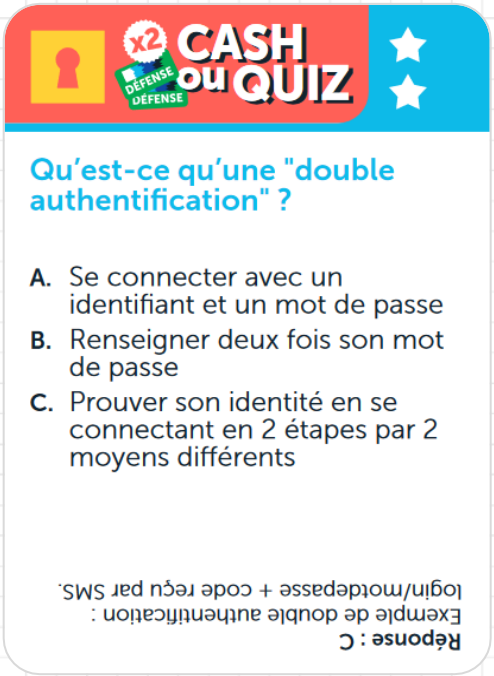
Explications

Notre boite mail est une mine d'or pour un cybercriminel : il peut y trouver plein d'informations personnelles 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 du 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 exemple par notification ou SMS sur le téléphone.

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

5. Thématique « Mot de passe » - Niveau 2



Explications

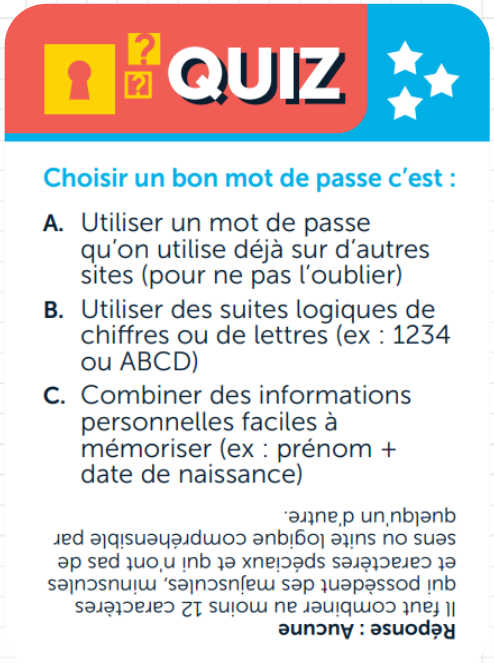
Pour renforcer la sécurité des accès, de plus en plus de services proposent cette option.

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, 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 cybercriminel 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

5. Thématique « Mot de passe » - Niveau 3



Explications

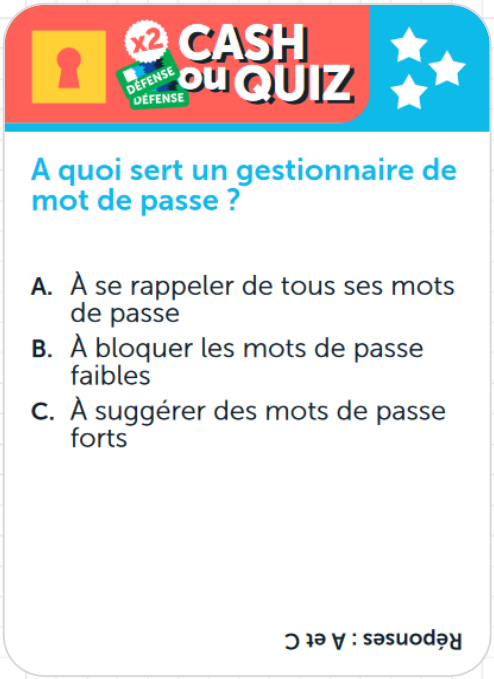
Pour pirater un compte, la première chose qu'un cybercriminel va faire, c'est de tester des combinaisons avec des mots du dictionnaire, des suites logiques ou encore avec des informations qu'il a pu récupérer facilement sur la victime, par exemple son prénom, sa date de naissance, ou encore le nom de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

5. Thématique « Mot de passe » - Niveau 3



Explications

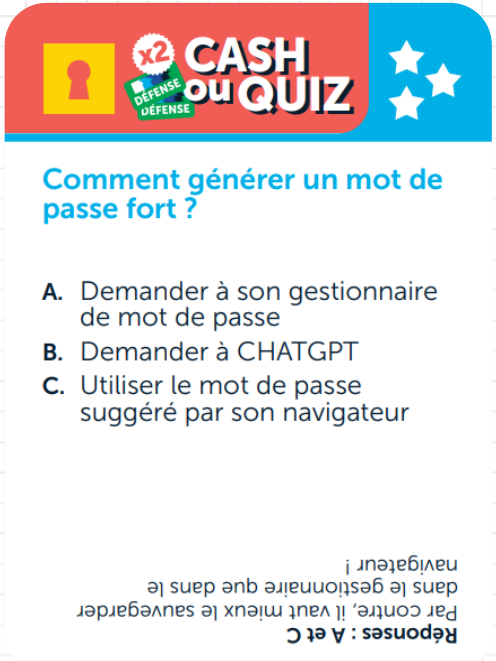
Il est quasiment impossible de retenir les dizaines de mots de passe longs et complexes !

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

5. Thématique « Mot de passe » - Niveau 3



Explications

Pour générer un mot de passe fort, il est recommandé d'utiliser un gestionnaire de mots de passe qui crée des mots complexes, uniques et difficiles à deviner. Les navigateurs proposent aussi souvent des mots de passe suggérés, mais leur stockage est moins sécurisé qu'un gestionnaire dédié.

Il est déconseillé d'utiliser ChatGPT pour générer des mots de passe car ils ne sont pas vraiment aléatoires, peuvent être stockés et exposés, et ne respectent pas les recommandations officielles qui privilégient les gestionnaires de mots de passe dédiés et sécurisés.

Source : https://www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/cybersecurite/pourquoi-et-comment-utiliser-un

5. Thématique « Mot de passe »

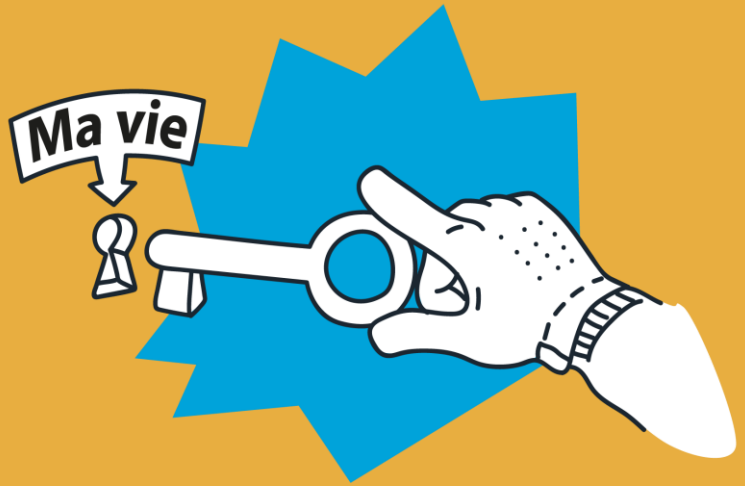
Pour aller plus loin - Mots de passe

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.



6. Thématique
Vie privée

6. Thématique « Vie privée » - Niveau 1

Explications

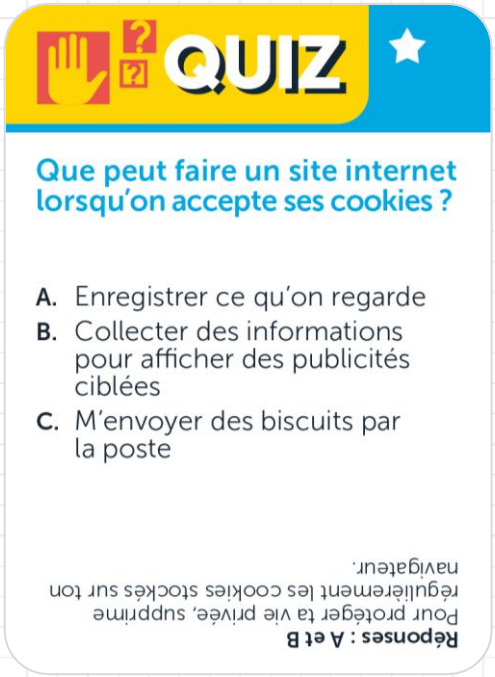
L'utilisation d'un compte privé est essentielle pour partager des informations personnelles en limitant l'accès aux seules personnes que l'on connaît et en qui on a confiance.

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

6. Thématique « Vie privée » - Niveau 1



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

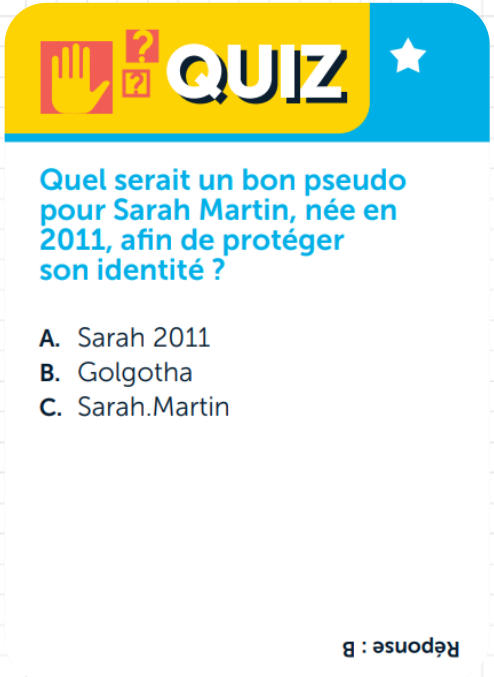
Explications

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 mémoriser par exemple le contenu d'un 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 consentement préalable au dépôt de cookies, il est conseillé de les refuser par défaut.

6. Thématique « Vie privée » - Niveau 1



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

Explications

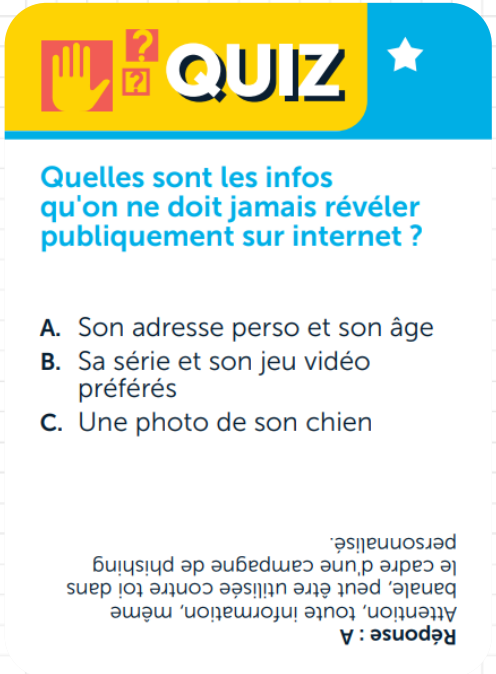
Il est important d'adopter de bons réflexes pour naviguer sur internet et limiter les risques, comme créer un pseudonyme pour les réseaux sociaux.

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.

6. Thématique « Vie privée » - Niveau 1



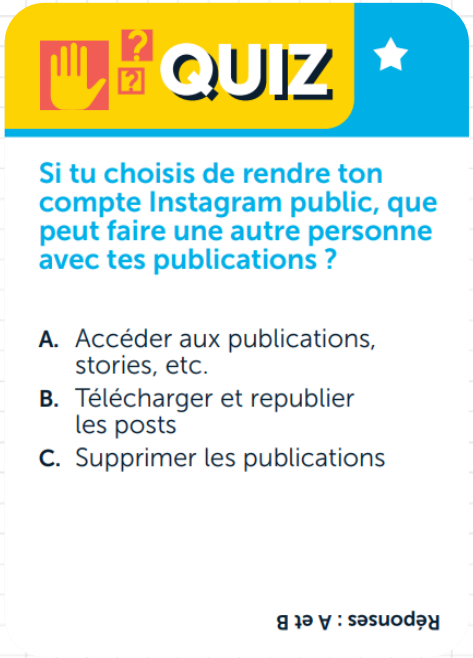
Explications

Pour limiter les risques d'internet, il est important de ne pas donner 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/

6. Thématique « Vie privée » - Niveau 1



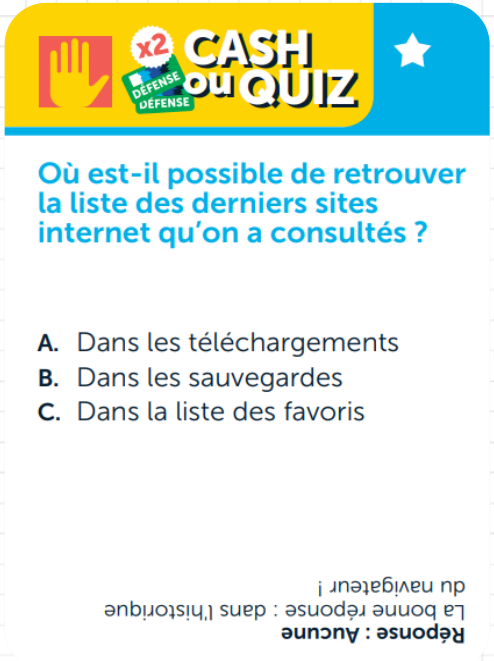
Explications

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

6. Thématique « Vie privée » - Niveau 1



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.

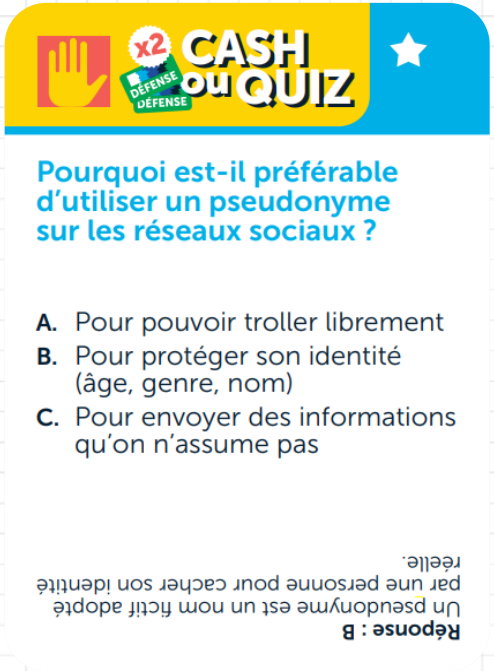
Ainsi, les requêtes, les recherches effectuées, les sites web visités sont conservés dans l'historique. N'importe quelle personne ayant accès à un ordinateur peut consulter l'historique de la session ouverte.

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

6. Thématique « Vie privée » - Niveau 1



Explications

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

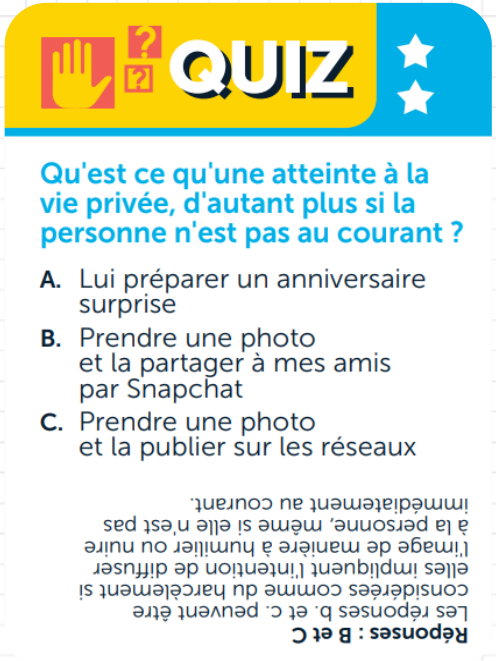
Cela peut également un moyen de prévention contre des prédateurs en ligne, ciblant notamment les enfants.

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

6. Thématique « Vie privée » - Niveau 2



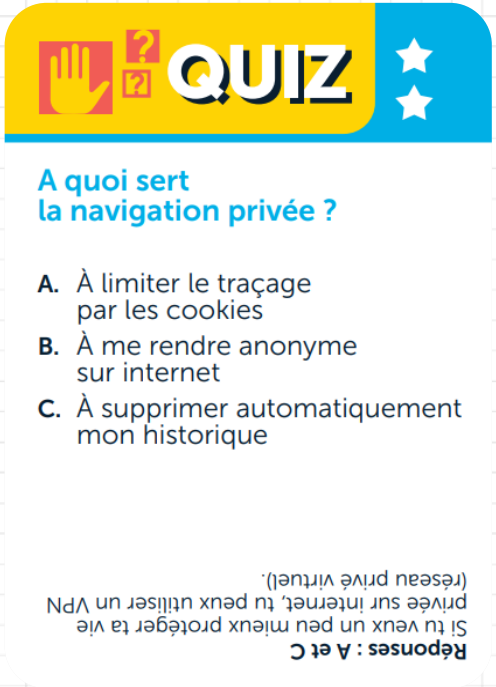
Explications

Une atteinte à la vie privée consiste à collecter, diffuser ou utiliser des informations ou images personnelles d'une personne sans son consentement, ce qui est encore plus grave si elle n'en est pas informée. Par exemple, prendre une photo d'une personne et la partager à ses amis via Snapchat ou la publier sur les réseaux sociaux constitue une violation de la vie privée sans son accord.

Cette définition est cadrée par le RGPD (Règlement Général sur la Protection des Données) et confirmée par la CNIL, qui insiste sur la nécessité d'obtenir le consentement de la personne concernée avant toute diffusion d'informations ou d'images personnelles.

Source : Droit à l'image et respect de la vie privée | Service-Public.fr

6. Thématique « Vie privée » - Niveau 2



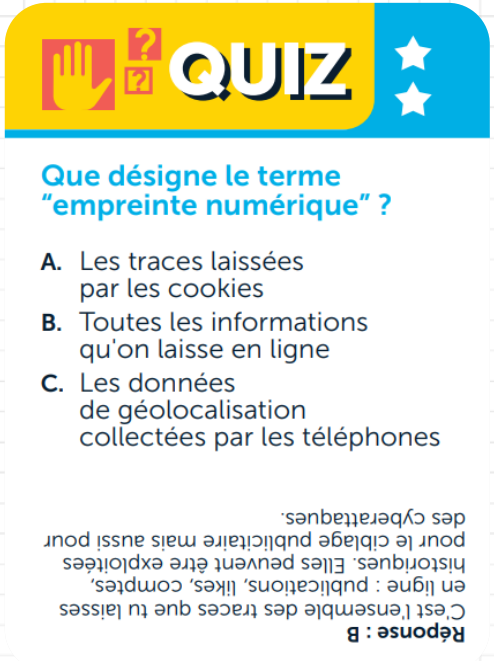
Explications

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

6. Thématique « Vie privée » - Niveau 2



Explications

Une empreinte numérique désigne l’ensemble des traces laissées par une personne ou une organisation lors de ses activités en ligne, qu’elles soient volontaires (posts sur les réseaux sociaux, inscriptions, achats) ou involontaires (cookies, adresses IP, données de navigation).

Ces données, actives ou passives, permettent d’identifier, profiler et suivre un utilisateur sur Internet, parfois sans son consentement ni sa connaissance. L’empreinte numérique est souvent permanente et difficile à effacer, avec des implications pour la vie privée et la sécurité.

Source : Fingerprinting | CNIL

3. Thématique « Cyberdéfense » - Niveau 2

Si j'utilise la même photo de profil pour plusieurs comptes, on peut facilement faire le lien entre mes profils.

A. Vrai
B. Faux

Réponse : Vrai
Grâce à la recherche d'image inversée ou aux IA.

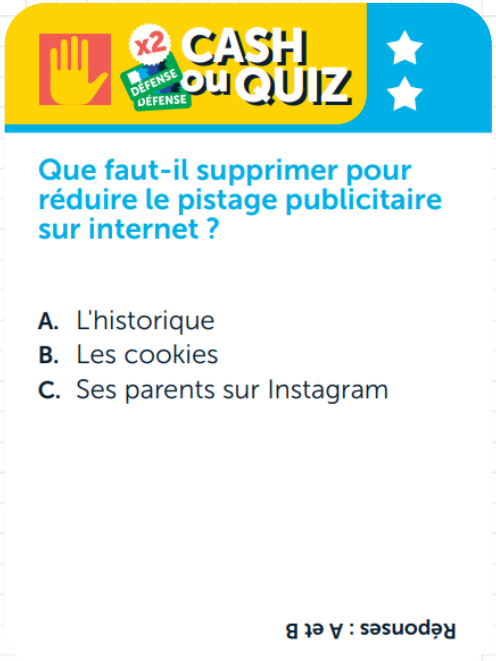
Explications

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/

6. Thématique « Vie privée » - Niveau 2



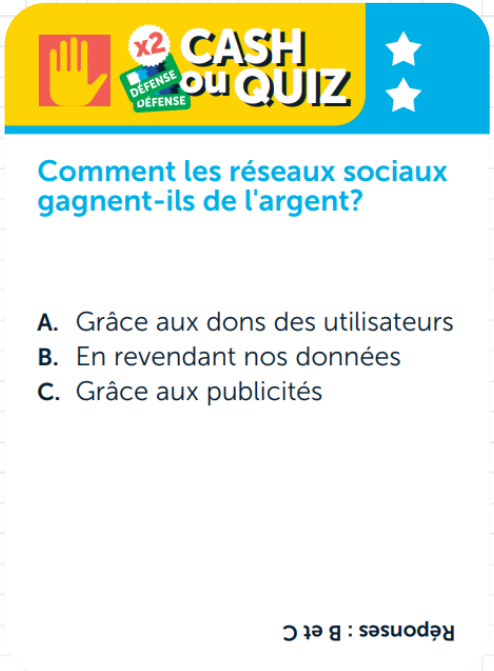
Explications

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

6. Thématique « Vie privée » - Niveau 2



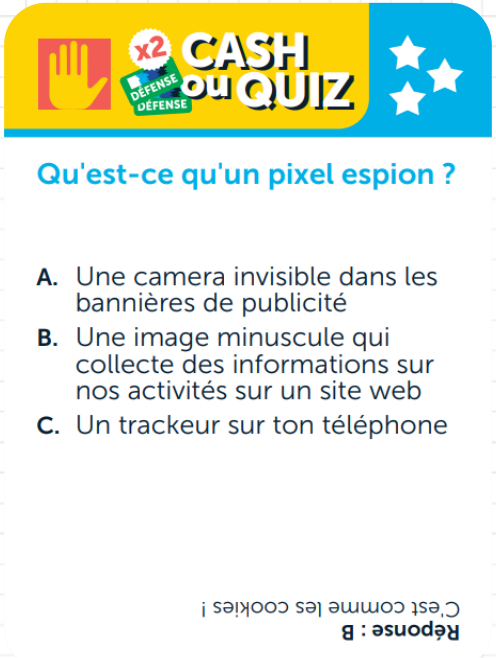
Explications

La plupart des plateformes de réseaux sociaux, gratuites pour les utilisateurs, génèrent des revenus via la publicité. Plus les utilisateurs passent de temps sur ces services, plus ils sont exposés à des publicités, augmentant ainsi les revenus des plateformes.

De plus, nos données peuvent être revendues pour créer des publicités ciblées, maximisant ainsi l'efficacité des campagnes publicitaires et augmentant encore les profits des plateformes. Cela souligne le risque de compromission de la vie privée et la nécessité de gérer soigneusement nos informations personnelles en ligne pour éviter les abus et l'exploitation non désirée de nos données.

Source : https://www.francetvinfo.fr/replay-radio/le-fil-des-reseaux/comment-les-reseaux-sociaux-transforment-nos-donnees-en-or_6260481.html

6. Thématique « Vie privée » - Niveau 2



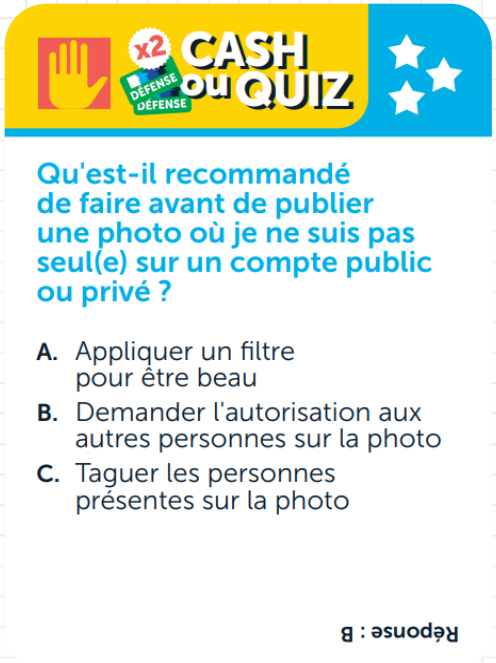
Explications

Un pixel espion (ou tracking pixel, web beacon, balise pixel) est une toute petite image numérique, généralement invisible car transparente et ne mesurant qu'1x1 pixel, intégrée dans un site web, un email ou une publicité. Lorsqu'un utilisateur ouvre une page ou un message contenant ce pixel, celui-ci se charge depuis un serveur tiers et permet de collecter des informations sur son comportement, comme le fait d'avoir consulté la page ou l'email, l'adresse IP, le type d'appareil, l'heure d'ouverture, voire d'établir un suivi cross-site ou cross-mail.

Selon la CNIL, le pixel espion est un outil de traçage soumis au consentement explicite des utilisateurs, notamment dans les emails, afin de protéger leur vie privée.

Source : Tracking pixel/Web beacon ou « pixel espion » | CNIL

6. Thématique « Vie privée » - Niveau 3



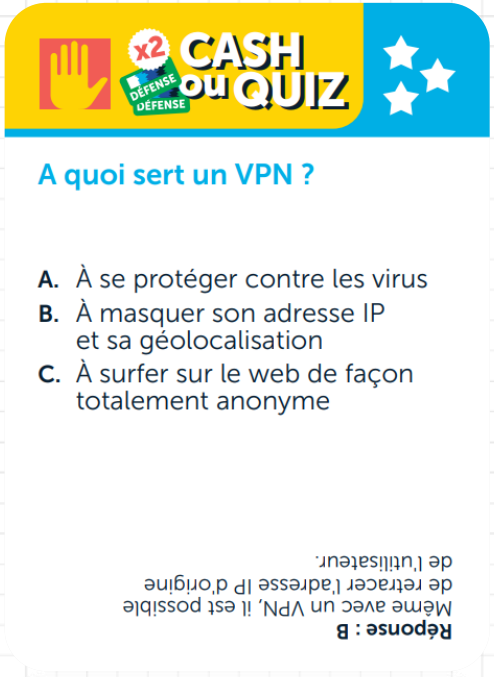
Explications

Obtenir le consentement explicite de chaque personne sur la photo avant publication est une obligation légale fondée sur le droit à l'image, le respect de la vie privée, et le RGPD.

La CNIL recommande cette démarche même sur les comptes privés et conseille d'être attentif également à la gestion des tags et à la suppression sur demande.

Source : https://www.cnil.fr/fr/cnil-direct/question/le-droit-limage-sapplique-t-il-sur-internet

6. Thématique « Vie privée » - Niveau 3



Explications

Un VPN ne protège pas directement contre les virus ; il sécurise et chiffre votre connexion Internet pour préserver votre confidentialité et empêcher l'interception des données, mais il ne détecte ni ne supprime les logiciels malveillants.

En revanche, certains VPN intègrent des fonctionnalités de blocage de sites malveillants ou de phishing, ce qui apporte une protection complémentaire, mais limitée. Pour une sécurité complète, il est recommandé d'utiliser conjointement un VPN et un antivirus, l'antivirus assurant la détection, le blocage et la suppression des virus tandis que le VPN protège la confidentialité et la communication.

Source : Est-ce qu'un VPN peut me protéger contre les virus ? - Numerama

Pour aller plus loin - Vie privée

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

- https://www.cnil.fr/fr/guide-de-la-securite-des-donnees-personnelles-nouvelle-edition-2024
- https://www.cnil.fr/fr/diffusion-de-donnees-piratees-la-suite-dune-cyberattaque-quels-sont-les-risques-et-les-precautions
- Cybermalveillance.gouv I 10 mesures essentielles assurer votre sécurité numérique
- https://www.clemi.fr/sites/default/files/clemi/Familles/Publications/Le%20guide%20de%20la%20famille%20Tout-Ecran/guide_emi_la_famille_tout_ecran.pdf

Jeux pour apprendre à protéger sa vie privée :

- CNIL I Un jeu de cartes pour rester net sur internet
- https://www.cnil.fr/fr/donnees-paires-sonnelles-jouez-apprenez-protegez-votre-vie-privee

7. Cartes « Cyberattaque » et « Défense »

Les cartes « Attaquant »

Les cartes « Attaque » (1/3)

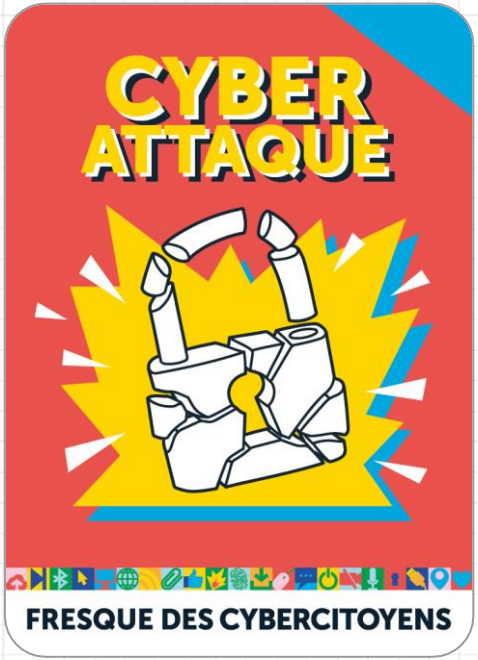
Les cartes « Attaque » (2/3)

Les cartes « Attaque » (3/3)

Les cartes « Impact » (1/3)

Les cartes « Impact » (2/3)

Les cartes « Impact » (3/3)



Cartes « Défense » (1/2)

J'utilise un mot de passe complexe et diffférent pour chacun de mes comptes.

1

Je télécharge les mises à jour automatiquement et j'ai une protection antivirus à jour.

2

Je choisis de ne pas «liker», commenter ni partager pour éviter de propager le contenu.

3

Je vérifie l'expéditeur et le lien avant de cliquer, surtout si le message est inattendu ou urgent.

4

Je garde des preuves.

5

Je signale les personnes qui ont des propos intolérables ou qui sont agressives sur les réseaux sociaux.

6

Je vérifie régulièrement qu'aucune donnée dévalorisante ou intime n'est publiée sur moi.

7

J'en parle à un adulte en qui j'ai confiance ou je contacte des dispositifs dédiés (3018, 17Cyber).

8

Cartes « Défense » (2/2)

Je ne confie aucune information personnelle à un inconnu sur les réseaux.

9

Je restreins ma visibilité sur les réseaux sociaux en créant un compte privé et j'utilise un pseudonyme.

10

Je vérifie et croise les informations à l'aide de sources fiables.

11

Je réalise régulièrement des sauvegardes de mes données importantes.

12

Je bloque un utilisateur pour qu'il ne puisse plus accéder à mes contenus, me contacter ou apparaitre dans mon fil d'actualité.

13

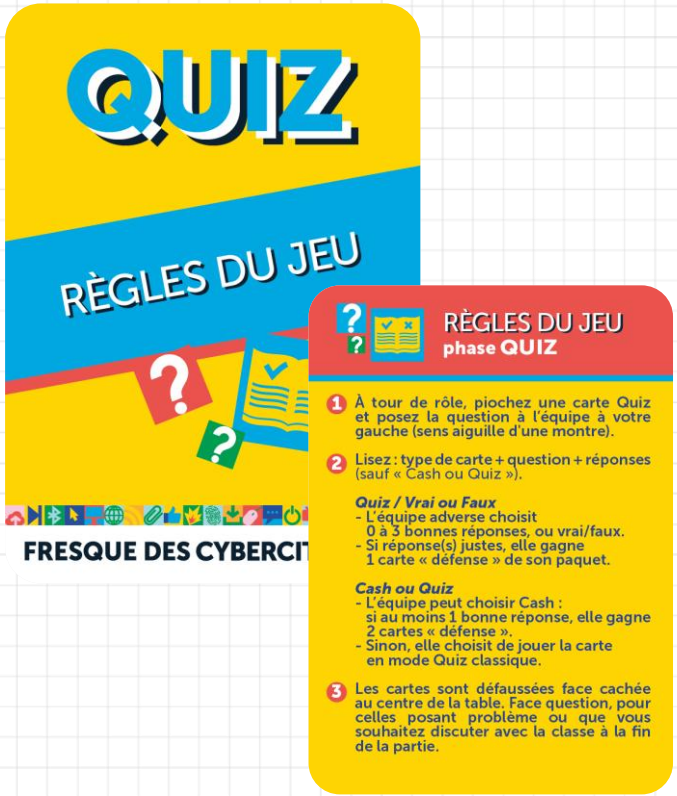
Je n'utilise pas de wifi public pour transmettre ou saisir des informations privées, comme un mot de passe.

14

J'active la double authentification quand je peux.

15

Cartes Règles du jeu



Pour toute remarque ou suggestion, contactez l'équipe de la Fresque des Cybercitoyens:

fresquedescybercitoyens@advens.fr