

Guide des cartes

2024 | Par



Comment utiliser ce guide ?

Ce guide des cartes et sources a pour objectif de recenser toutes les cartes « Quiz » du jeu, en fournissant des explications et en indiquant toutes nos sources. Il n'est pas nécessaire de l'avoir lu avant d'animer une session, mais il peut servir à trouver des réponses aux questions des participants ou pour vérifier nos sources.

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.

SOMMAIRE

1. Thématique Cyberharcèlement



[Niveau 1](#)

[Niveau 2](#)

[Niveau 3](#)

2. Thématique Désinformation



[Niveau 1](#)

[Niveau 2](#)

[Niveau 3](#)

3. Thématique Cyberdéfense



[Niveau 1](#)

[Niveau 2](#)

[Niveau 3](#)

4. Thématique Cyberattaque



[Niveau 1](#)

[Niveau 2](#)

[Niveau 3](#)

5. Thématique Mots de passe



[Niveau 1](#)

[Niveau 2](#)

[Niveau 3](#)

6. Thématique Vie privée



[Niveau 1](#)

[Niveau 2](#)

7. Autres cartes

[Cartes « Cyberattaque »](#)

[Cartes « Défense »](#)



1. Thématique Cyberharcèlement





QUIZ

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

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

Réponses : A, B et C
Exemple de preuve : capture d'écran.

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-cyberharcèlement-ou-harcèlement-en-ligne>





QUIZ

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

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

Réponses : A, B et C

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.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/que-faire-en-cas-de-cyberharcèlement-ou-harcèlement-en-ligne#definition-cyberharcèlement>





QUIZ



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

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

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

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/>





Répéter une rumeur sur quelqu'un peut être considéré comme du harcèlement.

Réponse : Vrai

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/>





Le harcèlement ou le cyberharcèlement peut conduire les victimes au décrochage scolaire, à la dépression voire au suicide.

Réponse : Vrai

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_Cyberharcèlement.pdf





Liker un commentaire insultant c'est participer à du harcèlement.

Réponse : Vrai

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-cyberharcèlement-ou-harcèlement-en-ligne>





**VRAI
ou FAUX**



Si on discute avec quelqu'un sur internet et qu'on peut voir ses photos, alors on peut lui faire confiance.

Réponse : Faux

Explications

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

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

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

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





**CASH
ou QUIZ**



Quel est le numéro gratuit et anonyme qui permet d'aider les victimes et les témoins de cyberharcèlement ?

- A. 3018
- B. 15
- C. 117 217

Réponse : A
Il existe aussi une application 3018.

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.

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





QUIZ



Parmi les propositions suivantes, lesquelles correspondent à la définition d'un cyberprédateur ?

- A. Un adulte qui cherche à draguer des adolescents ou enfants sur internet
- B. Une personne qui veut vendre des produits
- C. Un adulte qui cherche à piéger des jeunes en les mettant en confiance, par exemple avec des cadeaux

Réponses : A et C

Explications

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

Source : <https://spvm.qc.ca/fr/jeunesse/Cyberpredateur>





QUIZ



L'application 3018 propose les services suivants :

- A. Des réponses toutes faites à envoyer à son cyberharceleur
- B. Une aide pour faire supprimer des contenus sur les réseaux sociaux
- C. Un test de 2 min pour savoir si on vit une situation de harcèlement

Réponses : B et C

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.

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





QUIZ



Les cyberharceleurs peuvent être condamnés par la justice, même si :

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

Réponses : A, B et C

Explications

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

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

Sources :

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/que-faire-en-cas-de-cyberharcèlement-ou-harcèlement-en-ligne>

<https://www.service-public.fr/particuliers/vosdroits/F32239>





Contribuer à un groupe de discussion privé qui sert à se moquer de quelqu'un, c'est participer à du harcèlement.

Réponse : Vrai
Même si la victime n'est pas dans le groupe.

Explications

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

Le fait de réagir, par exemple liker, de rediffuser ou de valider les propos des harceleurs rend complice de la situation et peut également engager sa responsabilité devant la loi.

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





Prendre des photos ou des vidéos de quelqu'un, ce n'est pas participer à du harcèlement s'il ne le sait pas.

Réponse : Faux

Explications

Publier des photos et vidéos embarrassantes ou humiliantes sur quelqu'un constitue une forme de cyberharcèlement.

Même si l'on n'est pas directement concerné, il est possible de signaler la vidéo si elle apparaît sur un réseau social. En revanche, il est fortement conseillé de ne pas réagir, 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/informer/cyber-harcelement/>





Créer un faux compte à une vraie personne pour se moquer, c'est du harcèlement.

Réponse : Vrai

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.

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





QUIZ



En 2023, combien de collégiens ont été victimes de cyberharcèlement ?

- A. 1 collégien sur 10
- B. 1 collégien sur 5
- C. 1 collégien sur 4

Réponse : C

Explications

Ce chiffre est issu d'une étude datant de 2023 réalisée par l'association e-Enfance. Les chiffres sont éloquentes : 25% des élèves de collèges ont été confrontés au cyberharcèlement.

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

Source : Étude Audirep/Association e-Enfance, Juin 2023 => https://e-enfance.org/wp-content/uploads/2023/10/20231017_Infographie_Etude-Caisse-dEpargne_e-Enfance_Cyberharcelement.pdf





QUIZ



Concernant le numéro et l'application 3018, lesquelles de ces propositions sont vraies ?

- A. C'est anonyme, personne ne saura qu'on a appelé
- B. La police sera automatiquement contactée
- C. On peut appeler juste pour avoir des conseils

Réponses : A et C

Explications

Voici les accompagnements proposés via l'application 3018 :



La mise en relation directe par tchat ou téléphone avec un professionnel du 3018 pour une prise en charge rapide et personnalisée.



Le stockage des preuves du harcèlement vécu (captures d'écran, photos, liens url, etc.) dans un coffre-fort numérique et sécurisé, ainsi que la possibilité de transférer tout ou une partie de ces preuves aux équipes 3018.



L'auto-évaluation de sa situation à l'aide du quiz "Suis-je harcelé ?", pour encourager la victime à demander de l'aide.



Un accès rapide à des fiches conseil sur le harcèlement scolaire et le cyberharcèlement, pour s'informer sur ses droits et savoir comment réagir.

Source : <https://e-enfance.org/app-3018/>





CASH ou QUIZ



A quoi peut-on reconnaître qu'une personne est victime de harcèlement ?

- A. Elle est triste et parfois isolée
- B. Une ou plusieurs personnes l'insultent dans son dos ou se moquent
- C. Des personnes publient des choses sur elle sur internet sans lui demander

Réponses : A, B et C
Dans ce cas il est important de réagir,
même si on ne connaît pas bien la victime.

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 en quelques minutes pour identifier si l'on vit une situation de harcèlement.

Source :



1. Thématique "Cyberharcèlement"

Pour aller plus loin - Cyberharcèlement

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

- [Ministère de l'éducation nationale | pHARe : un programme de lutte contre le harcèlement à l'école](#)

Des conseils pour faire face au cyberharcèlement :

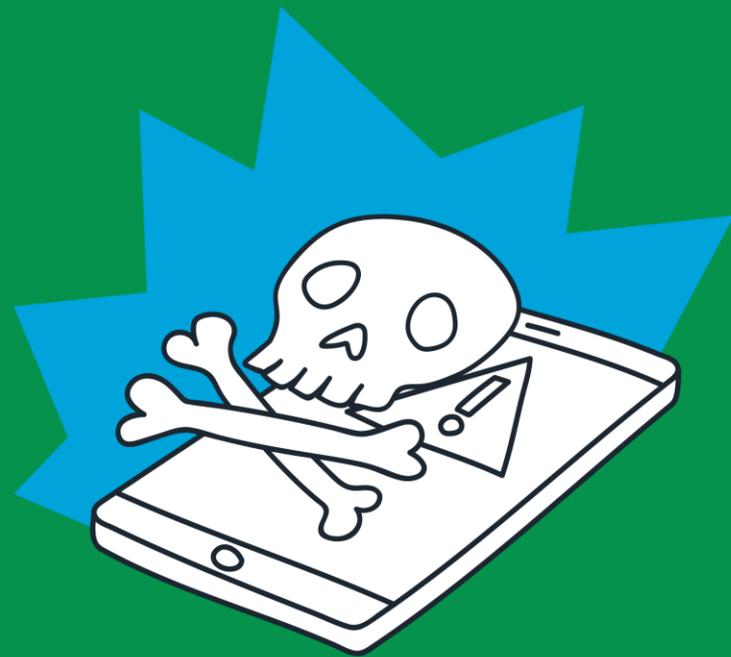
[CNIL | Faire face au cyberharcèlement](#)

[Fondation Enfance | Réagir en tant que professeur ou chef d'établissement](#)

Pour en parler avec des jeunes :

- [Pièce de théâtre de l'association pratique | Le chat](#)
- [Pièce de théâtre Cie Ariadne | Ces filles-là](#)
- [Webtoon - Cybervengers](#)
- [Webtoon Editions Dupuis | Les Combats Invisibles](#)





2. Thématique Désinformation





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

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

Réponses : A, B et C

Explications

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

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

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

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



2. Thématique “Désinformation” - Niveau 1



VRAI ou FAUX ★

Les contenus qui sont recommandés sur les réseaux sociaux sont forcément vérifiés par la plateforme.

Réponse : faux

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 1



VRAI ou FAUX ★

Toutes les informations sur Wikipédia sont vraies.

Réponse : Faux
C'est en général une bonne source d'info, mais on peut y trouver des erreurs.

Sources :

<https://www.1jour1actu.com/culture/a-quoi-ca-sert-wikipedia>
[Wikipédia:Vérifiabilité — Wikipédia \(wikipedia.org\)](https://fr.wikipedia.org/wiki/Wikip%C3%A9dia:V%C3%A9rifiabilit%C3%A9)

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. Ceci est très utile.

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 Wikipédiens.

Ainsi, 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



VRAI ou FAUX ★

Une *fake news* se propage plus vite qu'une vraie information.

Réponse : Vrai

Fake news se traduit en français par « fausse information »

Explications

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

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

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





Comment peut-on vérifier une information ?

- A. Contrôler si la source est fiable
- B. Demander à une copine
- C. Faire des recherches sur différents médias

Réponses : A et C
On peut croiser les informations sur différents sites d'information.

Explications

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

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

Source : <https://www.info.gouv.fr/actualite/lutter-contre-les-fake-news>





? QUIZ

Quelle est la recette d'une *fake news* ?

- A. Le titre est sensationnel et accrocheur
- B. Le contenu est long et détaillé
- C. Des sources officielles sont citées

Réponse : A

Explications

Les fake news, ou fausses informations, sont construites de diverses manières, allant du simple canular à la désinformation volontaire. Elles peuvent inclure des chiffres inventés, des images retouchées ou des vidéos sorties de leur contexte.

Par exemple, une vidéo réelle mais ancienne peut être réutilisée pour manipuler l'opinion publique en lui donnant un sens différent. De plus, certains sites sensationnalistes cherchent avant tout à attirer des clics en déformant la réalité avec des titres accrocheurs, visant à générer des revenus publicitaires. Les canulars, quant à eux, reposent sur des récits imaginaires conçus pour divertir, mais peuvent parfois tromper les internautes.

Source : <https://www.clemi.fr/ressources/ressources-pedagogiques/des-fake-news-aux-multi-ples-facettes>





? QUIZ

Pourquoi des personnes partagent des fausses informations ?

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

Réponses : A, B et C
C'est pourquoi il est important de vérifier ses sources pour éviter d'être manipulé.

Explications

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

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

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

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





? QUIZ

Quelle est la différence entre un journaliste et un influenceur ?

- A. L'influenceur doit vérifier que ce qu'il dit est vrai
- B. C'est le même métier
- C. Le journaliste est soumis à des règles liées à son métier

Réponse : C

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



**VRAI
ou FAUX**



Les fausses informations
partagées sur les réseaux
sociaux peuvent entraîner
de graves conséquences, et
même des morts.

Réponse : Vrai
Par exemple, en Inde, une fake news
lançé sur WhatsApp a provoqué une
vague de lynchage.

Explications

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

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

Sources :

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

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



VRAI ou FAUX

La recherche inversée d'images permet de retrouver l'origine d'une image sur internet.

Réponse : Vrai

La recherche inversée fonctionne avec Google Lens ou TinEye.

Explications

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

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

Sources :

<https://tineye.com/>

<https://lens.google.com/intl/fr/>

La majorité des fake news sont générées par des intelligences artificielles.

Réponse : Vrai

Explications

Une fake news est définie comme une information fausse et délibérément créée pour nuire à une personne, un groupe social, une organisation ou un pays.

Avec l'avènement des IA génératives, la production de contenus volontairement trompeurs s'est démultipliée. Ces technologies permettent de créer des textes, images et vidéos de manière automatisée, rapide et réaliste, rendant la détection de la désinformation plus complexe. Par exemple, des deepfakes peuvent manipuler des vidéos pour faire dire ou faire des actions à des personnes qu'elles n'ont jamais dites ou faites.

Source : <https://www.newsguardtech.com/special-reports/ai-tracking-center/>



Il y a des personnes qui sont payées pour propager de fausses informations.

Réponse : Vrai

Explications

Début 2023, une centaine de journalistes de 30 médias internationaux, réunis au sein du consortium Forbidden Stories, a publié le résultat d'une enquête de plus de 6 mois sur l'industrie de la désinformation : l'enquête s'appelle « Story Killers ». Cette enquête a révélé les ressorts utilisés par les entreprises et les mercenaires qui vendent désormais des services "clé en main" à des États ou des hommes politiques dans le but d'influencer les opinions, manipuler des élections, ou détruire des réputations au détriment de l'information et de la démocratie.

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

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





**VRAI
OU FAUX**



**Les intelligences artificielles
n'écrivent pas de théories
du complot et préviennent
toujours quand elles ne sont
pas complètement sûres
de leurs réponses.**

Réponse : Faux

Sources :

<https://www.lesechos.fr/tech-medias/intelligence-artificielle/intelligence-artificielle-generative-la-revolution-chatgpt-en-marche-1935018>

<https://www.futura-sciences.com/tech/actualites/intelligence-artificielle-chatgpt-probleme-desinformation-104281/>

Explications

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

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





Dans quel but certaines personnes ou organisations créent et publient de fausses informations ?

- A. Pour faire changer la réputation de quelqu'un, en bien ou en mal
- B. Pour gagner de l'argent
- C. Pour manipuler les gens et leur faire croire ce qu'on leur dit

Le fake news sont créées pour des raisons politiques, idéologiques ou financières.
Réponses : A, B et C

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

Explications

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

Pour aller plus loin - Désinformation

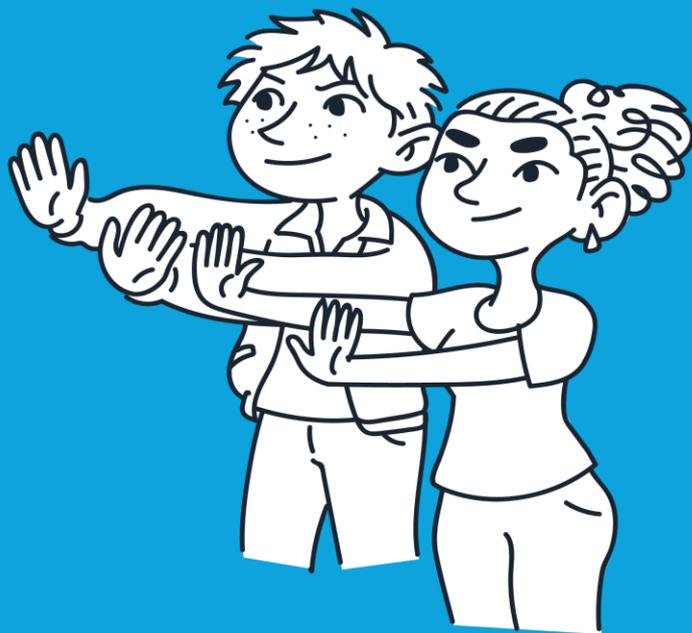


Comprendre et réagir face aux fake news :

- [CLEMI | Réagir et agir face aux fakes news](#)
- [Guide pratique du CLEMI | La famille tout-écran](#)
- [Lumni | Fake news et désinformation](#)

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

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



3. Thématique Cyberdéfense





À quoi sert un antivirus ?

- A. À naviguer sur internet de façon anonyme
- B. À bloquer les virus
- C. À bloquer les tentatives d'arnaques

Réponse : B

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](#)





Comment installer de façon sécurisée des applications sur son smartphone ?

- A. Via un lien sur Youtube
- B. Depuis des plateformes de confiance (Apple Store, Google Play, etc...)
- C. Depuis des sites recommandés par ses amis

Réponse : B

Explications

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

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

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





Quand doit-on sauvegarder ses données ?

- A. Le plus régulièrement possible
- B. Après s'être fait pirater
- C. Quand on a le temps

Réponse : A

Explications

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

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

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

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





QUIZ

Comment peut-on sauvegarder ses données ?

- A. En les mettant sur un cloud
- B. En les mettant sur un disque dur externe ou une clé USB
- C. En les apprenant par cœur

Réponses : A et B
Le cloud est un espace en ligne pour stocker et accéder à des données partout.

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>





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

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

Réponse : C

Explications

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

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

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

Sources :

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/antivirus>

[Cybermalveillance.gouv.fr - Comment sécuriser mes appareils pour qu'ils ne soient pas attaqués par des virus ? - Vidéo Dailymotion](#)





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

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

Réponse : C

Explications

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

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

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

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





Le wifi public est aussi sécurisé que la 4G / 5G.

Réponse : Faux
Les wifi publics ont souvent une faible sécurité. Un hacker peut facilement surveiller ce que tu fais.

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>





VRAI ou FAUX

Si on va sur un site internet illégal on a beaucoup plus de risques d'être infecté par un virus.

Réponse : Vrai

Explications

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

Cybermalveillance.gouv alerte sur la dangerosité des sites suivants :

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

Source : <https://www.digitalcitizensalliance.org/issues/unholy-triangle-report/>





VRAI ou FAUX

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

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/>







Quelle est la différence entre "http" et "https", au début de l'adresse d'un site web ?

A. Le site en "http" est plus fiable
B. Le site en "https" est français
C. Le site en "https" est plus sécurisé

Réponse : C

Explications

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

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

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

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

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





QUIZ



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

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

Réponses : A et B

Explications

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

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

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





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

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

Réponse : B

Explications

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

Si l'on est sur un site web, il faut bien regarder le coin inférieur gauche du navigateur où apparaîtra 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>





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

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

Réponse : B

Explications

Contrairement à 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 hacker 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>





Comment détecter le piratage de son téléphone ?

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

Réponses : A, B et C

Sources :

<https://www.avg.com/fr/signal/bitcoin-miner-malware>

[Pegasus \(logiciel espion\) — Wikipédia \(wikipedia.org\)](#)

Explications

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

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

D'autres 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 aux 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.





Chiffrer des informations,
c'est les rendre
incompréhensibles en
utilisant un code secret.

Réponse : Vrai
Seuls ceux qui connaissent le code
pourront déchiffrer les informations.

Explications

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

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

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

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

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





Il existe un site internet qui permet de savoir si son numéro de téléphone ou son email a été piraté.

Réponse : Vrai
Le site s'appelle : "Have I been pwned ?"
(haveibeenpwned.com)

Explications

Créé en 2013 par Troy Hunt, l'application ressense 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 hackers 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://fr.wikipedia.org/wiki/Have_I_Been_Pwned%3F



3. Thématique « Cyberdéfense »

Pour aller plus loin - Cyberdéfense



Comprendre comment se protéger contre les cyberattaques :

- [Cybermalveillance.gouv](https://cybermalveillance.gouv.fr/) | [Cyberguide famille](#)
- [Ministère de l'économie](#) | [Comment assurer sa sécurité numérique](#)
- [Cybermalveillance.gouv](https://cybermalveillance.gouv.fr/) | [10 mesures essentielles assurer votre sécurité numérique](#)
- [Agence Nationale de Sécurité des Systèmes d'Information \(ANSSI\)](https://www.anssi.fr/) - [Guide des bonnes pratiques de l'informatique](#)

Pour aller plus loin dans la formation à la cybersécurité :

- [Cybermalveillance.gouv](https://cybermalveillance.gouv.fr/) | [MOOC sens-cyber](#)
- [ANSSI](https://www.anssi.fr/) | [MOOC secnumacademie](#)





4. Thématique Cyberattaque





QUIZ



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

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

Réponses : B et C
Les wifi publics ont souvent une faible sécurité. Un hacker peut facilement surveiller ce que tu fais.

Sources :

[Cybermalveillance.gouv.fr](https://www.cybermalveillance.gouv.fr) - WiFi public : comment empêcher le vol de mes données ? - Vidéo Dailymotion

[Cybermalveillance.gouv.fr](https://www.cybermalveillance.gouv.fr) - Quels risques prend-on en se connectant sur les réseaux #WiFi gratuits ? - Vidéo Dailymotion





QUIZ

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

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

Réponse : A

Explications

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

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

Sources :

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/10-mesures-essentielles-assurer-securite-numerique>

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mises-a-jour>





QUIZ



Que doit-on faire si on trouve une clé USB dans la rue ?

- A. Vérifier ce qu'il y a dessus pour la rendre à son propriétaire
- B. La garder : on sait jamais, ça pourrait servir
- C. La jeter à la poubelle

Réponse : C
Il pourrait y avoir un virus.

Explications

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

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

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

Sources :

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

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/antivirus>





QUIZ



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

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

Réponses : A et C

Explications

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

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

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





QUIZ

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

- A. Je ne clique pas sur le lien contenu dans le SMS
- B. Je réponds au SMS pour en savoir plus
- C. Je supprime le SMS si je pense qu'il est frauduleux

Réponses : A et C

Explications

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

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

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

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





QUIZ

Sur quoi peuvent être revendues les données qu'un hacker a volées ?

- A. Sur Vinted
- B. Sur le dark web
- C. Sur Leboncoin

Réponse : B
Même s'il n'y a pas que ça, le dark web est surtout connu pour des trafics illégaux.

Explications

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

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

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

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





QUIZ

Que faire si j'ai identifié un message qui me semble être du *phishing* (hameçonnage en français) ?

- A. Prévenir un adulte
- B. Supprimer le message
- C. Faire ce que le message me demande, pour vérifier si c'est vraiment une arnaque

Réponses : A et B
L'adulte pourra faire un signalement sur la plateforme Pharos pour éviter que d'autres personnes soient piratées.

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>





QUIZ

Qu'est-ce qu'un *ransomware* ?

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

Réponse : A
Ransomware se traduit par rançongiciel en français.

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-ranconiciel-definition>





QUIZ



Qu'est-ce que le *phishing* ?

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

Réponse : A
Le phishing se traduit par hameçonnage
en français.

Explications

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

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

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

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

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





QUIZ

Parmi les adresses de sites internet suivantes, lesquelles vous semblent suspectes ?

- A. Fnac.achat-pas-cher.fr
- B. Fnak.ru
- C. Fnac.com

Réponses : A et B

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 : l 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/>





QUIZ

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

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

Réponse : A

Explications

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

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

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

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

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





QUIZ

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

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

Réponses : B et C

Explications

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

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

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

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





QUIZ



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

- A. Les mots de passe que l'on tape sur internet
- B. Les sites que l'on consulte
- C. Les messages WhatsApp

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

Sources :

[Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) - WiFi public : comment empêcher le vol de mes données ? - Vidéo Dailymotion

[Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) - Quels risques prend-on en se connectant sur les réseaux #WiFi gratuits ? - Vidéo Dailymotion





QUIZ

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

- A. Créer un faux wifi qui a le même nom que le vrai wifi public
- B. Utiliser un VPN
- C. Se connecter et regarder les messages non chiffrés qui sont envoyés

Réponses : A et C

Explications

Il est facile pour un hacker 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.cnit.fr/fr/utiliser-un-wi-fi-public-voici-4-precautions-prendre>





QUIZ



J'ai cliqué sur un lien ou une pièce-jointe et je pense que j'ai téléchargé un virus. Que dois-je faire ?

- A. Éteindre mon téléphone ou ordi, le virus va disparaître
- B. Prévenir un adulte
- C. Couper la connexion wifi, ça évite de le diffuser sur d'autres appareils connectés

Réponses : B et C

Explications

Si on pense avoir téléchargé un virus, le premier réflexe à avoir est de prévenir un adulte et de couper internet, pour éviter toute connexion entre le hacker 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>





Quelle technique d'attaque consiste à rendre indisponible des services sur internet en envoyant de très nombreuses demandes ?

- A. Ransomware
- B. Phishing
- C. Déni de service

Réponse : C

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>







Quelle technique d'attaque consiste à tester toutes les combinaisons possibles de mots de passe ?

- A. Déni de service
- B. Brute force
- C. Man in the middle

Réponse : B

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 »

Pour aller plus loin - Cyberattaque

Comprendre et réagir face aux cyberattaques :

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

Les jeux pour parler de cybersécurité :

- [Cybermalveillance.gouv | Mallette cyber inclusion numérique](#)
- [Région académique Bourgogne-Franche-Comté | Le kit CyberEnjeux de l'ANSSI](#)
- [Eduscol | Education et cybersécurité](#)
- [Cyber Duel de Game Partners](#)

Autre ressource :

[Bande dessinée - Les enquêtes de Seven](#)





5. Thématique Mots de passe





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

- A. 8
- B. 12
- C. 20

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

Explications

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

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



Il suffit de quelques secondes à un hacker pour craquer un mot de passe simple, ou composé d'informations publiques telles que : prénom, nom, date de naissance, etc.

Réponse : Vrai

Explications

Une technique automatisée, dite par « force brute », 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 hacker 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



**VRAI
ou FAUX**

Si on a plusieurs mots de passe, il faut les noter sur un papier.

Réponse : Faux
Quelqu'un pourrait trouver le papier !

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 boîte 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>





QUIZ

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

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

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

Explications

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

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

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

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





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

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

Réponse : B

Explications

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

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

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





QUIZ



Pourquoi doit-on activer la double authentification ?

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

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

Explications

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

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

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

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





Quelles sont les deux conditions pour créer un mot de passe fort ?

- A. Utiliser un mot compliqué
- B. Avoir au moins 12 caractères
- C. Contenir au moins 1 majuscule, 1 minuscule, 1 chiffre et 1 caractère spécial

Réponses : B et C

Explications

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

Pour empêcher ce type d'attaque, il est admis qu'un bon mot de passe doit comporter au minimum 12 signes : c'est le critère de longueur du mot de passe. Un mot de passe complexe comprend également des majuscules, des minuscules, des chiffres et des caractères spéciaux. Un mot de passe dit « fort » cumule le critère de longueur et de complexité.

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





Pourquoi doit-on verrouiller son téléphone avec un mot de passe ou un code ?

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

Réponses : A et B
L'empreinte digitale et la reconnaissance faciale sont un peu moins sécurisées, mais c'est mieux que rien.

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 2



VRAI ou FAUX

Si on a accès à la boîte mail de quelqu'un, on peut pirater presque tous ses comptes qui n'ont pas de double authentification.

Réponse : Vrai
Exemple de double authentification :
login/mot de passe + code reçu par SMS.

Explications

Notre boîte 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 boîte 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>







Qu'est-ce qu'une "double authentification" ?

- A. Se connecter avec un identifiant et un mot de passe
- B. Renseigner deux fois son mot de passe
- C. Prouver son identité en se connectant en 2 étapes par 2 moyens différents

Réponse : C

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

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 hacker réussit à trouver un mot de passe, il a peu de chances d'accéder au deuxième moyen d'authentification.

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





Choisir un bon mot de passe
c'est :

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

Réponse : Aucune

Explications

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

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

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

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





QUIZ



On m'a volé mon téléphone.
Mon code PIN est 0000, mais
j'ai un code pour déverrouiller
l'écran. Que peut-il se passer ?

- A. Le voleur pourrait récupérer des données sur mon téléphone
- B. Personne ne pourra accéder à mes données
- C. Si je désactive ma carte SIM, les données dessus sont supprimées

Réponses : A et C

Explications

Le code PIN est un code d'accès composé d'au moins 4 chiffres qui sert à verrouiller l'accès à la carte SIM d'un téléphone.

On le choisit généralement au moment de l'acquisition du téléphone, mais il est souvent configuré par défaut avec un code standard, par exemple « 0000 » ou « 1234 ». Il est important de le changer à la réception du téléphone. En effet, sans ce code PIN, l'accès à la carte SIM du téléphone est bloqué. En revanche, si on garde le code par défaut, une personne qui trouve ou vole le téléphone pourra accéder aux données stockées sur la carte SIM, même si vous avez un moyen de verrouillage de l'écran (empreinte, code, ...). Enfin, si la carte SIM a été désactivée, en contactant son opérateur, les données stockées sur celle-ci seront supprimées et donc inaccessibles.

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







A quoi sert un gestionnaire de mot de passe ?

- A. À se rappeler de tous ses mots de passe
- B. À bloquer les mots de passe faibles
- C. À suggérer des mots de passe forts

Réponses : A et C

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 »

Pour aller plus loin - Mots de passe

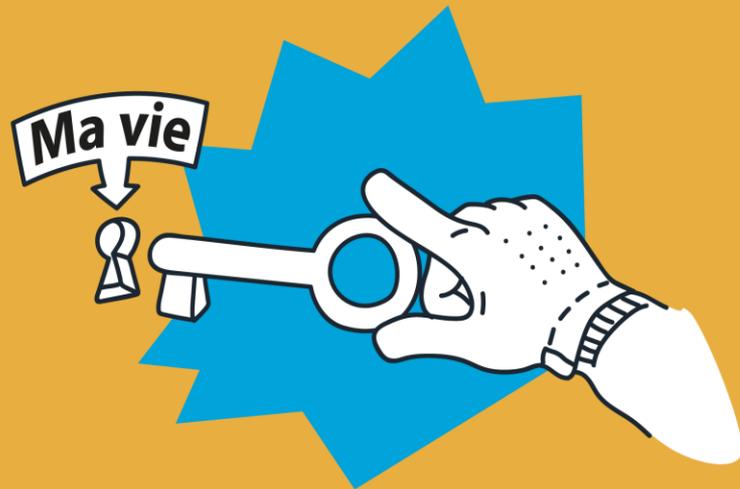


Choisir de bons mots de passe :

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

Comprendre le fonctionnement des mots de passe :

- [Micode sur Youtube | Stocker son mot de passe sur son navigateur... ou pas.](#)



6. Thématique

Vie privée





QUIZ



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

- A. Passer son profil privé en public
- B. Accepter les invitations d'autres pâtisseries sur son compte privé
- C. Créer un nouveau compte Instagram public

Réponse : C

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>





QUIZ

Que peut faire un site internet lorsqu'on accepte ses cookies ?

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

Réponses : A et B

Sources :

<https://www.cnil.fr/fr/definition/cookie>

<https://www.cnil.fr/fr/cookies-et-autres-traceurs/comment-se-protger/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.





QUIZ

Quel serait un bon pseudo pour Sarah Martin, née en 2011 ?

- A. Sarah 2011
- B. Golgotha
- C. Sarah.Martin

Réponse : B

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.

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





QUIZ



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

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

Réponse : A

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/>





QUIZ

En général, sur un réseau social, quand le profil est "public", cela veut dire que tout le monde peut :

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

Réponses : A, B et C

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



VRAI ou FAUX

Il est possible de demander à un réseau social ou site internet de supprimer un contenu choquant ou insultant, même si ce n'est pas sur moi.

Réponse : Vrai

Explications

Les contenus illicites (incitation à la haine, violence contre les personnes ou les animaux, homophobie, pédophilie, etc.) peuvent être signalés sur la plateforme PHAROS, qui est gérée par des policiers et des gendarmes spécialisés.

Certaines plateformes de réseaux sociaux proposent également leur propre système de signalement, en voici quelques exemples : [Instagram](#), [Snapchat](#), [Discord](#), [TikTok](#), [WhatsApp](#), [YouTube](#), [Facebook](#), [Twitter](#).

Sources :

<https://www.service-public.fr/particuliers/vosdroits/F31979>

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/que-faire-en-cas-de-cyberharcèlement-ou-harcèlement-en-ligne#definition-cyberharcèlement>



6. Thématique « Vie privée » - Niveau 1



VRAI ou FAUX

Il est possible de demander à un réseau social ou site internet de supprimer un contenu sur soi.

Réponse : Vrai

Explications

Les contenus illicites (incitation à la haine, violence contre les personnes ou les animaux, homophobie, pédophilie, etc.) peuvent être signalés sur la plateforme PHAROS, qui est gérée par des policiers et des gendarmes spécialisés.

Certaines plateformes de réseaux sociaux proposent également leur propre système de signalement, en voici quelques exemples : Instagram, Snapchat, Discord, TikTok, WhatsApp, YouTube, Facebook, Twitter.

Sources :

<https://www.service-public.fr/particuliers/vosdroits/F31979>

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/que-faire-en-cas-de-cyberharcèlement-ou-harcèlement-en-ligne#definition-cyberharcèlement>





VRAI ou FAUX ★

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

Réponse : Vrai

Explications

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

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

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





Où est-il possible de retrouver la liste des derniers sites internet qu'on a consultés ?

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

Réponse : A

Explications

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

Ainsi, les requêtes, les recherches effectuées, les sites web visités sont conservés dans l'historique. 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-l-historique-de-navigation>





Pourquoi est-il préférable d'utiliser un pseudonyme sur les réseaux sociaux ?

- A. Pour pouvoir troller librement
- B. Pour protéger son identité (âge, genre, nom)
- C. Pour envoyer des informations qu'on n'assume pas

Réponse : B

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-protger>

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.





QUIZ



À quoi sert la navigation privée ?

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

Réponses : A et C

Explications

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

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

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





Comment les réseaux sociaux gagnent de l'argent ?

- A. Grâce aux dons des utilisateurs
- B. En revendant nos données
- C. Grâce aux publicités

Réponses : B et C

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





Que faut-il supprimer pour réduire le pistage publicitaire sur internet ?

A. L'historique
B. Les cookies
C. Ses parents sur Facebook

Réponses : A et B

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-l-historique-de-navigation>

<https://www.cnil.fr/fr/cookies-et-autres-traceurs/comment-se-protger/maitriser-votre-navigateur>



6. Thématique « Vie privée »

Pour aller plus loin - Vie privée

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

- [CNIL | Les droits pour maîtriser vos données personnelles](#)
- [CNIL | 1 heure pour adopter de meilleurs réflexes pour votre vie privée numérique](#)
- [CNIL | La navigation privée pour limiter les risques de piratage de vos comptes en ligne](#)
- [Service de police de la Ville de Montréal \(SPVM\) | Informations sur les cyberprédateurs](#)
- [Cybermalveillance.gouv | 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 | Découvrez le jeu immersif Les gardiens du Numérique à la cité des sciences et de l'industrie](#)
- [CNIL | Un jeu de cartes pour rester net sur internet](#)





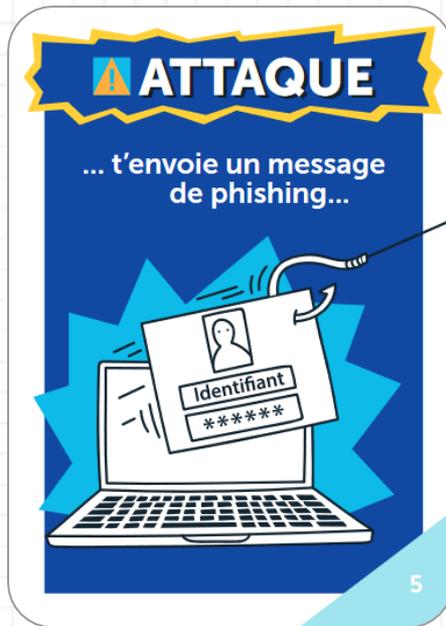
7. Cartes « Cyberattaque » et « Défense »



Les cartes « Attaquant »



Les cartes « Attaque » (1/2)



Les cartes « Attaque » (2/2)



Les cartes « Impact » (1/2)



Les cartes « Impact » (2/2)



Cartes « Défense » (1/2)

J'utilise un mot de passe complexe et j'active la double authentification quand je peux.

1

J'ai une protection antivirus à jour.

2

Je télécharge les mises à jour automatiquement.

3

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

4

Je bloque les personnes qui sont agressives sur les réseaux sociaux.

5

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

6

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

7

Si je suis témoin ou victime de cyberharcèlement ou de chantage, j'en parle à un adulte en qui j'ai confiance.

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 ou plusieurs comptes.

10

Si je me suis fait pirater, j'en parle avec un adulte en qui j'ai confiance.

11

Je réalise régulièrement des sauvegardes de mes données importantes.

12

Lorsque je vais sur internet, j'utilise un pseudonyme.

13

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

14

J'utilise un mot de passe différent pour chacun de mes comptes.

15



