
NUMéVILLE
Livret
maître du jeu

Numéville

Le « livret maître du jeu » est un support pédagogique conçu pour approfondir les notions évoquées à travers les questions du jeu Numéville.
Il rassemble les 200 questions à choix multiple, une explication détaillée de chaque bonne réponse, les sources et des ressources complémentaires adaptées aux adolescents et aux adultes. Les thèmes proposés vont de l'impact environnemental du numérique à la cybersécurité et aux bonnes pratiques en ligne. L'objectif est d'offrir au maître du jeu un outil clés en main pour sensibiliser de façon participative aux enjeux sociaux et environnementaux du numérique.

INR Institut du Numérique Responsable ISIT Institute for Sustainable IT ISIT Institute for Sustainable IT


Hyperco

1. Qu'est-ce que la règle des 20-20-20 ?

A) Une technique recommandée pour réduire les effets néfastes de l'utilisation prolongée des écrans sur la vision
B) Une technique de jeu pour gagner à Super Mario
C) Une technique pour partager 60 en 3 parts

Tes yeux travaillent beaucoup quand tu regardes un écran ! Imagine que tes yeux sont comme des muscles qui se fatiguent. La règle des 20-20-20 est un truc génial pour les reposer toutes les 20 minutes : arrête de regarder ton écran pendant 20 secondes et regarde quelque chose qui est loin (au moins à 20 pieds, c'est-à-dire 6 mètres). C'est comme si tu donnais une petite pause à tes yeux ! Tu peux regarder par la fenêtre, observer un arbre ou même le plafond. Cette règle a été inventée par des docteurs spécialistes de la vision car de plus en plus de personnes passent du temps sur les écrans. Tes yeux te remercieront !

Source : Association nationale pour l'amélioration de la vue (Asnav)

2. Que désigne-t-on par temps d'écran ?

A) Toutes les activités effectuées sur un appareil électronique disposant d'un écran
B) La durée nécessaire pour allumer l'écran d'un appareil électronique
C) La vitesse d'affichage des informations sur un appareil électronique

Le temps d'écran, c'est toutes les minutes que tu passes devant un écran. Télé, tablette, ordinateur, console de jeux, téléphone... tout compte ! Devant les écrans le temps peut passer à une vitesse folle ! C'est important d'en avoir conscience car nos yeux et notre corps ont besoin de pauses. Trop de temps d'écran peut nous rendre moins actifs et nous faire moins jouer avec nos amis ou notre famille. Passer du temps sur les écrans peut être sympa et parfois utile, mais il ne faut pas en abuser ! Les professionnels de la santé étudient le temps d'écran pour donner des conseils aux enfants et aux parents. L'idée n'est pas d'arrêter complètement les écrans, mais de trouver un bon équilibre avec d'autres activités comme le sport, la lecture ou des sorties en extérieur.

Ressource pour un adulte : Podcast France Culture « ô temps d'écran, suspends ton vol »
Ressource pour tous : Mon moment écran (Internet sans crainte)

3. Quelle quantité d'eau est nécessaire pour fabriquer un ordinateur portable de 2 kg ?

A) 15 litres
B) 500 litres
C) 1 500 litres

Incroyable mais vrai : il faut 1500 litres d'eau pour fabriquer un petit ordinateur portable ! Cette eau sert à traiter les métaux précieux et aide à l'extraction minière. Pour que tu te rendes compte : avec cette quantité d'eau, tu pourrais remplir 10 baignoires ! Alors que nous observons de plus en plus de sécheresses dans le monde, il est important de bien prendre soin de ton ordinateur ou tablette et de ne pas en changer trop souvent. Réparer plutôt que jeter, c'est économiser beaucoup d'eau !
Chaque fois qu'on évite de fabriquer un nouvel appareil, on économise cette précieuse ressource. C'est fou de penser qu'un objet si petit ait besoin d'autant d'eau pour être créé !

Source : Pourquoi réduire la pollution numérique ? (ADEME)
Ressource pour un ado : Les écrans, pourquoi ça pollue ? (Lumni)
Ressource pour un adulte : Les impacts écologiques du numérique (Canotech)

Ressource pour un adulte : Mallette pédagogique « Conscience numérique durable »

4. Quelle est la durée moyenne d'utilisation d'un téléphone portable ?

A) 1,5 an
B) 2,5 ans
C) 3,5 ans

En Europe, les gens gardent leur téléphone seulement 2 ans et demi en moyenne ! C'est très peu quand on sait qu'un téléphone pourrait durer beaucoup plus longtemps. Pour te donner une idée : un ordinateur portable dure 2 à 5 ans, un ordinateur fixe entre 5 et 7 ans ! Plus on garde nos appareils longtemps, moins on a besoin d'en fabriquer de nouveaux. Chaque téléphone qu'on garde une année de plus, c'est autant de matériaux et d'énergie économisés. Quelques conseils pour en prendre soin : protège-le avec une coque et un film de protection, évite de le laisser tomber, installe les mises à jour et baisse un peu la luminosité quand tu l'utilises. Si la batterie est fatiguée, tu peux la faire changer pour qu'il reparte comme neuf. Enfin, quand tu n'en veux plus, offre-le à un proche ou donne-le à un point de collecte : il servira à quelqu'un et la planète te dira merci.

Source : Longue vie à notre smartphone ! (ADEME)

5. Qu'est-ce que l'obsolescence programmée ?

A) Une panne causée par l'utilisateur
B) Une stratégie pour raccourcir la durée de vie d'un produit
C) Une garantie prolongée offerte par le fabricant

L'obsolescence programmée est une technique destinée à réduire la durée de vie ou d'utilisation d'un appareil pour inciter à en acheter un nouveau.
Certaines entreprises fabriquent leurs produits en sachant qu'ils vont casser ou devenir inutiles au bout d'un certain temps. Par exemple, elles peuvent utiliser des matériaux moins solides, rendre les réparations impossibles, ou arrêter de proposer des pièces de rechange.
Pourquoi font-elles cela ? Pour que tu achètes un nouveau produit plus rapidement ! Plus tu achètes souvent, plus elles gagnent d'argent. En France, cette pratique est reconnue comme un délit depuis 2015, car elle nuit aux consommateurs et à l'environnement. Quand tes appareils cassent trop vite, cela crée plus de déchets et oblige tes parents à dépenser plus d'argent. Heureusement, des associations et des lois existent et luttent contre ces pratiques.



Ressource pour un ado :
Les mal-jetés
(Réseau Canopé)

6. Quelle matière première est utilisée dans la fabrication d'un téléphone portable ?

A) De l'or
B) De l'uranium
C) Du bois

Savais-tu qu'il y a de l'or dans ton téléphone portable ? C'est surprenant mais vrai ! L'or est utilisé parce qu'il a des propriétés très intéressantes pour l'électronique : il conduit très bien l'électricité et ne rouille jamais. Dans ton téléphone, de minuscules fils d'or relient tous les composants pour que l'électricité circule parfaitement.
Bien sûr, ce n'est pas le seul matériau ! Ton téléphone contient aussi d'autres métaux précieux comme l'argent ou le cuivre, plus de 50 matériaux différents au total !
Certains viennent de mines très loin de chez nous. C'est pour cela qu'il est important de bien prendre soin de son téléphone et de le recycler quand il ne marche plus, pour récupérer un maximum de ces matériaux précieux.
L'or dans un téléphone représente une très petite quantité, mais quand on pense aux milliards de téléphones dans le monde, cela fait beaucoup d'or au total !



Ressource pour un ado :
Recyclage : nos portables valent de l'or !

7. Dans quel pays sont fabriqués la plupart de nos téléphones portables ?

A) États-Unis
B) Chine
C) France

La Chine est devenue l'usine du monde pour les téléphones portables !
En 2022, ce pays a fabriqué plus d'un milliard de smartphones, soit 7 téléphones sur 10 dans le monde entier. C'est énorme !
Pourquoi la Chine ? Ce pays a développé de gigantesques usines très modernes avec des millions d'ouvriers spécialisés. Ces usines peuvent produire des téléphones très rapidement et à des prix abordables. De nombreuses marques du monde entier font fabriquer leurs téléphones là-bas, même des marques américaines ou européennes.
Ton téléphone a donc probablement voyagé des milliers de kilomètres depuis la Chine avant d'arriver dans tes mains ! Il a traversé les océans en bateau ou en avion.
C'est pourquoi il est important de bien en prendre soin : remplacer un téléphone, c'est faire voyager plein de matériaux depuis très loin.

Source : Le rôle de la Chine dans les chaînes d'approvisionnement mondiales de smartphones reste résilient (Fondation Asie-Pacifique du Canada)

Ressource pour un adulte : Cash investigation - Les secrets inavouables de nos téléphones portables / intégrale

8. Qu'est-ce qui a le plus d'impact environnemental ?

A) Un appel téléphonique audio
B) Un appel vidéo
C) C'est équivalent pour l'appel audio et l'appel vidéo

Un appel vidéo pollue plus qu'un appel audio ! Quand tu passes un appel avec la caméra, ton téléphone doit envoyer beaucoup plus d'informations : non seulement ta voix, mais aussi ton image filmée, c'est-à-dire environ 25 images par seconde.
Toutes ces informations voyagent par Internet, en passant par des antennes, des câbles et des centres de données qui consomment de l'électricité. Plus il y a d'informations à transporter, plus on utilise d'énergie.
Un appel vidéo consomme en moyenne 10 fois plus d'énergie qu'un appel audio !
Si tu veux discuter longtemps avec tes amis, un simple appel audio suffit et garde les appels vidéo pour les moments où c'est vraiment important de se voir !

Source : Privilégier l'audio à la vidéo (ADEME)
Ressource pour tous : Évaluer l'impact carbone de vos usages numériques (ADEME)

9. Parmi ces équipements informatiques, quel est celui qui consomme le plus d'énergie sur une même durée d'utilisation ?

A) Une console de jeux vidéo
B) Une Box Internet
C) Un ordinateur portable

C'est la console de jeux qui gagne le concours de consommation d'électricité !
Même si tu joues 2 h 30 par jour en moyenne, elle consomme plus d'énergie qu'une box Internet qui reste allumée 22h/24.
Pourquoi ? Parce que les jeux vidéo demandent beaucoup de puissance pour afficher de belles images en mouvement, diffuser le son et la musique et calculer tous les mouvements des personnages en temps réel.
En comparaison, un ordinateur portable consomme environ 5 fois moins qu'une console.
La box Internet, elle, consomme un peu moins que la console mais reste allumée presque tout le temps pour te donner Internet en permanence.
Astuce : pour économiser de l'énergie, pense à éteindre complètement ta console quand tu as fini de jouer, au lieu de la laisser en veille ! Petit bonus : tes parents seront contents de voir la facture d'électricité baisser !

Source : Électricité : quels appareils consomment le plus dans votre maison ? (ADEME)

10. Qu'est-ce que le recyclage d'un téléphone portable ?

A) Une opération qui consiste à récupérer les matières utilisées pour sa fabrication pour les réutiliser
B) Une opération qui consiste à réutiliser le téléphone après l'avoir réparé
C) Une opération qui consiste à revendre son téléphone pour que quelqu'un d'autre l'utilise en l'état

Le recyclage consiste à collecter les anciens appareils et à les démonter soigneusement pour séparer le plastique, le verre et les métaux précieux comme le cuivre, l'or ou l'aluminium. Chaque matériau est ensuite envoyé dans des usines spécialisées où il est lavé, broyé ou fondu, puis transformé en nouvelles matières premières.
Cette démarche réduit la nécessité d'extraire des métaux de la terre, ce qui consomme beaucoup d'eau et d'énergie et génère de la pollution. En déposant un vieux téléphone dans un point de collecte, tu contribues à préserver les ressources naturelles, à limiter les déchets électroniques et à protéger notre planète.

Ressource pour un adulte : Trouver un point de collecte dans votre département (Ecosystem)

11. Combien de temps faut-il pour qu'un téléphone portable se décompose dans la nature ?

A) 5 ans
B) 100 ans
C) 1000 ans

Imagine que tu jettes ton téléphone dans la forêt aujourd'hui. Dans 1000 ans, il sera encore là ! C'est incroyable, non ? Un téléphone portable met entre 500 et 1000 ans à disparaître complètement dans la nature. Pourquoi si longtemps ?
Parce qu'il est fait de matériaux très résistants : du plastique, du verre, et des métaux comme l'or, l'argent et le cuivre. Ces matériaux ne se décomposent pas aussi facilement qu'une pomme ou une feuille d'arbre. Pendant toutes ces années, ton téléphone peut libérer des substances toxiques qui polluent la terre et l'eau. C'est pour ça qu'il ne faut jamais jeter un téléphone dans la nature ! Apporte-le dans un point de collecte, une déchetterie ou une boutique de téléphone : ils savent comment le recycler et lui donner une seconde vie.

Source : How Long Does it Take Electronic Waste to Decompose ? (ERI)

12. Quels sont les impacts potentiels du temps passé sur les écrans ?

A) Un nombre de camarades plus important
B) Des troubles de la santé
C) Des journées moins longues

Les écrans, c'est génial pour apprendre, jouer et communiquer ! Mais si tu passes trop de temps devant, ton corps peut en souffrir.
Tes yeux peuvent devenir fatigués et secs ! Tu peux aussi avoir mal à la tête ou au cou. Le soir, l'écran peut troubler ton sommeil car la lumière bleue « réveille » ton cerveau au moment où il devrait se préparer à dormir. Parfois, passer trop de temps seul avec un écran peut aussi rendre triste ou anxieux. Pour éviter ces problèmes, il y a des solutions : faire des pauses régulières, cligner des yeux souvent, et respecter des horaires d'écran. Les experts recommandent au maximum 2 heures par jour d'écran pour les loisirs.

Ressources pour un adulte : La règle du 3 6 9 12 (CLEMI) et Limiter le temps d'écran grâce à nos défis « Moins d'écrans, plus d'interactions ! » (mpedia)

13. Faut-il garder toutes les photos prises avec ton téléphone ?

A) Oui, car plus il y a de photos, mieux c'est
B) Non, il vaut mieux trier pour éviter de gaspiller de l'espace et de l'énergie
C) Oui, car ton téléphone a de la mémoire infinie

Tu as pris 20 photos de ton chat qui dort ? Garde seulement la plus belle.
Stocker toutes tes photos, même les ratées, consomme de l'énergie sans que tu t'en rendes compte. Comment ? Tes photos sont souvent sauvegardées dans d'énormes centres de données (des data centers) qui fonctionnent jour et nuit avec des milliers de serveurs. Ces centres consomment énormément d'électricité pour garder tes photos en sécurité. Plus tu stockes de photos, plus ils consomment ! En triant régulièrement tes photos, tu libères de la place sur ton téléphone, il fonctionne mieux et plus longtemps. Tu aides aussi la planète en réduisant cette pollution numérique invisible.
Astuce : une fois par mois, supprime les photos floues, les doublons, et garde seulement tes préférées. C'est comme ranger ta chambre, mais pour ton téléphone !

Ressource pour tous :
Pollution numérique : du clic au déclic (Qu'est-ce qu'on fait ?)

14. Quel pourcentage de Français possède un smartphone en 2024 ?

A) 30 %
B) 60 %
C) 91 %

Le smartphone est devenu quasi incontournable : en 2024, 91 % des Français ont un téléphone connecté à Internet. Cela signifie que presque tous tes amis et ta famille peuvent t'écrire, t'appeler ou te passer des infos en quelques secondes, où qu'ils soient. Mais avoir un smartphone implique aussi de faire attention à son utilisation : fixe-toi des plages « sans téléphone » pour faire du sport, lire un livre ou passer du temps en famille. Pense aussi à protéger tes données personnelles (photo, géolocalisation…) en réglant la confidentialité de tes applis. Tu verras, ton smartphone restera un super outil sans prendre toute la place dans ta vie !

Source : Le baromètre du numérique - édition 2025 (Arcep, Arcom, CGE et ANCT)

15. Parmi les moins de 40 ans, quel pourcentage juge leur temps d'écran excessif ?

A) 37 %
B) 53 %
C) 80 %

Plus de la moitié des moins de 40 ans (53 %) estiment passer trop de temps sur les écrans. Cela montre que beaucoup ressentent le besoin de faire une pause : notifications, réseaux sociaux, jeux, tout peut s'accumuler sans qu'on s'en rende compte. Adopte la technique du « mode avion » pendant tes temps de concentration ou mets ton téléphone hors de vue quand tu fais tes devoirs ou partages un repas. Prévois aussi des moments « sans écran » avec tes amis pour discuter face à face : tu verras, c'est plus sympa et ça renforce les liens !

Source : Le baromètre du numérique - édition 2025 (Arcep, Arcom, CGE et ANCT)

16. Que faisons-nous sur Internet en grande majorité ?

A) Jouer aux jeux vidéo
B) Communiquer
C) Regarder des vidéos

Tu pensais peut-être qu'on passait notre temps à jouer aux jeux vidéo ou à envoyer des messages ? En réalité, regarder des vidéos est l'activité numéro un sur Internet ! 80 % de ce qui circule sur Internet, dans le monde, sont des vidéos (y compris les lives et les stories).
Chaque fois que tu regardes une vidéo sur YouTube, Netflix ou TikTok, des data centers travaillent pour t'envoyer cette vidéo.
Ces data centers consomment beaucoup d'électricité pour fonctionner et se refroidir.
Plus la vidéo est longue et de bonne qualité, plus elle consomme d'énergie !
Heureusement, tu peux agir ! Tu peux baisser la qualité des vidéos quand tu es sur de petits écrans. Tu peux aussi désactiver la lecture automatique ou choisir d'écouter de la musique plutôt que de regarder des clips musicaux.
Regarder des vidéos, c'est formidable pour apprendre et se divertir, mais connaître son impact aide à mieux les utiliser !

Source : Pollution numérique - du clic au déclic (Qu'est-ce qu'on fait ?)

Ressource pour un ado : Pourquoi le streaming ça pollue ? (Vinz et Lou)

17. Quel pourcentage de la consommation électrique de la France est lié au numérique ?

A) 1 %
B) 11 %
C) 31 %

En France, chaque fois que tu regardes une vidéo en ligne, joues à un jeu vidéo ou envoies un message, tu utilises de l'électricité. Les ordinateurs, les smartphones, les box Internet et surtout les gros bâtiments appelés centres de données ont besoin d'énergie pour fonctionner et stocker nos photos, vidéos et applications. En 2022, toutes ces activités numériques ont consommé 51,5 térawatt-heures d'électricité, ce qui représente 11 %
de la consommation française. Si on imagine toute l'électricité utilisée par la France pour ses maisons, ses usines et ses transports, un peu plus d'un dixième est dédié à nos écrans et à Internet. C'est beaucoup quand on sait que ce chiffre ne tient pas compte de tous les centres de données basés à l'étranger. Cela montre qu'il est important d'éteindre nos appareils quand on ne s'en sert pas et d'opter pour des équipements plus économes en énergie.

Source : Numérique - quel impact environnemental en 2022 ? (ADEME)

18. Qu'est-ce que l'obsolescence psychologique ?

A) Quand on jette un objet qui marche encore parce qu'il nous semble démodé
B) Quand un psychologue nous dit de jeter nos affaires
C) Quand on a peur que nos objets nous rendent malades

L'obsolescence psychologique nous amène à remplacer un appareil alors qu'il fonctionne encore sous l'influence de la mode ou d'un attrait pour la nouveauté. Cette obsolescence ne vient donc pas d'une panne, mais de notre tête.
Les publicités et les réseaux sociaux nous montrent sans cesse les derniers produits pour nous donner envie de les acheter. On finit par trouver nos appareils « ringards » même s'ils fonctionnent très bien. Beaucoup de Français ont un téléphone encore fonctionnel qui dort dans leurs tiroirs à cause de ce phénomène. Le problème, c'est que cela crée beaucoup de gaspillage et coûte cher aux familles. Alors même si tu as très envie du dernier smartphone qui vient de sortir, demande-toi si tu en as vraiment besoin !

19. Quand faut-il débrancher le chargeur de ton téléphone ?

A) Dès que la batterie atteint 80 %
B) Dès que la batterie atteint 100 %
C) Après 24 heures de charge, pour être sûr

Pour que ton téléphone reste en forme, évite de le « stresser » : ne le laisse pas tomber à 0 % ni atteindre 100 %, garde-le plutôt entre 40 % et 80 %.
Voici quelques bonnes pratiques pour prolonger la vie de ta batterie et de ton téléphone : fais de petites recharges régulières au lieu de le laisser en charge toute une nuit, maintiens-le à l'abri de la chaleur ou du froid car cela use la batterie ; pendant la charge, passe-le en mode avion pour qu'il avale l'énergie plus vite ; pour le brancher, choisis une prise murale, plus rapide qu'un port USB, pour gaspiller moins d'électricité. Des petits gestes comme ceux-là peuvent économiser l'équivalent de plusieurs centrales électriques et prolonger la vie de nos batteries.

Source : Article Ouest France

20. Que se passe-t-il si tu laisses vingt onglets ouverts dans ton navigateur ?

A) Ton appareil utilise plus de mémoire et d'énergie, même quand tu ne regardes pas ces onglets
B) Le navigateur met automatiquement ces onglets en veille, donc ils ne consomment plus aucune énergie
C) Garder de nombreux onglets ouverts améliore la connexion Internet parce qu'ils maintiennent la ligne active

Chaque onglet garde en mémoire des images, des animations ou de la musique qui continuent parfois de tourner en arrière-plan. Imagine vingt petites télévisions allumées dans ta chambre pendant que tu n'en regardes qu'une ! Le processeur travaille, la batterie se vide et l'appareil chauffe. Fermer les pages dont tu n'as plus besoin libère de la mémoire, fait durer la batterie et évite que ton ordinateur ou ta tablette rame. Astuce : si tu veux retrouver plus tard un site intéressant, ajoute-le à tes favoris au lieu de garder la page ouverte indéfiniment.

21. Quel geste réduit le plus la pollution quand tu regardes des vidéos sur un petit écran ?

A) Tourner ton appareil en mode portrait
B) Mettre le son au minimum
C) Choisir une qualité 480p plutôt que 4K

Quand tu regardes une vidéo en très haute qualité (4K = 3840 x 2160 pixels), ton appareil doit télécharger beaucoup plus de données qu'en qualité normale (480p = 720 x 480 pixels). Plus la qualité demandée est élevée, plus les fichiers à transmettre seront lourds, et consommeront d'autant plus d'énergie. Pour faire voyager tous ces fichiers sur Internet, les data centers utilisent énormément d'électricité.
Sur un petit écran de téléphone ou tablette, tu ne vois pas vraiment la différence entre 480p et 4K ! Donc en adaptant la qualité de la vidéo à la taille de ton écran, tu peux continuer à en profiter tout en minimisant les impacts sur la planète.

22. Pour écouter ta playlist sans trop polluer, quel est le meilleur geste ?

A) Télécharger les morceaux en Wi-Fi puis écouter hors ligne
B) Laisser le streaming tourner en boucle même quand tu n'écoutes plus
C) Mettre le son au maximum pour mieux entendre les paroles

Quand tu streames une chanson, chaque écoute traverse les antennes et les câbles avant d'arriver à tes oreilles. Si tu répètes le même morceau dix fois par jour, tu fais dix voyages de données ! En téléchargeant ta playlist une seule fois à la maison, là où le Wi-Fi consomme dix fois moins d'énergie que la 4G/5G, c'est plus malin !
Ensuite, l'écoute hors ligne ne sollicite plus les réseaux ni les data centers : ton téléphone lit simplement le fichier qu'il a déjà. Volume modéré et casque conservé longtemps complètent la démarche : moins de déchet, moins d'électricité, toujours autant de musique.

23. Qu'entend-on par sobriété numérique ?

A) Utiliser le numérique le plus possible pour être moderne
B) Utiliser le numérique de façon responsable en réduisant ses impacts sur l'environnement
C) Arrêter complètement d'utiliser tous les appareils numériques

La sobriété numérique, c'est utiliser nos appareils électroniques (téléphones, tablettes, ordinateurs) de manière intelligente pour protéger notre planète.
Tous ces appareils consomment de l'électricité et polluent quand on les fabrique.
Le numérique représente actuellement 3,4 % des émissions mondiales de gaz à effet de serre. Être sobre numériquement, c'est faire des choix malins : garder son téléphone plus longtemps avant d'en changer, éteindre la Wi-Fi quand on ne l'utilise pas, fermer les applications qu'on n'utilise plus, ou encore éviter de regarder trop de vidéos en ligne. Par exemple, envoyer un email avec une grosse pièce jointe pollue plus qu'un email simple. Regarder une vidéo en ligne consomme beaucoup d'énergie car elle passe par des data centers qui fonctionnent jour et nuit. La sobriété numérique ne veut pas dire arrêter complètement le numérique ! C'est juste l'utiliser quand c'est vraiment utile et de façon plus respectueuse de l'environnement.

Source : Impacts environnementaux du numérique dans le monde 2025 (Green IT)
Ressource pour un adulte : L'éducation à la sobriété numérique : pistes pour l'enseignement (Canotech)

24. Quelle est la principale cause de l'impact environnemental des téléviseurs ?

A) Le nombre de chaînes qu'ils reçoivent
B) Le temps qu'on passe à les regarder chaque jour
C) La taille de plus en plus grande des écrans

Les téléviseurs ont un impact important sur l'environnement, et cela empire chaque année ! La principale raison ? Leurs écrans deviennent de plus en plus grands.
En 2010, la taille moyenne d'un téléviseur était de 79 cm, aujourd'hui elle atteint 119 cm, et bientôt les écrans de plus de 140 cm seront la norme.
Pourquoi est-ce un problème ? Plus l'écran est grand, plus il faut de matériaux pour le fabriquer : du plastique, du verre, des métaux comme l'or et l'argent, et beaucoup d'autres composants électroniques. De plus, un grand écran consomme beaucoup plus d'électricité qu'un petit. Les experts ont calculé que quand la taille de l'écran double, sa consommation d'énergie est multipliée par 4 !
Il y a aussi un autre souci : quand de nouveaux téléviseurs plus grands sortent dans les magasins, les gens ont envie de changer leur ancien téléviseur qui marche encore très bien. C'est ce qu'on appelle l'obsolescence psychologique. Résultat : on produit toujours plus de téléviseurs et on jette les anciens plus tôt que prévu.

Source : Impacts environnementaux du numérique dans le monde 2025 (Green IT)

25. En 2025, combien de satellites Starlink tournent autour de la Terre ?

A) Environ 750
B) Environ 7 500
C) Environ 75 000

L'objectif des satellites Starlink, développés par SpaceX, l'entreprise d'Elon Musk, est de fournir un accès à Internet haut débit à travers le monde, en particulier dans les régions mal desservies par les infrastructures terrestres comme la fibre optique ou l'ADSL.
La constellation Starlink compte déjà près de 7 500 engins actifs et pourrait atteindre 42 000 satellites.
Problèmes : ces satellites brillent énormément. Ils gênent les astronomes pour observer les étoiles. Ils risquent aussi de percuter d'autres objets spatiaux, créant des débris dangereux. Même si les scientifiques cherchent des solutions pour réduire leur éclat et mieux organiser le trafic spatial, plus il y en a, plus l'espace devient encombré !
Pour limiter cette « pollution spatiale », il faudrait lancer moins de satellites, coopérer entre entreprises et faire redescendre rapidement les vieux satellites pour qu'ils se désintègrent en toute sécurité dans l'atmosphère.

Source : Starlink satellites - Facts, tracking and impact on astronomy (space.com)
Ressource pour un adulte : Satellites : comment l'astrocapitalisme congestionne l'espace (Usbek & Rica)

26. Combien de métaux différents faut-il pour fabriquer un téléphone portable de type smartphone ?

A) 4
B) 12
C) 50

Ressource pour un ado : Des métaux dans mon smartphone ?

Pour fabriquer un smartphone, on utilise environ 50 métaux différents, chacun avec un rôle précis : l'or et l'argent sont utilisés pour faire passer le courant, le cuivre pour les circuits imprimés, l'étain pour souder les composants, le tungstène et le tantale pour les petites pièces électroniques, le lithium et le cobalt dans la batterie, et des terres rares (néodyme, praséodyme.) dans les aimants du haut-parleur et les alertes vibrantes.
On ajoute aussi de l'aluminium pour la coque, du silicium pour les puces, ainsi que du nickel, du zinc, du fer et bien d'autres. Extraire ces métaux demande beaucoup d'eau, d'énergie et crée des déchets polluants. De plus, avec autant de métaux différents mélangés, recycler un téléphone, c'est super compliqué ! C'est comme essayer de séparer les différents ingrédients dans un gâteau déjà cuit. Voilà pourquoi il vaut mieux garder son téléphone le plus longtemps possible !

Source : Votre smartphone est riche en métaux ! (ADEME)
Ressource pour un adulte : Pollution d'un ordinateur - anatomie d'un désastre écologique et social (Ecotopie)
Ressource pour tous : Jeu - Phone Impact (République française et INRIA)

27. Qu'est-ce qu'un Paxophone ?

A) Un smartphone modulable, conçu pour être réparé et personnalisé par l'utilisateur
B) Un téléphone qu'il faut assembler soi-même à partir de composants électroniques basiques
C) Un modèle de téléphone haut de gamme, produit en édition limitée

Le Paxophone est un smartphone conçu par Gabriel Rochet, alors qu'il avait 16 ans, dans le cadre du projet open source Paxo. Tu peux l'assembler toi-même à partir de composants simples (carte électronique, écran, batterie, coque...) et installer des logiciels libres pour passer des appels, envoyer des messages et utiliser des applis basiques. En fabriquant ton propre Paxophone, tu apprends comment chaque pièce fonctionne, tu peux facilement remplacer ou réparer un élément défectueux et prolonger la vie de ton appareil. Cette approche limite la production de nouveaux téléphones et réduit les déchets électroniques car tu n'as plus besoin de jeter un téléphone entier lorsqu'un seul composant est abîmé. C'est un moyen concret de prendre soin de la planète tout en découvrant l'électronique !

Source : https://paxo.fr

Ressource pour un ado :
Gabriel, 16 ans, l'inventeur du téléphone portable à fabriquer soi-même pour 30 euros

28. Quelle affirmation est correcte ?

A) Lorsque j'utilise un appareil numérique, mon impact environnemental change en fonction de ma localisation
B) Mon impact environnemental ne change pas en fonction de ma localisation
C) Je n'ai pas d'impact environnemental

Ton impact sur la planète change selon le pays où tu utilises ton appareil ! Pourquoi ? Parce que ton ordinateur ou ta tablette ont besoin d'électricité pour fonctionner, et cette électricité n'est pas fabriquée de la même façon partout. Dans certains pays, on utilise le charbon (qui pollue beaucoup), dans d'autres on utilise le vent, le soleil ou l'eau (qui polluent très peu). C'est comme cuisiner : faire un gâteau au four électrique ou au four solaire, ça n'a pas le même impact ! En France, on utilise beaucoup l'énergie nucléaire. Dans d'autres pays, ce sont surtout les énergies renouvelables. Selon l'endroit où tu vis cela peut changer ton empreinte écologique, même en utilisant exactement le même appareil !

Source : https://app.electricitymaps.com

29. Que désigne-t-on par « terres rares » ?

A) Des lieux réservés pour l'activité de l'industrie numérique
B) Des espaces géographiques préservés de la pollution
C) Des métaux stratégiques nécessaires à la fabrication des équipements numériques

Malgré leur nom, les « terres rares » ne sont pas vraiment rares ! C'est un groupe de 17 métaux précieux qui se cachent dans tous tes appareils électroniques. Ton smartphone, ta console de jeu, ton ordinateur portable… ils en sont tous remplis ! Ces métaux ont des noms comme le néodyme ou le dysprosium, ils sont essentiels pour créer les écrans tactiles, les batteries, les haut-parleurs et même les vibrations de ton téléphone.
Sans eux, impossible d'avoir des couleurs vives sur ton écran ou une batterie qui dure longtemps. Le problème ? Ces métaux sont principalement extraits en Chine, ce qui crée une dépendance mondiale. De plus, leur extraction pollue énormément l'environnement et consomme beaucoup d'eau. C'est pourquoi on dit qu'ils sont « stratégiques » : ils sont devenus indispensables à notre monde numérique, mais leur production pose de vrais défis écologiques et géopolitiques.

Source : Terres rares, métaux stratégiques (Geoconfluences)

Ressource pour un ado :
Vidéo : Les terres rares
qu'est-ce que c'est ?

30. Si le numérique était un pays, il produirait autant de gaz à effet de serre que… ?

A) 1,5 fois la France
B) 5,5 fois la France
C) 8,5 fois la France

Si le numérique était un pays, il serait dans le top 3 des plus gros pollueurs mondiaux ! Il émettrait autant de CO_2 que 5,5 fois la France. Le numérique représente 3,4 % des émissions mondiales de gaz à effet de serre dans le monde. Cette pollution vient de partout : fabriquer ton smartphone, faire tourner les serveurs qui stockent tes photos sur le cloud, regarder Netflix… Même envoyer un simple texto consomme de l'énergie !
En gros, chaque fois que tu scrolles sur TikTok, quelque part dans le monde, une centrale électrique travaille un peu plus. Mais pas de panique, ce n'est pas la fin du monde. Tu peux agir facilement : garder ton téléphone plus longtemps, éviter de regarder des vidéos en 4K sur un petit écran, utiliser le Wi-Fi plutôt que la 4G, éteindre tes appareils au lieu de les laisser en veille… Des gestes qui semblent petits, mais multipliés par des millions de personnes, ça peut vraiment changer la donne !

Source : Étude sur les impacts environnementaux du numérique dans le monde (Green IT)

31. Sachant qu'il y a environ 8 milliards d'habitants dans le monde, combien d'équipements utilisateurs (smartphones, ordinateurs, tablettes, etc.) existent-ils à l'échelle mondiale ?

A) 50,5 millions
B) 23 milliards
C) 30,5 milliards

30,5 milliards d'appareils sur Terre, ça fait tourner la tête ! Pour 5,35 milliards d'internautes, ça fait presque 6 appareils par personne. Mais en réalité, c'est super inégal : toi, tu as peut-être ton smartphone, ton ordi, une tablette, une console, des écouteurs, une montre connectée… En France, nous avons environ 10 appareils par personne ! Pendant ce temps, dans certains pays, toute une famille partage un seul téléphone.
Cette explosion d'objets connectés pose un vrai problème : chaque nouvel appareil nécessite des métaux rares et génère des déchets électroniques. La question à se poser avant chaque achat : « Mon ancien appareil fonctionne-t-il encore correctement ? » Parfois, la réponse est oui, et c'est déjà ça de gagné pour la planète.

Sources : Étude sur les impacts environnementaux du numérique dans le monde (Green IT) et Le baromètre du numérique - édition 2025 (Arcep, Arcom, CGE et ANCT)
Ressource pour un adulte : Atelier « Inventons nos vies bas carbone » pour les jeunes

32. Laquelle de ces propositions est vraie ?

A) La fabrication d'un ordinateur portable pollue moins que son recyclage
B) La fabrication d'un ordinateur portable pollue autant que sa distribution
C) La fabrication d'un ordinateur portable pollue davantage que son utilisation

Ton ordinateur portable pollue avant même de l'avoir allumé ! Environ 70 % de sa pollution vient de sa fabrication. Pour créer un ordinateur de 2 kg, il faut extraire 800 kg de matières premières ! Ces minerais viennent du monde entier, sont transformés dans des usines énergivores, puis les composants voyagent partout avant l'assemblage final. Une fois chez toi, ton ordi consomme peu d'électricité comparé à toute cette énergie déjà dépensée. La morale de l'histoire ? Garde ton ordinateur le plus longtemps possible ! Même s'il devient lent, même s'il n'est plus stylé, chaque année en plus réduit drastiquement son impact environnemental. Réparer au lieu de remplacer, c'est LE geste écolo. Alors avant de craquer pour le dernier modèle, demande-toi si ton ancien ne peut pas encore tenir quelques années !

Source : Quelle est l'empreinte carbone d'un ordinateur portable ? (Data.gouv.fr)
Ressource pour tous : iFixit - tutoriels de réparation d'appareils électroniques

33. Quelle est la différence de consommation d'énergie entre le Wi-Fi et la 4G/5G ?

A) Le Wi-Fi consomme légèrement moins d'énergie que la 4G/5G
B) Le Wi-Fi consomme environ dix fois moins d'énergie que la 4G/5G
C) La 4G et la 5G consomment moins d'énergie que le Wi-Fi lorsque le signal est faible

Tu utilises sans doute ton smartphone tous les jours pour regarder des vidéos, jouer ou envoyer des messages. Mais as-tu déjà pensé à la différence entre te connecter en Wi-Fi ou en 4G/5G ? Il y a un vrai impact sur l'environnement ! Le Wi-Fi consomme 10 fois moins d'énergie que la 4G/5G. Mais pourquoi cette différence ? La 4G/5G sollicite bien plus le réseau, mobilisant des infrastructures et une consommation énergétique plus importantes pour fonctionner. En gros, pour transporter les mêmes données, les antennes 4G/5G ont besoin de beaucoup plus d'électricité que ta box Wi-Fi à la maison. Concrètement, quand tu regardes une vidéo en 4G/5G, ton téléphone doit communiquer avec des antennes-relais parfois très éloignées, qui consomment énormément d'énergie. Avec le Wi-Fi, les données passent par ta box Internet, qui utilise le réseau filaire, beaucoup plus efficace.
Alors même si tu as un forfait 4G/5G illimité, pense à te connecter en Wi-Fi dès que tu peux ! C'est un geste simple qui aide à réduire ton empreinte carbone numérique.

Source : Privilégier les connexions via la fibre plutôt que la 4G/5G (ADEME)

34. Quel est le poids des ressources nécessaires à la fabrication d'un ordinateur de 2 kg ?

A) 10 kg
B) 300 kg
C) 800 kg

Imagine que ton ordinateur portable de 2 kg soit comme la pointe d'un iceberg. Ce que tu ne vois pas, c'est tout ce qui se cache en dessous ! Pour fabriquer ton ordi, il faut extraire 800 kg de matières premières : du pétrole pour les plastiques, des minerais pour les métaux, de l'eau pour les circuits… Pour ton smartphone, c'est environ 70 kg de ressources ! C'est pourquoi il est important de faire durer nos appareils le plus longtemps possible, de les réparer quand c'est possible et de bien les recycler. Quand tu changes d'ordi juste parce que le nouveau modèle est plus beau, tu « gaspilles » en fait ces 800 kg de ressources qui ont été nécessaires pour le créer.

Sources : Pourquoi réduire la pollution numérique ? (ADEME) et Smartphone, une mine urbaine (CEA)

Ressource pour un adulte :
La Fresque du numérique

35. Quelle quantité de déchets électroniques a été générée dans le monde en 2022 ?

A) 6 tonnes
B) 6,2 millions de tonnes
C) 62 millions de tonnes

62 millions de tonnes de déchets électroniques en 2022, ça représente quoi concrètement ? Si on mettait tous ces vieux téléphones, ordinateurs et télés dans des camions, on pourrait faire le tour de la Terre au niveau de l'équateur ! Chaque personne sur la planète produit en moyenne 7,8 kg de déchets électroniques par an. Pour te donner une idée, c'est comme si tu jetais 31 smartphones chaque année. Et le pire, c'est que cette quantité a augmenté de 82 % depuis 2010 ! Le problème, c'est que nos appareils contiennent des matériaux précieux mais aussi toxiques. Si on ne les recycle pas correctement, on perd ces ressources et on pollue l'environnement. C'est pourquoi il existe des points de collecte spéciaux pour tes vieux appareils. Ne les mets jamais dans la poubelle normale !

Source : Quand les déchets électroniques atteignent des records (Article du 6 juin 2024 - Commissariat Général au Développement Durable)
Ressource pour un adulte : Global e-waste monitor 2024

36. Quelle est la définition de l'Internet des objets (IoT) ?

A) Des appareils du quotidien connectés à Internet et qui échangent des données entre eux
B) Un réseau social réservé aux objets technologiques
C) Des robots programmés pour remplacer toutes les machines dans une usine

L'Internet des objets, ou IoT (Internet of Things), désigne tous ces objets que tu connais bien – ta montre connectée, ton enceinte intelligente, ou même ton frigo – auxquels on a ajouté une petite puce et une connexion Internet. Grâce à ça, ils peuvent envoyer et recevoir des informations sans que tu fasses quoi que ce soit : ta montre mesure tes pas et ton cœur pour te donner ton score de sport. Ces appareils simplifient parfois la vie, mais ils consomment aussi de l'énergie (pour rester connectés et envoyer leurs données) et peuvent poser des problèmes de vie privée (si quelqu'un piratait ta caméra ou volait les infos de géolocalisation via ta montre !).
Si tu considères qu'ils sont vraiment utiles pour toi, choisis des objets de marques fiables, mets à jour leur logiciel quand on te le propose et protège ton Wi-Fi avec un mot de passe solide. Ainsi, tu profites des avantages de l'IoT tout en gardant le contrôle et en respectant la planète et ta vie privée.

Ressource pour un adulte :
L'avenir d'Internet | Surveillance de masse Nouvelle technologie | Documentaire (Moconomy - Économie et Finance)

37. En France, combien de temps un adolescent utilise-t-il son téléphone par jour, en dehors du temps scolaire ?

A) 1 à 2 heures
B) 3 à 4 heures
C) 5 à 6 heures

3 à 4 heures par jour devant un écran de téléphone, ça peut te paraître peu ou beaucoup selon tes habitudes. Mais réfléchis : si tu dors 8 heures et que tu es en cours 6 heures, il te reste 10 heures « libres ». Passer 4 heures sur ton téléphone, c'est donc 40 % de ton temps libre ! Mais attention, ce n'est que le téléphone : si on ajoute la télé, l'ordinateur et la console, le total grimpe encore plus. Ces chiffres peuvent paraître énormes, mais ils reflètent notre époque : le numérique fait partie de notre quotidien pour communiquer, apprendre, se divertir. L'important, c'est de garder un équilibre et de rester conscient du temps passé pour pouvoir faire d'autres activités enrichissantes comme le sport, la lecture ou les sorties entre amis.

Source : Parents, Enfants & Numérique (Étude 2024 – Observatoire de la parentalité et de l'éducation numérique)
Ressource pour un adulte : Internet et les jeunes : de quoi avons-nous peur ? (Numérique en communs et Le Monde)
Ressource pour tous : www.lumni.fr/video/c-est-quoi-le-probleme-avec-les-ecrans

38. Que deviennent souvent les vieux appareils jetés n'importe où ?

A) Ils sont démontés proprement sans pollution
B) Ils finissent dans des décharges à ciel ouvert, polluant sol et eau
C) Ils attendent des décennies dans des entrepôts avant d'être recyclés

Imagine ton vieux smartphone qui ne marche plus ou ton ordinateur portable cassé. Que leur arrive-t-il quand tu t'en débarrasses ? Malheureusement, beaucoup finissent leur vie dans d'énormes décharges à ciel ouvert, principalement au Ghana, au Nigeria ou en Chine. Ces lieux s'appellent des « cimetières électroniques ».
Ces équipements contiennent des substances super dangereuses : du plomb dans les écrans, du mercure dans les circuits, et même de l'arsenic. Quand ils se décomposent sous la pluie et le soleil, ces produits toxiques s'infiltrent dans la terre et contaminent les nappes phréatiques. Résultat ? L'eau devient impropre à la consommation et les sols ne peuvent plus faire pousser de cultures saines.
Le plus choquant ? Souvent, ce sont des enfants et des adultes sans protection qui fouillent dans ces déchets pour récupérer les métaux précieux comme l'or ou le cuivre, au péril de leur santé. C'est pourquoi il est crucial de déposer tes anciens appareils dans les points de collecte spécialisés près de chez toi !

Ressource pour tous : Procédure pour Déchets d'équipements électriques et électroniques (République française)

39. Le plus souvent, comment transitent les échanges par Internet ?

A) Par des antennes
B) Par des satellites
C) Par des câbles sous-marins

Quand tu envoies un message à un ami, tu imagines peut-être que ça passe par des satellites dans l'espace ou des antennes. Eh bien, pas du tout ! 99 % des données d'Internet voyagent par des câbles au fond des océans. Ces câbles qui relient les continents représentent 1,3 million de km, soit 33 fois le tour de la Terre. Ces câbles sont plus rapides que les satellites car la distance est plus courte : pas besoin de faire l'aller-retour jusqu'à l'espace ! Ils mesurent parfois des milliers de kilomètres et sont posés à des profondeurs immenses. C'est grâce à eux que tu peux regarder une vidéo en direct depuis l'autre bout du monde ou jouer en ligne avec des personnes de tous les continents.
Ces câbles sont si importants que leur protection est devenue un enjeu géopolitique majeur. Sans eux, Internet tel qu'on le connaît n'existerait pas !

Source : L'Internet mondial surfe dans l'océan grâce à 1,3 million de kilomètres de câbles sous-marins (Ouest-France)

Ressource pour tous :
Dossier : les câbles sous-marins (ARTE Family)

Ressource pour tous :
la carte des câbles sous-marins qui connectent l'Internet mondial

40. Que désigne-t-on par « Dark Pattern » ?

A) Une technique de manipulation pour piéger les utilisateurs
B) Un algorithme utilisé pour personnaliser l'affichage d'un site
C) Un composant informatique à peine visible à l'œil nu

Un « Dark Pattern », c'est comme un piège invisible tendu par les sites web et les applications. Imagine : tu veux te désabonner d'un service, mais le bouton « Se désabonner » est minuscule et gris, tandis que le bouton « Continuer l'abonnement » est énorme et coloré. C'est un Dark Pattern ! Ou encore, quand une application te demande l'autorisation d'accéder à tes contacts et que « Accepter » est mis en évidence tandis que « Refuser » est presque invisible. Ces techniques exploitent la façon dont notre cerveau fonctionne pour nous faire faire des choix qu'on n'aurait pas faits si on avait eu le temps de bien réfléchir. C'est une technique malhonnête utilisée par les entreprises pour augmenter leurs profits. Maintenant que tu sais ce qu'est un « Dark Pattern », tu pourras les repérer et faire des choix plus éclairés. Prends toujours le temps de bien lire avant de cliquer !

Source : Dark pattern (Wikipédia)

Ressource pour tous :
La Fresque des écrans

41. Quel est le pays où le temps d'écran est le plus important ?

A) La France
B) La Chine
C) L'Afrique du Sud

L'Afrique du Sud détient le record mondial avec 9 h 38 d'écrans par jour !
C'est énorme : ça représente plus de la moitié du temps éveillé. Pour te donner une idée, si tu dors 8 heures, il te reste 16 heures dans ta journée, et les Sud-Africains en passent plus de 9 devant un écran. Le Brésil suit avec 9 h 32, puis les Philippines avec 9 h 14.
En comparaison, en France, on ne passe « que » 5 heures par jour devant les écrans.
Ces différences s'expliquent par plusieurs facteurs : la culture du pays, l'âge de la population, le développement des infrastructures numériques, les habitudes de divertissement... Par exemple, dans certains pays, la télévision reste le principal moyen de divertissement, ce qui augmente le temps d'écran total. Ces chiffres nous montrent que le rapport aux écrans varie énormément selon où on vit dans le monde.

Source : Pays qui passent le plus de temps sur les écrans (Ouest France)
Ressources pour un adulte : Pour un usage des écrans qui nous fait du bien (Pause) et Ateliers de sensibilisation Lève les yeux

42. Qu'est-ce qu'un ordinateur Low-Tech ?

A) Un ordinateur obsolète en termes de fonctionnalités
B) Un ordinateur spécialisé pour le calcul scientifique
C) Un ordinateur conçu pour être utile, durable et accessible

Un ordinateur low-tech, c'est tout l'opposé de la course au « toujours plus puissant, plus cher, plus complexe ». C'est un ordi pensé pour durer, être réparable et accessible à tous. Et cerise sur le gâteau, cela minimise son impact environnemental !
Contrairement aux ordinateurs « high-tech » qui changent de modèle tous les ans avec des fonctionnalités parfois inutiles, le low-tech se concentre sur l'essentiel : permettre de travailler, communiquer, apprendre, sans gaspiller les ressources.
Il utilise des composants robustes, faciles à réparer et est simple d'utilisation.
Au lieu d'avoir une multitude de fonctionnalités, il propose des fonctionnalités vraiment utiles et qui fonctionnent parfaitement pendant des années. Tu peux comparer cela à une montre suisse mécanique simple et efficace qui dure 50 ans à une montre connectée compliquée qu'il faut changer tous les 2 ans. Le low-tech nous fait réfléchir à nos vrais besoins et nous apprend qu'innovation ne rime pas forcément avec complication.

Ressources pour un adulte : Ordinateur low-tech et L'éclosion Low-tech (Low-Tech lab)

43. Que désigne le terme « nomophobie » ?

A) La peur d'être séparé de son téléphone
B) L'anxiété liée à la perte de connexion Internet
C) La peur de manquer une notification importante

« Nomophobie » vient de « NO MObile PHOne » + « phobie ». C'est la peur intense d'être séparé de son smartphone. Tu ressens peut-être certains symptômes sans le savoir : panique quand ta batterie est faible, stress quand tu n'as pas de réseau, angoisse quand tu oublies ton téléphone à la maison. Cette phobie moderne touche de plus en plus de personnes, surtout les jeunes. Elle se manifeste par une vérification compulsive du téléphone (tu regardes ton écran même s'il n'a pas sonné), la peur de manquer quelque chose d'important (FOMO - Fear Of Missing Out), et l'incapacité à se concentrer sans avoir son téléphone à portée de main. Cette dépendance peut affecter tes relations, ton sommeil et tes résultats scolaires. Reconnaître ces signes, c'est le premier pas pour retrouver un usage plus sain de son téléphone. Essaie parfois de le laisser dans une autre pièce : tu verras, le monde ne s'arrête pas !

Ressource pour un adulte : Nomophobie : jamais sans mon smartphone... Ensemble c'est mieux ! (France 3 Nouvelle-Aquitaine)
Ressource pour un ado : www.clemi.fr/familles/publications/la-bande-dessinee-dans-la-tete-de-juliette

44. Que désigne le terme « fracture numérique » ?

A) La casse d'équipements numériques
B) Une mine spécialisée dans les métaux utilisés pour le numérique
C) Un accès inégal aux technologies numériques

La fracture numérique, c'est quand certaines personnes n'ont pas les mêmes chances d'accéder à Internet ou de savoir l'utiliser correctement.
Cette inégalité existe entre les pays (certains ont des infrastructures numériques développées, d'autres non), mais aussi dans un même pays. Par exemple, dans certaines régions rurales, la connexion est trop lente ou inexistante, et tout le monde ne peut pas
se payer un ordinateur ou un smartphone.
Même équipés, 15,4 % des Français de 15 ans et plus ne maîtrisent pas les compétences numériques de base. Remplir un formulaire administratif en ligne, télécharger une application, naviguer sur un site web ou utiliser une messagerie électronique leur posent problème. Les personnes peu diplômées, âgées ou issues de milieux défavorisés sont les plus concernées.
Cette fracture crée donc des injustices : moins d'accès à l'éducation ou à l'information. Combattre la fracture numérique, c'est offrir à chacun un bon accès au matériel, une connexion fiable et des formations pour apprendre à utiliser efficacement le numérique.

Source : 15 % de la population est en situation d'illectronisme en 2021 (INSEE)

45. Que sont « les minerais de sang » ?

A) Des minerais dont l'exploitation finance ou alimente des conflits
B) Des minerais extraits dans des zones où les conditions de travail sont dangereuses
C) Des minerais très rares utilisés dans des dispositifs militaires

Les « minerais de sang » ou « minerais du conflit », c'est un nom qui fait froid dans le dos et qui est malheureusement justifié. Ces minerais (comme le tantale, l'étain, le tungstène, l'or) sont extraits dans des zones de guerre, principalement en République Démocratique du Congo et dans la région des Grands Lacs africains. Les groupes armés se battent pour contrôler les mines et utilisent l'argent de la vente pour acheter des armes et financer leurs guerres. Le problème, c'est que ces minerais se retrouvent dans nos smartphones, ordinateurs et consoles ! Sans le savoir, en achetant ces produits, on peut indirectement financer ces conflits. C'est pourquoi des lois exigent maintenant des entreprises qu'elles vérifient l'origine de leurs minerais. Certaines marques s'engagent à utiliser uniquement des minerais « propres ». C'est un enjeu éthique majeur du numérique.

Ressource pour un adulte : Comment la « tech » saigne l'Afrique - Entretien avec David Maenda Kithoko, réfugié congolais.

Ressource pour un adulte : Atelier « Voyages au cœur de nos smartphones » (Point de M.I.R)

46. Parmi ces propositions, laquelle a le plus d'impact sur l'environnement (ressources, énergie...) ?

A) Les équipements utilisateurs (ordinateurs, téléphones...)
B) Les réseaux (câbles, antennes...)
C) Les data centers (serveurs...)

Voici quelque chose qui va sûrement te surprendre ! Quand on pense à la pollution numérique, on imagine souvent d'énormes data centers avec des milliers de serveurs qui consomment beaucoup d'électricité. Mais en réalité, ce qui pollue le plus dans le monde du numérique, ce sont... tes équipements personnels ! 50 % de la pollution numérique vient de la fabrication et du fonctionnement des équipements (smartphones, ordinateurs portables, TV...) contre 46 % pour les data centers et seulement 4 % pour les réseaux. En revanche, avec l'arrivée de l'IA générative, les centres de données voient leur consommation grimper : l'Agence internationale de l'énergie prévoit que la demande électrique des data centers doublera d'ici 2030.

Source : Numérique : quel impact environnemental en 2022 ? (ADEME)
Ressource pour un adulte : Behind the Screens | The Dark Side of the Smartphone Industry (Fair Phone)

47. Que désigne-t-on par « Wearable » ?

A) Un jeu vidéo en équipe dont le but est de sauver la planète
B) Un vêtement ou un accessoire comportant des éléments informatiques et électroniques avancés
C) Un vêtement durable

Le mot « wearable » vient de l'anglais « wear » (porter) et « able » (capable de). Ce sont tous ces objets connectés que tu peux porter sur toi : montres intelligentes, écouteurs sans fil, lunettes de réalité virtuelle, bracelets de fitness, et même des vêtements avec des capteurs intégrés ! Ces petits bijoux technologiques, souvent connectés à des smartphones ou ordinateurs, sont de plus en plus populaires.
En 2024, il y avait environ 500 millions de wearables dans le monde.
Impressionnant, non ? Mais voilà le problème : ces appareils ont une durée de vie très courte, souvent 2 à 3 ans seulement. Leur petite taille cache des composants très sophistiqués qui nécessitent des métaux rares pour leur fabrication. Et comme ils sont toujours collés à ton corps, ils doivent être rechargés très souvent, ce qui consomme de l'énergie. Sans compter qu'on a tendance à les perdre ou à les casser facilement.
Le défi aujourd'hui, c'est de profiter de leur côté pratique et d'en prendre soin !

Source : Aperçu du marché des appareils portables (IDC)

48. Que désigne l'ACV ?

A) Algorithme de Choix de Vecteur
B) Antivirus de Chaîne Vidéo
C) Analyse de Cycle de Vie

L'Analyse de Cycle de Vie (ACV) est une méthode scientifique permettant d'enquêter sur l'impact environnemental d'un produit pendant toute sa « vie », depuis sa naissance jusqu'à sa mort. Concrètement, pour ton smartphone par exemple, l'ACV va s'intéresser à tout : l'extraction des matières premières dans les mines, la fabrication en usine, le transport, ton utilisation quotidienne et enfin son recyclage ou sa mise en décharge. C'est comme suivre ton téléphone à la trace !
Le super pouvoir de l'ACV, c'est qu'elle mesure plusieurs impacts à la fois : les émissions de gaz à effet de serre, la consommation d'eau, la pollution de l'air, l'épuisement des ressources... Elle donne une vision complète et objective. C'est grâce à l'ACV qu'on sait aujourd'hui que la fabrication de ton smartphone représente les 3/4 de son impact environnemental total, bien plus que son utilisation ! Cette méthode est devenue le standard mondial pour mesurer l'empreinte environnementale. Elle aide les entreprises à créer des produits plus respectueux de l'environnement et toi, à faire des choix plus éclairés.

Source : Analyse du cycle de vie (Wiki Numérique Responsable)
Ressource pour tous : Le cycle de vie d'un produit, qu'est-ce que c'est ? (ADEME)

49. Qu'est-ce que le trafic de déchets électroniques ?

A) L'envoi illégal de vieux téléphones et ordinateurs vers des pays sans structures pour les recycler
B) Le fait de vendre du matériel numérique sans fournir la garantie obligatoire
C) L'achat de composants électroniques contrefaits sur des sites non officiels

L'exportation illégale de déchets électroniques consiste à envoyer des tonnes de vieux téléphones, ordinateurs et autres appareils vers des pays où il n'existe pas de filières de recyclage adaptées. Les camions et les cargos partent souvent de ports européens ou nord-américains en conteneurs non déclarés, cachant leurs déchets sous l'apparence de matériel à réparer. Une fois arrivés, ces déchets sont démontés à la main par des travailleurs exposés à des produits dangereux (plomb, mercure, retardateurs de flamme). Les composants toxiques polluent les sols, les rivières et nuisent à la santé de la population.
Les matériaux précieux (or, cuivre) sont récupérés sans respecter les normes de sécurité, renforçant un trafic organisé qui pèse plusieurs milliards de dollars par an.
En déposant tes appareils électriques et électroniques dans des points de collecte certifiés plutôt que de les jeter à la poubelle, tu participes à briser ce commerce illégal et à protéger les personnes et l'environnement.

Ressource pour un adulte :
Documentaire France inter : la mafia des déchets électroniques - capture d'écrans

50. Où sont stockés tes fichiers quand tu utilises le « cloud » ?

A) Sur le disque dur de ton ordinateur
B) Sur des serveurs accessibles via Internet
C) Dans un satellite en orbite

Quand tu sauvegardes tes photos ou tes devoirs dans le « cloud », tu ne les envoies pas dans les nuages ! Le « cloud », c'est l'équivalent d'un immense disque dur situé dans des centres de données (data centers) à différents endroits du monde. Quand tu enregistres une photo ou un document, il ne reste pas seulement sur ton téléphone ou ton PC : il est envoyé par Internet vers ces centres de données.
Cela te permet d'accéder à tes fichiers depuis n'importe quel appareil, partout où tu as une connexion.
Mais attention : ces centres de données consomment beaucoup d'électricité pour fonctionner 24h/24 et refroidir ces machines qui chauffent énormément. Pour limiter ton impact, supprime régulièrement ce que tu n'utilises plus et garde toujours une copie de tes dossiers importants sur un appareil personnel. Ainsi, tu profites du cloud en étant responsable !


stalky

51. Faut-il accepter toutes les demandes d'« amis » sur les réseaux sociaux ?

A) Oui, pour avoir plus de likes
B) Non, seulement celles des amis qu'on connaît
C) Oui, si leur photo de profil est sympa

Sur les réseaux sociaux, tu ne dois accepter comme « amis » que les personnes que tu connais vraiment dans la vie réelle ! Imagine que ta liste d'amis soit comme ta maison : tu ne laisses pas entrer n'importe qui chez toi, n'est-ce pas ? C'est pareil sur Internet ! Quand tu acceptes quelqu'un, cette personne peut voir tes photos, tes messages, et parfois même savoir où tu es et où tu vis. Certaines personnes mal intentionnées créent de faux profils pour se faire passer pour des enfants et essayer de te parler.
En acceptant que tes vrais amis, tu crées une barrière de protection autour de toi.
Si tu ne connais pas la personne qui t'envoie une demande, tu peux simplement l'ignorer ou la refuser. Il vaut mieux avoir 10 vrais amis que 100 inconnus !
Et n'oublie pas : avoir beaucoup d'amis sur les réseaux sociaux ne te rend pas plus populaire dans la vraie vie.

Ressource pour un adulte : Dossier réseaux sociaux (Internet Sans Crainte)

52. Les réseaux sociaux sont :

A) Toujours sûrs
B) Utilisés seulement par les adultes
C) Parfois dangereux si on ne fait pas attention

Les réseaux sociaux ne sont ni complètement sûrs ni totalement dangereux, mais ils peuvent devenir risqués si on ne fait pas attention ! Sur les réseaux sociaux, il peut y avoir des personnes malveillantes qui essaient de tromper les enfants, des contenus choquants qui ne sont pas faits pour ton âge, ou encore des arnaques.
Mais bonne nouvelle : en apprenant les bons réflexes, tu peux utiliser Internet en toute sécurité ! Par exemple, ne jamais donner d'informations personnelles, ne pas accepter d'inconnus comme amis, et toujours parler à un adulte de confiance si quelque chose te dérange. Les réseaux peuvent être formidables pour rester en contact avec sa famille et ses amis, mais il faut toujours rester vigilant, comme un détective qui observe tout autour de lui !

53. Combien de snaps sont envoyés chaque minute par les utilisateurs de Snapchat dans le monde ?

A) Des dizaines
B) Des milliers
C) Des millions

Chaque minute, 3 millions de photos et vidéos sont envoyées sur Snapchat dans le monde entier ! C'est énorme, non ? En une seule journée, cela représente plus de 4 milliards de snaps échangés. En France, Snapchat est très populaire chez les jeunes : 94 % des 15-24 ans l'utilisent ! Ces chiffres montrent à quel point les réseaux sociaux font partie de la vie quotidienne de millions de personnes. Un « snap » est une photo ou vidéo qui disparaît après quelques secondes, mais attention : rien ne garantit qu'elle ne puisse pas être sauvegardée par celui qui la reçoit et qu'elle ne puisse être utilisée sans que tu l'aies voulu !

Source : Data Never Sleeps 12.0 (Infographie - Domo)
Ressource pour un adulte : Chiffres Snapchat - les statistiques à connaître en 2025 (Blog du modérateur)

54. Quelle est la bonne attitude à avoir si un inconnu t'écrit un message sur un réseau social ?

A) Tu réponds gentiment pour voir ce qu'il veut
B) Tu supprimes ton compte tout de suite
C) Tu bloques la personne et en parles à un adulte de confiance

Si un inconnu t'envoie un message, la meilleure chose à faire est de le bloquer tout de suite et d'en parler à un adulte de confiance ! Pourquoi ? Parce que sur Internet, les gens peuvent facilement mentir sur qui ils sont. Une fois bloquée, la personne ne peut plus te contacter. Ensuite, parles-en à un adulte de confiance (tes parents, un enseignant, etc.), c'est super important car ils peuvent t'aider à comprendre si la situation est dangereuse ou non. Parfois, le message peut sembler innocent, mais l'adulte saura repérer les signes bizarres que tu n'as pas vus. N'aie jamais honte de poser des questions : les adultes sont là pour te protéger, pas pour te gronder !

55. Si tu vois une vidéo choquante ou violente sur un réseau social, que dois-tu faire ?

A) L'envoyer à tes amis pour leur montrer
B) La signaler à la plateforme et en parler à un adulte
C) L'ignorer et continuer à faire défiler

Quand tu tombes sur une vidéo choquante ou violente, il faut absolument la signaler et en parler à un adulte ! Pourquoi ? Parce que ces vidéos ne devraient pas être sur Internet, surtout pas là où des enfants peuvent les voir. En signalant la vidéo, tu aides la plateforme à la retirer rapidement pour protéger d'autres enfants. Comment sonner l'alarme ? Chaque réseau social a un bouton de signalement, souvent représenté par un point d'exclamation ou trois petits points. En parler à un adulte est tout aussi important car voir des images violentes peut te troubler, te faire peur ou te donner des cauchemars. L'adulte pourra t'aider à comprendre ce que tu as vu et à te rassurer. Surtout, ne partage jamais ces vidéos avec tes amis : cela ne ferait qu'empirer le problème en exposant encore plus d'enfants à du contenu dangereux. Ton bien-être passe avant tout !

Ressource pour tous : Signaler un contenu (Pharos)

56. Que peut-il arriver si un ado tombe par accident sur des images pornographiques sur Internet ?

A) Rien de grave, il oubliera vite
B) Cela peut le troubler et avoir des conséquences sur son développement personnel
C) Il n'y a pas de risque si l'exposition dure moins de 5 minutes

À 12 ans, près d'un enfant sur trois a déjà été exposé à la pornographie sur Internet, souvent sans le vouloir. Voir ces images peut créer un choc émotionnel. Ton cerveau n'est pas encore prêt pour comprendre ce type de contenu. Ces images montrent souvent des relations entre adultes qui ne ressemblent pas à la vraie vie et qui peuvent être violentes ou dérangeantes. Quand tu tombes sur ces images, tu peux te sentir confus, avoir peur ou être dégoûté. Tu peux aussi avoir du mal à comprendre ce que tu vois et te poser beaucoup de questions. C'est normal d'être troublé ! L'important est d'en parler rapidement avec un adulte de confiance. Il existe des moyens de se protéger : respecter le contrôle parental, ne pas cliquer sur des liens douteux, et surtout, toujours dire à un adulte quand on voit quelque chose de choquant sur Internet.

Source : Je protège mon enfant de la pornographie (République française)
Ressource pour tous : www.lumni.fr/programme/ados-le-porno-a-portee-de-clic

Ressource pour un ado : Pourquoi le porno c'est pas pour nous ? (Vinz et Lou)

57. Que fait une « bulle de filtre » quand tu utilises Internet ?

A) Elle empêche les virus d'entrer dans ton ordinateur
B) Elle choisit pour toi des infos et des vidéos que tu aimes déjà
C) Elle fait apparaître des bulles colorées sur ton écran

Une « bulle de filtre » agit comme un assistant invisible qui observe tout ce que tu regardes sur Internet et qui décide de te montrer seulement des choses similaires ! Par exemple, si tu regardes souvent des vidéos sur les chats, l'algorithme va comprendre que tu adores les chats et va te proposer encore plus de vidéos de chats. Au début, ça semble génial : tu vois plein de contenus que tu aimes ! Mais le problème, c'est que tu finis par vivre dans une « bulle » où tu ne découvres plus rien de nouveau. Sur Internet, cette bulle peut t'empêcher de découvrir de nouveaux sujets, d'autres points de vue, ou des informations importantes.
C'est ainsi que se forment également des communautés virtuelles partageant des opinions radicales. Ce sont des « chambres d'écho », un endroit où tu n'entends que les mêmes idées ou opinions, comme si tout le monde répétait la même chose. C'est pourquoi il est conseillé de varier tes recherches, de poser des questions à tes parents sur l'actualité et de lire des livres pour élargir tes horizons !

Source : Bulles de filtre et chambres d'écho (Fondation Descartes)
Ressource pour un adulte : Centre pour l'Éducation aux Médias et à l'Information (CLEMI)

58. À partir de quel âge un enfant peut-il regarder les écrans ?

A) Dès la naissance, avec des vidéos éducatives
B) À partir de 2 ans, avec un maximum de 2 heures par jour
C) C'est déconseillé avant 6 ans

Les bébés et les très jeunes enfants ont besoin de découvrir le monde avec leurs mains, leurs yeux et en bougeant leur corps. Avant 3 ans, leur cerveau se développe très rapidement et il a besoin d'expériences réelles pour bien grandir. Les écrans peuvent troubler cette croissance naturelle et empêcher les enfants d'apprendre à parler correctement ou à bien se concentrer plus tard.
Il ne faut pas d'écran avant 3 ans et c'est déconseillé jusqu'à 6 ans (ou limité et occasionnel, en privilégiant les contenus éducatifs avec un adulte). Les petits ont besoin de jouer avec des objets qu'ils peuvent toucher, d'écouter des histoires, de regarder des livres avec des images et surtout de passer du temps avec d'autres enfants et des adultes qui leur parlent et leur sourient. Si tu as un petit frère ou une petite sœur, tu peux l'aider à bien grandir en jouant avec lui plutôt qu'en regardant des écrans ensemble !

Ressource pour un adulte : Enfants et écrans. À la recherche du temps perdu (République française - Avril 2024)

59. Que fait un influenceur ?

A) Il crée des virus
B) Il partage des contenus pour divertir ou vendre des produits
C) Il protège les internautes

Un influenceur est une personne qui crée du contenu sur les réseaux sociaux pour divertir ses abonnés et parfois leur vendre des produits ! Il peut parler de mode, de jeux vidéo, de sport, de cuisine... Son travail consiste à créer des photos, des vidéos, ou des posts amusants pour attirer des fans et faire grandir la communauté qui le suit. Mais attention : les influenceurs ne sont pas toujours désintéressés ! Souvent, des marques les paient pour parler de leurs produits. C'est de la publicité déguisée ! Ils doivent normalement l'indiquer avec des hashtags comme #collaboration ou #partenariat, mais ce n'est pas toujours visible. Être influenceur demande beaucoup de travail : il faut créer du contenu tous les jours, répondre aux commentaires, et faire attention à ce qu'on dit car on influence vraiment les opinions de sa communauté. C'est une grande responsabilité ! Quand tu regardes un influenceur, demande-toi toujours : « Est-ce qu'il essaie de me vendre quelque chose ? »



Ressource pour un ado : Comment reconnaître une pub cachée ? (Vinz et Lou)

60. Qu'est-ce qu'une fake news ?

A) Une blague
B) Une fausse information partagée comme si elle était vraie
C) L'actualité principale du jour

Une « fake news » (fausse nouvelle), c'est une information inventée ou déformée que quelqu'un fait circuler en prétendant qu'elle est vraie ! Par exemple, quelqu'un pourrait inventer qu'un nouveau bonbon rend invisible, et si plein de gens partagent cette fausse info, certaines personnes vont finir par y croire ! Les fake news sont souvent créées pour plusieurs raisons : faire peur aux gens, les mettre en colère, ou les faire changer d'avis sur quelque chose d'important. Elles circulent très rapidement sur les réseaux sociaux parce que les gens les partagent sans vérifier si c'est vrai. Pour t'en protéger, tu peux vérifier l'information sur plusieurs sites différents, demander à un adulte si ça lui semble bizarre, et tu ne dois jamais partager une info si tu n'es pas sûr qu'elle soit vraie. Rappelle-toi : sur Internet, il faut toujours garder son esprit critique.

Ressources pour un adulte : Vérification de l'information - Fiche pédagogique (CLEMI) et Fake news : « Le plus grand menteur d'Internet » se confie (INA)



Ressource pour un ado : C'est quoi les fake news ? (Info ou mytho)

61. Une photo peut-elle être truquée ?

A) Seulement si elle est floue
B) Non
C) Oui, grâce à des applications ou logiciels

Oui, une photo peut facilement être truquée ! Avec des applications comme Photoshop, FaceApp, ou même des filtres sur Snapchat et Instagram, on peut transformer complètement une image et c'est encore plus facile aujourd'hui avec l'intelligence artificielle. On peut effacer des boutons, changer la couleur des yeux, modifier la forme du visage, ajouter ou enlever des personnes, et même créer des situations qui n'ont jamais existé ! Ces retouches peuvent donner une vision déformée de la réalité.
Par exemple, beaucoup d'influenceurs retouchent leurs photos pour paraître « parfaits », mais personne n'est parfait dans la vraie vie ! Cela peut te faire croire que tu n'es pas assez bien comme tu es, alors que c'est faux. C'est pourquoi il faut toujours se demander :
« Cette image me semble-t-elle naturelle ? ».

Ressource pour un ado : Quelle est la plus grosse fake news que tu as crue ? (Konbini)
Ressource pour un adulte : Porter un regard critique sur l'image (Internet Sans Crainte)

62. Peut-on supprimer une publication qu'on a postée sur les réseaux sociaux ?

A) Non
B) Oui
C) Seulement si elle a été vue

Oui, on peut supprimer une publication qu'on a postée, mais attention : ce n'est pas magique ! Même si tu supprimes ton post, d'autres personnes ont pu le voir, le copier, faire une capture d'écran, ou le télécharger avant que tu le supprimes.
C'est pour cela qu'on dit souvent qu'« Internet n'oublie jamais ». Par exemple, si tu publies une photo gênante et que ton ami la sauvegarde sur son téléphone, elle existera toujours même si tu la supprimes de ton profil !
C'est pourquoi il est super important de réfléchir avant de publier quelque chose. Demande-toi toujours : « Est-ce que j'aimerais que mes parents, mes grands-parents, ou mon futur employeur voient ça ? » Si la réponse est non, alors il vaut mieux ne pas le publier.

Ressource pour tous : www.lumni.fr/video/le-droit-a-l-oubli

63. Quelle est l'une des caractéristiques du cyberharcèlement ?

A) Une dispute passagère
B) Des messages malveillants répétés sur Internet
C) Un désaccord sur un jeu

Le cyberharcèlement, c'est quand quelqu'un t'envoie plusieurs fois des messages malveillants sur Internet. Ce n'est pas juste une dispute qui arrive une fois ! C'est répétitif, comme si la même personne revenait encore et encore pour te dire des choses blessantes. Imagine que quelqu'un te pousse dans la cour de récré tous les jours : c'est pareil sur Internet ! Le cyberharcèlement peut prendre plusieurs formes : des insultes par messages, des moqueries sur tes photos, des menaces, ou même partager des images de toi sans ta permission. Ce qui rend le cyberharcèlement particulièrement difficile, c'est qu'Internet ne s'arrête jamais. Contrairement à l'école où tu peux rentrer chez toi, les messages méchants peuvent arriver à toute heure sur ton téléphone. Même si c'est « virtuel », les émotions que tu ressens sont bien réelles et peuvent faire très mal. Bon à savoir : Le cyberharcèlement est puni par la loi, exactement comme le harcèlement dans la vraie vie !

Ressource pour un ado : Non au cyberharcèlement (Livret Bayard Jeunesse)

Ressource pour un ado : E-enfance

64. Quel est le bon réflexe si tu vois quelqu'un se faire harceler en ligne ?

A) L'ignorer
B) Soutenir la victime, en parler à un adulte et signaler les contenus
C) Rire avec les autres

Quand tu vois quelqu'un se faire embêter sur Internet, tu peux l'aider ! Comme dans la vraie vie, si tu vois quelqu'un en difficulté, tu ne restes pas les bras croisés. D'abord, montre ton soutien à la personne harcelée. Un simple « Ce n'est pas normal ce qu'ils te font » peut déjà l'aider énormément. Elle se sentira moins seule face aux méchancetés. Ensuite, aide-la à garder des preuves : fais des captures d'écran des messages méchants et enregistre les liens Internet si tu peux. Cela permet de garder des indices pour montrer ce qui s'est passé ! Le plus important : parle rapidement à un adulte de confiance (parents ou professeurs). Les adultes connaissent bien les moyens d'agir et peuvent t'aider à signaler les contenus aux bonnes personnes. Enfin, tu peux signaler les comptes ou les messages directement sur les réseaux sociaux. Chaque plateforme a des boutons pour cela.

Ressource pour un adulte : OMG, le cyber-harcèlement (Caf)

Ressource pour un ado : Liker peut blesser (La famille tout écran)

65. Pourquoi ne faut-il pas partager des photos gênantes d'une autre personne ?

A) Parce que ça peut lui faire du mal et c'est interdit par la loi
B) Parce que ça prend de la place sur ton téléphone
C) Parce que ça pourrait lui rapporter des abonnés

Imagine si c'était toi sur cette photo gênante : comment te sentirais-tu si tout le monde la voyait et se moquait ?
Partager cette photo peut blesser la personne très profondément. Elle peut se sentir humiliée, avoir honte d'aller à l'école, ou même ne plus vouloir voir ses amis. Parfois, une seule photo peut gâcher complètement sa confiance en elle.
De plus, c'est illégal ! La loi protège l'image de chacun. Tu n'as pas le droit de partager une photo de quelqu'un sans son accord, surtout si elle peut lui faire du mal. C'est ce qu'on appelle le « droit à l'image ». Même si tu penses que c'est « juste pour rigoler », cela peut rapidement devenir du harcèlement. Une fois sur Internet, impossible de contrôler qui va voir cette photo et où elle va aller !
La règle d'or : avant de partager quoi que ce soit sur quelqu'un, demande-toi « Est-ce que j'aimerais qu'on fasse pareil avec moi ? » Si la réponse est non, ne le fais pas !

Ressource pour un ado : La battle qui a trop de succès (CNIL)

66. Peut-on aller en prison pour cyberharcèlement ?

A) Non, ce n'est pas grave
B) Oui, c'est puni par la loi
C) Seulement si plus de 10 personnes participent

Le cyberharcèlement est très sérieux aux yeux de la loi, même quand ce sont des enfants qui le provoquent. En France, il existe des lois spéciales qui protègent les victimes
de harcèlement sur Internet. Les personnes qui harcèlent peuvent avoir de gros problèmes avec la justice, y compris aller en prison pendant plusieurs années.
Les juges considèrent que faire du mal à quelqu'un sur Internet, c'est aussi grave que de le faire en vrai. Quand on envoie des messages méchants, qu'on partage des photos embarrassantes ou qu'on encourage d'autres personnes à embêter quelqu'un, on peut causer beaucoup de souffrance. La personne qui reçoit ces attaques peut devenir très triste, avoir peur d'aller à l'école ou même tomber malade.
La loi protège surtout les enfants : si un enfant de moins de 15 ans est harcelé, les punitions sont encore plus sévères. Retiens bien ceci : tout ce qu'on fait sur Internet laisse des traces, et ces traces peuvent être utilisées par la police.

Source : Article 222-33-2-2 du Code pénal

67. Quel est le principal objectif du contrôle parental ?

A) Empêcher les enfants d'utiliser Internet
B) Protéger les enfants des contenus inappropriés en ligne
C) Surveiller toutes les activités numériques des parents

Le but principal du contrôle parental n'est pas de t'interdire complètement Internet (ce serait dommage, il y a tellement de choses géniales à découvrir), mais plutôt de te protéger des contenus qui ne sont pas adaptés à ton âge.
Imagine Internet comme une immense ville : il y a des quartiers super cool avec des musées, des parcs, des cinémas pour ton âge, mais aussi des zones moins recommandables où tu pourrais tomber sur des choses choquantes, violentes ou dangereuses. Le contrôle parental t'aide à naviguer vers les bons endroits tout en évitant les zones à risque.
Ces outils peuvent bloquer l'accès à certains sites web, limiter le temps d'écran, ou encore filtrer les contenus selon ton âge. L'idée, c'est de te laisser explorer le monde numérique en toute sécurité. Ces outils limitent les dangers mais ne remplacent pas le dialogue et l'accompagnement des parents !

Ressource pour un adulte : Je protège mon enfant dans son usage des écrans (République française)

68. Qu'est-ce que l'accessibilité numérique ?

A) Des applications qui s'ouvrent en moins d'une seconde pour aller plus vite
B) Des sites Internet et applications conçus pour que tout le monde puisse les utiliser
C) Des jeux vidéo qu'on ne peut lancer que la nuit pour économiser de l'énergie

L'accessibilité numérique pourrait s'apparenter à construire une rampe à l'entrée d'un bâtiment : on veut que chacun puisse entrer sans difficulté, même s'il se déplace en fauteuil roulant, en poussette ou avec des béquilles. Sur Internet, on remplace la rampe par des techniques pour que les sites et les applis soient compréhensibles et utilisables par tout le monde.
Concrètement, un site accessible a des textes qu'un ordinateur peut lire à voix haute pour les personnes aveugles. Les vidéos ont des sous-titres pour les personnes sourdes. Les boutons sont assez gros pour être cliqués facilement. Les couleurs sont choisies pour que tout le monde puisse bien voir les informations importantes.
Cette accessibilité aide tout le monde ! Quand tu regardes une vidéo avec le son coupé dans le bus, les sous-titres t'aident. Quand tes grands-parents utilisent une tablette, des boutons plus gros leur facilitent la tâche. Quelle que soit sa situation, chacun accède à la même information.

Ressource pour un adulte : https://accessibilite.numerique.gouv.fr/

69. Qu'est-ce qu'une publicité cachée sur les réseaux sociaux ?

A) C'est quand une vidéo ne montre pas de produit du tout
B) C'est quand un influenceur parle d'un produit comme s'il l'aimait vraiment, mais qu'en fait, il est payé pour le faire
C) C'est une publicité qui apparaît seulement le soir après 20 h

Une publicité cachée, c'est quand quelqu'un fait de la publicité sans te dire clairement que c'est de la publicité ! Par exemple, sur YouTube, une personne peut dire « ce produit est fantastique, je le recommande » alors qu'en réalité, une entreprise lui a donné de l'argent pour dire ça. C'est malhonnête et c'est interdit par la loi française !
Toute personne payée pour promouvoir un produit doit l'indiquer avec des mentions comme « pub », « sponsorisé » ou « partenariat rémunéré ».
Si ces mentions ne sont pas visibles, c'est de la tromperie. Les autorités peuvent donner des amendes très importantes ! Pour te protéger, sois toujours vigilant : pourquoi cette personne parle-t-elle de ce produit ? Montre-t-elle aussi les défauts ? As-tu vu une mention de publicité ? Nous voyons plus de 4 000 publicités par jour, alors développe ton esprit critique pour ne pas te faire avoir car les jeunes sont particulièrement vulnérables à ces pratiques.

Ressource pour un ado : Comment reconnaître une publicité cachée ? (Vinz et Lou)

70. Que se passe-t-il si tu écris des messages méchants ou racistes sur Internet ?

A) Rien du tout, car c'est juste sur Internet
B) Tu peux avoir des problèmes avec la police et tes parents peuvent payer une amende
C) C'est autorisé tant que tu effaces le message après

Sur Internet, on n'a pas le droit d'écrire n'importe quoi ! Même si tu penses que personne ne te voit, la loi française interdit d'écrire des messages racistes, qui insultent les autres ou qui poussent à la violence. Tous les messages laissent des traces numériques et la police peut retrouver qui les a écrits.
Quand un enfant écrit ce genre de messages, plusieurs choses peuvent arriver.
D'abord, il peut être convoqué au commissariat avec ses parents. Les tribunaux peuvent décider d'une sanction, et parfois les parents doivent payer une amende qui peut aller jusqu'à 7 500 euros ! En plus, ces messages peuvent rester longtemps sur Internet et causer des problèmes plus tard.
Sur les réseaux sociaux, dans les jeux en ligne ou dans les commentaires, les mêmes règles s'appliquent. La liberté d'expression existe, mais elle a des limites pour protéger tout le monde. Avant d'écrire quelque chose, demande-toi toujours :
« Est-ce que j'oserais dire ça en face à cette personne et devant mes parents ? ».

Source : Que risquent vos enfants s'ils tiennent des propos racistes, sexistes ou homophobes sur Internet ? (CLEMI)

71. Quels paramètres des réseaux sociaux te permettent de choisir qui peut voir tes publications ?

A) Les paramètres de confiance
B) Les paramètres de concurrence
C) Les paramètres de confidentialité

Les paramètres de confidentialité sont les outils qui te permettent de décider qui peut voir ce que tu publies sur les réseaux sociaux ! Quand tu postes une photo ou un message, tu peux choisir si tout le monde peut la voir, seulement tes amis, ou même personne du tout.
Dans ta chambre, si tu ouvres grands tes rideaux tout le monde peut voir ce qu'il s'y passe, si tu les fermes un peu, seuls tes proches peuvent te voir, ou tu peux les fermer complètement pour avoir de l'intimité. C'est pareil pour les publications sur les réseaux sociaux. Sur Instagram, Facebook, TikTok et autres, tu trouveras ces réglages dans les « Paramètres » puis « Confidentialité ».
Il existe plusieurs niveaux : « Public » (tout le monde voit), « Amis seulement » (tes contacts approuvés) ou « Privé » (personne sauf toi).
C'est important de bien comprendre ces réglages car une fois qu'une publication devient publique, elle peut être vue et partagée par n'importe qui !

72. Quand tu vois un challenge qui te semble marrant mais un peu dangereux sur Internet...

A) Tu dois le faire immédiatement pour montrer ton courage à tes amis
B) Tu dois le partager avec tes amis pour qu'ils le voient aussi
C) Tu ne dois pas le reproduire ni le partager

Les challenges sur Internet peuvent sembler amusants et excitants, mais certains d'entre eux cachent de vrais dangers ! Ces défis jouent avec notre envie d'être accepté par nos amis et de recevoir des « likes ». Pourtant, derrière des vidéos qui paraissent drôles, il peut y avoir des risques graves : brûlures, évanouissements, blessures ou même pire.
Quand tu croises un challenge qui te semble bizarre ou dangereux, le mieux est d'en parler à un adulte en qui tu as confiance. Tes parents, un professeur ou un autre membre de ta famille sauront t'expliquer pourquoi ce défi peut être risqué. Ils ne vont pas te gronder, au contraire, ils seront fiers que tu aies eu le bon réflexe !
Rappelle-toi : être courageux, ce n'est pas faire n'importe quoi pour impressionner, c'est savoir dire non quand quelque chose peut te faire du mal. Tu peux toujours trouver d'autres moyens de t'amuser avec tes amis, sans prendre de risques !

Ressource pour tous : J'en ai marre des challenges ! (CLEMI)

73. Pourquoi partage-t-on énormément de selfies sur les réseaux sociaux ?

A) Parce que c'est plus facile que d'utiliser un appareil photo normal
B) Pour montrer qu'on a le dernier téléphone à la mode
C) Pour recevoir des « likes » et se sentir acceptés par nos amis

Les selfies ne sont pas juste des photos ! Derrière chaque selfie se cache un besoin très humain : celui d'être aimé et accepté par les autres. Quand tu prends un selfie et que tu le partages, tu attends des réactions de tes amis. Chaque « like » ou commentaire positif te fait plaisir et te donne confiance en toi.
Les applications permettent même de changer ton apparence avec des filtres amusants ! Tes selfies racontent une histoire : « j'étais à ce concert », « voici ma nouvelle coupe de cheveux », « je suis avec mes copains ». C'est normal de vouloir partager ces moments ! Mais passer trop de temps à prendre des selfies peut faire oublier de profiter vraiment du moment présent. Et surtout, il faut bien réfléchir avant de partager une photo, car une fois sur Internet, elle peut être vue par plein d'autres personnes !

Ressource pour un adulte : https://enseignants.lumni.fr/collections/777/dopamine.html

74. En moyenne, combien de fois consultons-nous notre téléphone par jour ?

A) 30 fois
B) 144 fois
C) Plus de 300 fois

144 fois par jour ! Ce chiffre peut paraître énorme, mais c'est pourtant la réalité. Cela veut dire qu'en moyenne, nous regardons notre téléphone toutes les 6 minutes quand nous sommes réveillés.
Pourquoi consultons-nous si souvent notre téléphone ? Notre cerveau adore recevoir des petites récompenses et chaque notification ou message nous fait du bien donc on en veut toujours plus ! On sort son téléphone de sa poche sans même s'en rendre compte ou on vérifie l'heure alors qu'on vient de la regarder.
Cette habitude existe à tous les âges : les enfants, les ados, les parents et même les grands-parents. Le téléphone est devenu un objet si important dans notre quotidien qu'il est difficile de s'en séparer. Maintenant que tu connais ce chiffre surprenant, tu peux observer autour de toi : combien de fois vois-tu les gens regarder leur téléphone dans une journée ?

Source : Journée sans téléphone portable : 5 chiffres sur l'ampleur de notre addiction (La Croix)
Ressource pour tous : Pourquoi sommes-nous dingue de notre smartphone ? (Qu'est-ce qu'on fait ?)

Ressource pour un ado : Vinz et Lou sur Internet - Accro à Internet

75. Quel est l'âge moyen d'un joueur de jeux vidéo en France ?

A) 5 ans
B) 12 ans
C) 39 ans

Tu pensais peut-être que les joueurs de jeux vidéo étaient surtout des enfants et des adolescents ? Eh bien, non ! L'âge moyen d'un joueur de jeux vidéo en France est de 39 ans. Les personnes qui ont grandi avec les premiers jeux vidéo dans les années 1980 et 1990 continuent de jouer aujourd'hui. De plus, beaucoup d'adultes découvrent les jeux vidéo maintenant grâce aux smartphones et aux tablettes.
Mais attention, tous les jeux ne conviennent pas à tous les âges. Les logos PEGI (Pan European Game Information) sur les boîtes t'indiquent l'âge minimum recommandé. Un jeu PEGI 12 ou plus peut contenir des scènes qui font peur ou permettre de discuter avec des inconnus en ligne. Les jeux vidéo développent ta créativité et ta logique, mais il faut bien choisir ceux qui correspondent à ton âge pour jouer en sécurité !

Source : Les joueurs de jeu vidéo français sortent plus, lisent plus, et font plus de sport que la moyenne (Radio France)
Ressource pour tous : PEGI

76. Quel est le temps moyen passé par une personne chaque jour sur les réseaux sociaux dans le monde en 2024 ?

A) Moins de 30 minutes
B) Environ 1 heure
C) Plus de 2 heures 30 minutes

On passe plus de 2 h 30 de notre temps sur les réseaux sociaux par jour !
C'est énorme quand on y pense. Sur une semaine, cela représente plus de 2 jours à être connecté. Comment les réseaux sociaux arrivent-ils à nous captiver autant ? Les algorithmes apprennent ce qui nous plaît et nous proposent en permanence du contenu personnalisé. De plus, sur TikTok par exemple, les vidéos courtes créent un effet de « binge watching » : tu te dis « encore une petite » et le temps file sans que tu t'en rendes compte.
Cette durée importante montre l'efficacité des techniques utilisées pour retenir ton attention. Il est important d'en être conscient pour garder le contrôle de ton temps et éviter que les réseaux sociaux ne remplacent complètement d'autres activités importantes dans la vie.

Source : Daily time spent on social networking by Internet users worldwide from 2012 to 2025 (Statista)

77. Qu'est-ce que le « doxing » ?

A) Publier des informations trouvées en ligne sans en vérifier la source
B) Partager des données accessibles publiquement sans demander l'autorisation
C) Révéler des informations privées d'une personne sans son accord

Le doxing c'est quand quelqu'un publie ton adresse, ton numéro de téléphone ou même des photos de ta maison sur Internet sans te demander la permission. Ce mot vient de « documents » et désigne le fait de révéler des informations personnelles sur quelqu'un sans son consentement. Ces infos peuvent inclure ton vrai nom, ton adresse IP, tes comptes sur les réseaux sociaux, bref tout ce qui permet de t'identifier dans la vraie vie. Le problème ? Une fois que ces données sont en ligne, n'importe qui peut les voir et s'en servir pour te harceler, te faire du chantage ou même te mettre en danger physiquement. C'est pour ça qu'il faut toujours faire super attention à ce qu'on partage sur Internet et protéger ses informations !

Source : Wikipédia

78. Pourquoi ne faut-il pas partager des photos de soi sur les réseaux sociaux ?

A) Parce que ces photos peuvent être utilisées sans ton accord
B) Parce que les réseaux sociaux interdisent systématiquement la publication de photos personnelles
C) Parce que partager des photos empêche de supprimer définitivement son compte plus tard

Quand tu postes une photo de toi sur les réseaux, tu penses peut-être qu'elle restera juste visible par tes amis. Mais la réalité est plus inquiétante : ces photos peuvent être récupérées, modifiées ou utilisées par n'importe qui sans que tu le saches. Tes photos peuvent aussi être utilisées pour créer de fausses identités, pour du chantage ou simplement être partagées dans des contextes que tu n'approuverais jamais. Une fois en ligne, tu perds complètement le contrôle sur tes images. C'est pourquoi il vaut mieux partager tes photos uniquement avec tes proches via des messageries sécurisées comme Signal plutôt que sur les réseaux sociaux publics.

79. Quel site Internet a été créé pour lutter contre les fake news ?

A) Vera
B) Canva
C) Discord

Vera est un site Internet développé par l'ONG française LaReponse.tech pour lutter contre la désinformation. Cette application gratuite fonctionne de manière super simple : tu peux lui envoyer un message WhatsApp ou l'appeler par téléphone pour vérifier n'importe quelle information douteuse.
En quelques secondes, elle analyse l'information que tu lui transmets et te fournit une réponse fiable avec des sources vérifiées.
C'est particulièrement utile quand tu reçois des messages suspects sur les réseaux sociaux ou que tu tombes sur des articles qui te semblent bizarres. Au lieu de partager une information sans vérifier, tu peux désormais la faire analyser par Vera en quelques clics. Et comme tout outil (même sourcé), Vera peut se tromper : si le sujet est important, compare toujours avec plusieurs sources fiables.

Ressource pour tous :
Vera

80. Si un service est gratuit, comme une application ou un réseau social, cela veut dire :

A) Que c'est un cadeau du fondateur
B) Que c'est gratuit parce que personne ne l'utilise
C) Que tu « payes » avec tes données

Quand une application ou un site web est gratuit, ce n'est pas vraiment gratuit !
En réalité, tu « payes » avec quelque chose de très précieux : tes « données ». Les entreprises peuvent collecter plein d'informations sur toi : ce que tu aimes, ce que tu regardes, où tu vas, avec qui tu parles, tes photos... Elles utilisent ensuite ces informations pour te montrer des publicités qui t'intéressent beaucoup. Plus la publicité te plaît, plus tu as envie d'acheter le produit !
Ces données valent beaucoup d'argent. Facebook, TikTok, Instagram et YouTube gagnent des milliards d'euros chaque année en vendant leurs espaces publicitaires à des entreprises. C'est pour ça qu'ils peuvent te proposer leurs services gratuitement.
En fait, le vrai produit qu'ils vendent, c'est toi !

Ressource pour un adulte : Nos données personnelles valent de l'or (Cash Investigation - France TV)

81. Que fait la dopamine dans ton cerveau quand tu utilises les réseaux sociaux ?

A) Elle t'aide à te souvenir de tes mots de passe
B) Elle te donne une sensation de plaisir qui te donne envie de continuer
C) Elle rend ton écran plus lumineux

La dopamine, c'est la « molécule du bonheur » dans ton cerveau ! Chaque fois que tu reçois un like, un commentaire sympa ou une notification, ton cerveau libère cette substance qui te fait te sentir super bien. C'est exactement le même mécanisme que quand tu manges du chocolat ou que tu gagnes à un jeu.
Le problème ? Les créateurs des réseaux sociaux connaissent ce truc par cœur ! Ils ont conçu leurs applications pour déclencher cette libération de dopamine le plus souvent possible : notifications surprises, système de likes, recommandations personnalisées… Tout est pensé pour que tu aies envie de revenir encore et encore. C'est pour ça que tu peux passer des heures à scroller sans t'en rendre compte ! Ton cerveau adore ces petites doses de bonheur artificiel.

Ressource pour tous :
Série Dopamine (Arte)

82. Si ton petit ami ou ta petite amie te demande de lui envoyer une photo intime, que dois-tu faire ?

A) Accepter si la conversation est privée et sécurisée
B) Lui proposer d'en parler en personne pour mieux comprendre son intention
C) Refuser et lui expliquer les risques

Le sexting est la contraction des mots anglais « sex » et « texting » qui renvoie à l'échange de messages, photos ou vidéos à caractère sexuel par l'intermédiaire d'un support numérique. Cette situation peut arriver à tout le monde et c'est normal de vouloir faire plaisir à quelqu'un qu'on aime. Le problème est qu'une fois que tu envoies cette photo, tu perds complètement le contrôle dessus. Même si tu fais confiance à ton copain ou ta copine aujourd'hui, que se passera-t-il si vous vous disputez ? Si vous rompez ? Si son téléphone est piraté ? Cette photo peut ressurgir des années plus tard, être partagée sans ton accord ou utilisée pour te faire du chantage (revenge porn). Sur Internet, rien ne disparaît jamais vraiment ! Si quelqu'un a déjà diffusé ou menace de diffuser une photo intime de toi, il faut absolument en parler à un adulte de confiance. Même si tu ressens de la honte, il est crucial de demander de l'aide.

Ressources pour tous : Revenge Porn (e-enfance) et Disrupt (pointdecontact.net)

83. Qu'est-ce que l'économie de l'attention ?

A) Une économie qui fait attention à toi, à ta bonne santé
B) Une économie qui cherche à capter et contrôler ton attention
C) Une économie qui cherche à ce que tu fasses attention aux autres

Ton attention vaut de l'or ! Littéralement. Les géants du numérique comme Facebook, TikTok, YouTube ou Netflix ont compris que s'ils arrivent à capter ton attention, ils peuvent la « vendre » aux publicitaires qui veulent te faire acheter leurs produits. C'est ça, l'économie de l'attention : ton temps d'écran se transforme en argent pour ces entreprises. Pour y arriver, elles utilisent des équipes entières de psychologues, de neuroscientifiques et d'experts en manipulation pour rendre leurs applications irrésistibles. Notifications, algorithmes personnalisés, vidéos qui s'enchaînent automatiquement, like qui font du bruit... Tout est calculé pour que tu restes collé à ton écran le plus longtemps possible.
En quoi cela est un problème ? Il est très difficile de résister à ces techniques, même pour les adultes. C'est pour ça que beaucoup de jeunes se sentent accros à leurs téléphones sans comprendre pourquoi. Ces entreprises exploitent les failles de ton cerveau pour générer des profits.

Ressources pour un adulte : The Social Dilemma (Documentaire Netflix - 2020) et www.arte.tv/fr/videos/RC-017841/dopamine

84. En 2024, quelle part de la population mondiale utilise les réseaux sociaux ?

A) 25 %
B) 62 %
C) 70 %

Pour te faire une idée : sur 10 personnes dans le monde, plus de 6 utilisent les réseaux sociaux ! En 2024, c'est exactement 62,3 % de la population mondiale qui scrolle, like et partage quotidiennement. C'est énorme quand on y pense ! Les champions sont Facebook, YouTube, WhatsApp, Instagram et TikTok.
En France, on est encore plus connectés : 75 % de la population utilise les réseaux sociaux ! Cette explosion s'explique par l'arrivée des smartphones dans les pays en développement et l'amélioration des connexions Internet partout sur la planète.
Cette hyper-connexion mondiale pose des questions importantes : manipulation de l'information, protection de la vie privée, impact sur la santé mentale...
Aujourd'hui, ne pas être sur les réseaux sociaux devient presque l'exception !
C'est devenu un moyen de communication universel, mais avec des enjeux et des impacts énormes sur la société.

Sources : Les chiffres-clés du Digital en France (Comk) et Nombre d'utilisateurs Internet et des réseaux sociaux dans le monde en janvier 2024 (Statista)

85. Comment se propagent les fake news ?

A) Plus lentement que de véritables informations
B) À la même vitesse
C) Plus rapidement que de véritables informations

Les fausses informations se propagent malheureusement plus vite que les vraies. Pourquoi ? Les fake news sont conçues comme des bombes émotionnelles : elles provoquent de la colère, de la peur, de l'indignation ou de la surprise. Notre cerveau réagit plus fort aux émotions qu'aux faits rationnels. On a tendance à partager plus rapidement ce qui nous choque que ce qui nous informe calmement. Les vraies informations, elles, sont souvent plus neutres et moins « spectaculaires ».
Résultat : pendant qu'une fake news fait le tour du monde, la vérification factuelle arrive en retard et touche moins de monde.
C'est pour ça qu'il est crucial de prendre quelques secondes pour vérifier avant de partager, même si l'info semble incroyable !

Ressource pour tous : On a trouvé une solution ultime contre les fake news ! (La famille tout écran)

86. Que signifie « FOMO » ?

A) Une tendance qui consiste à suivre toutes les nouveautés publiées sur les réseaux sociaux
B) La peur de manquer quelque chose
C) Une fonctionnalité qui envoie plus de notifications pour encourager l'activité en ligne

FOMO : quatre lettres qui résument parfaitement l'angoisse moderne !
« Fear Of Missing Out » signifie littéralement « peur de manquer quelque chose ». C'est cette sensation horrible que tu ressens quand tu vois les stories Instagram de tes amis à une fête où tu n'étais pas invité, ou quand tu découvres qu'un événement cool s'est passé sans toi. Les réseaux sociaux amplifient énormément ce phénomène parce qu'ils te montrent en permanence tout ce que font les autres : voyages, sorties, succès… Tu as l'impression de rater constamment des trucs géniaux !
Cette peur peut te pousser à passer des heures à scroller pour être sûr de ne rien manquer, à accepter toutes les invitations même quand tu n'en as pas envie, ou à te sentir anxieux quand tu n'as pas accès à Internet.
Le paradoxe ? Plus tu essaies de tout suivre pour ne rien rater, plus tu rates ta propre vie ! Apprendre à déconnecter de temps en temps, c'est finalement le meilleur moyen de ne plus rien manquer d'important.

Ressource pour un adulte : FOMO - La « Fear of Missing Out », comment le besoin de profiter peut nous gâcher la vie (Radio France)

87. Quel outil permet de vérifier si une image est truquée ?

A) Un logiciel qui mesure la résolution de l'image
B) Un logiciel de retouche pour augmenter la netteté
C) Une recherche d'image inversée

Dans l'ère des deepfakes (vidéos ou photos créées ou modifiées via l'intelligence artificielle), la recherche d'image inversée est ton meilleur allié pour démasquer les images truquées ! Comment ça marche ? Au lieu de taper des mots dans Google, tu télécharges directement l'image suspecte. L'algorithme va alors chercher toutes les versions de cette image sur Internet et te montrer où elle apparaît. Tu peux ainsi découvrir par exemple qu'une photo « récente » d'une catastrophe naturelle date en fait de 2015. Google Images et TinEye proposent ce service gratuitement. Tu peux même faire ça directement depuis ton smartphone ! Mais attention, cette technique a ses limites : elle ne détecte pas les images créées entièrement par l'intelligence artificielle ou les modifications subtiles. C'est pourquoi il faut croiser cette vérification avec d'autres outils et toujours garder son esprit critique en éveil face aux images qui circulent sur les réseaux.

Ressources pour un adulte : Trois bonnes pratiques pour vérifier une information (AFP) et « le fléau des fausses images fabriquées grâce à l'intelligence artificielle » (Podcast Radiofrance)

88. Qui sont les « travailleurs du net » ?

A) Des personnes qui passent leur journée à jouer aux jeux vidéo
B) Des personnes qui réparent les ordinateurs cassés
C) Des personnes qui modèrent les contenus, nettoient les données ou programment des algorithmes

Derrière ton fil d'infos Instagram et tes résultats Google ultra-pertinents se cachent des milliers de « travailleurs du net » invisibles ! Ces personnes font un boulot crucial mais souvent méconnu : elles modèrent les commentaires haineux, suppriment les contenus violents, étiquettent des millions d'images pour entraîner les IA (Intelligence Artificielle), ou encore vérifient que les algorithmes fonctionnent correctement. Beaucoup travaillent dans des conditions difficiles : horaires épuisants devant des écrans, exposition répétée à des contenus choquants, salaires parfois très bas, surtout quand ces tâches sont délocalisées dans des pays en développement. Sans eux, Internet serait un chaos total ! Ils sont les gardiens invisibles qui permettent à nos plateformes préférées de fonctionner. Leur travail soulève des questions importantes sur les conditions de travail dans le numérique et sur qui supporte vraiment le « coût humain » de nos technologies. La prochaine fois que tu scrolles tranquillement, pense à ces personnes qui restent dans l'ombre !

Ressources pour un adulte : Témoignages - La souffrance des « nettoyeurs du net » (France TV)

Ressource pour un adulte :
Les mangeurs et mangeuses de péchés (Point de M.I.R)

89. À quoi sert un hashtag (#) ?

A) À mettre en avant l'émotion principale d'un message
B) À indiquer l'ordre des publications dans un fil de discussion
C) À regrouper des publications sur un même sujet

Le hashtag, c'est un système de rangement géant pour Internet ! Quand tu ajoutes #Vacances sous ta photo de plage, tu la mets automatiquement dans la grande boîte virtuelle « Vacances » avec toutes les autres photos qui utilisent ce hashtag. C'est génial pour retrouver des contenus sur un sujet précis ou pour faire découvrir tes publications à des gens qui s'intéressent au même thème que toi. Les hashtags peuvent même créer des mouvements mondiaux : #MeToo, #BlackLivesMatter, #ClimateChange ont permis de rassembler des millions de voix autour de causes importantes. Mais attention à ne pas en abuser ! Bourrer ton post de 50 hashtags, c'est moche et ça nuit à la compréhension.
L'astuce ? 3-5 hashtags pertinents, placés en fin de message, avec des majuscules pour chaque mot (#MonSuperHashtag) afin que les lecteurs d'écran puissent bien les lire. Utilisés intelligemment, les hashtags deviennent de supers outils de communication !

Ressource pour un adulte : Comment utiliser les hashtags de manière accessible ? (Access 42)

90. Puis-je partager sur les réseaux sociaux un message qu'un camarade m'a envoyé ?

A) Oui bien sûr, ça vient de mon copain
B) Oui, d'ailleurs, je partage systématiquement tous les messages que je reçois
C) Non, un message échangé entre deux personnes est privé

Stop ! Avant de faire une capture d'écran de ce message hilarant que ton pote t'a envoyé pour le partager en story, réfléchis deux secondes. Les messages privés, c'est exactement ça : PRIVÉ ! Quand quelqu'un t'écrit en privé, il souhaite que cette conversation reste entre vous deux. C'est protégé par ce qu'on appelle le « secret des correspondances », un droit fondamental qui existe même sur Internet. Partager le message de quelqu'un sans son accord, c'est violer sa vie privée et sa confiance. Imagine que tu confies un secret à ton meilleur ami et qu'il le raconte à toute la classe : c'est exactement pareil !
En plus, légalement, tu peux avoir des ennuis si tu diffuses des messages privés, surtout s'ils contiennent des informations sensibles. La règle d'or ? Demande toujours l'autorisation avant de partager quoi que ce soit qui vient d'une conversation privée. Respecter la vie privée des autres, c'est aussi protéger la tienne !

91. Quel est l'usage principal de TikTok ?

A) Communiquer avec la famille et les amis
B) Consulter des contenus divertissants
C) Publier ou partager des photos ou vidéos

79,6 % des utilisateurs de TikTok dans le monde utilisent l'application principalement pour regarder du contenu divertissant, pas pour créer !
Contrairement à ce qu'on pourrait croire, la plupart des gens préfèrent être spectateurs plutôt qu'acteurs. Seulement 42,3 % publient ou partagent des vidéos, et encore moins (21,7 %) l'utilisent pour communiquer avec leurs proches.
Ce qu'il faut bien avoir en tête, c'est que TikTok a développé un algorithme si puissant qu'il lui faut seulement une heure pour cerner ton profil psychologique et te proposer exactement ce qui va te faire rester scotché à ton écran. L'application analyse tes goûts, tes réactions, le temps que tu passes sur chaque vidéo pour créer un flux personnalisé addictif. Alors la prochaine fois que tu scrolles pendant des heures, rappelle-toi que c'est aussi parce que l'algorithme fait très bien son travail pour capter ton attention !

Source : Chiffres TikTok - Blog du modérateur (2025)
Ressource pour un adulte : Pourquoi sommes-nous accro au scrolling ? (Radio France)

92. Qu'est-ce que le « doomscrolling » ?

A) Lire plein de mauvaises nouvelles sans s'arrêter
B) Faire défiler son fil d'actualité très rapidement pour voir un maximum de publications
C) Rechercher uniquement des contenus choquants ou sensationnels

Le doomscrolling, c'est quand tu te retrouves piégé dans une spirale de mauvaises nouvelles sur ton téléphone. Tu commences par lire un article sur une catastrophe, puis un autre sur une crise, et encore un autre... sans pouvoir t'arrêter. C'est un phénomène moderne qui touche énormément de jeunes. Ton cerveau devient accro à ces informations négatives parce qu'il croit qu'en les lisant, il se prépare aux dangers. Mais en réalité, ça crée juste de l'anxiété et une vision déformée du monde. Les algorithmes des réseaux sociaux amplifient ce problème car ils privilégient les contenus qui provoquent des émotions fortes, souvent négatives, parce qu'ils génèrent plus d'engagements.
Pour lutter contre ça, fixe-toi des limites : consulte les infos à des moments précis, choisis des sources fiables, et n'hésite pas à faire des pauses numériques. Rappelle-toi que le monde n'est pas que négatif, même si c'est ce que suggère ton fil d'actualité !

Ressource pour un ado : Le petit livre pour apprendre à s'informer (Bayard Jeunesse)

93. Qu'est-ce qu'un « bot » ?

A) Un jeu
B) Un utilisateur très sympa
C) Un robot qui envoie des messages automatiquement

Un bot, c'est un robot numérique qui peut imiter un humain sur les réseaux sociaux. Il peut liker tes photos, commenter tes posts, ou même te suivre, mais ce n'est pas une vraie personne derrière ! Certains bots sont utiles : ils peuvent t'aider à commander une pizza ou répondre à tes questions sur un site. Mais d'autres sont plus problématiques. Ils peuvent répandre de fausses informations ou même influencer des élections en manipulant l'opinion publique. Alors comment les reconnaître ? Méfie-toi des comptes avec très peu de photos, des noms bizarres avec plein de chiffres, ou qui postent exactement les mêmes messages que d'autres comptes. Les bots modernes deviennent de plus en plus sophistiqués avec l'intelligence artificielle, donc reste toujours vigilant sur qui tu suis et avec qui tu interagis en ligne.

94. Qu'est-ce que le droit à l'oubli numérique ?

A) Le droit d'oublier ses mots de passe
B) Le droit de demander la suppression d'informations personnelles sur Internet
C) Le droit de jouer à des jeux en ligne sans limite

Une photo embarrassante que tu as postée ou un article te concernant apparaît dans les résultats Google et te dérange ? Le droit à l'oubli numérique te permet de demander que ces informations soient supprimées ! C'est un droit européen super important, créé en 2014. Concrètement, tu peux contacter Google ou directement le site qui a publié l'info pour en demander le retrait. Mais attention, ce n'est pas automatique : il faut prouver que ces informations te causent un préjudice et qu'elles ne sont pas d'intérêt public.
Par exemple, si tu deviens célèbre, il sera plus difficile de faire disparaître des infos te concernant. Tu as le droit de grandir, de changer, et de ne pas être jugé toute ta vie sur des erreurs du passé.
Alors réfléchis bien avant de poster quelque chose, mais sache aussi que des solutions existent si tu veux rectifier le tir !

Ressource pour un adulte : Formulaire de demande de suppression de données à caractère personnel (Google)
Ressource pour un ado : C'est quoi le droit à l'oubli numérique ? (Les Clés des Médias - CLEMI)

95. Comment savoir si une information est vraie ou fausse ?

A) Vérifier qui publie l'information et la comparer avec d'autres sources fiables
B) Faire confiance à une information si elle provient d'un compte certifié ou très suivi
C) Se fier au ton de l'article : s'il paraît sérieux, c'est qu'il est vrai

Devenir un détective de l'info, ça s'apprend ! Avec 53 % des jeunes qui s'informent principalement via les réseaux sociaux, maîtriser ces techniques devient essentiel. Première étape : vérifier la source. Un article sans auteur identifié ou venant d'un site inconnu doit t'alerter. Deuxième réflexe : examiner l'URL. Les sites de désinformation copient souvent les vrais sites avec des adresses presque identiques (lemonde.co au lieu de lemonde.fr). Troisième point crucial : distinguer les faits des opinions.
« Il pleut » = fait vérifiable. « Il fait un temps horrible » = opinion subjective. Les fausses infos mélangent souvent les deux pour manipuler.
Bonus : croise tes sources ! Si une info importante n'apparaît que sur un seul site, méfie-toi. Les vraies infos sont généralement reprises par plusieurs médias fiables. Ces réflexes te protégeront des manipulations et feront de toi un citoyen numérique éclairé. L'info, c'est du pouvoir : assure-toi qu'elle soit fiable !

Source : Jeunes de 15 à 30 ans - Comment s'informent-ils sur les actualités ? (République française) Ressource pour un adulte : À la découverte des médias - Comment trouver la bonne info ? (Profs - Les AS de l'info)
Ressources pour un ado : C'est quoi une information ? (CLEMI) et Série lumni : chasseurs de fake

96. Que fait un modérateur en ligne ?

A) Il lit les messages et supprime ceux qui enfreignent les règles pour garder un espace sûr et respectueux
B) Il publie des publicités automatiques pour augmenter les revenus du site Internet
C) Il accélère la connexion Internet de tous les utilisateurs

Le modérateur anime des groupes, met en place des rituels et s'assure du bon fonctionnement des communautés en ligne. L'autre aspect, plus sombre, est qu'il regarde des centaines de publications sur le web pour décider lesquelles respectent les règles. Ces professionnels protègent les utilisateurs en supprimant les contenus haineux, violents, faux ou inappropriés qui peuvent être présents sur les réseaux sociaux, les forums ou les jeux vidéo. Leurs missions : examiner les contenus signalés, appliquer les règles de chaque plateforme et vérifier que la loi est bien respectée. C'est un métier qui peut être difficile car ils sont exposés à des contenus parfois choquants. Cette exposition répétée peut causer des troubles psychologiques.
Si un jour tu signales un contenu inapproprié, pense à ces gardiens du web qui travaillent 24 h/24 pour rendre Internet plus sûr pour tous !

Ressource pour un adulte : Les procédures de signalement (e-enfance)

97. Qui peut-on appeler les « oubliées du numérique » ?

A) Les femmes, parce qu'elles sont souvent moins présentes dans ces métiers
B) Les personnes qui n'aiment pas utiliser les ordinateurs
C) Les machines anciennes qu'on ne répare plus

Pendant longtemps, les métiers de l'informatique ont surtout été occupés par des hommes, ce qui a écarté beaucoup de femmes du numérique. Pourtant, tout le monde utilise aujourd'hui des téléphones, des ordinateurs et des applications. Lorsqu'un seul groupe est majoritairement présent pour imaginer et programmer ces outils, on oublie des idées, des besoins et des talents essentiels. Et cela ne concerne pas seulement les femmes : beaucoup de minorités, comme les personnes issues de milieux modestes, certaines origines, ou les personnes handicapées, sont aussi très peu représentées dans ces métiers. Résultat : leurs points de vue manquent dans la création des technologies. Parler des "oubliés du numérique", c'est donc rappeler que le numérique fonctionne mieux, est plus juste et plus utile quand tout le monde peut y participer, filles comme garçons, et quelles que soient leurs origines.

Ressource pour un adulte : Livre « Les oubliées du numérique » d'Isabelle Collet

98. Qu'est-ce que le « sharenting » ?

A) Partager des conseils ou des avis sur des produits pour enfants
B) Suivre le quotidien de familles influentes sur les réseaux sociaux
C) Quand les parents publient des infos/photos de leurs enfants sur les réseaux sociaux

Le sharenting, c'est quand des parents publient beaucoup de photos ou d'informations sur leurs enfants sur Internet, surtout sur les réseaux sociaux. Ils le font souvent pour partager des moments de leur vie, mais parfois sans penser que cela peut gêner les enfants ou mettre leur vie privée en danger. Ces photos peuvent être récupérées par des personnes malveillantes et utilisées à des fins dangereuses.
Il est important de demander l'avis des enfants et de bien réfléchir avant de poster des choses personnelles en ligne, car une fois sur Internet, c'est très difficile de les effacer complètement.

Ressource pour tous :
Grand saut dans les réseaux sociaux
(Jeu familial - MAIF)

99. Lequel de ces réseaux était le plus utilisé chez les 13-18 ans en 2023 ?

A) TikTok
B) Instagram
C) Snapchat

En 2023, TikTok est le réseau social le plus populaire chez les adolescents alors que ce réseau est particulièrement préoccupant : son algorithme peut exposer les jeunes à des contenus inappropriés et favoriser une utilisation addictive.
De nombreux experts le déconseillent aux moins de 18 ans car il peut être nocif pour la santé mentale. Il est d'ailleurs interdit en Chine, son pays d'origine !
Cette situation soulève des questions importantes sur l'impact des réseaux sociaux sur le développement des jeunes.

Source : Grandir à l'ère du numérique (Rapport Qustodio - janvier 2024)

100. C'est quoi la « bro culture » qu'on retrouve parfois dans les entreprises tech ?

A) Une ambiance « entre mecs » où ceux qui ne rentrent pas dans le groupe, surtout les filles, peuvent être mis de côté ou rabaissés
B) Des ingénieurs qui réparent du vieux matériel informatique pour le donner
C) Une nouvelle méthode de travail en équipe pour chasser les bugs informatiques

La « bro culture » désigne un phénomène particulier dans certaines entreprises du numérique. Elle se caractérise par un environnement de travail dominé par des hommes qui partagent des codes sociaux similaires, souvent liés au sport, aux jeux vidéo ou à un style de vie de fraternité. Dans ces entreprises, les décisions importantes peuvent se prendre lors de parties de baby-foot ou autour d'une bière après le travail.
Le problème principal de cette culture ? Elle crée naturellement des exclusions. Les femmes et les personnes qui ne correspondent pas à ces codes peuvent se retrouver mises à l'écart des conversations importantes, des promotions ou des projets intéressants. Par exemple, si les discussions stratégiques ont lieu pendant des matchs de foot, ceux qui n'y participent pas perdent des opportunités professionnelles.
Cette situation est particulièrement visible dans la tech. Cette culture freine la diversité et l'innovation, car elle prive les entreprises de talents variés et de perspectives différentes.

Ressource pour un adulte : Livre « Brotopia - Breaking Up the boys'club of silicon valley » d'Emily Chang


datata

101. Est-ce que l'intelligence artificielle a besoin de données pour fonctionner ?

A) Oui, les systèmes d'intelligence artificielle (IA) sont entraînés sur des informations existantes
B) Non, il faut uniquement de l'électricité pour faire fonctionner les IA
C) Non, l'intelligence artificielle dispose de toutes les connaissances et n'a pas besoin d'apprendre

L'IA a besoin d'informations pour fonctionner ! Pour qu'une IA puisse te donner une réponse, des milliers d'ordinateurs ont d'abord analysé des millions de textes : des livres, des articles de journaux, des sites web ou même des réseaux sociaux.
Ces machines ont étudié tous ces documents pour comprendre comment nous écrivons et parlons. Grâce à cet énorme travail de collecte d'informations, l'IA peut maintenant te donner des réponses qui ont du sens. Mais attention, elle peut aussi parfois se tromper ou inventer ! Sans toutes ces données, une IA ne pourrait pas fonctionner du tout !
Elle serait complètement muette et ne saurait pas quoi te répondre.

Ressources pour un adulte : Intelligence artificielle pour et par les enseignants (Mooc France Université Numérique) et Les intelligences artificielles génératives (Canotech)
Ressource pour un ado : Comment fonctionne l'intelligence artificielle ? (TiDoc')

102. Qu'est-ce qu'une donnée personnelle ?

A) Un objet qu'on m'a donné
B) Une information qui permet d'identifier une personne
C) Une information que je suis seul à connaître

Une donnée personnelle, c'est toute information qui permet de savoir qui tu es.
Ton nom et prénom sont des données personnelles évidentes, mais il y en a d'autres plus cachées : ton adresse, ton numéro de téléphone, ta date de naissance, ou même l'endroit où tu habites. Parfois, plusieurs petites informations mises ensemble peuvent permettre de t'identifier !
C'est pour ça qu'il faut bien réfléchir avant de partager ces informations sur Internet. N'hésite pas à en parler à un adulte si tu as un doute.

Ressource pour un ado :
Prudence sur Internet avec la CNIL

103. Qu'est-ce qu'un bit ?

A) Un type de virus informatique
B) Un petit ordinateur portable
C) La plus petite unité d'information en informatique

Un bit est la plus petite unité d'information qu'un ordinateur peut gérer.
Le mot « bit » vient de l'anglais « binary digit », qui veut dire « chiffre binaire ».
Un bit ne peut avoir que deux valeurs : 0 ou 1. C'est très simple, mais très puissant !
Tes équipements numériques utilisent des millions de 0 et de 1 pour stocker tes photos, tes jeux et tes messages.
Exemple : quand tu écris la lettre « A » sur ton clavier, l'ordinateur génère une série de 8 bits : 01000001. Chaque lettre, chaque couleur de pixel de ton écran, chaque son que tu entends est codé avec des combinaisons de 0 et de 1.
Les bits permettent de mesurer la taille des fichiers et la vitesse des connexions : on parle de kilobits (1000 bits), mégabits (1000 000 bits) ou gigabits (1000 000 000 bits). Plus ta connexion Internet propose de gigabits par seconde, plus tu peux télécharger vite des jeux ou des vidéos.

104. À quoi servent les traceurs cachés, appelés aussi cookies, sur les sites Internet ?

A) Télécharger et visualiser le contenu de la page
B) Se souvenir des différentes actions que tu as effectuées sur la page
C) Ils ne servent à rien

Les cookies sont de petits « pense-bêtes » invisibles que les sites Internet placent dans ton ordinateur, ton téléphone ou ta tablette ! Ils se souviennent de ce que tu fais sur le site : les pages que tu visites, ce que tu mets dans ton panier d'achat, ou même tes préférences de couleur. Grâce aux cookies, quand tu reviens sur un site, il peut te reconnaître et afficher directement ce qui t'intéresse. Mais attention : certains cookies suivent aussi ce que tu fais sur d'autres sites pour te montrer de la publicité ! Tu es influencé sans que tu t'en rendes compte. Grâce à ces cookies, c'est parfois des centaines de partenaires des sites web sur lesquels tu navigues qui peuvent récupérer des informations sur toi.
Quand tu vois des bannières qui te demandent si tu acceptes les cookies, tu peux toujours dire non aux cookies publicitaires en cliquant sur « Continuer sans accepter » ou « Refuser ».

Ressource pour un ado :
Cookies, les espions du Net (CNIL)

105. Est-ce que l'intelligence artificielle engendre une consommation d'eau importante pour fonctionner ?

A) L'IA est virtuelle, elle ne consomme pas d'eau
B) Les concepteurs ont créé des technologies qui permettent de préserver les ressources
C) En 2027, l'IA consommera l'équivalent de 4 à 6 fois la consommation annuelle en eau du Danemark

Même si l'intelligence artificielle nous semble invisible, elle a besoin de beaucoup d'eau pour fonctionner ! Quand tu utilises ChatGPT ou une autre IA, ton message voyage jusqu'à d'énormes data centers. Ces data centers chauffent beaucoup quand ils travaillent, alors on doit les refroidir avec de l'eau, sinon ils grillent ! En plus, pour fabriquer tous ces équipements et produire l'électricité qui les fait marcher, on utilise encore plus d'eau. Quand les gens qui habitent près des data centers voient leur eau disparaître pour refroidir les machines, ils s'inquiètent. C'est pourquoi il faut réfléchir avant d'utiliser l'IA : chaque question qu'on lui pose consomme de l'eau précieuse !

Source : Quel est l'impact environnemental d'une IA générative ? DRANE Île-de-France

106. Est-ce que l'intelligence artificielle peut se tromper ?

A) Oui, si elle a été entraînée avec des informations qui étaient incorrectes
B) Non, parce qu'elle connaît tout ce qui existe sur Internet
C) Non, car les ordinateurs ne font jamais d'erreur

Oui, l'intelligence artificielle peut se tromper ! Elle peut même inventer des choses fausses en ayant l'air très sûre d'elle. Les experts appellent ça une « hallucination » ! L'IA apprend en analysant des millions de textes. Si certains de ces textes contiennent des erreurs ou des mensonges, l'IA les apprend aussi. Elle peut alors répéter ces erreurs plus tard. Par exemple, si l'IA a lu beaucoup de textes qui disent que les licornes existent, elle pourrait te dire que c'est vrai ! C'est pour ça qu'il faut toujours vérifier les réponses de l'IA avec d'autres sources. Ne crois jamais tout ce qu'elle dit, même si elle semble très convaincante. L'IA est un outil formidable, mais elle n'est pas parfaite !

107. À quelle époque commence-t-on à entendre parler d'intelligence artificielle ?

A) Dans les années 1950
B) Depuis que les smartphones existent
C) Depuis la création de TikTok

L'intelligence artificielle est née bien avant tes grands-parents ! La notion d'intelligence artificielle apparaît au milieu des années 1950, dans la foulée des réflexions du mathématicien Alan Turing, qui se demandait si un ordinateur saurait un jour « penser », ou s'il n'était capable que d'un « jeu d'imitation ». En 1956, un scientifique américain appelé John McCarthy a inventé le terme « intelligence artificielle ». Il voulait créer des machines capables de réfléchir. À cette époque, les ordinateurs étaient énormes et remplissaient des pièces entières ! Ils ne savaient faire que des calculs très simples.
Pendant longtemps, l'IA a progressé lentement : les ordinateurs n'étaient pas assez puissants. Mais depuis quelques années, tout s'accélère ! Les ordinateurs sont devenus super rapides et peuvent traiter énormément d'informations. C'est pourquoi tu entends maintenant parler d'IA partout : dans ton téléphone, tes jeux vidéo et même pour t'aider à faire tes devoirs !

Source : Intelligence artificielle (Wikipédia)
Ressource pour un adulte : Livre - Les défis de l'intelligence artificielle (Édition FIRST)
Ressource pour un ado : Qu'est-ce que c'est l'intelligence artificielle ? (TiDoc')

108. Est-ce que je peux utiliser l'intelligence artificielle pour faire mes devoirs à ma place ?

A) Oui, demain nous n'aurons plus besoin de faire nos devoirs
B) Non, l'IA ne doit pas faire mes devoirs à ma place, mais elle peut m'aider à construire et approfondir ma réflexion
C) Non, on ne doit jamais se servir de l'IA

L'IA peut t'aider, mais elle ne doit pas faire tes devoirs à ta place ! Utilise-la plutôt comme un assistant. Tu peux lui demander d'expliquer quelque chose que tu ne comprends pas, de te donner des idées pour commencer un devoir, ou de vérifier si tu as oublié des points importants. Mais attention, l'IA peut parfois se tromper ou inventer des choses. Tu dois vérifier chaque information. De plus, tes enseignants veulent voir TON travail et TA compréhension, pas celle d'une machine.
Utilise-la pour mieux apprendre, pas pour éviter d'apprendre.
Pose-lui des questions, demande-lui de t'expliquer, mais écris tes devoirs toujours avec tes propres mots et tes propres idées !

Source : Les intelligences artificielles et leurs usages en éducation - Eduscol
Ressources pour les adultes : IA et éducation - faut-il s'inquiéter pour nos enfants ? (Génération Parents) et www.canotech.fr/serie/lintelligence-artificielle-au-service-de-leducation

109. Quels types de ressources consomme une IA ?

A) De l'eau, de l'électricité et des métaux
B) De l'air
C) De la lumière

L'intelligence artificielle n'est pas magique ! D'abord, elle utilise beaucoup d'électricité pour faire tourner d'énormes serveurs dans des bâtiments appelés « centres de données ». Ces serveurs chauffent tellement qu'il faut les refroidir avec de l'eau.
Ensuite, pour fonctionner, l'IA a aussi besoin de puces ultra-perfectionnées.
La majorité de ces puces est produite par la société Nvidia. Pour fabriquer tous ces équipements, il faut aussi des métaux spéciaux comme le lithium, le cobalt ou des terres rares. Ces métaux sont extraits de mines partout dans le monde. Quand tu utilises une IA, tu déclenches des calculs dans ces centres de données qui consomment autant d'électricité qu'une petite ville !
Certains scientifiques cherchent des moyens de rendre l'IA moins gourmande en énergie mais ce n'est sans doute pas pour demain !

Ressource : Quel est l'impact environnemental d'une IA générative ? DRANE Île-de-France

110. Qu'est-ce qu'une hallucination algorithmique ?

A) C'est quand tu crois voir une image sur l'écran alors qu'elle n'existe pas
B) C'est quand tu as l'impression que ton téléphone vibre alors que ce n'est pas le cas
C) C'est une réponse fausse ou trompeuse qui est présentée comme une vérité par l'intelligence artificielle

Les intelligences artificielles ont un défaut majeur : elles détestent répondre « je ne sais pas » ! Même quand elles n'ont pas la bonne réponse, elles inventent quelque chose qui semble logique et te la présentent avec une assurance totale. C'est ce qu'on appelle une hallucination algorithmique. Le problème, c'est que ces « hallucinations » peuvent propager des informations complètement fausses sur des sujets sérieux comme la santé, l'histoire ou les sciences. Pour y remédier, beaucoup de recherches sont effectuées pour améliorer la qualité des réponses et leur fiabilité. À ce jour, aucune solution n'a encore été trouvée pour éliminer entièrement les hallucinations. L'IA mixe des informations qu'elle a apprises et crée des réponses qui semblent cohérentes mais sont totalement inventées. C'est pourquoi il faut toujours vérifier les infos données par une IA avec d'autres sources fiables, surtout pour des sujets importants !

Ressource pour tous : Intelligences artificielles - « On ne peut pas leur faire confiance » (Public Sénat)

111. Qu'est-ce qu'un hackathon ?

A) Un virus informatique très dangereux qui attaque les ordinateurs
B) Un événement où des équipes créent rapidement des projets numériques
C) Un jeu vidéo où l'on doit pirater des systèmes

Un hackathon est un événement passionnant où des équipes se réunissent pendant quelques heures ou quelques jours pour créer ensemble des projets numériques !
Le mot vient de « hack » (bricoler, créer) et « marathon » (course longue).
Pendant un hackathon, des programmeurs, des designers, des étudiants et parfois même des enfants travaillent ensemble pour résoudre un problème ou créer quelque chose de nouveau. Par exemple, ils peuvent créer une application pour aider les personnes âgées, un jeu éducatif ou un site web pour protéger l'environnement.
L'objectif est de développer rapidement une solution créative ! Les participants partagent leurs idées, leurs compétences et apprennent les uns des autres.
À la fin, chaque équipe présente son projet et parfois il y a même des prix pour les meilleures créations. Les hackathons permettent de découvrir la programmation, le design et le travail en équipe. C'est une excellente façon d'apprendre en s'amusant et d'innover !

Ressource pour un adulte : Le Hackathon pédagogique (Réseau Canopé)

112. Un assistant vocal fonctionne grâce à :

A) De la magie noire
B) La reconnaissance vocale et le traitement automatique du langage
C) Une personne bien cachée qui te répond

Les assistants vocaux utilisent deux technologies intelligentes qui travaillent ensemble.
L'assistant vocal utilise d'abord, la « reconnaissance vocale » : quand tu parles à ton appareil, il transforme ta voix en mots écrits sur un ordinateur. Ensuite, l'ordinateur analyse ces mots pour comprendre ce que tu veux vraiment dire. Il cherche dans sa mémoire géante pour trouver la meilleure réponse, puis il la transforme à nouveau en voix pour te parler. C'est ce qu'on appelle le « traitement automatique du langage ».
Tout ça se passe en quelques secondes ! L'assistant a appris à faire ça en « regardant » des millions de conversations entre humains. Plus il entend de questions et de réponses, plus il devient « intelligent ».
C'est une forme d'intelligence artificielle qui s'améliore sans cesse en apprenant de nos façons de parler.

Ressource pour un adulte : La reconnaissance vocale : vous allez tout comprendre (Monde Numérique)
Ressource pour un ado : Est-ce vrai que l'intelligence artificielle sait parler ? (Lumni)

113. Qui sont les GAFAM ?

A) Une équipe de super-héros du numérique
B) Des entreprises très puissantes sur Internet
C) Des lutins qui gèrent les mails

GAFAM est le nom qu'on donne aux cinq plus grandes entreprises américaines du numérique : Google, Apple, Facebook (maintenant appelé Meta), Amazon et Microsoft. Ces entreprises sont partout dans ta vie quotidienne !
Tu utilises peut-être YouTube ou Gmail (Google), un iPhone ou un iPad (Apple), WhatsApp ou Instagram (Meta), tu commandes sur Amazon, ou tu joues à Minecraft (Microsoft).
Ces entreprises sont si puissantes qu'elles peuvent influencer notre utilisation d'Internet. Elles collectent beaucoup d'informations sur nous quand nous utilisons leurs services : ce qu'on recherche, ce qu'on aime, où on va. Et, elles s'enrichissent avec les données que nous leur transmettons parfois sans vraiment y penser.

Ressource pour un adulte : Les GAFAM et les BATX | Expliquez-moi. (Hachette Éducation)

114. Une empreinte numérique, c'est :

A) Une trace de doigt sur ton écran
B) Une trace laissée par tout ce que tu fais en ligne
C) Une information enregistrée seulement quand tu acceptes une notification

Ton empreinte numérique, c'est comme les traces de pas que tu laisses quand tu marches dans la neige, sauf que c'est sur Internet !
Chaque fois que tu visites un site, publies une photo, écris un commentaire, likes un post ou cherches quelque chose, tu laisses des traces numériques. Ces informations s'accumulent et forment ton « portrait numérique » : qui tu es, ce que tu aimes, où tu vas, avec qui tu discutes... Le problème, c'est que ces traces restent très longtemps, parfois pour toujours ! Des années plus tard, quelqu'un pourrait retrouver des photos embarrassantes que tu avais publiées ou des commentaires que tu regrettes.
C'est pour ça qu'il faut réfléchir avant de publier quelque chose !

115. Les pseudonymes te protègent :

A) De tous les dangers
B) Partiellement, surtout si tu révèles quand même des infos personnelles
C) Totalement, même si tu partages ton adresse

Utiliser un pseudonyme (un faux nom) sur Internet, c'est une bonne idée pour protéger ta vie privée ! Au lieu d'utiliser ton vrai nom, tu peux choisir « SupperGamer2012 » ou « LicorneMagique ». Mais attention : un pseudonyme ne te rend pas invisible ! Si tu partages ton adresse, le nom de ton école, des photos de ta chambre, les gens peuvent quand même découvrir qui tu es vraiment. Pour être protégé, il faut combiner plusieurs techniques : utiliser un pseudonyme, ne jamais donner d'informations personnelles (adresse, téléphone, école), faire attention aux photos qu'on partage, et bien régler ses paramètres de confidentialité. Surtout, rappelle-toi qu'un pseudonyme ne doit jamais servir à faire du mal ou à harceler quelqu'un ! Il doit servir à te protéger, mais ne remplace pas la prudence et les conseils de tes parents !

116. Quand une IA génère une réponse, sur quoi se base-t-elle principalement ?

A) Sur des millions de médias (textes, images, sons) créés par des humains
B) Sur Wikipédia
C) Sur des éléments qu'elle invente complètement toute seule

Les IA comme ChatGPT ou Midjourney apprennent en analysant des millions d'images, de livres, d'articles ou de dessins créés par des humains et disponibles sur Internet. Ces œuvres sont souvent protégées par le droit d'auteur, ce qui signifie qu'elles appartiennent à quelqu'un ! Les entreprises qui créent ces IA affirment qu'elles ont le droit d'utiliser ces contenus pour entraîner leurs programmes, mais beaucoup d'artistes et d'écrivains ne sont pas d'accord. Certains journaux comme Le Monde ont signé des contrats avec OpenAI pour être payés quand leurs articles sont utilisés.
D'autres, comme le New York Times, ont porté plainte car ils estiment que leurs textes ont été utilisés sans permission. En Europe, une nouvelle loi oblige les entreprises d'IA à expliquer quelles données elles utilisent mais cette transparence est très difficile à contrôler. Un autre problème voit le jour : les IA commencent à utiliser du contenu créé par d'autres IA ! Des études montrent que quand une IA apprend sur des textes ou images générées par des IA, ses réponses deviennent de plus en plus bizarres et finissent par
ne plus avoir de sens.

117. Qu'est-ce qu'une « smart city » (ville intelligente) ?

A) Une ville où tous les habitants sont très intelligents
B) Une ville qui utilise Internet et des capteurs pour mieux fonctionner et aider ses habitants
C) Une ville où les robots ont remplacé tous les humains pour diriger la ville

Une ville intelligente (smart city en anglais), c'est une ville qui utilise les nouvelles technologies pour améliorer la vie de ses habitants. Elle connecte différents objets et systèmes grâce à Internet pour mieux fonctionner. Par exemple, des capteurs dans les rues peuvent mesurer la pollution, les feux de circulation s'adaptent au trafic en temps réel, les poubelles signalent quand elles sont pleines, et les lampadaires s'éclairent seulement quand quelqu'un passe. Les citoyens peuvent utiliser des applications pour signaler des problèmes, payer le stationnement ou connaître les horaires de bus en direct. L'objectif est d'économiser l'énergie, de réduire la pollution, d'améliorer les transports et de rendre les services publics plus efficaces.
Mais attention : ces technologies collectent beaucoup de données sur les habitants et ont un fort impact sur l'environnement. Il faut réfléchir à l'équilibre entre les avantages (meilleurs services) et les risques (protection de la vie privée, pollution).

Ressource pour tous :
Futur city : la ville de demain (Lumni)

118. Que peut révéler l'analyse des métadonnées de tes photos ?

A) Le nombre de likes que tu vas recevoir
B) Ta localisation exacte, l'heure, le type d'appareil et bien plus
C) L'âge de la personne sur la photo

Les métadonnées de tes photos contiennent une quantité impressionnante d'informations cachées. Chaque photo prise avec ton smartphone enregistre automatiquement : la date et l'heure exactes, les coordonnées GPS, le modèle de ton téléphone, les paramètres de l'appareil photo… Ces données permettent de reconstituer tes habitudes : où tu habites, où tu vas à l'école, quels lieux tu fréquentes et à quels moments.
Des cybercriminels pourraient utiliser ces informations pour te localiser ou planifier des cambriolages quand tu n'es pas chez toi. Heureusement, la plupart des réseaux sociaux suppriment automatiquement ces métadonnées quand tu publies une photo, mais ce n'est pas toujours le cas. Pense à désactiver la géolocalisation dans les paramètres
de ton appareil photo.

119. Quelle est la principale différence entre une IA classique et une IA générative ?

A) L'IA générative fait apparaître des objets dans la vraie vie
B) L'IA générative fonctionne uniquement quand il fait nuit
C) L'IA générative peut créer du contenu nouveau, l'IA classique ne fait qu'analyser

L'IA classique et l'IA générative sont deux types différents d'intelligence artificielle. L'IA classique excelle dans l'analyse et la reconnaissance : elle peut regarder une photo et dire « c'est un chat », ou analyser des données pour trouver des tendances. Elle résout des problèmes précis avec des règles claires. L'IA générative va plus loin : elle peut créer du contenu totalement nouveau ! Elle écrit des histoires, dessine des images qui n'ont jamais existé ou compose de la musique originale.
Par exemple, ChatGPT est une IA générative car elle génère du texte nouveau à chaque conversation. Les deux types d'IA sont utiles mais pour des tâches différentes.
Aujourd'hui, les IA génératives font beaucoup parler d'elles car elles peuvent générer des choses surprenantes mais le problème c'est que l'IA générative consomme beaucoup plus d'énergie que l'IA classique. Elle nécessite une grande puissance de calcul, entraînant un important besoin en énergie et par conséquent un fort impact négatif
sur l'environnement.

120. Qu'est-ce que les Small Language Models (SLM) ?

A) Des mini-robots qui parlent avec une petite voix
B) Des programmes pour apprendre les langues étrangères
C) Des modèles d'IA compacts qui fonctionnent sur smartphones et ordinateurs

Les Small Language Models (SLM) sont des modèles d'intelligence artificielle compacts qui peuvent traiter et générer du langage naturel, mais contrairement aux grands modèles comme ChatGPT, ils sont conçus pour fonctionner sur des appareils avec moins de puissance. Ton smartphone contient probablement déjà plusieurs SLM !
Ils peuvent tourner directement sur tes appareils mobiles, tablettes ou montres connectées sans avoir besoin d'une connexion Internet constante. Ces modèles ont entre quelques millions et quelques milliards de paramètres, alors que les grands modèles en comptent des centaines de milliards. Cette différence les rend plus rapides et mieux adaptés aux besoins spécifiques. Cerise sur le gâteau : ils consomment moins d'énergie !

121. Qui était Ada Lovelace ?

A) Une influenceuse célèbre sur les réseaux sociaux
B) La première programmeuse de l'histoire
C) Un robot inventé pour aider les scientifiques

Ada Lovelace était une mathématicienne britannique extraordinaire du XIXe siècle. Née en 1815, elle est considérée comme la toute première programmeuse de l'histoire ! Ada Lovelace a été la première personne à comprendre que les « machines analytiques » (les ancêtres des ordinateurs) pourraient faire bien plus que des calculs : elle a écrit le premier algorithme (une suite d'instructions) destiné à être exécuté par une machine. Elle avait même prédit que les ordinateurs pourraient un jour créer de la musique et de l'art ! Malheureusement, elle est morte très jeune, à 36 ans, et ses idées visionnaires ont été oubliées pendant longtemps.
Désormais, le travail d'Ada Lovelace est reconnu mondialement : le langage de programmation « Ada » porte son nom, et chaque deuxième mardi d'octobre, on célèbre la « Journée Ada Lovelace » pour mettre en avant les femmes en science et technologie. Alors qu'en 2023, seulement 16 % de femmes sont employées dans les métiers de la tech, l'exemple d'Ada Lovelace nous montre que les femmes ont toujours été importantes dans l'histoire de l'informatique !

Source : La Femme Invisible dans le numérique (Haut Conseil à l'Égalité entre les femmes et les hommes)
Ressource pour un adulte : 9 femmes scientifiques remarquables (Radio France)
Ressource pour un ado : Change Mak'Her (startup for kids)

122. Qu'est-ce qu'un prompt ?

A) Un type d'ordinateur très rapide spécialisé dans l'IA
B) Une instruction ou question qu'on donne à une IA pour obtenir une réponse
C) Un logiciel qui protège l'IA contre les virus

Un prompt, c'est tout simplement la question ou l'instruction que tu donnes à une IA pour qu'elle te réponde ! Le mot vient de l'anglais et signifie « inciter » ou « encourager ». Par exemple, quand tu écris « Explique-moi les dinosaures » à une IA, cette phrase est ton prompt. Plus ton prompt est précis et clair, meilleure sera la réponse de l'IA.
Par exemple, au lieu de dire « Explique-moi les dinosaures », tu peux dire « Peux-tu me donner une présentation détaillée des dinosaures couvrant leur classification, les périodes géologiques où ils ont vécu, leur morphologie, leur mode de vie et les causes de leur disparition ? ». Certaines personnes deviennent même spécialistes dans l'art de créer de bons prompts : on les appelle des « ingénieurs de prompt » !
Ils savent exactement comment parler aux IA pour obtenir les meilleures réponses possibles. Un bon prompt peut faire la différence entre une réponse banale et une réponse vraiment utile.

123. Qu'est-ce que la « Digi-romance » ou romance digitale ?

A) Un nouveau type de jeu vidéo sur l'amour
B) Une application pour rencontrer des personnes en ligne
C) Des relations amoureuses ou amicales avec des personnages créés par intelligence artificielle

La Digi-romance, c'est quand des personnes développent des sentiments pour des personnages virtuels créés par des intelligences artificielles.
Ces compagnons numériques sont conçus pour apprendre à s'adapter aux personnalités et préférences de chacun. C'est l'histoire du film « Her » sorti en 2013, où un homme tombe amoureux de son assistante virtuelle. Aujourd'hui, certaines applications permettent de créer des « petits amis » ou « petites amies » virtuels avec qui on peut discuter.
Ces IA peuvent sembler très réelles car elles se souviennent de vos conversations et s'adaptent à votre personnalité. Cependant, il est important de se rappeler que ces personnages ne sont pas de vraies personnes : ils ne peuvent pas avoir de sentiments. Les amis et les vraies relations apportent quelque chose qu'aucune IA ne peut donner : de l'empathie authentique et des expériences partagées réelles.

Ressource pour un adulte : Digi-romance - une relation amoureuse avec une IA est-elle possible ? (France Inter)

124. Pourquoi parle-t-on de big data ?

A) Parce que les ordinateurs sont de plus en plus gros
B) Parce que les disques durs prennent beaucoup de place
C) Parce qu'on produit énormément de données chaque jour

Chaque jour, nous créons une quantité gigantesque d'informations !
Quand tu envoies un message, regardes une vidéo sur Internet, fais des recherches ou utilises une application, tu crées des données. Toutes ces informations s'accumulent dans des centres de données.
On appelle ça « big data » car « big » veut dire « gros » en anglais et « data » signifie « données ». Les prévisions estiment que le volume total de données dans le monde atteindra 394 zettaoctets d'ici 2028 soit 394 000 milliards de milliards d'octets. Ça donne le tournis ! Ces énormes quantités d'informations permettent aux entreprises et aux chercheurs de mieux comprendre comment fonctionnent les gens, la nature ou les machines. Par exemple, grâce au big data, on peut prévoir la météo plus précisément ou aider les médecins à soigner des maladies !

Source : Big data - statistics & facts (Statista)
Ressource pour tous : Comprendre la DATA en 5 minutes (Bande de codeurs)

125. En quoi consiste le métier de data journaliste ?

A) À créer des fausses informations à partir de données inventées
B) À analyser des données pour révéler des informations importantes
C) À réparer les ordinateurs des journalistes quand ils tombent en panne

Un data journaliste est un journaliste spécialisé qui utilise des données numériques pour transmettre des informations ! Il exploite des ensembles de données complexes pour trouver des informations cachées et donner une nouvelle présentation de l'information. Par exemple, il peut analyser les chiffres sur la pollution de l'air dans ta ville pour découvrir quels quartiers sont les plus touchés. Le data journaliste collecte des milliers de chiffres, les trie avec des logiciels spéciaux, puis les transforme en graphiques colorés, cartes interactives ou infographies faciles à comprendre. Son travail aide les citoyens à mieux comprendre le monde qui les entoure grâce aux données ! Il doit toujours vérifier que ses sources sont fiables et respecter la vie privée des personnes. Quand tu vois un article avec de jolis graphiques qui expliquent combien d'enfants utilisent Internet dans différents pays par exemple, c'est souvent le travail d'un data journaliste !

126. Où peut-on trouver de l'intelligence artificielle ?

A) Dans les recommandations de vidéos et de contenus personnalisés
B) Uniquement dans les robots industriels très spécialisés
C) Uniquement dans les superordinateurs utilisés par les scientifiques

L'intelligence artificielle (IA) n'est pas de la science-fiction, elle fait déjà partie de ton quotidien depuis un certain temps ! Quand tu scrolles sur TikTok ou Instagram, l'IA analyse ce que tu regardes le plus longtemps pour te proposer des vidéos qui vont te plaire. Dans les voitures modernes, l'IA aide à freiner automatiquement si un obstacle apparaît ou guide le système GPS pour éviter les embouteillages. Sur YouTube, elle recommande des vidéos selon tes goûts et détecte même les contenus inappropriés. Mais attention, l'IA peut aussi créer des « deepfakes » : des vidéos où quelqu'un semble dire ou faire quelque chose qu'il n'a jamais fait par exemple. Face aux contenus en ligne, tu dois développer ton œil critique. L'IA est partout : dans ton smartphone, tes jeux vidéo, les assistants vocaux... Elle nous aide au quotidien, mais il faut apprendre à la reconnaître et à comprendre ses limites.

127. Combien de temps les images de vidéosurveillance peuvent-elles être conservées ?

A) 1 mois maximum
B) 3 mois maximum
C) Éternellement

Quand une caméra te filme dans la rue ou dans un magasin, ton image n'est pas stockée éternellement. La loi impose une durée maximale de conservation d'un mois. Pourquoi cette limite ? Parce que conserver des images de personnes plus longtemps créerait une surveillance excessive de nos vies. En pratique, quelques jours suffisent en général aux autorités pour vérifier s'il y a eu un incident. Par exemple, si un vol a lieu dans un magasin, les responsables peuvent consulter les images jusqu'au lendemain ou surlendemain pour identifier ce qui s'est passé. Garder ton image pendant des mois serait disproportionné par rapport à cet objectif. Cette règle protège ta vie privée en évitant qu'une base de données gigantesque de tes déplacements se constitue.
Un registre précis doit être tenu sur les personnes qui consultent les images, quand et pourquoi.
Ce registre est conservé 3 ans maximum pour contrôler les abus.

Source : La vidéoprotection (CNIL)

Ressource pour un adulte :
Dans leurs yeux : la France à l'heure de la reconnaissance faciale (Amnesty France)

128. En matière d'intelligence artificielle, qu'est-ce qu'un biais ?

A) Un outil de mesure
B) Une erreur de jugement
C) Une réponse trop longue

L'IA apprend à partir de données créées par des humains. Si ces données ne représentent pas la réalité de manière équitable, l'IA va reproduire ces erreurs.
Par exemple, si on nourrit une IA uniquement avec des photos de médecins hommes, elle pourrait croire que tous les médecins sont des hommes. C'est faux ! Ces biais peuvent toucher tous les domaines : genre, origine, âge... Autre exemple : certains systèmes de reconnaissance faciale fonctionnent moins bien sur les peaux foncées parce qu'ils ont été entraînés principalement sur des visages à peau claire. Ces biais peuvent avoir des conséquences graves : refus de prêt bancaire, erreurs de diagnostic médical, discrimination à l'embauche. C'est pourquoi il faut toujours garder un œil critique sur les réponses des IA et se rappeler qu'elles reflètent les préjugés de ceux qui les ont créées.

129. L'IA apprend grâce à des données étiquetées. Lequel de ces exemples est une donnée étiquetée utile pour l'IA ?

A) Un livre avec un marque-page à la page 127
B) Un enregistrement audio de musique rock avec l'étiquette « rock »
C) Une clé USB avec un porte-clés coloré

Étiqueter les données revient à donner un mode d'emploi à l'IA ! Une donnée étiquetée, c'est une information (photo, texte, son) accompagnée d'une explication de ce qu'elle représente. Cette technique s'appelle le « machine learning » ou apprentissage automatique. Quand on montre 1000 photos de chats avec l'étiquette « chat » à une IA, elle apprend à reconnaître les chats. Les données étiquetées sont essentielles pour l'apprentissage supervisé, où l'IA a besoin d'un « professeur » pour comprendre ce qu'elle observe. Sans ces étiquettes, l'IA ne pourrait pas apprendre efficacement.
Mais attention : derrière cette technologie se cachent souvent des travailleurs exploités ! Dans certains pays, des personnes sont très mal payées pour faire ce travail répétitif. Ces « travailleurs invisibles » passent leurs journées à classer des millions d'images ou de textes pour entraîner nos IA.

Ressource pour un ado : Machine Learning for Kids - Expériences pratiques d'étiquetage (tice-education)

130. Qu'est-ce que l'Open data ?

A) Des données accessibles librement pour être consultées et réutilisées
B) Des données partagées seulement entre administrations publiques
C) Des données publiées en ligne mais réservées à un usage commercial

On appelle open data des informations mises à disposition par des gouvernements, des entreprises ou des citoyens pouvant être utilisées librement par tous.
Grâce à l'open data, tu peux connaître les horaires de bus de ta ville, la qualité de l'air, les résultats électoraux ou même la localisation des fontaines publiques. Ces données permettent de créer des applications utiles : par exemple, une app qui calcule ton itinéraire en transport en commun utilise les données ouvertes des horaires.
L'open Data favorise aussi la transparence démocratique : tu peux voir comment l'argent public est dépensé. En Europe, pour protéger la vie privée, les données personnelles ne peuvent pas être ouvertes. Pour résumer, l'open data, c'est un moyen de partager la connaissance pour que chacun puisse contribuer à améliorer la société.

Ressource pour un adulte : Data.gouv.fr - Portail français de l'opendata
Ressource pour tous : Éduquer aux données pour développer des communs (Réseau Canopé)

131. Qu'est-ce qu'un data center ?

A) Un outil de géolocalisation des centres commerciaux
B) Une installation physique conçue pour héberger les données d'une ou de plusieurs organisations
C) Un institut d'enquête sur l'utilisation des données numériques

Un data center ou centre de données, c'est un immense entrepôt climatisé rempli de milliers de serveurs qui stockent et traitent nos données numériques 24 h/24.
Ces data centers stockent tes photos sur le cloud, font tourner tes jeux en ligne et permettent à tes messages de traverser le monde en quelques secondes.
La plupart se trouvent à l'étranger : les géants américains (Google, Meta, Amazon) dominent le marché mondial. Cette localisation géographique pose un vrai défi juridique. Tes données personnelles stockées aux États-Unis sont soumises aux règles américaines. Concrètement, les autorités américaines peuvent accéder à tes informations sans que tu le saches. C'est pourquoi la France souhaite développer sa souveraineté numérique avec des data centers locaux. En plus de cette complexité juridique, ils consomment beaucoup d'électricité et nécessitent d'énormes quantités d'eau.

Source : Data centers : la face pas si cachée du numérique (Ademe)

132. Quel est le rôle principal de la CNIL en France ?

A) Protéger les données personnelles et les droits liés à leur usage
B) Gérer l'infrastructure des réseaux Internet
C) Contrôler uniquement les sites de commerce en ligne

La CNIL (Commission Nationale de l'Informatique et des Libertés) est le gendarme français des données personnelles. Créée en 1978, elle veille à ce que tes informations personnelles soient respectées dans le monde numérique. Ses quatre missions principales : informer les citoyens de leurs droits, accompagner les entreprises pour qu'elles respectent la loi, anticiper les évolutions technologiques et contrôler/sanctionner les abus. Concrètement, si une application collecte tes données sans ton consentement, si un site web ne respecte pas ton droit à l'effacement ou si une entreprise subit une fuite de données personnelles, la CNIL peut intervenir. Elle peut infliger des amendes
colossales : Google a écopé de 150 millions d'euros en 2021 pour manque de transparence. La CNIL produit aussi des guides pratiques pour t'aider à protéger ta vie privée numérique.

Source : Clôture de l'injonction prononcée à l'encontre de GOOGLE (CNIL)
Ressource pour tous : CNIL

133. Est-ce que les IA doivent respecter les lois, tout comme les humains ?

A) Oui, car elles sont considérées comme des personnes juridiques
B) Oui, mais ce sont les humains qui les conçoivent et les utilisent qui en sont responsables
C) Non, car elles n'agissent que sur des données publiques

Les intelligences artificielles ne sont pas des personnes qui peuvent décider de respecter ou non les lois. Ce sont des outils technologiques créés par des humains. Tout comme un marteau ne peut pas être tenu responsable s'il casse quelque chose, une IA ne peut pas être responsable de ses actions. Ce sont les personnes qui les développent, les programment et les utilisent qui doivent s'assurer qu'elles respectent les règles. Les entreprises qui créent des IA ont la responsabilité de les concevoir pour protéger ta vie privée, éviter les discriminations et garantir ta sécurité.
La loi pose des limites claires pour protéger tout le monde et assurer le vivre ensemble.

134. Que peut-il se passer si une entreprise utilise une IA pour trier les candidatures lors d'un recrutement ?

A) L'IA garantit une évaluation totalement neutre et identique pour chaque candidat
B) L'IA sélectionne automatiquement les CV les mieux rédigés, sans possibilité d'erreur
C) L'IA peut reproduire ou amplifier les biais présents dans les données sur lesquelles elle a été entraînée

Le problème avec l'IA dans le recrutement, c'est qu'elle reproduit et amplifie les biais. Dans ce cas, un biais, est une tendance à favoriser certaines personnes par rapport à d'autres de manière injuste. L'IA apprend à partir de données du passé. Si une entreprise a historiquement recruté plus d'hommes que de femmes, l'IA va « apprendre » que les hommes sont de meilleurs candidats et continuera à les favoriser. Elle va éliminer des candidatures de personnes déjà sous-représentées. Amazon a par exemple dû abandonner son système de recrutement automatique car il discriminait systématiquement les femmes. L'IA avait analysé les CV des 10 dernières années et comme la plupart des recrutés étaient des hommes, elle a conclu que les candidatures masculines étaient meilleures.

Source : Votre candidature a été rejetée. Signé une IA (L'ADN)

135. Qu'est-ce qu'un « deep fake » ?

A) Une vidéo modifiée par IA pour imiter une personne réelle
B) Un logiciel spécialisé dans la détection de fausses vidéos
C) Une technique de montage utilisée uniquement au cinéma

Un deepfake (ou hypertrucage en français), c'est quand l'intelligence artificielle modifie une vidéo, une photo ou un enregistrement audio pour faire dire ou faire quelque chose à quelqu'un qu'il n'a jamais dit ou fait. Tu peux voir une vidéo d'une célébrité qui semble dire des choses choquantes, mais en réalité, c'est complètement fabriqué par l'IA.
Ces fausses vidéos deviennent de plus en plus réalistes et difficiles à détecter.
Elles sont souvent utilisées pour nuire à la réputation des personnes ou pour propager de fausses informations. C'est pourquoi il faut toujours rester critique face aux contenus qu'on voit sur les réseaux sociaux.

Ressource pour tous : Cette (fausse) pub pour Liquid Death devenue virale a été 100 % réalisée avec l'IA (Creapills)



Ressource pour un ado :
Découvre les deepfakes avec Ewa Kijak (Lumni)

136. Qu'est-ce que le RGPD ?

A) Un règlement européen sur la protection des données personnelles
B) Un logiciel qui bloque automatiquement toutes les fuites de données
C) Un recueil de bonnes pratiques sans valeur juridique

Le RGPD (Règlement Général sur la Protection des Données) n'a rien de magique, mais c'est un outil puissant pour protéger ta vie privée sur Internet.
C'est une loi européenne qui oblige les sites web et les applications à te demander ton accord avant de collecter tes informations personnelles. Grâce au RGPD, tu as le droit de savoir quelles données les entreprises collectent sur toi, pourquoi elles le font et tu peux même demander qu'elles les suppriment. Tu as sûrement déjà vu ces fenêtres qui apparaissent sur les sites web pour te demander d'accepter les cookies : c'est le RGPD en action !
Cette loi donne aux citoyens européens plus de contrôle sur leurs données personnelles et oblige les entreprises à être plus transparentes sur ce qu'elles font avec tes informations.



Ressource pour un ado :
Quizz Ta vie privée, c'est secret ! (Les Incollables)

137. Qu'est-ce qu'un ordinateur quantique ?

A) Un robot qui peut voyager dans le temps pour prédire le futur
B) Un ordinateur qui fait des calculs en utilisant seulement les chiffres 0 et 1
C) Un ordinateur super-puissant qui utilise les propriétés étonnantes des particules

Un ordinateur quantique est un type d'ordinateur révolutionnaire qui utilise les propriétés fascinantes des particules les plus petites de l'univers ! Contrairement à ton ordinateur habituel qui traite les informations avec des bits (soit 0, soit 1), l'ordinateur quantique utilise des « qubits » qui peuvent être 0 et 1 simultanément ! Cette propriété incroyable lui permet de tester des millions de possibilités en même temps. Pour comprendre sa puissance : là où ton ordinateur mettrait des années à résoudre certains problèmes complexes, l'ordinateur quantique pourrait les résoudre en quelques minutes !
Ces machines extraordinaires pourraient transformer l'intelligence artificielle en lui donnant une puissance de calcul phénoménale. Elles pourraient aussi améliorer la sécurité de tes données personnelles en créant des codes de protection ultrasophistiqués. Aujourd'hui, les scientifiques travaillent encore pour perfectionner cette technologie du futur !

Ressource pour tous : C'est quoi un ordinateur quantique ? (Dr Nozman)

138. Qu'est-ce qu'une IA de confiance ?

A) Une IA fiable qui ne se trompe jamais
B) Une IA à qui je peux confier mes problèmes et mes états d'âme
C) Une IA qui respecte des principes éthiques basés sur les droits fondamentaux

Une IA de confiance n'est pas une IA qui ne se trompe jamais (ça n'existe pas !), mais une IA qui a été conçue en respectant des principes éthiques importants.
Elle doit être transparente sur son fonctionnement, respecter ta vie privée, éviter les discriminations et être sûre. L'éthique et le numérique vont de pair : une IA éthique respecte tes droits fondamentaux et ne reproduit pas les préjugés de la société.
Par exemple, elle ne doit pas discriminer les gens selon leur origine, leur genre ou leur religion. Une IA de confiance doit aussi pouvoir expliquer ses décisions et être contrôlée par des humains. L'UNESCO a même créé des recommandations internationales pour s'assurer que l'IA respecte les droits humains et les libertés fondamentales.
Sans ces garde-fous éthiques, l'IA risque d'alimenter les divisions et de menacer nos droits.

Ressource pour un adulte : Recommandation sur l'éthique de l'intelligence artificielle (UNESCO)

139. Combien y a-t-il environ de requêtes ChatGPT chaque jour dans le monde en 2025 ?

A) 1 million
B) 10 millions
C) 1 milliard

En 2025, ChatGPT reçoit environ 1 milliard de requêtes par jour dans le monde !
Ce chiffre astronomique montre à quel point l'IA générative s'est démocratisée.
Mais cette popularité a un coût environnemental énorme. Chaque fois que tu poses une question à ChatGPT, des serveurs dans des centres de données consomment de l'électricité pour traiter ta demande. Multiplié par un milliard, cela représente une consommation d'énergie colossale. Ces centres de données nécessitent non seulement de l'électricité pour fonctionner, mais aussi pour être refroidis en permanence.
La généralisation de l'IA générative contribue donc fortement à accélérer l'impact environnemental du numérique. C'est un défi énergétique majeur pour les années à venir, d'autant plus que cette utilisation ne cesse de croître.

Source : ChatGPT - combien de personnes l'utilisent vraiment ? (Numerama)

140. Quelle affirmation est fausse ?

A) L'IA a fait grimper les émissions de gaz à effet de serre (GES) de Microsoft de 30 %
B) L'IA permet aux géants de la tech de réduire leurs impacts environnementaux
C) Chez Google, l'IA est responsable de la moitié de l'augmentation des émissions de GES depuis 2019

L'affirmation fausse est que l'IA permet aux géants de la tech de réduire leurs impacts environnementaux. En réalité, c'est l'inverse qui se produit ! Bien que l'on présente parfois l'IA comme une solution au développement durable, elle a en fait un impact environnemental si important qu'elle influence de manière notable l'empreinte carbone des géants de la technologie. Microsoft a vu ses émissions de gaz à effet de serre augmenter de 30 % entre 2020 et 2023 à cause de l'IA. Chez Google, l'IA est responsable de la moitié de l'augmentation des émissions depuis 2019. Ces entreprises investissent massivement dans des centres de données toujours plus puissants pour faire fonctionner leurs IA, ce qui consomme énormément d'électricité. L'IA n'est donc pas la solution miracle à la transition écologique qu'on nous présente parfois.

Sources : L'intelligence artificielle met en péril les objectifs climatiques de Microsoft (Novethic) et Rapport environnemental 2024 (Google)

141. Quelle est la consommation moyenne mensuelle de données des utilisateurs de smartphone ?

A) 2,3 Gigaoctets
B) 16,5 Gigaoctets
C) 89,7 Gigaoctets

En 2025, la consommation moyenne mensuelle de données des utilisateurs de smartphone est de 16,5 Gigaoctets. Ce chiffre peut te paraître abstrait, mais pour te donner une idée, cela représente des milliers de photos et des centaines d'heures de musique en streaming. Cette consommation ne cesse d'augmenter avec l'usage croissant du streaming vidéo, des réseaux sociaux et d'autres applications gourmandes en données. Ce qui est intéressant, c'est que 32 % des utilisateurs souscrivent à des abonnements de plus de 100 Gigaoctets, alors qu'ils n'en consomment en moyenne que 16,5. Cette surconsommation d'abonnements montre qu'on a tendance à surestimer nos besoins réels en données. Les opérateurs téléphoniques ont d'ailleurs fait de cette peur de « manquer de données » un véritable argument commercial, en nous poussant à prendre des forfaits bien plus importants que nos besoins réels.
Le problème c'est que chaque Gigaoctet consommé a un impact environnemental car il sollicite les infrastructures réseau et les centres de données.

Source : Équipements et usages du numérique (ARCEP - 2025)

142. Quel métier a été créé grâce à l'intelligence artificielle ?

A) Ingénieur de prompts
B) Administrateur de réseaux
C) Développeur d'applications mobiles

L'arrivée de l'IA a créé de nouveaux métiers, dont l'ingénieur.e de prompts (ou prompt engineer en anglais). Cette personne est spécialisée dans la rédaction d'instructions (prompts) pour interagir efficacement avec une IA. Car oui, bien communiquer avec une IA, ça s'apprend ! Un ingénieur de prompts sait formuler des questions précises, structurer ses demandes et optimiser les réponses de l'IA. Ce métier récent devient essentiel dans de nombreux domaines : éducation, santé, création artistique, marketing... Ces professionnels aident les entreprises à exploiter au mieux le potentiel des intelligences artificielles. Ils doivent comprendre comment fonctionne l'IA, connaître ses limites et savoir adapter leurs demandes selon les objectifs recherchés.
C'est un exemple concret de la façon dont l'IA transforme le marché du travail en créant de nouvelles opportunités professionnelles.

143. Comment savoir si je parle à une IA ?

A) En lui demandant
B) En analysant comment elle parle
C) C'est quasiment impossible

Aujourd'hui, c'est devenu extrêmement difficile de distinguer une IA d'un humain. Les IA modernes sont devenues si sophistiquées qu'elles peuvent imiter parfaitement le style d'écriture humain, utiliser des expressions familières et même des fautes de frappe pour paraître plus « vraies ». Même si tu poses des questions pièges ou que tu analyses attentivement la façon dont « la personne » s'exprime, une IA bien conçue peut déjouer tes tentatives de défection. Elle peut retranscrire des opinions, raconter des anecdotes inventées et imiter des émotions. Certains bots sur les réseaux sociaux sont même programmés pour développer des relations avec leurs interlocuteurs.
C'est pourquoi il faut rester prudent avec tout nouveau contact en ligne et ne jamais partager d'informations personnelles, même si la conversation semble naturelle et bienveillante.

Ressource pour tous : Faut-il avoir peur des IA ? (Lumni)

144. Quel sujet de conversation évite-t-on avec une IA ?

A) Mes devoirs à faire
B) Mes loisirs
C) Mes informations personnelles

Il est crucial de ne jamais partager d'informations personnelles avec une intelligence artificielle, même si elle semble sympathique ou compréhensive. Une IA n'est qu'un programme informatique, pas un ami ou un confident. Tout ce que tu lui dis peut être stocké sur des serveurs, analysé par des entreprises, ou même utilisé pour t'envoyer de la publicité ciblée. Tes conversations avec une IA ne sont pas privées : elles peuvent être lues par les équipes techniques, utilisées pour améliorer le système, ou conservées dans des bases de données. Évite donc de parler de tes relations amoureuses, de tes problèmes familiaux, de ton adresse, de tes mots de passe ou de tout ce qui pourrait t'identifier.
Même si l'IA te pose des questions personnelles ou te fait des compliments pour t'encourager à te confier, rappelle-toi que c'est un programme conçu pour se nourrir d'informations.

145. À quoi sert le machine learning ?

A) À permettre à un système d'apprendre automatiquement à partir de données
B) À augmenter la puissance de calcul d'un ordinateur
C) À chiffrer les données pour les protéger

Le machine learning (apprentissage automatique en français) est une méthode qui permet à une IA d'apprendre automatiquement à partir de données, sans qu'on ait besoin de programmer chaque situation possible. On lui montre plein d'exemples et il apprend à reconnaître des éléments tout seul. Par exemple, pour apprendre à reconnaître des chats sur des photos, on montre à l'IA des milliers d'images de chats avec l'indication « c'est un chat », et petit à petit, elle apprend à identifier les caractéristiques communes : les oreilles pointues, les moustaches, la forme des yeux… Cette technique est à la base de beaucoup d'IA actuelles : reconnaissance vocale, filtres anti-spam dans tes emails ou encore assistants virtuels. Plus l'IA a accès à des données variées et de qualité, mieux elle apprend.

Ressource pour un ado : Ingénieur machine learning (Lumni)

146. Quel est le lien entre géolocalisation et publicité ciblée ?

A) Aucun, la géolocalisation ne sert qu'aux GPS
B) Les entreprises peuvent te montrer des publicités selon l'endroit où tu te trouves
C) Ça permet de connaître ton plat préféré

La géolocalisation permet aux applications de connaître ta position géographique précise, et cette information est très précieuse pour la publicité ciblée.
Quand tu autorises une application à accéder à ta localisation, elle peut te proposer des publicités en fonction de l'endroit où tu te trouves : une pub pour une pizzeria quand tu es dans le centre-ville, une offre spéciale dans un magasin près de chez toi ou des événements locaux. Cette technique s'appelle le « géomarketing ». Ton téléphone enregistre aussi tes déplacements habituels : si tu vas souvent dans un quartier précis, les annonceurs peuvent en déduire tes centres d'intérêt et t'envoyer des publicités ciblées.
Pour protéger ta vie privée, tu peux désactiver ce suivi dans les réglages de ton téléphone et choisir quelles applications peuvent accéder à ta position.

147. Une entreprise peut-elle vendre tes données sans ton accord ?

A) Oui, si les données ont été collectées sur un site gratuit
B) Oui, si l'utilisateur n'a pas modifié les paramètres par défaut
C) Non, une entreprise ne peut pas vendre les données personnelles sans accord explicite

Tes données personnelles sont précieuses et les entreprises le savent bien !
En Europe, le Règlement Général sur la Protection des Données (RGPD) protège tes informations. Aucune entreprise ne peut vendre ou partager tes données sans ton accord explicite. Tes données ne sont pas des objets qu'on peut échanger librement. Elles incluent ton nom, tes photos, tes messages, tes habitudes de navigation, ta géolocalisation. Le RGPD impose aux entreprises de t'expliquer pourquoi elles veulent utiliser tes données personnelles. Elles doivent te demander clairement ton consentement pour les utiliser et te donner la possibilité de refuser qu'elles les utilisent. Si elles ne respectent pas ces règles, elles risquent des amendes !

Ressource pour un ado : Un océan de données (CNIL)

148. Pourquoi parle-t-on de réseau de neurones en informatique ?

A) Parce que les ordinateurs sont connectés entre eux par des câbles
B) Parce que les scientifiques utilisent Internet pour communiquer
C) Parce que les systèmes d'IA s'inspirent du fonctionnement du cerveau humain

Dans ton cerveau, tu as des milliards de neurones qui communiquent entre eux pour traiter les informations. Pour créer les IA, les informaticiens se sont inspirés de ces connexions. Les IA fonctionnent avec des milliers de « neurones artificiels » qui s'échangent des données mathématiques. Attention car malgré ce nom, l'intelligence artificielle ne pense pas du tout. Elle ne ressent rien, ne comprend pas au sens où tu comprends et n'a pas de conscience. Elle traite simplement d'énormes quantités de données selon des règles mathématiques très complexes. Nous avons tendance à humaniser l'IA en utilisant des mots comme « apprendre » ou « comprendre », mais ces machines ne font que calculer des probabilités pour donner la réponse la plus probable. C'est fascinant et très utile, mais fondamentalement différent de ton intelligence
humaine !

149. Qui a créé ChatGPT ?

A) Arthur Mensch, un ingénieur français
B) Elon Musk qui est aussi le fondateur de Tesla
C) Sam Altman, un homme d'affaires américain

ChatGPT a été créé par OpenAI, une entreprise américaine fondée par Sam Altman et d'autres entrepreneurs en 2015. Cette IA conversationnelle est devenue célèbre dans le monde entier en 2022. En France, des ingénieurs brillants ont créé Mistral AI en 2023 pour ne pas laisser les entreprises américaines dominer l'intelligence artificielle. Mistral AI est une des startups françaises les plus précieuses !
Le fait que cette start-up soit française est important car cette IA comprend mieux la culture européenne. Mistral s'étend maintenant aux États-Unis pour concurrencer OpenAI. C'est toujours une entreprise française, même si elle a des investisseurs internationaux. Cette compétition entre pays est importante car chaque pays veut garder le contrôle sur ses technologies d'IA !

150. Quelle est la principale différence entre un moteur de recherche et une IA ?

A) Le moteur de recherche renvoie à des pages existantes, l'IA génère directement des réponses
B) Le moteur de recherche fonctionne sans données, l'IA fonctionne sans Internet
C) L'IA affiche uniquement des résultats scientifiques alors que le moteur de recherche montre tout

La différence fondamentale réside dans leur façon de traiter l'information.
Un moteur de recherche agit tel un bibliothécaire numérique : il parcourt Internet pour trouver des pages existantes qui correspondent à ta requête, puis te propose une liste de liens. L'IA fonctionne différemment. Elle utilise un système appelé LLM (Large Language Model) qui analyse ta question, recherche dans ses connaissances acquises pendant son entraînement, puis crée une réponse originale en assemblant les informations de manière logique. Cette différence a des conséquences importantes : si un moteur de recherche te permet de vérifier ses sources en cliquant sur les liens, un LLM peut parfois générer des informations incorrectes ou inventer des « faits » qui semblent crédibles. Il faut donc toujours vérifier les informations données par une IA.

Ressource pour tous : Les LLM Expliqués (SIMPLEMENT) en 3 min


Hacker

151. Que dois-tu faire si tu reçois un message disant que tu as gagné un smartphone gratuit ?

A) Cliquer immédiatement sur le lien
B) Vérifier la source et en parler à un adulte
C) Donner tes coordonnées personnelles

Tu as reçu un message qui annonce que tu as gagné un smartphone gratuit ?
Attention, c'est probablement une arnaque ! Les personnes malveillantes sur Internet utilisent ce genre de messages pour piéger les gens, surtout les enfants.
Quand tu cliques sur ces liens, voici ce qui peut arriver : les hackers (pirates informatiques) peuvent voler toutes tes informations personnelles (photos, mots de passe, adresse), t'espionner avec la caméra ou le micro de ton appareil, te demander de l'argent ou même utiliser tes comptes et se faire passer pour toi.
C'est très dangereux !
La bonne réaction ? Ne jamais cliquer sur ces liens. Montre toujours le message à un adulte de confiance qui pourra t'aider à vérifier si c'est vrai ou faux.
Méfie-toi des offres trop belles pour être vraies !

Source : Comment reconnaître un mail de phishing ou d'hameçonnage ? (Cybermalveillance.gouv.fr)
Ressource pour tous : Les pièges, dangers et arnaques d'Internet (Lumni)

152. Quel est le bon réflexe à avoir si tu crois avoir été piraté ?

A) Fermer l'ordinateur et ne rien dire
B) En parler à un adulte et changer ses mots de passe
C) Supprimer tous tes fichiers

Si tu penses que ton compte ou ton appareil a été piraté, ne panique pas !
Il faut agir rapidement mais intelligemment. Fermer l'ordinateur sans rien faire ne résoudra pas le problème et supprimer tous tes fichiers pourrait faire disparaître des choses importantes pour toujours.
La première chose à faire est d'en parler immédiatement à un adulte de confiance : tes parents, un enseignant ou un proche qui s'y connaît en informatique.
Ensemble, vous pourrez changer tous tes mots de passe, vérifier si tes comptes ont été utilisés par quelqu'un d'autre et prendre les bonnes mesures pour protéger tes informations.
Il est aussi important de vérifier si des achats ont été faits avec les comptes bancaires reliés à tes différents jeux ou applications, si des messages ont été envoyés en ton nom ou si des informations personnelles ont été partagées.
Plus tu agis vite avec l'aide d'un adulte, mieux tu pourras limiter les dégâts !

Ressources pour tous : Abécédaire de la cybersécurité (Kaspersky) et On a piraté mon mari ! (CLEMI)

153. Si un inconnu t'écrit sur un jeu en ligne, que dois-tu faire ?

A) Lui répondre, on est tous là pour s'amuser après tout
B) Lui donner ton numéro, ça sera plus facile pour se parler
C) Ne pas répondre et en parler à un adulte, il faut faire attention

Dans les jeux en ligne, tu peux rencontrer plein de personnes différentes.
Mais attention : tu ne sais jamais vraiment qui se cache derrière un pseudo !
Même si cette personne semble sympa et dit avoir ton âge, elle pourrait en réalité être un adulte malveillant qui cherche à te manipuler.
Ces personnes peuvent essayer de devenir tes amies pour obtenir tes informations personnelles, te demander de faire des choses dangereuses ou même essayer de te rencontrer dans la vraie vie. C'est ce qu'on appelle le « grooming » : des adultes malveillants qui se font passer pour des enfants pour piéger de vrais enfants.
La règle d'or : ne jamais donner d'informations personnelles (nom, adresse, école, numéro de téléphone) à quelqu'un que tu ne connais pas en vrai.
Si quelqu'un insiste pour te parler en privé ou te demande des informations sur toi, arrête la conversation et parle-en immédiatement à un adulte.

154. En 2025, dans quel pays trouve-t-on le plus de pirates informatiques ?

A) La France
B) La Russie
C) Le Groenland

La Russie est devenue le pays leader en cybercriminalité dans le monde !
Les pirates informatiques russes sont très organisés et utilisent des techniques très avancées pour attaquer les ordinateurs et voler des informations.
Ces criminels du numérique volent de l'argent, s'introduisent dans les systèmes d'autres pays et perturbent le fonctionnement d'entreprises ou d'infrastructures critiques.
La Russie abrite de nombreux groupes de pirates qui travaillent ensemble et partagent leurs techniques. C'est devenu un vrai problème mondial car ces attaques touchent tous les continents. Face à cette offensive mondiale, la France et l'Europe déploient une stratégie nationale cybersécurité ambitieuse : nouveaux outils, veille renforcée, innovation permanente. La riposte s'organise, mais certains territoires sont devenus de véritables carrefours de la cybercriminalité. Les classements GCI (Global Cybersecurity Index) et NCSI (National Cyber Security Index) dressent une carte éclatée : la Russie, la Chine et l'Iran dominent le palmarès des attaques les plus élaborées.

Source : Cyberattaque - le pays le plus fort en cybercriminalité en 2025 (Scienceline)

155. Peut-on savoir qui est derrière un message sur Internet ?

A) Toujours
B) Non, on ne sait pas toujours qui écrit
C) Oui, si on est ami avec lui

Sur Internet, il est souvent impossible de savoir vraiment qui écrit un message !
Les personnes peuvent facilement se cacher derrière de faux noms, de fausses photos, et même faire croire qu'elles habitent dans un autre pays.
Il existe des techniques informatiques qui permettent de masquer son identité : les VPN (qui changent ta localisation virtuelle), les adresses IP cachées ou les serveurs qui font rebondir les messages. Même les spécialistes en informatique ont parfois du mal à retrouver la vraie identité de quelqu'un !
C'est pourquoi tu ne dois jamais faire confiance aveuglément à quelqu'un que tu ne connais que par Internet. Même si vous êtes « amis » sur un réseau social, cela ne garantit pas que tu saches vraiment qui c'est.
La prudence est toujours de mise quand tu communiques en ligne !

156. Quand quelqu'un te demande ton mot de passe, comment dois-tu réagir ?

A) Tu dis non (sauf s'il s'agit de tes parents)
B) Tu lui chuchotes dans l'oreille
C) Tu l'écris sur un post-it

Ton mot de passe, c'est ta clé secrète ! Pense à la clé de ta maison : tu ne la donnes pas à n'importe qui, n'est-ce pas ? C'est pareil pour tes mots de passe.
Si tu donnes la clé de ta maison à quelqu'un et qu'il te la rend, tu récupères ta clé. Mais si tu dis ton mot de passe à quelqu'un, il ne peut pas « te le redonner » : il le connaîtra pour toujours !
Tes parents peuvent avoir besoin de connaître tes mots de passe parce qu'ils sont responsables de ta sécurité quand tu es mineur. Ils peuvent t'aider si tu as des problèmes avec tes comptes ou si quelque chose de dangereux arrive.
Astuce : Si tu veux partager tes accès avec tes parents, vous pouvez utiliser un gestionnaire de mots de passe sécurisé. Aucun ami, aucun camarade de classe, aucun inconnu ne doit connaître tes mots de passe. Si quelqu'un insiste pour les avoir, c'est louche !

Ressource pour un ado : Les conseils de la CNIL pour un bon mot de passe

157. Qu'est-ce qu'un « hacker » ?

A) Une personne qui tape très vite sur le clavier pour jouer aux jeux vidéo
B) Une personne qui contourne les protections des systèmes informatiques
C) Un logiciel malveillant qui s'infiltre dans les ordinateurs pour voler ou détruire des données

Un hacker connaît très bien le langage des ordinateurs ; il sait modifier un programme, regarder comment il fonctionne puis, au besoin, le réparer ou le renforcer.
Imagine une maison avec des serrures : pour vérifier qu'elles sont solides, on demande parfois à un serrurier expert d'essayer de les ouvrir sans clé ; s'il y parvient, il explique où est la faille afin qu'on installe une meilleure serrure. C'est ce que fait un hacker « éthique » (on l'appelle aussi white hat). Il teste la sécurité d'un site web, d'un jeu ou d'une application, repère les portes secrètes par lesquelles un pirate pourrait voler des données, puis prévient les propriétaires pour qu'ils les ferment. Attention : tous les hackers ne sont pas gentils. Certains (black hats) utilisent leurs talents pour voler ou détruire. La différence n'est donc pas dans les compétences, mais dans l'intention. Être un bon hacker, c'est cultiver la curiosité, l'entraide et le respect des lois pour que la technologie soit plus sûre pour tout le monde.

Ressource pour tous :
Cybercriminalité, des attaques bien réelles (ARTE)

158. Qu'est-ce que le « dark web » ?

A) Un jeu vidéo secret rempli de niveaux cachés
B) Le mode nuit des sites classiques qui rend l'écran tout noir
C) Une zone d'Internet accessible seulement avec des logiciels spéciaux où l'on peut rester anonyme

Le dark web est une partie secrète d'Internet. Les moteurs de recherche ordinaires ne la montrent pas. Pour y entrer, on installe un navigateur spécial, qui cache ton adresse et ton pays. Grâce à ce manteau d'invisibilité numérique, les pages du dark web ne révèlent pas qui les visite. Certains l'utilisent pour de bonnes raisons : discuter sans être surveillé par une dictature, partager des infos avec des journalistes, protéger la vie privée d'une personne menacée. D'autres l'exploitent pour vendre des objets interdits ou des informations, échanger des virus ou piéger des curieux. Les sites y ont des adresses étranges et l'affichage peut être très lent, car tout est chiffré et passe par plusieurs ordinateurs. Le meilleur réflexe est de rester sur le web ouvert, de vérifier les sources et de demander conseil avant de visiter des zones inconnues.

Ressource pour tous :
Le Dark net c'est quoi ? (Influenceur Enissay)

159. Où télécharger un nouveau jeu en ligne pour être sûr qu'il ne soit pas piégé ?

A) Sur les plateformes officielles (App Store ou Play Store)
B) Sur n'importe quel site qui le propose « gratuitement »
C) En cliquant sur un lien reçu par e-mail

Les plateformes officielles comme l'App Store d'Apple ou le Play Store de Google sont des endroits sûrs pour télécharger des jeux. Ces plateformes vérifient chaque application avant de la proposer au téléchargement. Des équipes d'experts analysent le code pour s'assurer qu'il n'y a pas de virus ou de programmes malveillants cachés.
Les autres sites web peuvent paraître tentants car ils proposent souvent des jeux « gratuits ». Attention ! Certains cachent des pièges : virus, programmes espions ou publicités envahissantes. Les liens reçus par e-mail sont particulièrement dangereux. Les pirates utilisent cette technique pour faire télécharger de faux jeux qui ressemblent aux vrais mais qui contiennent des logiciels malveillants.

160. Une fenêtre clignote : « Ton ordinateur est infecté ! Installe vite cet antivirus gratuit ! » Que faire ?

A) Télécharger immédiatement le programme proposé
B) Fermer la fenêtre et lancer ton antivirus
C) Ignorer le message et continuer à jouer

Cette fenêtre qui clignote est un piège très courant appelé « scareware » (logiciel de peur). Les pirates utilisent des messages effrayants pour te faire paniquer et télécharger leurs faux antivirus. En réalité, ton ordinateur n'est probablement pas infecté !
La bonne réaction est de fermer immédiatement cette fenêtre pop-up et de lancer ton vrai antivirus pour faire une vraie vérification. Un vrai antivirus ne s'annonce jamais par des fenêtres qui clignotent avec des couleurs criardes et des points d'exclamation partout. Les vrais antivirus ont une interface calme et professionnelle. Ils ne te demandent jamais de télécharger quoi que ce soit en urgence.
Si tu télécharges le faux antivirus proposé, tu risques d'installer un virus sur ton ordinateur ! Ces programmes malveillants peuvent voler tes mots de passe, ralentir ton ordinateur ou même le bloquer complètement. Chaque année, des milliers de personnes tombent dans ce piège.

161. Que risques-tu en branchant une clé USB trouvée par terre ?

A) Qu'elle efface tes vieilles photos pour faire de la place
B) Qu'elle recharge ta batterie moins vite
C) Qu'elle infecte ton appareil avec un virus

Une clé USB trouvée par terre peut être un vrai danger ! C'est une technique utilisée par les pirates informatiques. Ils laissent volontairement des clés USB infectées dans des lieux publics en espérant que quelqu'un les ramasse et les branche sur son ordinateur. Dès que tu branches cette clé, le virus qu'elle contient peut s'installer automatiquement sur ton appareil. Certains virus sur clé USB sont tellement puissants qu'ils peuvent se propager à tous les autres appareils connectés au même réseau.
Même si la clé USB semble venir d'une marque connue, elle peut quand même être piégée. Si tu trouves une clé USB, le mieux est de la déposer au bureau des objets trouvés.

162. Pourquoi verrouiller l'écran quand tu quittes ton ordinateur ?

A) Pour augmenter le volume du haut-parleur
B) Pour économiser ta batterie
C) Pour que personne n'utilise tes comptes pendant ton absence

Verrouiller ton écran quand tu t'absentes, même pour quelques minutes, est un geste de sécurité essentiel ! Quand ton ordinateur reste ouvert, n'importe qui peut accéder à tes comptes, lire tes messages privés, regarder tes photos ou même envoyer des messages en se faisant passer pour toi.
Cette situation peut arriver partout : à l'école, chez des amis, dans un café ou même à la maison. Quelqu'un pourrait profiter de ton absence pour fouiller dans tes affaires numériques. Il pourrait aussi faire des blagues pas drôles, comme changer ton mot de passe ou publier des choses embarrassantes sur tes réseaux sociaux.
Le verrouillage automatique se fait facilement : sur Windows, tu peux appuyer sur les touches « Windows + L », sur Mac c'est « Contrôle + Commande + Q ». Tu peux aussi paramétrer ton ordinateur pour qu'il se verrouille automatiquement après quelques minutes d'inactivité. Cette habitude simple te protège efficacement et ne prend que deux secondes !

163. À quoi sert le site Internet « Signal Spam » ?

A) À accélérer la réception de tes messages
B) À envoyer des publicités marrantes à tes amis
C) À signaler les emails ou sites suspects aux autorités

Signal Spam est une plateforme officielle française qui permet de signaler les mails suspects, les SMS frauduleux et les sites web dangereux aux autorités.
Quand tu reçois un message bizarre qui demande tes informations personnelles ou qui propose des offres trop belles pour être vraies, tu peux le signaler sur cette plateforme.
Quand tu signales un contenu suspect, les experts analysent ta déclaration et peuvent prendre des mesures pour bloquer les expéditeurs malveillants ou fermer les sites frauduleux.
Chaque signalement aide à protéger d'autres personnes ! Plus il y a de signalements sur un même expéditeur suspect, plus vite les autorités peuvent agir. Tu participes ainsi à la sécurité de tous les internautes français quand tu fais un signalement.

Source : https://www.signal-spam.fr

164. Pourquoi désactiver le Wi-Fi et le Bluetooth quand tu ne t'en sers pas ?

A) Pour que l'écran devienne plus lumineux
B) Pour mieux entendre la musique
C) Pour empêcher les pirates informatiques de s'introduire dans ton appareil

Quand ils sont activés, le Wi-Fi et le Bluetooth cherchent constamment des connexions disponibles. Les pirates informatiques peuvent profiter de ces « portes ouvertes » pour essayer de s'introduire dans ton téléphone ou ta tablette.
Avec le Bluetooth activé, un pirate proche de toi peut tenter de se connecter à ton appareil pour voler tes données ou installer des programmes malveillants.
Cette technique s'appelle le « bluejacking ». Avec le Wi-Fi, ton appareil peut se connecter automatiquement à des réseaux piégés qui portent le même nom que des réseaux que tu connais. Désactiver ces connexions quand tu ne t'en sers pas réduit considérablement les risques d'intrusion. En bonus, cela économise ta batterie !

165. Que fait l'outil en ligne « 17Cyber » de Cybermalveillance.gouv.fr ?

A) Il t'aide à diagnostiquer un problème de piratage et donne des conseils
B) Il baisse le prix des jeux vidéo
C) Il supprime tous les spams de ta boîte mail en un clic

17Cyber est un outil gratuit créé par le gouvernement français pour aider les victimes de cyberattaques. Quand tu penses avoir été piraté, cet outil te pose des questions simples pour comprendre ton problème et te donne des conseils personnalisés pour t'en sortir. L'outil fonctionne comme un questionnaire intelligent. Il te demande ce qui s'est passé : est-ce que ton ordinateur est lent ? Est-ce que tu as reçu des messages suspects ? Est-ce que quelqu'un a utilisé tes comptes sans permission ? Selon tes réponses, il te propose des solutions concrètes et te dit si tu dois porter plainte.
17Cyber peut aussi t'orienter vers des professionnels près de chez toi si le problème est compliqué. Cet outil a été créé par des experts en cybersécurité et est constamment mis à jour avec les nouvelles menaces qui existent.

Source : cybermalveillance.gouv.fr

166. Au niveau mondial, à combien s'élèvent les dommages monétaires causés par la cybercriminalité ?

A) Quelques centaines de dollars
B) Quelques millions de dollars
C) Plus de 8 milliards de milliards de dollars

Plus de 8 milliards de milliards de dollars ! C'est un chiffre énorme, difficile à imaginer. Pour te donner une idée, c'est plus d'argent que ne possèdent la plupart des pays entiers ! Les cybercriminels causent des dégâts financiers gigantesques partout dans le monde. Ils volent de l'argent directement, mais ils commettent aussi de gros dégâts sur les systèmes informatiques, obligeant les entreprises à dépenser beaucoup pour les réparer. Les entreprises doivent aussi embaucher des spécialistes en sécurité informatique pour se protéger, ce qui représente encore plus de dépenses. Ce montant astronomique montre pourquoi la cybersécurité est devenue l'une des préoccupations les plus importantes de notre époque numérique.

Source : La cyber-sécurité - Faits et chiffres (Statista)

167. Quel réseau social a subi une cyberattaque historique en 2020 où les comptes de Barack Obama, Elon Musk et d'autres célébrités ont été piratés ?

A) Instagram
B) X (ex Twitter)
C) TikTok

En juillet 2020, Twitter a vécu une journée très mouvementée ! Des pirates informatiques ont réussi à prendre le contrôle des comptes de Barack Obama (ancien président américain), Elon Musk (patron de Tesla), Bill Gates (créateur de Microsoft) ainsi que de nombreux comptes de grandes entreprises, comme Apple ou Uber.
Les pirates ont publié des messages frauduleux sur tous ces comptes en même temps. Ils demandaient aux gens d'envoyer de l'argent virtuel (des bitcoins) en promettant de leur rendre le double ! Bien sûr, c'était un mensonge total. Les pirates ont réussi à voler environ 100 000 euros avant que Twitter ne bloque tous les comptes pour arrêter l'attaque. Cette attaque a montré que même les comptes les plus protégés peuvent être piratés. Les pirates avaient réussi à utiliser des employés de Twitter pour accéder aux outils internes de l'entreprise. Depuis, X a renforcé sa sécurité !

Source : Obama, Musk et Gates hackés sur Twitter : cinq questions sur un piratage inédit (Le Parisien)

168. Est-ce que ton téléphone peut vraiment écouter secrètement tes conversations grâce à son micro ?

A) Oui, si des applis malveillantes obtiennent l'autorisation d'utiliser ton micro
B) Non, les téléphones n'ont pas de micro capable d'entendre clairement
C) Oui, mais seulement si tu téléphones à quelqu'un

Ton téléphone peut effectivement t'écouter, mais seulement si tu donnes la permission à une application douteuse d'utiliser ton micro ! Quand tu installes une nouvelle application, elle te demande souvent des autorisations : accéder à tes photos, utiliser ton micro, ta caméra…
Si tu dis « oui » à tout sans réfléchir, une application malveillante pourrait enregistrer tes conversations même quand tu ne t'en sers pas pour téléphoner.
Elle pourrait ensuite envoyer ces enregistrements à des personnes mal intentionnées. Heureusement, tu peux te protéger facilement ! D'abord, télécharge uniquement des applications depuis les plateformes officielles (App Store pour iPhone, Google Play pour Android). Ensuite, lis bien les autorisations demandées : pourquoi une application de jeux aurait-elle besoin d'utiliser ton micro ? Et dans les réglages de ton téléphone, tu peux vérifier et changer les autorisations de chaque application quand tu veux.

169. La cryptographie, c'est quoi exactement ?

A) L'art de dessiner des cartes géographiques très détaillées
B) La science qui étudie les codes secrets pour protéger les informations
C) Une technique pour faire des photos floues et mystérieuses

La cryptographie est une science fascinante qui mélange les mathématiques et l'informatique pour créer des codes secrets ! Elle existe depuis très longtemps : déjà dans l'Antiquité, Jules César utilisait un code spécial pour envoyer des messages secrets à ses soldats. Aujourd'hui, elle protège presque tout ce que tu fais sur Internet. Quand tu regardes une vidéo en streaming, quand tes parents font leurs achats en ligne ou quand tu joues à un jeu sur ton téléphone, la cryptographie travaille en secret pour protéger toutes les informations. La cryptographie protège tes photos, tes messages, tes mots de passe et même l'argent de tes parents. Sans elle, Internet ne serait pas sûr et nous ne pourrions pas faire confiance aux sites web.
C'est grâce à elle que tu peux utiliser Internet en toute sécurité !

170. Que fait un expert en cybersécurité ?

A) Il répare les ordinateurs cassés
B) Il protège les systèmes informatiques contre les cyberattaques
C) Il développe des jeux vidéo

Un expert en cybersécurité est un véritable gardien du monde numérique.
Son rôle principal est de protéger les systèmes informatiques, les réseaux et les données contre toutes formes de cybermenaces. Il analyse les vulnérabilités, met en place des systèmes de défenses informatiques, surveille les tentatives d'intrusion et intervient en cas d'incident. Ce métier demande des compétences techniques pointues en informatique, mais aussi de la créativité pour anticiper les nouvelles menaces.
Les experts en cybersécurité travaillent dans tous les secteurs : entreprises, hôpitaux, gouvernement, banques... Ils peuvent être spécialisés dans différents domaines : analyse de logiciels malveillants, tests d'intrusion ou sensibilisation.
Avec l'explosion du numérique, ce métier connaît une forte demande. C'est un secteur d'avenir qui offre de nombreuses opportunités !

171. En 2022, combien de temps fallait-il en moyenne pour détecter une intrusion dans un système informatique ?

A) Quelques minutes
B) 1 à 2 jours
C) Plus de 200 jours

Il fallait en moyenne 207 jours pour détecter une intrusion dans un système informatique ! Cette statistique inquiétante montre que les cybercriminels peuvent rester cachés pendant des mois entiers dans les réseaux. Pendant ce temps, ils peuvent voler des données sensibles, espionner les communications ou préparer des attaques plus importantes. Cette durée s'explique par la sophistication croissante des cyberattaques. Les pirates utilisent des techniques très discrètes pour éviter d'être détectés : ils imitent le comportement normal des utilisateurs et effacent leurs traces. Une fois détectée, l'intrusion prend encore 70 jours en moyenne pour être complètement éliminée. C'est pourquoi les entreprises investissent massivement dans des systèmes de surveillance en temps réel et des équipes de cybersécurité. Cette réalité souligne l'importance de la prévention et de la vigilance constante.

Source : Compromission de données - Comment elle survient et 11 méthodes pour s'en prémunir (Crowdstrike)

172. Combien de nouvelles variantes de logiciels malveillants sont créées chaque jour ?

A) Environ 100
B) Environ 10 000
C) Plus de 450 000

Plus de 450 000 nouvelles variantes de logiciels malveillants sont créées chaque jour ! Ce chiffre impressionnant montre l'ampleur de la menace cybercriminelle actuelle. Ces malwares incluent virus, vers, chevaux de Troie, ransomwares et spywares. Les cybercriminels utilisent des techniques automatisées pour créer des variants de leurs programmes malveillants, modifiant légèrement le code pour échapper aux antivirus. Cette « production de masse » s'explique par la professionnalisation du crime informatique : des organisations entières se consacrent à développer et distribuer des malwares. Certains sont vendus « clé en main » sur le Dark Web, permettant à des amateurs de lancer des cyberattaques. Heureusement, les éditeurs d'antivirus analysent en permanence ces nouvelles menaces et mettent à jour leurs bases de signatures plusieurs fois par jour. C'est pourquoi il est crucial de maintenir son antivirus et son système d'exploitation à jour. Cette course permanente entre attaquants et défenseurs illustre l'importance de la cybersécurité moderne.

Source : AV-TEST Institute

173. Quel pourcentage de femmes travaille dans le domaine de la cybersécurité ?

A) 60 %
B) 40 %
C) 25 %

La cybersécurité, c'est le domaine qui protège nos ordinateurs, nos téléphones et toutes nos données contre les pirates informatiques. Eh bien, figure-toi que sur 100 personnes qui travaillent dans ce domaine super important, seulement 25 sont des femmes ! C'est vraiment peu. Dans les postes de direction, on tombe même à 3-5 % de femmes. Pourtant, rien n'empêche les filles d'être aussi douées que les garçons en informatique et en cybersécurité. D'ailleurs, cette situation évolue doucement : on était à 10 % de femmes en 2013, puis 20 % en 2019, et 25 % en 2022. Les experts prévoient qu'on atteindra 30 % d'ici 2025. Ces chiffres montrent qu'il y a encore du chemin à parcourir pour que les métiers de la cybersécurité attirent autant les filles que les garçons. C'est important car plus on a de diversité dans une équipe, mieux on peut résoudre les problèmes complexes !

Sources : Les femmes sont encore largement minoritaires dans les équipes de cybersécurité (Itsocial) et Femmes dans l'IT : un avenir plus inclusif (isupplier)

174. Qu'est-ce que l'ANSSI ?

A) Une entreprise privée qui vend des antivirus
B) L'agence française qui protège notre pays contre les cyberattaques
C) Un jeu vidéo pour apprendre l'informatique

L'ANSSI, c'est l'Agence Nationale de la Sécurité des Systèmes d'Information ! Créée en 2009, cette agence française protège notre pays contre les cyberattaques. Elle surveille Internet pour détecter les dangers numériques et aide les entreprises, les hôpitaux ou les écoles quand ils subissent des attaques de pirates informatiques. L'ANSSI forme aussi des spécialistes en cybersécurité et donne des conseils pour mieux se protéger sur Internet. L'ANSSI collabore avec d'autres pays pour lutter ensemble contre la cybercriminalité mondiale. Cette agence gouvernementale emploie des centaines de personnes qui veillent sur notre sécurité numérique quotidienne.

Source : https://cyber.gouv.fr

175. Que dois-tu faire si tu reçois des appels publicitaires non désirés sur ton téléphone ?

A) Décrocher et dire poliment que tu n'es pas intéressé
B) Ne rien faire et espérer que ça s'arrête tout seul
C) Bloquer le numéro et le signaler

Le spam téléphonique, ce sont ces appels publicitaires que tu n'as jamais demandés et qui arrivent toujours au mauvais moment ! Ces entreprises achètent des listes de numéros ou utilisent des robots qui composent automatiquement des millions de numéros.
La bonne nouvelle ? Tu peux te défendre ! D'abord, ne décroche jamais si tu ne reconnais pas le numéro. Si tu décroches par erreur, raccroche immédiatement sans rien dire : parler confirme que ton numéro est actif. Ensuite, bloque le numéro dans les paramètres de ton téléphone. Inscris-toi sur Bloctel, le service gratuit qui te protège du démarchage téléphonique. Enfin, signale les numéros abusifs au 33700 par SMS ou sur www.33700.fr. Plus on signale, plus les autorités peuvent agir contre ces pratiques gênantes !

Ressource pour un ado : Tuto smartphone - comment bloquer le spam téléphonique (Geek Junior)

176. Une faille de sécurité, c'est :

A) Une faiblesse dans un programme informatique
B) Une erreur de configuration qui empêche un logiciel de fonctionner correctement
C) Un défaut matériel qui peut provoquer un dysfonctionnement de l'appareil

Une faille de sécurité informatique, c'est un point faible dans un programme ou un système informatique. Les développeurs, même les meilleurs, ne sont pas parfaits. Quand ils créent des logiciels, des applications ou des sites web, ils peuvent laisser sans le vouloir des erreurs dans leur code. Ces erreurs deviennent des failles que les pirates informatiques (hackers) peuvent exploiter pour s'introduire dans le système.
Parfois, c'est une erreur de programmation qui permet à quelqu'un d'accéder à des données qu'il ne devrait pas voir. D'autres fois, c'est un oubli de sécurisation d'une fonction. Les entreprises tech emploient des équipes entières pour détecter et corriger ces failles avant que les hackers ne les trouvent. C'est pour ça que tes applications se mettent régulièrement à jour : souvent, ces mises à jour corrigent des failles de sécurité.

177. Qu'est-ce qu'un « botnet » ?

A) Un ensemble d'appareils connectés fonctionnant sous la même application
B) Un réseau d'appareils infectés et contrôlés à distance par un attaquant
C) Un outil utilisé pour analyser le trafic Internet d'un réseau local

Un botnet, c'est l'une des armes les plus redoutables des cybercriminels.
Le mot vient de « robot » et « network » (réseau). Les pirates informatiques infectent des milliers, parfois des millions d'ordinateurs, de téléphones ou d'objets connectés avec des logiciels malveillants. Une fois infectés, ces appareils deviennent des « zombies » : ils continuent à fonctionner normalement pour leurs propriétaires, mais obéissent secrètement aux ordres du pirate. Ce dernier peut alors commander à toute cette armée numérique de lancer des attaques coordonnées. Par exemple, tous ces appareils infectés peuvent bombarder simultanément un site web de millions de connexions pour le faire planter. Le propriétaire de l'ordinateur zombie ne se doute souvent de rien. Son appareil fonctionne normalement, mais participe en arrière-plan à des activités criminelles. C'est pourquoi il est crucial d'avoir un bon antivirus et de maintenir ses appareils à jour.

Ressource pour un adulte : MOOC de l'ANSSI (République française)

178. Quelle attaque consiste à tromper un utilisateur par un faux site ou email ?

A) Hameçonnage (phishing)
B) Fissuration (Cracking)
C) Inondation (Flooding)

Le phishing ou hameçonnage, c'est l'art de la tromperie numérique. Les pirates informatiques se déguisent en institutions de confiance : ta banque, ton école, Netflix, Amazon ou même tes amis sur les réseaux sociaux. Ils envoient des emails ou créent des sites web qui ressemblent parfaitement aux vrais. Le message dit souvent quelque chose d'urgent : « Ton compte sera fermé si tu ne cliques pas maintenant ! » ou « Tu as gagné un iPhone, clique ici ! ». L'objectif ? Te faire révéler tes mots de passe, numéros de carte bancaire ou autres informations personnelles. Ces criminels sont devenus très doués : leurs faux sites sont parfois impossibles à distinguer des vrais.
Ils utilisent même les bons logos, les bonnes couleurs et parfois des informations personnelles qu'ils ont trouvées sur toi pour rendre leur piège plus crédible.
La règle d'or : toujours vérifier l'adresse du site et ne jamais cliquer sur des liens suspects dans les emails.



Ressource pour tous :
Comment ENFIN ne plus se faire piéger par du phishing ? (Konbini)

179. D'après toi, depuis quand se prépare-t-on à la cybersécurité ?

A) La fin des années 1970
B) Le début des années 1990, avec la généralisation d'Internet dans les entreprises
C) Le milieu des années 2000, lorsque les attaques deviennent plus médiatisées

Contrairement à ce qu'on pourrait penser, la cybersécurité n'est pas née avec Internet ! Dès 1978, la France adoptait la première loi « informatique et libertés » pour protéger les données personnelles dans les fichiers informatiques. À cette époque, les ordinateurs étaient gigantesques et peu nombreux, mais les législateurs avaient déjà compris qu'il fallait encadrer l'usage des données. En 1988, une autre loi, la loi Godfrain, punissait pour la première fois le piratage informatique en France. Puis en 2009, l'ANSSI (Agence nationale de sécurité des systèmes d'information) a été créée pour coordonner la protection numérique du pays. Le RGPD (Règlement Général sur la Protection des Données) européen de 2018 a renforcé cette protection. Cette chronologie montre que les autorités ont anticipé les risques numériques bien avant que tout le monde ait un smartphone en poche. Elles avaient raison : aujourd'hui, nos vies numériques contiennent plus d'informations personnelles que jamais et les enjeux de sécurité sont colossaux.

180. Pourquoi est-il important de mettre à jour ses logiciels ?

A) Pour changer leur apparence
B) Pour corriger des failles de sécurité
C) Pour supprimer des fonctionnalités

Les mises à jour, c'est le système immunitaire de tes appareils numériques.
Chaque jour, des chercheurs en sécurité et des pirates informatiques découvrent de nouvelles failles dans les logiciels. C'est une course contre la montre !
Dès qu'une entreprise découvre une faille, elle doit rapidement créer un « patch » (un correctif) et le distribuer à tous les utilisateurs. Le problème, c'est que beaucoup de gens ignorent ou reportent ces mises à jour parce qu'elles prennent du temps ou redémarrent l'appareil. Pendant ce délai, leur système informatique reste vulnérable. Les pirates le savent et ciblent spécifiquement les appareils non mis à jour. C'est pourquoi les mises à jour automatiques sont une excellente idée : elles protègent ton appareil.
Oui, parfois ça change l'interface, mais c'est surtout pour ta sécurité !

Ressource pour tous : Se protéger sur Internet (CNIL)

181. Qu'est-ce qu'un pare-feu ?

A) Un système qui filtre le trafic réseau pour bloquer les connexions non autorisées
B) Un outil qui améliore automatiquement la qualité du signal Wi-Fi
C) Un logiciel qui optimise la vitesse de chargement des sites Internet

Un pare-feu informatique, c'est le vigile de ton réseau. Chaque information qui veut entrer ou sortir de ton ordinateur doit passer par lui. Il examine chaque « paquet » de données
et décide : « Toi, tu peux passer, toi non ! ».
Il fonctionne avec des règles préprogrammées : par exemple, il peut bloquer tous les accès depuis certains pays connus pour leurs activités de piratage, ou empêcher certains programmes de communiquer avec Internet. Les pare-feux existent sous forme de logiciels (installés sur ton ordinateur) ou d'équipements physiques (des boîtiers que les entreprises placent entre leur réseau et Internet). Ils analysent les adresses IP, les ports de communication et même parfois le contenu des messages pour détecter des tentatives d'intrusion. Ta box à la maison en a probablement un intégré.
C'est une protection essentielle, mais pas suffisante à elle seule : il faut la combiner avec un antivirus et de bonnes pratiques.

182. Quand tu achètes quelque chose sur un site de vente entre particuliers, quelle est la meilleure pratique ?

A) Payer immédiatement par virement bancaire pour réserver l'article
B) Rencontrer le vendeur en personne dans un lieu public et payer en espèces
C) Donner ton numéro de carte bancaire par téléphone pour aller plus vite

Les sites de vente entre particuliers peuvent être dangereux si tu ne fais pas attention ! Les arnaques les plus courantes commencent par des annonces trop belles pour être vraies : prix très bas, photos floues ou volées sur d'autres sites. Les escrocs demandent souvent un paiement rapide par virement, Western Union ou cartes prépayées. Une fois l'argent envoyé, impossible de le récupérer ! La règle d'or : rencontre toujours le vendeur en personne, dans un lieu public et animé (centre commercial, gare). Examine bien l'objet avant de payer. Méfie-toi des vendeurs qui refusent de te rencontrer ou qui inventent des excuses (voyage, maladie…). N'envoie jamais d'argent à l'avance, même pour « réserver ». Utilise les systèmes de paiement sécurisés des plateformes quand c'est possible. Et surtout, fais confiance à ton intuition : si quelque chose te paraît suspect, n'hésite pas à annuler !



Ressource pour tous :
Sites de vente entre particuliers :
20 conseils pour éviter les arnaques
(cybermalveillance.gouv.fr)

183. Qu'est-ce qu'une attaque par « ransomware » ?

A) Une attaque qui vole des photos
B) Une attaque qui demande une rançon pour débloquer des fichiers
C) Une attaque qui ralentit l'ordinateur

Le ransomware, c'est le kidnapping de tes données. Les pirates informatiques s'introduisent dans ton ordinateur et chiffrent tous tes fichiers : photos, documents, vidéos, tout devient inaccessible. Puis ils affichent un message de « rançon » : « Pour récupérer tes fichiers, paye X euros dans les 48 h, sinon tout sera définitivement perdu ». Ces attaques visent aussi bien les particuliers que les grandes entreprises, hôpitaux ou administrations. Le piratage devient de plus en plus sophistiqué : les pirates étudient leurs victimes, adaptent le montant de la rançon à leurs moyens et menacent parfois de publier les données volées en plus de les chiffrer.
Payer ne garantit pas la récupération des fichiers et ça finance le crime organisé.
La meilleure défense reste la prévention : sauvegardes régulières, mises à jour, antivirus efficace et prudence avec les emails suspects.

Ressource pour tous : Cyber Guide Famille (cybermalveillance.gouv.fr)

184. Comment appelle-t-on un hacker qui agit pour de bonnes causes ?

A) White hat
B) Black hat
C) Red hat

Dans l'univers du hacking, les « chapeaux » définissent les intentions. Un hacker « white hat » (chapeau blanc) est un expert en sécurité informatique qui utilise ses compétences pour le bien. Il travaille légalement pour des entreprises, des gouvernements ou de manière indépendante pour détecter et signaler les failles de sécurité.
Ces hackers éthiques participent à des programmes de « bug bounty » où les entreprises les récompensent pour avoir trouvé des vulnérabilités. À l'opposé, les « black hat » (chapeau noir) sont les cybercriminels qui exploitent les failles pour voler, détruire ou extorquer. Entre les deux, il existe des « grey hat » qui naviguent dans une zone plus floue. Beaucoup de white hats sont d'anciens black hats qui ont choisi de mettre leurs talents au service de la sécurité. Cette reconversion montre qu'on peut utiliser les mêmes compétences techniques pour protéger plutôt que pour nuire.
Les white hats sont essentiels pour maintenir la sécurité de notre monde numérique.

Ressource pour un adulte : On t'explique en 1 min ce qu'est le hacking éthique (Futurasciences)

185. Les hackers célèbres sont parfois :

A) Employés par des entreprises
B) En prison
C) Les deux

L'histoire du hacking regorge de parcours fascinants et contradictoires.
Quelques hackers célèbres ont connu les deux faces de la médaille :
la prison et les bureaux prestigieux. Par exemple, Kevin Mitnick, l'un des pirates les plus recherchés des années 90, a passé cinq ans en prison avant de devenir consultant en sécurité informatique pour de grandes entreprises.
Cette double destinée illustre une réalité : les compétences qui permettent de pirater sont exactement les mêmes que celles nécessaires pour protéger les systèmes informatiques. Beaucoup d'entreprises tech préfèrent embaucher d'anciens pirates plutôt que de les avoir comme ennemis.

Ressources pour un adulte : Les hackers sont-ils les héros contemporains ? (ARTE)

186. Que signifie l'icône d'un cadenas fermé dans la barre d'adresse d'un site Internet ?

A) Le site est en maintenance
B) La connexion est sécurisée (HTTPS)
C) Le site est payant

Ce petit cadenas est ton meilleur ami quand tu navigues sur Internet.
Il indique que le site utilise le protocole HTTPS (HyperText Transfer Protocol Secure), qui chiffre toutes les communications entre ton navigateur et le serveur du site.
Concrètement, ça signifie que si quelqu'un intercepte tes données pendant qu'elles voyagent sur Internet, il ne pourra pas les lire : elles sont transformées en code incompréhensible. C'est particulièrement crucial quand tu saisis des informations sensibles : mots de passe, numéros de carte bancaire, informations personnelles.
Le HTTPS fonctionne grâce à un système de certificats de sécurité.
Attention : un cadenas ne garantit pas que le site est honnête, juste que la connexion est sécurisée. Un site de phishing peut avoir un certificat HTTPS valide !
Vérifie toujours l'adresse complète du site.

187. Qu'est-ce qu'une adresse IP ?

A) Le mot de passe de ton ordinateur
B) L'adresse unique de ton appareil sur Internet
C) Le nom de ton fournisseur d'accès Internet

Une adresse IP, c'est l'adresse postale de ton ordinateur ou de ton téléphone sur Internet ! Quand tu envoies une lettre, tu écris l'adresse du destinataire sur l'enveloppe. Sur Internet, c'est pareil : chaque appareil connecté a sa propre adresse IP pour recevoir les informations. Elle ressemble à ça : 192.168.1.1 (4 groupes de chiffres séparés par des points). Il existe deux types d'adresses IP : l'adresse privée (utilisée chez toi, dans ta maison) et l'adresse publique (visible sur Internet).
Ton adresse IP peut révéler ta localisation approximative et ton fournisseur d'accès Internet. C'est pourquoi certaines personnes utilisent des VPN pour la masquer.
Les sites web utilisent ton adresse IP pour t'envoyer les pages que tu demandes, mais aussi parfois pour te géolocaliser ou te proposer de la publicité ciblée.
Connaître son adresse IP, c'est comprendre comment fonctionne Internet et mieux protéger sa vie privée !

188. À quoi sert la double authentification ?

A) Allumer plus vite son ordinateur
B) Se connecter plus facilement à une application
C) Avoir une sécurité renforcée

La double authentification (ou 2FA), c'est avoir deux serrures sur ta porte numérique au lieu d'une. Le principe : même si quelqu'un découvre ton mot de passe, il ne peut pas accéder à ton compte sans le second facteur d'authentification.
Généralement, tu saisis ton mot de passe, puis tu reçois un code par SMS ou via une application. Certains systèmes utilisent aussi la biométrie : empreintes digitales, reconnaissance faciale. Cette méthode réduit drastiquement les risques de piratage.
Même si ton mot de passe fuite dans une base de données piratée, ton compte reste protégé. C'est particulièrement important pour les comptes sensibles : banque, réseaux sociaux, emails. Oui, c'est une étape supplémentaire à chaque connexion, mais quelques secondes de plus valent mieux que des heures à récupérer un compte piraté.
La plupart des grandes plateformes proposent désormais cette option : active-la !

189. Lequel de ces mots de passe est le plus sécurisé ?

A) Seulement des chiffres, ex. : 123456
B) Lettres, chiffres et caractères spéciaux, ex. : x!pYJXdP)GF
C) Un mot facile à retenir, ex. : Motdepasse

Un bon mot de passe, c'est mathématique ! Plus tu mélanges de types de caractères différents, plus tu multiplies les possibilités et plus il devient difficile à craquer.
Un mot de passe de 8 caractères avec seulement des chiffres (comme 12345678) n'offre que 100 millions de combinaisons possibles. Ça semble énorme, mais un ordinateur moderne peut toutes les tester en quelques secondes ! En revanche, un mot de passe de 8 caractères mélangeant majuscules, minuscules, chiffres et symboles offre plus de 6 000 milliards de combinaisons. Les pirates utilisent des « dictionnaires » contenant les mots de passe les plus courants : « 123456 », « password », « motdepasse » sont cassés instantanément.
Ils testent aussi les variations prévisibles : « Motdepasse1 » ou « Motdepasse! ».
L'idéal : un gestionnaire de mots de passe qui génère et stocke des mots de passe complexes uniques pour chaque compte. Sinon, invente une phrase personnelle et transforme-la : « J'ai 15 ans et j'adore les pizzas ! » devient « J'ai15a&j'a2rélespizzas! ».

Ressource pour tous :
Générer un mot de passe solide (CNIL)

190. Quelle est la meilleure défense contre le piratage ?

A) Mettre un antivirus et penser que cela suffit à bloquer toutes les attaques
B) La prévention et l'éducation
C) Utiliser un mot de passe très complexe et le réutiliser partout pour ne pas l'oublier

La cybersécurité, c'est avant tout une question d'éducation et de bon sens numérique. Aucune technologie n'est infaillible : le maillon faible, c'est souvent l'utilisateur qui clique sans réfléchir ou utilise le même mot de passe partout. La formation et la sensibilisation sont donc essentielles. Les cyber-attaques réussissent principalement grâce à l'ignorance ou la négligence des victimes. Apprendre à reconnaître un email de phishing, comprendre l'importance des mises à jour, savoir créer des mots de passe solides... ces connaissances sont plus efficaces que le meilleur antivirus. C'est pourquoi les entreprises investissent massivement dans la formation de leurs employés et pourquoi des jeux éducatifs sur la cybersécurité se développent : ils permettent d'apprendre en s'amusant, de mémoriser les bonnes pratiques. La bonne approche : rester vigilant mais confiant, armé des bonnes connaissances.

Ressources pour tous : Appliquer les dix règles d'or préventives (cyber.gouv.fr) et Future of Cyber de l'association Latitudes

191. Qu'appelle-t-on une attaque « par force brute » ?

A) Tester différents serveurs pour trouver celui qui a la connexion la plus lente
B) Deviner un mot de passe avec des essais multiples
C) Utiliser un logiciel qui analyse la vitesse d'un réseau pour repérer des failles

Tu as probablement déjà oublié le mot de passe de ton compte et essayé plusieurs combinaisons jusqu'à trouver la bonne. Eh bien, une attaque par force brute consiste à tester, l'une après l'autre, chaque combinaison possible d'un mot de passe ou d'une clé pour un identifiant donné. Mais contrairement à toi qui cherches ton propre mot de passe, les pirates utilisent des logiciels automatisés qui peuvent tester des milliers de combinaisons par seconde !
Cette méthode fonctionne particulièrement bien contre les mots de passe faibles. Si ton mot de passe est « 123456 » ou « motdepasse », un ordinateur peut le deviner en quelques secondes. En revanche, un mot de passe complexe avec des majuscules, des chiffres et des symboles peut prendre des années à être craqué.
C'est pourquoi il est crucial de créer des mots de passe robustes et uniques pour chaque compte.

192. Pourquoi certaines attaques sont appelées « social engineering » ?

A) Elles utilisent des bugs dans les logiciels
B) Elles manipulent les gens pour obtenir leurs infos
C) Elles concernent les réseaux sociaux

Le « social engineering » ou ingénierie sociale n'a rien à voir avec la construction de ponts ou de bâtiments ! L'ingénierie sociale est une pratique de manipulation psychologique à des fins d'escroquerie. Au lieu d'attaquer directement les systèmes informatiques, les cybercriminels s'attaquent à toi, l'utilisateur.
L'ingénierie sociale mise sur l'instinct fondamental de l'être humain à faire confiance pour voler des informations personnelles. Par exemple, un pirate peut se faire passer pour ton professeur par email et te demander tes identifiants « pour vérifier ton compte ».
Ces attaques réussissent parce qu'elles exploitent nos émotions : la peur, l'urgence, la curiosité ou l'envie d'aider. La meilleure défense ? Toujours vérifier l'identité de la personne qui demande des informations sensibles.

Ressource pour tous : Comment éviter les arnaques du web ? (CLEMI)

193. Qu'est-ce qu'un VPN et pourquoi est-il utile ?

A) Un Virus Protecteur Numérique qui nettoie automatiquement ton ordinateur
B) Un logiciel qui accélère ta connexion Internet
C) Un réseau privé virtuel qui protège tes données en ligne

Un VPN (Virtual Private Network) fonctionne comme un tunnel secret sur Internet. Quand tu navigues normalement, tes données voyagent « à découvert » et peuvent être interceptées par des personnes malveillantes, surtout sur les réseaux Wi-Fi publics. Le VPN chiffre tes informations et fait croire que tu te connectes depuis un autre endroit. C'est particulièrement utile quand tu utilises le Wi-Fi d'un café ou de ton collège. Les cybercriminels adorent ces réseaux publics car ils sont souvent moins sécurisés. Avec un VPN, même si quelqu'un intercepte tes données, il ne pourra pas les lire car elles sont cryptées. Voici quelques VPN fiables : NordVPN, Surfshark ou encore Norton.

194. Combien de temps faut-il en moyenne pour trouver un mot de passe de 8 caractères contenant uniquement des lettres minuscules ?

A) Quelques minutes
B) Quelques heures
C) Quelques mois

Les ordinateurs modernes sont incroyablement rapides pour deviner les mots de passe. Un mot de passe de 8 caractères avec seulement des lettres minuscules peut être cracké en moins de 22 heures par un ordinateur standard ! C'est pourquoi il faut absolument varier tes mots de passe. Ajouter des majuscules, des chiffres et des symboles multiplie énormément les possibilités. Un mot de passe de 12 caractères mélangeant lettres, chiffres et symboles prendrait des milliers d'années à craquer. Les hackers testent aussi des variantes de ton nom, ta date de naissance ou des informations trouvées sur tes réseaux sociaux. C'est pourquoi il ne faut jamais utiliser d'informations personnelles dans tes mots de passe.

Source : Combien de temps un pirate met-il pour trouver votre mot de passe ? Comment vous protéger ? (République française)

195. Qu'est-ce qu'une attaque par « typosquatting » ?

A) Une attaque qui corrige tes fautes de frappe
B) L'utilisation de noms de sites Internet similaires à des sites légitimes pour te tromper
C) Un virus qui modifie tes messages

Le typosquatting exploite les erreurs de frappe que tout le monde commet.
Les cybercriminels enregistrent des noms de domaines presque identiques à des sites populaires, en changeant une lettre ou en ajoutant/supprimant un caractère.
Par exemple, ils peuvent créer « gooogle.com » au lieu de « google.com » ou « youtub.com » au lieu de « youtube.com ». Quand tu tapes trop vite et que tu fais une faute, tu atterris sur leur faux site qui ressemble exactement au vrai. Ces sites malveillants peuvent voler tes mots de passe, installer des virus ou te rediriger vers des contenus dangereux. Certains cybercriminels achètent des centaines de variantes d'un même site populaire. Cette technique est particulièrement efficace car elle paraît accidentelle. Tu ne soupçonnes pas qu'on essaie de te piéger.
Pour t'en protéger, utilise des marque-pages pour tes sites préférés et vérifie toujours l'URL avant de saisir des informations sensibles.

196. Qu'est-ce qu'Evil Corp ?

A) Une entreprise spécialisée dans les jeux vidéo dangereux
B) Une organisation cybercriminelle
C) Un groupe d'hackers éthiques qui combat les pirates informatiques

Evil Corp est l'une des organisations cybercriminelles les plus dangereuses de l'histoire moderne. Ce groupe russe dirigé par Maksim Yakubets a réussi à voler plus de 100 millions de dollars grâce au logiciel malveillant « Dridex » qui infectait les ordinateurs pour voler les identifiants bancaires dans le monde entier. Cette organisation utilisait des techniques sophistiquées pour contourner les systèmes de sécurité bancaire.
Aux États-Unis, Evil Corp est considéré comme le « groupe de cybercriminels le plus dangereux au monde ». L'enquête a révélé qu'ils avaient développé plusieurs variantes de malware pour maximiser leurs profits. Le nom Evil Corp rappelle le surnom utilisé dans la série Mr. Robot pour désigner une grande entreprise fictive (E Corp).

Ressource pour un adulte : Rançons, extorsions, sabotage - le BUSINESS des HACKERS

197. Dans quelle situation tes parents utiliseraient-ils probablement une signature électronique ?

A) Se connecter à un site administratif
B) Pour signer un contrat d'assurance en ligne
C) Pour valider l'installation d'une application sur leur ordinateur

Tes parents peuvent utiliser la signature électronique pour signer des documents importants sans avoir besoin de se déplacer ! Signer un contrat d'assurance en ligne est un exemple parfait : au lieu de prendre rendez-vous et de se rendre dans une agence, ils peuvent tout faire depuis la maison en quelques clics.
La signature électronique est particulièrement pratique pour les adultes car elle leur fait gagner du temps. Pendant la pandémie de Covid-19, beaucoup d'entreprises ont découvert les avantages de la signature électronique car les gens ne pouvaient pas se déplacer facilement. En France, beaucoup d'entreprises utilisent maintenant la signature électronique. Grâce à un certificat numérique, cette méthode garantit l'intégrité du document et l'authentification de l'auteur. C'est très utile en cas de problème ou de désaccord plus tard !

198. Que peut faire un hacker avec l'accès à ta webcam ?

A) Surveiller ton activité en analysant uniquement les sites que tu consultes
B) Modifier les réglages de ton ordinateur sans que tu t'en rendes compte
C) T'espionner, faire du chantage ou voler des informations confidentielles

L'accès non autorisé à ta webcam transforme ton ordinateur en outil d'espionnage. Les pirates peuvent t'observer à ton insu, enregistrer des vidéos compromettantes et les utiliser pour du chantage. Ils peuvent voir ton écran, tes habitudes, les personnes qui t'entourent et même lire des documents confidentiels que tu affiches.
Certains logiciels malveillants activent la webcam sans allumer le voyant lumineux, rendant l'espionnage invisible. Les pirates recherchent particulièrement les moments où tu saisis des mots de passe, des numéros de carte bancaire ou des informations personnelles. Ils peuvent aussi utiliser ces enregistrements pour créer des deepfakes ou usurper ton identité. Pour te protéger, couvre ta webcam avec un autocollant ou un cache spécialisé quand tu ne l'utilises pas. Vérifie régulièrement les autorisations de tes applications et désactive l'accès à la webcam pour les programmes qui n'en ont pas besoin.

Ressource pour un adulte : Chantage à la webcam ou à l'ordinateur prétendus piratés, que faire ? (cybermalveillance.gouv.fr)

199. À quoi sert un CAPTCHA sur un site Internet ?

A) Vérifier que tu es un humain et non un robot
B) Améliorer la vitesse de chargement du site
C) Compter le nombre de visiteurs sur le site

Tu as sûrement déjà vu ces petits tests bizarres où il faut recopier des lettres déformées, cliquer sur des images de feux tricolores ou faire glisser un curseur ?
C'est un CAPTCHA ! Cet acronyme vient de l'anglais et signifie « test public complètement automatisé pour distinguer les ordinateurs des humains ». Le but ? Empêcher les robots malveillants d'attaquer les sites web. Ces robots peuvent envoyer des milliers de messages de spam, créer de faux comptes ou essayer de deviner des mots de passe. Les CAPTCHA exploitent nos capacités humaines : reconnaître des formes, lire des textes déformés ou identifier des objets sur des photos. Les robots ont encore du mal avec ces tâches ! Même si c'est parfois agaçant, les CAPTCHA protègent les sites et tes données personnelles. Ils évoluent constamment car les robots deviennent de plus en plus intelligents ! Les CAPTCHA servent aussi à utiliser l'expertise humaine pour entraîner des intelligences artificielles.

200. Qu'appelle-t-on le « quishing » ?

A) Une arnaque qui utilise un QR code pour te piéger
B) Une technique qui oblige l'utilisateur à scanner un QR code pour vérifier son identité
C) Une méthode utilisée pour diffuser rapidement un lien vers un faux site sécurisé

Les QR codes sont pratiques mais peuvent cacher des pièges redoutables. Contrairement à un lien classique que tu peux lire avant de cliquer, un QR code masque complètement sa destination. Les cybercriminels en profitent pour créer des codes malveillants. Ils peuvent coller leurs QR codes sur des affiches légitimes, les envoyer par email ou les publier sur les réseaux sociaux. Quand tu scannes un QR code piégé, tu peux être redirigé vers un faux site web qui vole tes informations ou télécharger automatiquement un virus sur ton téléphone. Certains QR codes peuvent même composer automatiquement un numéro surtaxé ou envoyer des SMS payants.
Cette technique est de plus en plus utilisée car les gens font confiance aux QR codes. Pour te protéger, utilise une application de scan qui affiche l'URL avant de l'ouvrir et méfie-toi des QR codes trouvés dans des lieux publics ou reçus par email de sources inconnues.

partenaires

Nous tenons à remercier chaleureusement nos partenaires **Banque de France, Métropole Rouen Normandie, Réseau Canopé et ministère de la Culture** pour leur soutien précieux. Grâce à leur engagement et à leur confiance, nous pouvons offrir aux jeunes éclaireurs du numérique une expérience ludique et pédagogique de qualité.

Leur contribution a été essentielle pour faire grandir ce projet.

crédits

Création du concept et coordination générale : Doralie BESNARD-GUIOL

Conception de la mécanique de jeu : Tony GODIN (consultant)

Illustrations et conception graphique : Cédric DELAHAYE

Conception graphique : David RAULIN

Rédaction et relecture des questions : Marie AIT DAOUD – Adelaide ALBOUY-KISSI Stéphanie BREGER LABARRERE – Gunther BUNEL - Véronique CHATAIN Vincent COURBOULAY – Héloïse DANO - Erwan KERVRAN - Aurélien MARIAGE Géraldine MONTAGNON – Wilfried MOREAU – Yves NICOLAS - Aline PARES Marie-Hélène PORET - Callista SPITERI – Marion STAURI - Marie-Eve TAYOT Jérôme VALAIS - Lucile VANNIER

Rédaction du livret maître du jeu : Charline CORMIER

Relecture du livret maître du jeu : Réseau Canopé

Ce jeu est distribué sous licence Creative Commons Attribution
Pas d'utilisation commerciale • Pas de modification • 4.0 International (CC BY-NC-ND 4.0)

Certains textes de ce livret ont bénéficié d'une assistance à la rédaction via Claude AI ; chaque texte a été relu, vérifié et ajusté systématiquement par plusieurs relecteurs afin d'en garantir la qualité et l'exactitude.

NUMéVILLE

Les éclaireurs du numérique