2026

Cahier de vacances numérique

- Quiz : Le numérique au quotidien
- Défi numérique
- Jeu des 7 erreurs : Le faux colis
- Mots mêlés
- Recette du bon mot de passe **Actualisé !**
- Mots croisés
- Vrai ou Faux
- Le petit dico du numérique

+ EXTRA BONUS

Sommaire

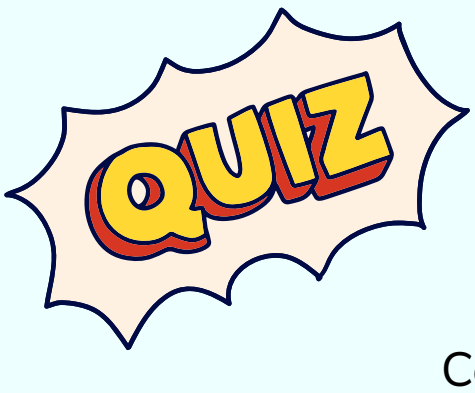
Bienvenue dans votre cahier de vacances numérique – édition 2026 !

Cette année encore, pas de devoirs ni de stress : juste le plaisir de jouer, de s'interroger et de découvrir.

Au programme : quiz, défis, jeux et un grand thème qui fait parler tout le monde… l'intelligence artificielle.

Pas de panique ! On l'aborde en douceur, avec curiosité et bonne humeur.
Installez-vous confortablement, prenez un stylo… et laissez-vous surprendre !

Bel été à tous,
Votre conseillère numérique.



“Le numérique au quotidien”

Coche la ou les bonnes réponses parmi les propositions.

1. À quoi sert une application sur un smartphone ?
□ À décorer l'écran
□ À accomplir une tâche précise (photos, météo, messagerie...)
□ À protéger le téléphone contre les chutes
□ À recharger la batterie plus vite

2. Qu'est-ce qu'un mot de passe sécurisé ?
□ Le prénom de ton animal de compagnie
□ Une combinaison longue mêlant lettres, chiffres et caractères spéciaux
□ Ta date de naissance
□ Le mot "password"

3. Que signifie le petit cadenas affiché dans la barre d'adresse d'un site ?
□ Le site est gratuit
□ La connexion entre ton navigateur et le site est chiffrée
□ Le site appartient à l'État
□ Tu es connecté à Internet

4. Qu'est-ce qu'un SMS d'hameçonnage ?
□ Un message publicitaire envoyé par une marque
□ Un message frauduleux imitant une entreprise de confiance pour récupérer tes données
□ Un SMS envoyé par erreur
□ Une notification de ton opérateur téléphonique

5. Parmi ces indices, lequel peut trahir une image générée par IA ?
□ Elle est toujours floue
□ On peut parfois repérer des détails étranges : doigts difformes, texte illisible, symétrie trop parfaite
□ Elle porte toujours un filigrane visible
□ Sa résolution est toujours très basse

6. Qu'est-ce que la double authentification ?
□ Avoir deux mots de passe différents pour le même compte
□ Une vérification en deux étapes pour accéder à un compte (mot de passe + code SMS par exemple)
□ Se connecter depuis deux appareils en même temps
□ Changer son mot de passe deux fois par an

7. Un chatbot peut-il se tromper ?
□ Non, il est connecté à Internet en temps réel et ses réponses sont toujours exactes
□ Oui, il peut produire des informations fausses présentées avec assurance
□ Non, il vérifie toujours ses sources avant de répondre
□ Oui, mais uniquement sur les sujets scientifiques

8. Qu'est-ce qu'une métadonnée ?
□ Un type de fichier vidéo
□ Une information cachée dans un fichier révélant sa date, son lieu de création ou l'appareil utilisé
□ Un mot de passe secondaire
□ Une publicité ciblée

9. Que permet le RGPD aux citoyens européens ?
□ D'utiliser Internet gratuitement
□ De demander à une entreprise de supprimer leurs données personnelles
□ D'accéder gratuitement à tous les services numériques européens
□ D'accéder aux données des autres utilisateurs

10. Qu'est-ce que l'empreinte numérique ?
□ La signature électronique d'un document officiel
□ L'ensemble des traces laissées par une personne sur Internet au fil de ses usages
□ Un outil de reconnaissance digitale sur smartphone
□ Le poids en mégaoctets d'un fichier numérique

Jeu des 7 erreurs : Le faux colis

Lis attentivement les deux versions de la situation ci-dessous. Le texte A présente une réaction prudente, le texte B contient 7 erreurs. À toi de les retrouver !

Texte A – La bonne réaction

Julie reçoit un SMS avec une photo montrant un colis portant son nom, accompagné du message : "URGENT : Votre colis est bloqué ! Payez 1,99€ de frais de réexpédition ici : http://laposte-livraison-colis.fr"

Méfiante, Julie observe la photo de plus près : les lettres de son nom semblent légèrement déformées et l'étiquette paraît trop parfaite — elle pense à une image générée par intelligence artificielle. Elle remarque aussi que le lien ne correspond pas au site officiel de La Poste. Elle ne clique pas dessus, ne rappelle pas le numéro expéditeur et se connecte directement au site officiel de La Poste depuis son navigateur. Aucun colis ne lui est destiné. Elle supprime le SMS et signale le numéro comme spam.

Texte B – La mauvaise réaction (avec 7 erreurs)

Julie reçoit un SMS avec une photo montrant un colis portant son nom, accompagné du message : "URGENT : Votre colis est bloqué ! Payez 1,99€ de frais de réexpédition ici : http://laposte-livraison-colis.fr"

Rassurée par la photo qui montre bien son nom, elle ne remarque pas que les lettres sont légèrement déformées. Elle clique sur le lien sans vérifier l'adresse et tombe sur une page ressemblant trait pour trait au site de La Poste. On lui demande ses coordonnées postales complètes, qu'elle saisit sans hésiter. Elle règle ensuite les 1,99€ avec sa carte bancaire. Quelques jours plus tard, elle reçoit des appels d'un numéro étranger qu'elle ne reconnaît pas, mais elle décroche quand même. Ne sachant pas comment joindre le livreur autrement, elle rappelle le numéro expéditeur pour demander s'il peut repasser le lendemain ou déposer le colis dans un point relais.

Recette du bon mot de passe
version 2.0

Ingrédients (pour 1 mot de passe bien costaud) :

- 1 pincée de majuscules (A à Z)
- 2 cuillères à soupe de minuscules (a à z)
- 1 poignée de chiffres croustillants (0 à 9)
- 1 cuillerée de caractères spéciaux (comme ! @ # $ % ? *)
- Une bonne dose de créativité

Préparation :

1. Préchauffez votre cerveau à température logique 🧠
2. Dans un bol, inventez une courte phrase qui n'existe que dans votre tête — quelque chose d'imaginaire ou d'absurde, que personne ne pourrait deviner : "Mon chat mange des étoiles filantes", "Le soleil sent la cannelle"...
3. Prenez les premières lettres de chaque mot et mélangez majuscules et minuscules.
4. Saupoudrez généreusement de chiffres — évitez votre date de naissance ou votre code postal, trop faciles à trouver !
5. Incorporez un ou deux caractères spéciaux pour relever le tout.
6. Mélangez bien : visez 12 à 14 caractères minimum pour un usage courant — plus c'est long, plus c'est fort !
7. Goûtez : votre mot de passe doit être unique, complexe et inoubliable pour vous seul.

Exemple gourmand :

✨ Mc@mEf14!

("Mon chat mange des étoiles filantes" → Mcmdef, transformé)

Astuce du chef :

Plus le mot de passe est long, plus il est fort !
Utilisez une phrase secrète transformée, comme :
Lc0uDr3Nt! — "Les cousins dressent des renards têtus"

À éviter absolument : votre prénom, celui d'un proche, votre ville, votre animal de compagnie — ces informations se trouvent facilement sur les réseaux sociaux !

Vrai ou Faux

Lis chaque affirmation et coche ta réponse. Les solutions sont en dernière page !

1. Un mot de passe comme "123456" est utilisé par des millions de personnes dans le monde.
□ Vrai □ Faux

2. Le petit cadenas dans la barre d'adresse d'un site garantit que ce site est fiable et sécurisé.
□ Vrai □ Faux

3. Une intelligence artificielle peut rédiger un e-mail, écrire un poème ou générer une image en quelques secondes.
□ Vrai □ Faux

4. Supprimer une photo de ses réseaux sociaux la fait disparaître définitivement d'Internet.
□ Vrai □ Faux

5. Un chatbot vérifie toujours ses informations avant de répondre.
□ Vrai □ Faux

6. Mon smartphone peut collecter des données sur mes habitudes même quand je ne l'utilise pas.
□ Vrai □ Faux

7. En Europe, j'ai le droit de demander à une entreprise de supprimer mes données personnelles.
□ Vrai □ Faux

8. Un deepfake est toujours facile à repérer à l'œil nu.
□ Vrai □ Faux

9. L'intelligence artificielle est totalement neutre et objective dans ses réponses.
□ Vrai □ Faux

10. Utiliser le même mot de passe sur plusieurs sites est risqué.
□ Vrai □ Faux

Challenge numérique

Défi numérique N°1 : Chaud devant !

Rédige le faux SMS d'arnaque le plus convaincant possible : un faux sms d'amende à payer pour excès de vitesse, que je dois régler sous 24h sous peine de majoration... Soigne le lien frauduleux, le ton alarmiste et les détails qui font mouche !

Défi numérique N°2 : Arnaque-moi si tu peux !

Tu as 2 minutes max pour me convaincre au téléphone que tu es un agent de La Poste, ma banque, ou les impôts... et que j'ai absolument besoin de te donner mes informations personnelles.

Prépare ton scénario, soigne ton discours, et voyons si tu arrives à me piéger !

À tenter via un appel téléphonique, un message vocal WhatsApp ou un enregistrement audio.

À vous de jouer !

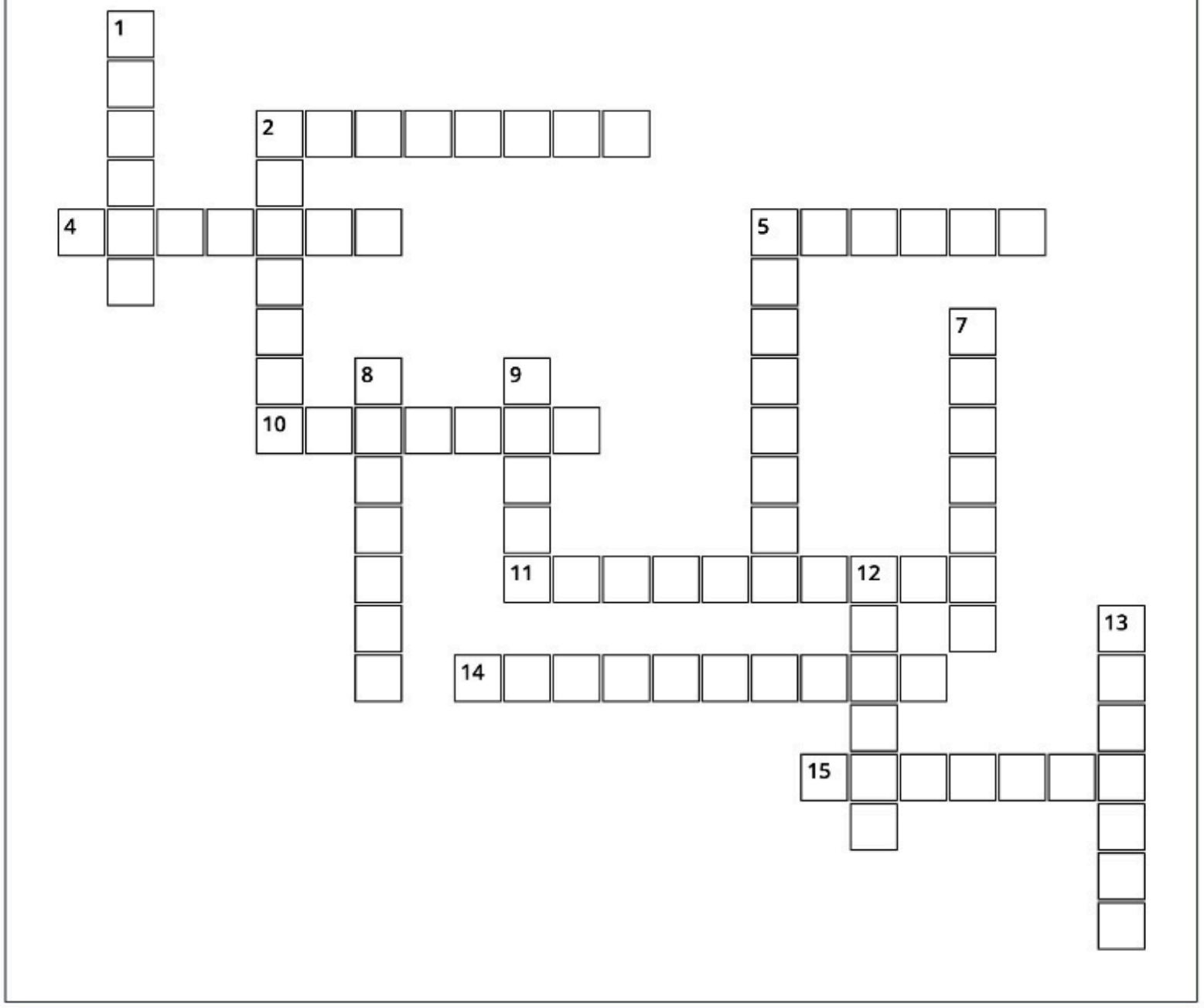
Mots mêlés

ALGORITHME
CHATBOT
CHIFFREMENT
DEEPFAKE
DONNÉES
EMPREINTE
HAMECONNAGE
NUMÉRIQUE
RGPD
VIRUS

N	B	I	G	V	F	D	E	E	P	F	A	K	E
U	F	V	I	R	U	S	D	M	I	S	E	G	I
M	M	I	H	J	W	K	D	Q	P	A	D	T	E
É	X	C	H	A	M	E	C	O	N	N	A	G	E
R	F	M	O	D	Y	Y	I	O	X	D	B	D	O
I	G	T	B	R	H	J	M	H	F	E	S	J	E
Q	J	B	R	E	C	H	A	T	B	O	T	T	M
U	T	G	N	G	W	L	U	M	Q	P	Z	B	P
E	M	A	L	G	O	R	I	T	H	M	E	S	R
A	Q	P	X	D	A	D	R	U	N	D	R	N	E
T	D	O	N	N	É	E	S	L	N	E	K	O	I
O	A	Q	J	W	H	N	W	R	G	P	D	X	N
Z	C	H	T	X	K	I	N	S	O	L	F	J	T
C	H	I	F	F	R	E	M	E	N	T	D	C	E

Mots croisés

Cybersécurité



Horizontal

2. Méthode pour sécuriser des données en les rendant illisibles.
4. Période durant laquelle un utilisateur est connecté à un service.
5. Ce terme désigne une personne qui accède illégalement à des systèmes informatiques.
10. Code qui tire parti d'une vulnérabilité dans un logiciel.
11. Copie de données pour prévenir leur perte.
14. Code secret pour accéder à un compte.
15. Logiciel nuisible conçu pour endommager un système.

Vertical

1. Personne qui pénètre dans des systèmes informatiques sans autorisation.
2. Utilisé pour protéger des informations, ce terme désigne un code secret.
5. Technique pour tromper les utilisateurs et voler des informations.
7. Informations stockées sur un ordinateur ou un serveur.
8. Logiciel espion qui collecte des informations à l'insu de l'utilisateur.
9. Programme malveillant qui infecte un ordinateur.
12. Ensemble d'ordinateurs connectés pour partager des informations.
13. Dispositif qui protège un réseau des intrusions.

Le petit dico du numérique

Adresse IP : Un numéro unique attribué à ton appareil quand il se connecte à Internet. Un peu comme une adresse postale, mais pour le monde numérique.

Algorithme : Une suite d'instructions données à un ordinateur pour qu'il accomplisse une tâche. C'est lui qui décide ce que tu vois en premier sur les réseaux sociaux !

Chatbot : Un programme capable de tenir une conversation écrite avec toi. ChatGPT en est l'exemple le plus connu aujourd'hui.

Chiffrement : Une technique qui transforme tes données en code illisible pour quiconque n'a pas la clé. Les messageries comme WhatsApp l'utilisent pour protéger tes échanges.

Deepfake : Une vidéo ou une image fabriquée par intelligence artificielle pour faire dire ou faire quelque chose à quelqu'un qui ne l'a jamais dit ni fait. Difficile à repérer à l'œil nu !

Double authentification : Une sécurité supplémentaire à la connexion : après ton mot de passe, on te demande un code reçu par SMS. Difficile à contourner pour un escroc !

Empreinte numérique : La trace que tu laisses chaque fois que tu utilises Internet : sites visités, achats, likes, recherches... Une empreinte que tu peux apprendre à réduire.

Hameçonnage : Une technique d'arnaque où un escroc se fait passer pour une entreprise de confiance (banque, La Poste, impôts...) pour récupérer tes données personnelles.

Métadonnées : Des informations cachées dans tes fichiers qui révèlent plus que tu ne crois : la date, l'heure, l'appareil utilisé, parfois même ta localisation lors d'une photo.

RGPD : Le Règlement Général sur la Protection des Données, une loi européenne qui encadre la façon dont les entreprises collectent et utilisent tes données personnelles. Tu as des droits — et tu peux les exercer !

BONUS 2.0

Les 10 raccourcis clavier de base à connaître

Windows+L : verrouiller son ordinateur rapidement; pratique quand on s'éloigne de son poste !
Windows+D : afficher ou masquer le bureau en un clic
Ctrl+T : ouvrir un nouvel onglet dans le navigateur
Ctrl+W : fermer l'onglet actif
Ctrl+Maj+N : ouvrir une fenêtre de navigation privée
Ctrl+S : enregistrer un document
Ctrl+F : rechercher un mot dans une page ou un document
Alt+Tab : basculer rapidement entre les fenêtres ouvertes
Ctrl+Z : annuler la dernière action
Impr écran : faire une capture de tout l'écran

Les raccourcis Windows à connaître

Windows+Maj+S : capture d'écran d'une zone précise à sélectionner
Ctrl+Maj+T : rouvrir un onglet fermé par erreur ; un classique très utile !
Windows+V : accéder à l'historique du presse-papiers pour retrouver ce que tu as copié précédemment
Windows+I : ouvrir directement les paramètres
Ctrl+Alt+Suppr : accéder aux options de sécurité (verrouiller, changer de session, gestionnaire des tâches)
F2 : renommer un fichier ou dossier sélectionné
Windows+E : ouvrir l'explorateur de fichiers
Ctrl+Maj+Echap : ouvrir directement le gestionnaire des tâches

BONUS  

Sélection films/séries :

Série Black Mirror (2011 -* , Charlie Brooker, Netflix)

- "Nosedive" (S3E1) — une société où chaque interaction est notée sur les réseaux sociaux. Parfait pour parler d'empreinte numérique et d'algorithmes.
- "The Entire History of You" (S1E3) — et si tu pouvais tout revivre en vidéo ? Interroge la mémoire, la vie privée et la surveillance.
- "Smithereens" (S5E2) — un homme prend en otage un employé d'un réseau social. Très ancré dans notre quotidien numérique.

"Ex Machina" (2014, Alex Garland)
Un programmeur est invité par le PDG de son entreprise à évaluer Ava, une intelligence artificielle à apparence humaine. Fascinant, troublant et très bien construit, une réflexion profonde sur ce que l'IA pourrait un jour ressentir... ou simuler. Oscar des meilleurs effets visuels 2016.

Sélection lectures :

"Le bug humain" — Sébastien Bohler
Pourquoi sommes-nous accros aux réseaux sociaux et incapables de décrocher de nos écrans ? Un neuroscientifique explique comment les algorithmes exploitent les failles de notre cerveau. Passionnant et accessible.

"Minuscules Fractures" — Alain Damasio
Un roman de science-fiction qui interroge notre rapport à la technologie et à la surveillance numérique. Poétique, engagé et profondément humain.

Sélection documentaire/Youtube :

"IA : nos nouveaux maîtres ?" (Arte)
Un documentaire clair et pédagogique sur ce que l'intelligence artificielle change concrètement dans nos vies — travail, santé, justice, création...

Chaîne YouTube : Micode
Vidéo conseillée : *"J'ai infiltré un réseau d'arnaqueurs au SMS"*
Michaël, alias Micode, vulgarise la cybersécurité et infiltre les réseaux d'arnaqueurs pour vous montrer comment ils opèrent. Une heure qui change le regard qu'on porte sur les SMS suspects !

Solutions

Quizz

1 : ✅ À accomplir une tâche précise
2 : ✅ Une combinaison longue mêlant lettres, chiffres et caractères spéciaux
3 : ✅ La connexion entre ton navigateur et le site est chiffrée
4 : ✅ Un message frauduleux imitant une entreprise de confiance
5 : ✅ On peut parfois repérer des détails étranges : doigts difformes, texte illisible, symétrie trop parfaite
6 : ✅ Une vérification en deux étapes
7 : ✅ Oui, il peut produire des informations fausses présentées avec assurance
8 : ✅ Une information cachée dans un fichier révélant sa date, son lieu de création ou l'appareil utilisé
9 : ✅ De demander à une entreprise de supprimer leurs données personnelles
10 : ✅ L'ensemble des traces laissées par une personne sur Internet au fil de ses usages

Jeu des 7 erreurs : Arnaque sms

✅ Les 7 erreurs à retrouver dans le texte B

- La photo générée par IA : les lettres du nom sont légèrement déformées — signe que l'image a été fabriquée.
- Le message alarmiste : "URGENT", "bloqué", paiement immédiat demandé — des signaux d'alarme classiques non détectés.
- Le lien frauduleux : http://laposte-livraison-colis.fr — faux domaine non vérifié avant de cliquer.
- Saisie des coordonnées postales complètes sur un site non vérifié.
- Paiement par carte bancaire sur un site frauduleux.
- Décrocher les appels d'un numéro étranger inconnu.
- Rappel du numéro expéditeur : confirme que la ligne est active et expose à une surfacturation.

Solutions

Vrai-Faux

✅ **Vrai** — "123456" reste l'un des mots de passe les plus utilisés et les plus piratés au monde.
✅ **Faux** — Le cadenas indique que la connexion est chiffrée, mais pas que le site est honnête. Un site frauduleux peut très bien avoir un cadenas !
✅ **Vrai** — C'est exactement ce que font les IA génératives comme ChatGPT ou Midjourney.
✅ **Faux** — Une photo publiée peut avoir été copiée, partagée ou archivée. La suppression ne garantit pas sa disparition totale.
✅ **Faux** — Un chatbot peut produire des informations fausses présentées avec assurance. On appelle ça une "hallucination".
✅ **Vrai** — Certaines applications collectent des données en arrière-plan. Pense à vérifier les autorisations dans tes réglages !
✅ **Vrai** — C'est l'un des droits garantis par le RGPD : le droit à l'effacement, aussi appelé "droit à l'oubli".
✅ **Faux** — Les deepfakes sont de plus en plus réalistes et difficiles à détecter, même pour des experts.
✅ **Faux** — Une IA est entraînée sur des données produites par des humains, elle peut donc reproduire des biais et des stéréotypes sans s'en rendre compte.
✅ **Vrai** — Si un site se fait pirater et que ton mot de passe est récupéré, tous tes autres comptes utilisant ce même mot de passe sont immédiatement vulnérables.

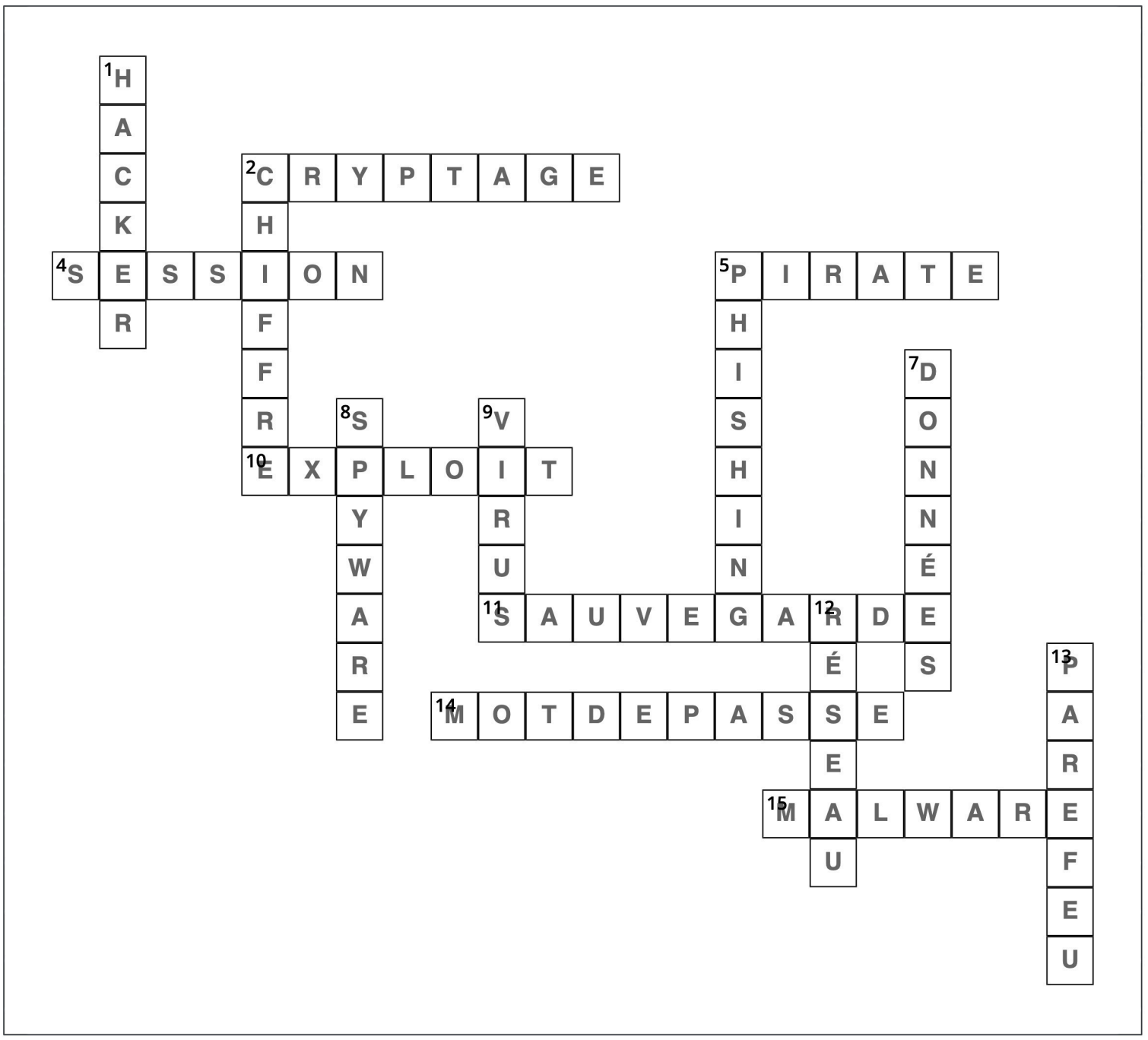
Mots mêlés

N	B	I	G	V	F	**D**	**E**	**E**	**P**	**F**	**A**	**K**	**E**
U	F	**V**	**I**	**R**	**U**	**S**	D	M	I	S	E	G	I
M	M	I	H	J	W	K	D	Q	P	A	D	T	E
É	X	C	**H**	**A**	**M**	**E**	**C**	**O**	**N**	**N**	**A**	**G**	**E**
R	F	M	O	D	Y	Y	I	O	X	D	B	D	O
I	G	T	B	R	H	J	M	H	F	E	S	J	**E**
Q	J	B	R	E	**C**	**H**	**A**	**T**	**B**	**O**	**T**	T	**M**
U	T	G	N	G	W	L	U	M	Q	P	Z	B	**P**
E	M	**A**	**L**	**G**	**O**	**R**	**I**	**T**	**H**	**M**	**E**	S	**R**
A	Q	P	X	D	A	D	R	U	N	D	R	N	**E**
T	**D**	**O**	**N**	**N**	**É**	**E**	**S**	L	N	E	K	O	**I**
O	A	Q	J	W	H	N	W	**R**	**G**	**P**	**D**	X	**N**
Z	C	H	T	X	K	I	N	S	O	L	F	J	**T**
C	**H**	**I**	**F**	**F**	**R**	**E**	**M**	**E**	**N**	**T**	D	C	**E**

Solutions

Mots croisés

Cybersécurité



Ce cahier marque la fin d'une belle aventure : après 5 ans à vos côtés, mon contrat de conseillère numérique se termine en septembre 2026.

Ces cinq années ont été une aventure riche en rencontres, en partages et en découvertes. Merci à chacun d'entre vous pour votre curiosité, votre bonne humeur et votre confiance.
Le numérique continuera d'évoluer, et vous avez désormais tous les outils pour l'apprivoiser avec sérénité.
C'est la plus belle des réussites.

Vous pouvez m'envoyer vos résultats, observations
et retours par mail. Je les lirai avec beaucoup de plaisir.

Prenez soin de vous, et bel été à tous !
Ophélie, votre conseillère numérique