CONSEILLER NUMÉRIQUE

pays de l'or AGGLOMÉRATION

MAJ JUILLET 2024

2H

ATELIER NUMERIQUE COLLECTIF

10 BONNES PRATIQUES ESSENTIELLES EN SECURITE INFORMATIQUE (POUR TOUS !)

Support d'atelier numérique Collectif
Thématique Sécurité Informatique

SYLVAIN BERTRAND
JEREMIE DAUM
Conseiller numérique

Programme de l'atelier numérique d'aujourd'hui

Présentation et vulgarisation

Bonnes pratiques de sécurité informatique

Quiz sur la sécurité informatique

CE QUE NOUS APPRENDRONS ET PRATIQUERONS :

- Vocabulaire et définitions pour simplifier la cyber sécurité
- Quelques exemples en vidéo
- Bonnes pratiques essentielles de sécurité informatique
- La base : avoir un mot de passe robuste
- Jouons ensemble à définir un mot de passe robuste
- Guide cyber sécurité officielle avec 10 bonnes pratiques

Votre intervenant

Jérémie Daum
Conseiller Numérique France Services

A votre disposition en antenne France Services sur l'Agglomération du Pays de l'Or pour un atelier numérique individuel sur **RENDEZ-VOUS** ou sur un atelier collectif **SUR INSCRIPTION**

conseiller.numerique.efs@paysdelor.fr

Agglomération du Pays de l'Or
Antenne France Services
de La Grande Motte et de Mauguio

Zone Aéroportuaire
300 Avenue Jacqueline Auriol – CS70040
34137 MAUGUIO CEDEX
Tél. 04 67 12 35 00

Ice Breaker - BRISONS LA GLACE

Faisons connaissance et découvrons le sujet du jour, **la SECURITE INFORMATIQUE** avec des questions faciles ! Mauvaises réponses acceptées :)

A vous la parole :

POUR VOUS C'est quoi la sécurité informatique ?

1 - C’est quoi la sécurité informatique ou la Cyber sécurité ?

Quelques définitions pour simplifier la Cyber sécurité pour tous

- **Système d'information (S.I.)** : ensemble organisé de ressources qui permet de collecter, stocker, traiter, et distribuer de l'**information** grâce à un **réseau** d'ordinateurs

- **Sécurité informatique** : la sécurité informatique est l'ensemble des techniques qui assurent que les ressources du **système d'information** (matérielles ou logicielles) d'une organisation soient utilisées uniquement dans le cadre (légal) où il est prévu qu'elles le soient.

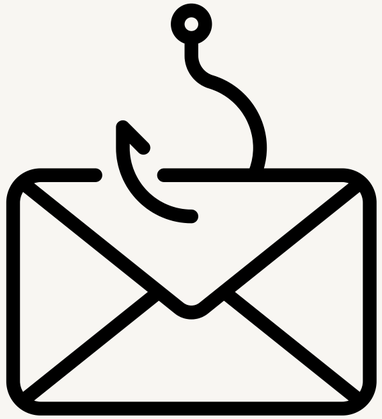
- **Cyber Espace** : l'ensemble des réseaux qui relient les **systèmes d'information** et les **objets connectés**

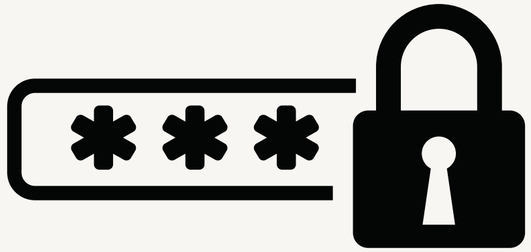
- **Pirate informatique** **:** un pirate cherche à exploiter une faille du **système d'information** de manière **malveillante (financier, politique, espionnage, atteinte à autrui...)**

- **Hacker** **:** un hacker est généralement un très bon bidouilleur qui cherche à sécuriser ou colmater une faille informatique pour le compte d'une entreprise de manière à la **protéger**

2 - Quelques exemples de piratages informatiques les plus fréquents en vidéo

Mettons des visages si possibles sur les principales techniques de piratages (ici avec humour)





Source des vidéos : **HACK ACADEMY**
https://www.youtube.com/@hackacademy2895

Les principales menaces Grand Public - HAMECONNAGE (Phishing) - Chiffres 2023

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

L'HAMEÇONNAGE (*PHISHING*)

- **Menace prédominante et principal vecteur d'attaque** pour les particuliers comme les professionnels
- **1,5 million de consultations et plus de 50 000 recherches d'assistance**
- **Principale origine de multiples cybermalveillances** (piratage de compte, débit bancaires frauduleux, virus, rançongiciel, faux conseillers bancaires...)
- **Un véritable écosystème cybercriminels de l'hameçonnage**
- **Smishing : le téléphone mobile reste une cible**
- **Quishing : Phénomène de l'année 2023 ?**

Source des infographies et chiffres : **Cyber Malveillance 2023**
https://www.cybermalveillance.gouv.fr/

Les principales menaces Grand Public - PIRATAGE DE COMPTE / USURPATION - Chiffres 2023

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

LE PIRATAGE DE COMPTE

- **Seconde menace majeure tous publics +22%**
- **Les messageries toujours particulièrement ciblées**
  (suivi des réseaux sociaux, comptes bancaires, opérateurs téléphoniques, comptes administratifs...)
- **Des origines diverses**
  (hameçonnage, fuite ou réutilisation de mots de passe, virus voleurs de mots de passe ie *Infostealers*...)
- **Cause majeure d'autres malveillances**
  (préjudice financier, usurpation d'identité, fraude au virement/RIB, chantage...)
- **Impacts pouvant être très importants pour les victimes**


20 minutes

Maine-et-Loire : Elle verse 26.000 euros à des arnaqueurs en pensant payer un artisan

ESCROQUERIE Les malfaiteurs ont eu accès à une facture d'un véritable maçon en piratant la boîte mail de leur victime

Source des infographies et chiffres : **Cyber Malveillance 2023**
https://www.cybermalveillance.gouv.fr/

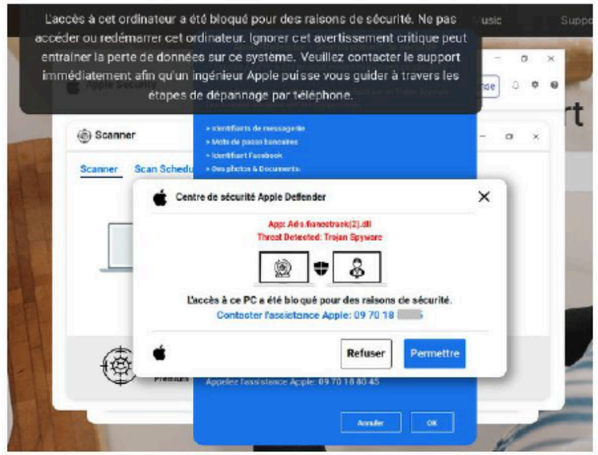
Les principales menaces Grand Public - FAUX SUPPORT TECHNIQUE - Chiffres 2023

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

FAUX SUPPORT TECHNIQUE

- 3e menace principale pour les particuliers
- Une menace majeure depuis plusieurs années
- + de 12 000 recherches d'assistance
- Des modes opératoires toujours plus agressifs
- Évolutions en 2023 : prise de contrôle des comptes bancaires en ligne
- Les préjudice peuvent aujourd'hui atteindre plusieurs milliers, voire dizaines de milliers d'euros



ZDNET

Pop-up agressives et call-center en Tunisie: le procès d'une arnaque au faux support informatique de grande ampleur commence à Paris

Quinze prévenus sont accusés d'avoir escroqué des milliers de victimes avec leurs pop-up faisant croire à un piratage d'ordinateur.

Source des infographies et chiffres : **Cyber Malveillance 2023**
https://www.cybermalveillance.gouv.fr/

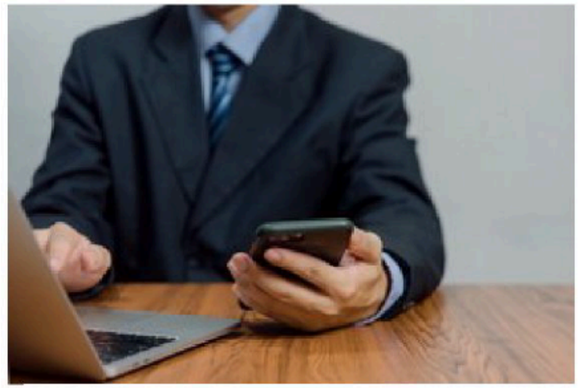
Les principales menaces Grand Public - FAUX CONSEILLERS BANCAIRES - Chiffres 2023

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

L'ESCROQUERIE AU FAUX CONSEILLER BANCAIRE

- Très forte expansion en 2023 **+78 %**
- **7e menace la plus fréquente** pour les particuliers
- **+ de 5 000 personnes ont demandé une assistance**
- **Origines :** hameçonnage, virus (infostealers)...
- **Des montants de préjudice de plusieurs milliers à centaines de milliers d'euros**
- **Évolutions en 2023 :** faux mails ou SMS de validation d'achat demandant de rappeler un numéro



E-Paiement : Transaction en cours de 899.99€ saisissez le code 244856 ou contactez le centre d'opposition au 018460

Source des infographies et chiffres : **Cyber Malveillance 2023**
https://www.cybermalveillance.gouv.fr/

En savoir plus et quiz pour déjouer les menaces de la Cyber Malveillance

https://www.cybermalveillance.gouv.fr/sens-cyber/apprendre

Source des infographies et chiffres : **Cyber Malveillance 2023**
https://www.cybermalveillance.gouv.fr/

3 - Identification, authentification, mot de passe, comment bien sécuriser sa pratique informatique ?

Identification, authentification, mot de passe
1 vidéo de 50 secondes pour comprendre

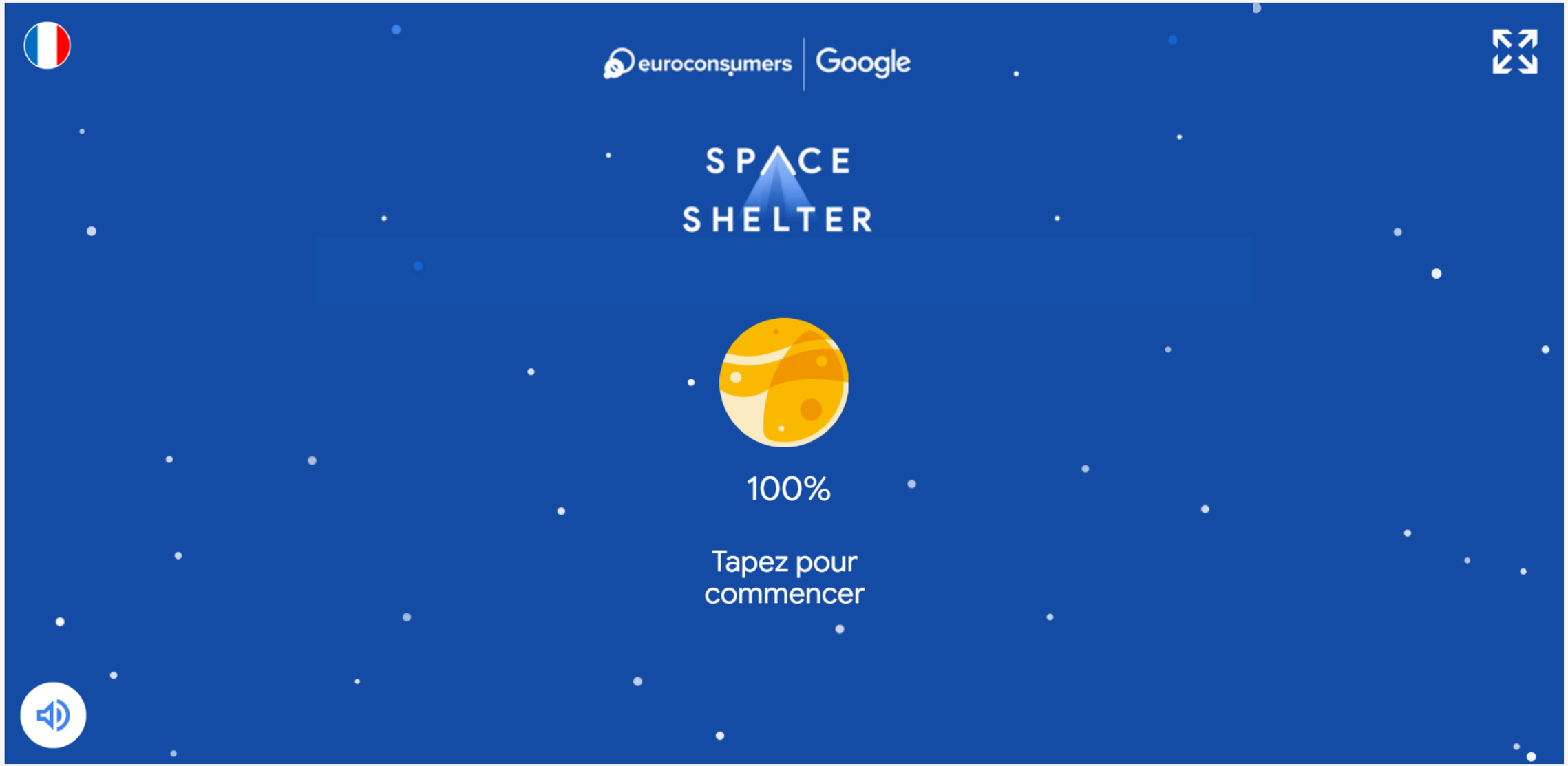
Source de la vidéo : ANNSI
https://www.ssi.gouv.fr/

POUR RESUMER : Ne pas confondre Identification et authentification

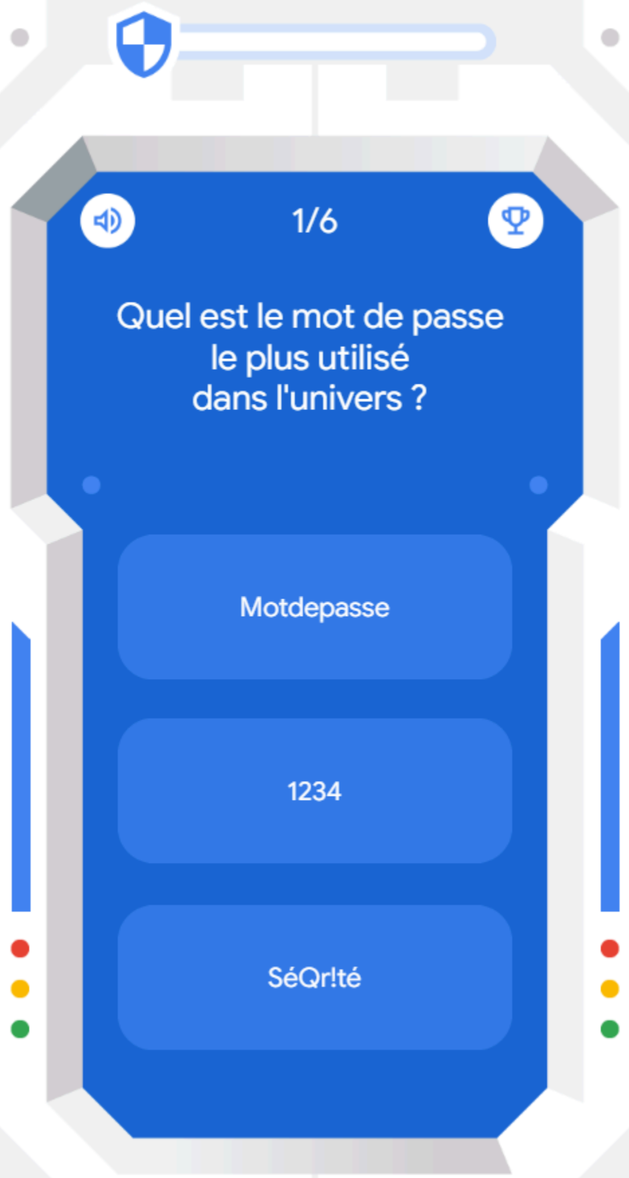
Source de la vidéo : ANNSI
https://www.ssi.gouv.fr/

Petit quiz de sécurité informatique pour se tester

https://spaceshelter.withgoogle.com/

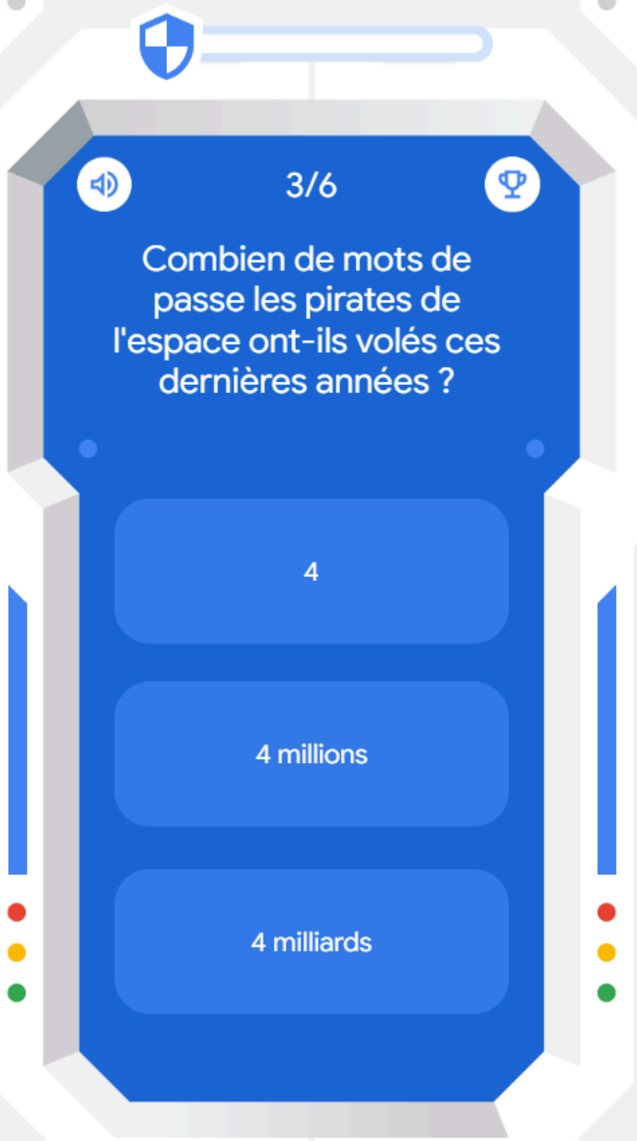


Mission Sécurité Informatique : 1

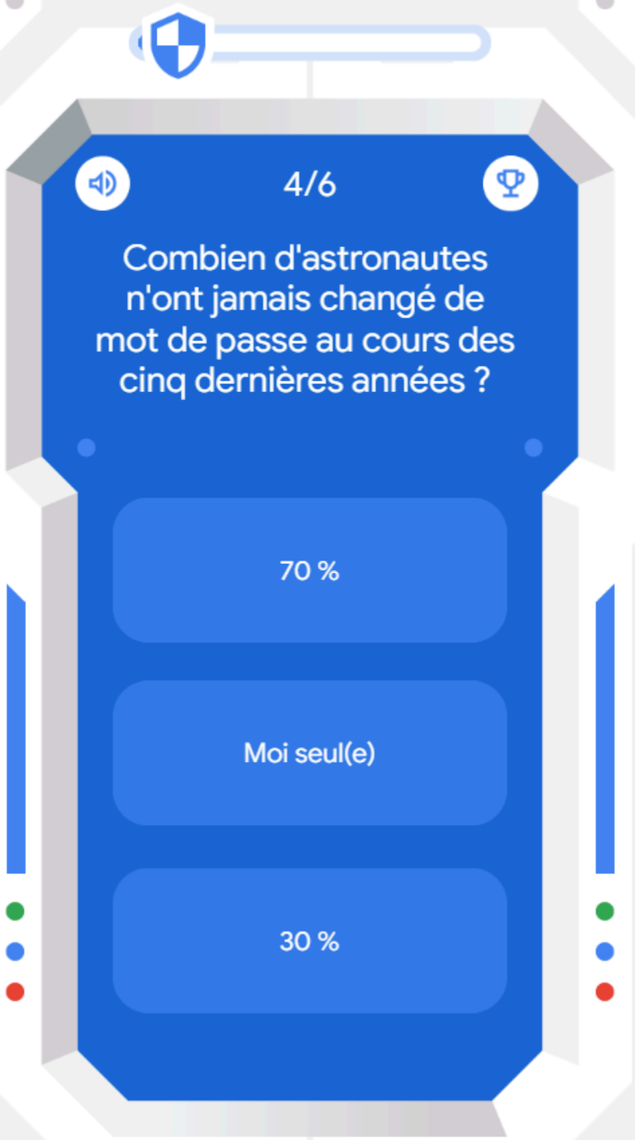


Mission Sécurité Informatique : 2

Mission Sécurité Informatique : 3



Mission Sécurité Informatique : 4

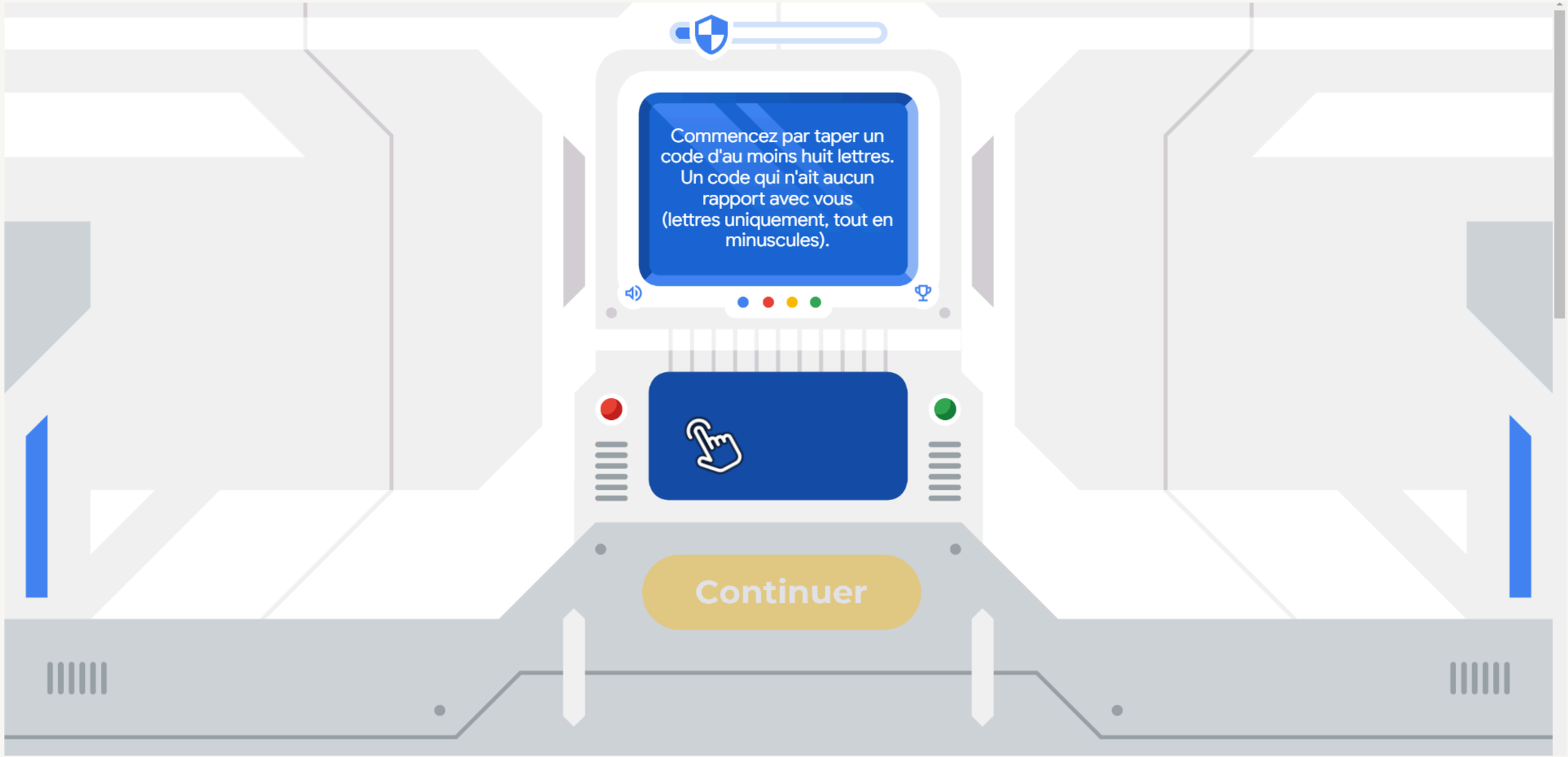


Mission Sécurité Informatique : 5

Mission Sécurité Informatique : 6

Faisons un petit jeu pour trouver un mot de passe ROBUSTE

https://spaceshelter.withgoogle.com/



4 - 10 Conseils de sécurité numérique à mettre en pratique à la maison...

Les 10 conseils tout public et famille sur la Cybermalveillance

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cyber-guide-famille-cybersecurite

Le Cyber Guide Famille, pour réviser ses connaissances en cybersécurité

Mot de passe, sauvegarde, mise à jour, piratage de compte... Révisez vos connaissances en cybersécurité avant de tenter votre chance au Cyber Quiz dès le 24 octobre 2022 !

Assistance aux victimes de cybermalveillance

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

10 Conseils de sécurité informatique à la maison

(consultez le guide officiel famille de Cyber Malveillance)

1. PROTÉGEZ VOS COMPTES AVEC DES MOTS DE PASSE ROBUSTES
2. SAUVEGARDEZ VOS DONNÉES RÉGULIÈREMENT
3. FAITES SANS TARDER LES MISES À JOUR DE SÉCURITÉ SUR TOUS VOS APPAREILS
4. UTILISEZ UN ANTIVIRUS
5. SOYEZ PRUDENTS LORS DE VOS ACHATS EN LIGNE
6. MÉFIEZ-VOUS DES MESSAGES SUSPECTS
7. APPRENEZ À MAÎTRISER VOS RÉSEAUX SOCIAUX
8. ÉVITEZ LES WI-FI PUBLICS OU INCONNUS
9. SÉCURISEZ VOS OBJETS CONNECTÉS
10. CYBERHARCÈLEMENT : PARLEZ-EN !

CYBER MALVEILLANCE .GOUV.FR

Assistance et prévention en sécurité numérique

Source des conseils : **Cyber Malveillance**
https://www.cybermalveillance.gouv.fr/

10 Conseils de sécurité informatique à la maison

(consultez le guide officiel famille de Cyber Malveillance)

LES CONSEILS

Pour réduire les risques et éviter un piratage de vos différents comptes en ligne, nous vous recommandons d'utiliser des mots de passe suffisamment longs, **complexes et différents** pour accéder à chacun de vos équipements et services. Au moindre doute, ou même par prévention, n'hésitez pas à **en changer et à activer la double authentification** chaque fois que possible pour renforcer votre sécurité. Enfin, utilisez un **gestionnaire de mots de passe** pour les stocker de manière sécurisée.

Afin de prévenir de tels risques, Cybermalveillance.gouv.fr vous recommande fortement de réaliser des **sauvegardes régulières** de l'ensemble de vos appareils en ayant au préalable identifié les données que vous estimez importantes. Pensez à en conserver une **copie sur un support externe** (clé USB, DVD ou disque dur externe), que vous débranchez une fois la sauvegarde effectuée, pour éviter qu'elle ne soit détruite également en cas de piratage ou d'infection de votre appareil par un virus. Il existe par ailleurs des **services en ligne, appelés « Cloud »**, qui offrent des fonctionnalités de sauvegarde de données. Ces solutions peuvent être gratuites ou payantes en fonction de la capacité de stockage dont vous avez besoin.

LES CONSEILS

Cybermalveillance.gouv.fr vous recommande d'**accepter les mises à jour de sécurité sur tous vos appareils** (ordinateurs, tablettes, téléphones mobiles, objets connectés...) dès qu'elles sont proposées pour corriger ces failles et ainsi vous protéger. Nous vous conseillons également de **vérifier régulièrement dans les paramètres de vos équipements et logiciels que les mises à jour sont bien appliquées** et d'activer l'option de téléchargement et d'installation automatique des mises à jour, si le logiciel le permet. Enfin, veillez à **ne télécharger les mises à jour uniquement depuis les sites officiels**, sinon, vous risqueriez de télécharger également un virus.

LES CONSEILS

Nous vous recommandons d'**utiliser un antivirus sur tous vos équipements** (ordinateur, tablette, téléphone mobile...). Il existe de **nombreuses solutions gratuites ou payantes** selon vos usages et le niveau de protection recherché. **N'hésitez pas à vérifier régulièrement que les antivirus de vos équipements sont bien à jour** et à procéder à des analyses approfondies (scans) pour vérifier que vous n'avez pas été infecté.

Choisissez de préférence un site d'achat français ou de l'Union Européenne : la réglementation européenne qui s'applique à tous ces sites en cas de litige vous protégera. Nous vous invitons également à **vérifier la notoriété et l'adresse des sites sur lesquels vous allez faire vos achats** : si c'est votre premier achat sur un site Internet, n'hésitez pas à taper son nom sur un moteur de recherche et à consulter les avis pour vous éviter des déconvenues. De plus, vérifiez bien l'adresse car un seul caractère dans le nom du site peut différer du site officiel. Et lorsque les offres sont trop alléchantes, nous vous conseillons de comparer le prix du produit recherché sur différents sites Internet pour vous assurer du caractère crédible de la vente. Enfin, **privilégiez les moyens de paiement les plus sécurisés** (Paylib, e-Carte Bleue...).

10 Conseils de sécurité informatique à la maison

(consultez le guide officiel famille de Cyber Malveillance)

LES CONSEILS

Premier réflexe : **ne pas cliquer sur le lien qui vous est proposé**. **Au moindre doute**, lors de la réception d'un message inattendu ou alarmiste, **nous vous recommandons de contacter directement l'organisme concerné par un autre moyen** (exemple : par téléphone ou en se connectant par soi-même à son compte en ligne). Il peut en effet s'agir d'un message d'hameçonnage (phishing) visant à vous piéger.

LES CONSEILS

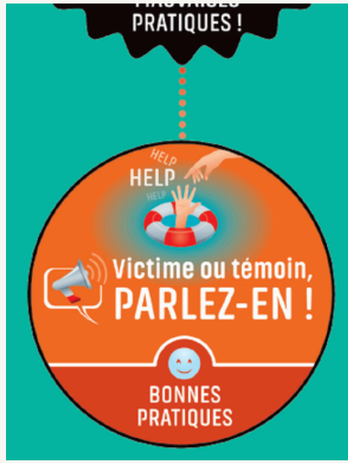
Pour utiliser les réseaux sociaux en toute sécurité et protéger l'accès à vos comptes, nous vous recommandons d'utiliser à la fois **des mots de passe robustes et systématiquement différents pour chaque service** mais aussi d'**activer la double authentification** lorsque cela est possible. Par ailleurs, nous vous recommandons de **vérifier régulièrement les paramètres de confidentialité de vos comptes** pour définir les options de visibilité de vos publications. Enfin, ne diffusez pas d'informations personnelles ou sensibles qui pourraient être utilisées pour vous nuire et bien sûr, **faites attention à qui vous parlez sur les réseaux.**

LES CONSEILS

En dehors de votre domicile, **nous vous suggérons de privilégier la connexion de votre abonnement téléphonique** (3G, 4G ou 5G) aux réseaux Wi-Fi publics. Si vous ne pouvez faire autrement, nous vous conseillons de vérifier scrupuleusement le nom du réseau proposé et celui affiché sur votre appareil et de **ne jamais y réaliser d'opérations sensibles** (paiement par CB, consultation de compte bancaire, renseignement d'informations confidentielles…).

LES CONSEILS

Dès la première utilisation de votre objet connecté, **changez le mot de passe par défaut** et utilisez un mot de passe suffisamment long et complexe pour sécuriser chacun de vos équipements. Nous vous conseillons également de réaliser les mises à jour de sécurité et celles de leurs applications dès qu'elles vous sont proposées.
Veillez aussi à **vérifier leurs paramètres de sécurité en fonction de vos usages** et à désactiver les fonctionnalités que vous n'utilisez pas.
Enfin, nous vous conseillons d'**éteindre systématiquement vos objets connectés lorsque vous ne les utilisez pas**.

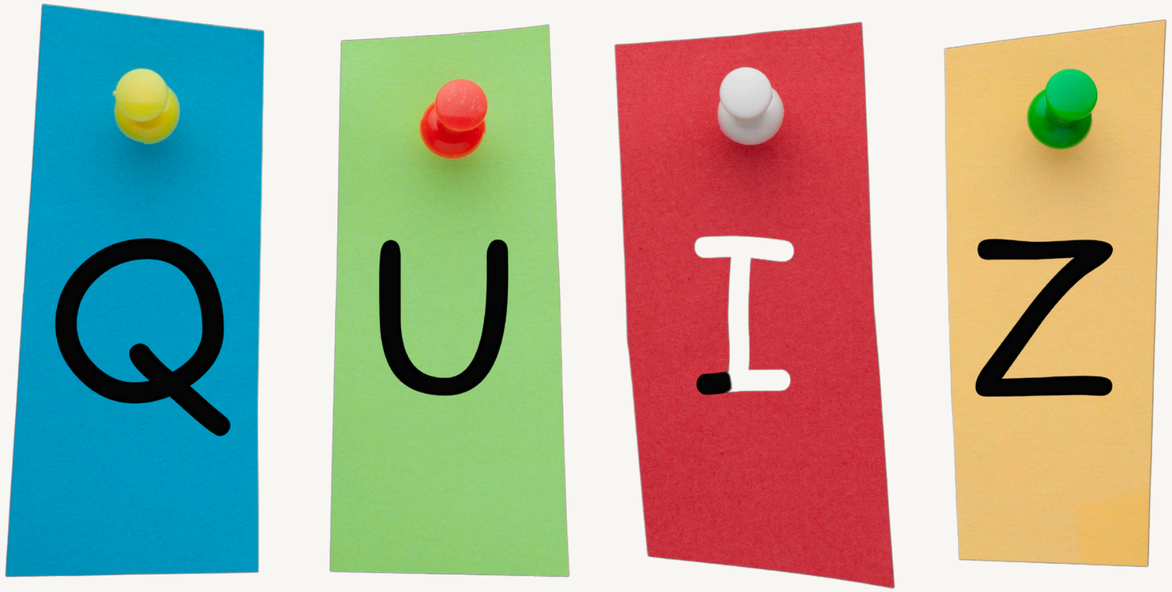


LES CONSEILS

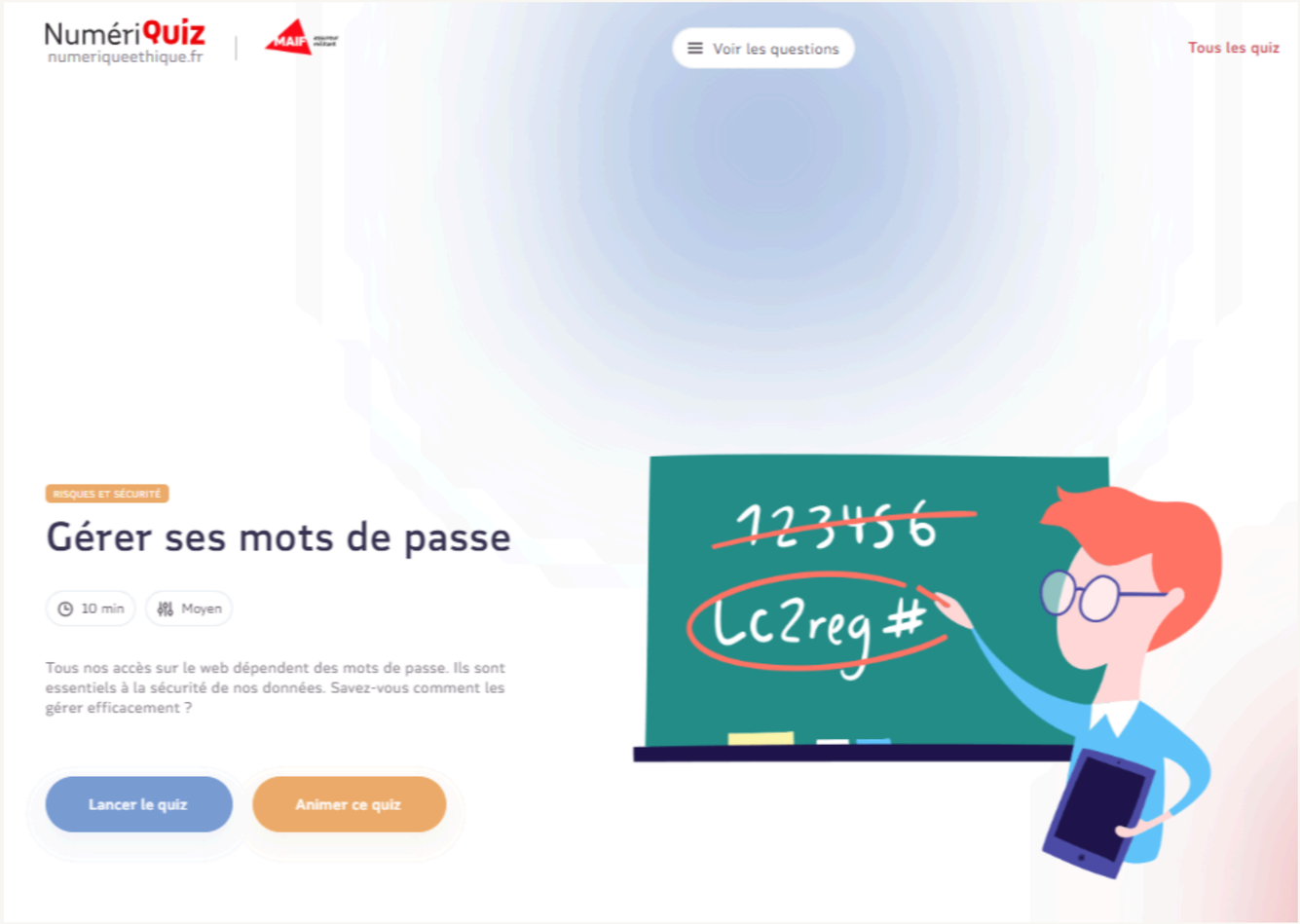
Il est important de ne pas rester seul face au cyberharcèlement et de libérer la parole dans un cadre apaisé. Aussi **nous vous conseillons d'aborder le sujet du cyberharcèlement en famille avec vos enfants pour expliquer de quoi il peut s'agir et de les encourager à vous en parler s'ils sont témoins, victimes ou susceptibles d'être contributeurs**.
Voici un exemple de questions pour engager la discussion : *Tu sais ce que c'est que le cyberharcèlement ? As-tu déjà vu des situations de cyberharcèlement ? Que ferais-tu si tu voyais ou subissais un cyberharcèlement ?*
Si un cyberharcèlement se produit dans le cadre scolaire, informez-en la direction de l'établissement pour qu'elle puisse prendre les mesures nécessaires.


QUESTIONS
?
?
REPONSES
?

Testez vos connaissances sur la sécurité informatique



Testez vos connaissances sur la sécurité informatique
Sur un **ordinateur** sur ce site https://numeriquiz.fr/quiz/gerer-ses-mots-de-passe



Source du QUIZ : **MAIF**
https://numeriquiz.fr/

Pour votre attention et pratique !

A bientôt pour un nouvel atelier numérique...

CERTIFICAT DE PARTICIPATION

CONSEILLER NUMÉRIQUE

pays de l'or AGGLOMÉRATION

Ce certificat est décerné à :

Nom / Prénom :

Nom de l'animateur de l'atelier :
Jérémie Daum

pour avoir participé avec succès à l'atelier numérique **Sécurité Informatique et Mot de passe**

Date de l'atelier :

Contacts du conseiller numérique France Services

Jérémie à la Grande Motte

Antenne France Services

Accès
Accès libre, Sur rendez-vous

place du 1er Octobre 1974, 34280 LA GRANDE MOTTE
Distance : 0.05 km

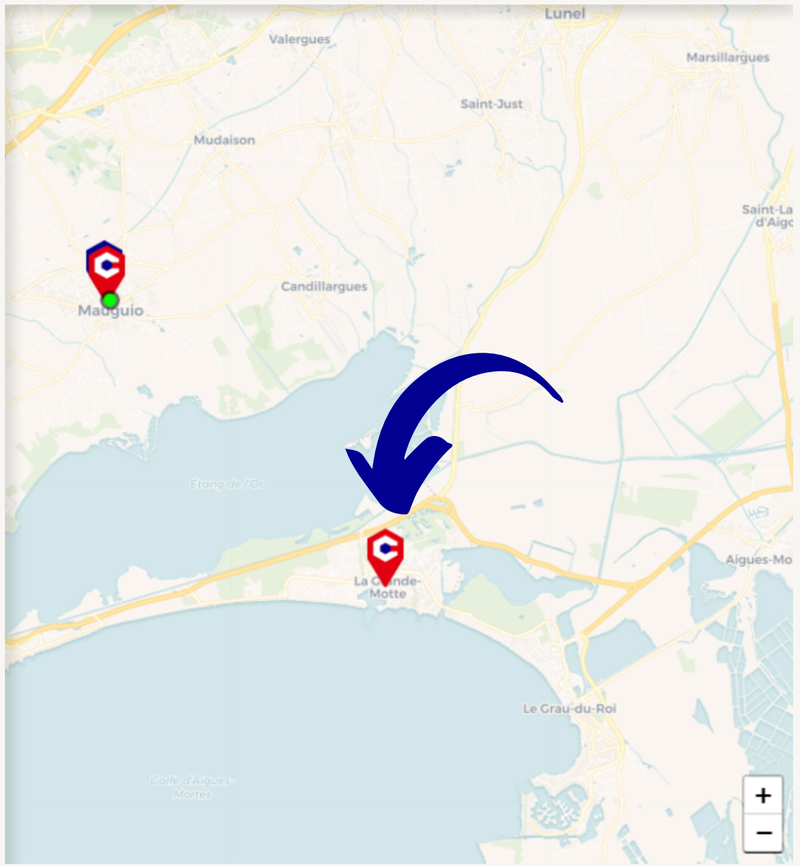
Horaires

Lun.	08h30 - 12h00 | 13h30 - 17h00
Mar.	08h30 - 12h00 | 13h30 - 17h00
Mer.	08h30 - 12h00 | 13h30 - 17h00
Jeu.	08h30 - 12h00 | 13h30 - 17h00
Ven.	08h30 - 12h00 | 13h30 - 17h00

1 conseiller numérique
Que peuvent-ils faire pour moi ?

Jérémie Daum

+33610098120
conseiller.numerique.efs@paysdelor.fr



Les 10 conseils tout public et famille
sur la Cybermalveillance

Téléchargez ou demandez nous le CYBER GUIDE :
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cyber-guide-famille-cybersecurite

Auteur de ce support pédagogique sous Licence Creative Commons By NC ND

Jérémie Daum Conseiller Numérique

conseiller.numerique.efs@paysdelor.fr

Date de la rédaction et mise à jour : **AOUT 2024**

Organisme d'accueil de médiation numérique : **Espaces France Services**

Communauté d'agglomération du Pays de l'Or
300 avenue Jacqueline Auriol
Zone aéroportuaire - CS 70040
34137 MAUGUIO Cedex
04 67 12 35 00
www.paysdelor.fr