



La cybersécurité est une **responsabilité de tous** ! Apprenons ensemble à **mieux nous protéger en ligne**

Dans notre monde connecté, Internet fait partie de notre quotidien : nous l'utilisons pour communiquer, apprendre, jouer et même faire des achats en ligne. Cependant, comme dans le monde réel, il existe aussi des **dangers sur Internet**. La **cybersécurité** est l'ensemble des **pratiques et des technologies** qui permettent de **protéger nos informations personnelles et nos comptes contre les menaces en ligne**.

Pourquoi la cybersécurité est-elle importante ?

1. Protection des données personnelles

- Nos informations (mots de passe, photos, messages privés) peuvent être volées si nous ne faisons pas attention.

2. Prévention des cyberattaques

- Les pirates informatiques (hackers) utilisent différentes techniques pour voler des comptes, envoyer des virus ou piéger les internautes.

3. Sécurité en ligne

- Une bonne cybersécurité permet d'utiliser Internet sans risques et d'éviter le cyberharcèlement, les arnaques ou l'usurpation d'identité.

Les règles essentielles pour être en sécurité sur Internet

- ✚ **Créer des mots de passe forts** : utiliser des lettres, chiffres et symboles.
- ✚ **Ne pas partager ses informations personnelles** sur les réseaux sociaux.
- ✚ **Faire attention aux liens et aux emails suspects** pour éviter le phishing.
- ✚ **Mettre à jour ses logiciels et antivirus** pour se protéger des virus.



L'importance des Mots de Passe en Cybersécurité

Le mot de passe est la **première barrière de protection** pour nos comptes et nos données personnelles. Il empêche les pirates informatiques d'accéder à nos **réseaux sociaux, emails, jeux en ligne et autres services**. Un mot de passe **faible** est comme une **porte ouverte** aux hackers, tandis qu'un mot de passe **fort** est comme une **forteresse difficile à franchir**.



Votre Mission

Créer un projet scratch mettant en scène **un agent de cybersécurité**.

- ✚ Dans **un premier temps**, cet agent **expliquera** l'importance des mots de passe dans la protection des données sous forme d'un mini-jeu ou d'une présentation interactive.
- ✚ Dans **un deuxième temps**, l'agent **demandera** à l'utilisateur de saisir un mot de passe. Il **analysera** sa sécurité en fonction de plusieurs critères. Puis, il **affichera** un message indiquant si le mot de passe est sécurisé ou non.

Notez Bien : Un mot de passe est considéré comme fort s'il dépasse 8 caractères. Il devra aussi contenir au moins deux lettres, deux chiffres et deux caractères spéciaux (**voir Annexe**).

Le programme exploitera **le code fourni en annexe pour calculer le score final**.

Votre projet doit contenir :

- **Minimum** 4 scènes,
- A partir de la deuxième scène le texte « Tunisia Coding Day V6 » doit **apparaître** jusqu'à la fin.
- Logo Stem, logo compétition **à la fin** du projet,
- Des **animations** et des **effets sonores**.
- Il ne faut pas mentionner **ni vos noms, ni le nom de l'équipe**.



ANNEXE : Calcul du score d'un mot de passe

Le score de sécurité d'un mot de passe est déterminé selon plusieurs critères.

Le score initial **commence à 0**.

Si la longueur du mot de passe est supérieure à 8 caractères **alors** on ajoute +1 au **score**.

Si le mot de passe contient plus de 2 caractères spéciaux (ex: @, #, \$, %) **alors** on ajoute +1 au **score**.

Si le mot de passe contient plus de 2 lettres (ex: a, b, c...) **alors** on ajoute +1 au **score**.

Si le mot de passe contient plus de 2 chiffres (ex: 1, 2, 3...) **alors** on ajoute +1 au **score**.

Si Score = 4 **alors** "Mot de passe fort et sécurisé"

Si Score = 3 **alors** "Mot de passe moyen"

Si Score ≤ 2 **alors** "Mot de passe faible et non sécurisé"

Ci-joints les blocs Scratch permettant le **calcul du score des lettres** dans un mot de passe.

