ACTIVITÉ (DÉCONNECTÉE) - LE JEU DU PENDU POUR DEVINER UN MOT DE PASSE

SÉCURITÉ > 4.1 PROTÉGER LES OUTILS NUMÉRIQUES

CONVIENT POUR	AGE	NIVEAU DE COMPÉTENCE	FORMAT	DROITS D'AUTEUR	LANGUE(S)
Elèves (école primaire), Elèves (école secondaire), Jeunes en décrochage scolaire	Adolescents, Enfants	Niveau 1	Fiche d'activité	Creative Commons (BY-SA)	Français

Un jeu en équipe basé sur le jeu du pendu, afin de sensibiliser à l'importance de créer des mots de passe forts

Objectif général	Connaissances
Temps de préparation pour l'animateur	moins d'une 1 heure
Domaine de compétence	4 - Protection de l'identité et des données personnelles
Temps requis pour compléter l'activité (pour l'apprenant)	0 – 1 heure
Nom de l'auteur	Thibault Dupiczak
Matériel supplémentaire	Feuilles et stylos - Tableau blanc (avec feutres) - Dés à 6 faces (1 dé/groupe de participants)
Ressource originellement créée	Français

DÉROULÉ

1 Introduction

Ce jeu ludique en équipe permet d'aborder avec les participant.e.s l'importance de créer des mots de passe sécurisés. Bien entendu, au-delà du jeu, il est nécessaire d'expliquer aux participant.es pourquoi il est important de sécuriser ses comptes sur Internet, et surtout de leur fournir quelques bonnes pratiques pour y arriver.

Conseil médiation :

Pour en savoir plus sur les mots de passe, nous vous conseillons de vous référer à la fiche « Outil – Les mots de passe »

2 Un mot de passe à toute épreuve

Pour introduire l'activité, commencer par faire un petit tour de table avec les participant.e.s pour leur demander sur quels types de plateformes ils ou elles sont inscrit.e.s (réseaux sociaux, jeux vidéo, comptes divers) quelle importance accordent ielles à la sécurité de leurs comptes et sur quels critères ielles se basent pour créer leurs mots de passe.

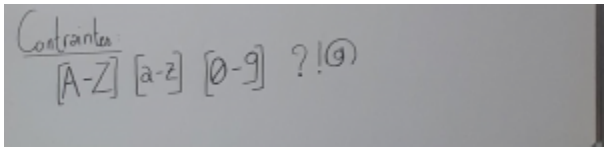
3 Place au jeu

Diviser le nombre de participant.e.s en 2 groupes (faire des équipes intergénérationnelles mixer les divers publics pour avoir des échanges plus intéressants).

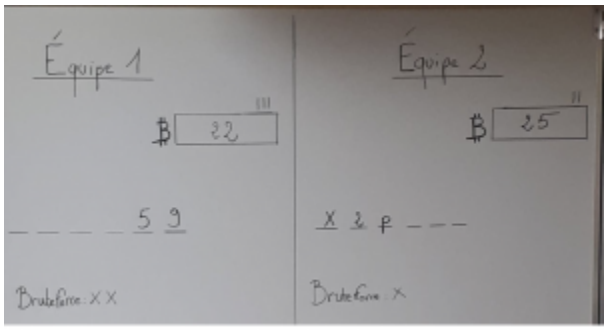
Chaque équipe détermine son mot de passe (avec certaines restrictions : types de caractères, nombre de caractères etc.). Le mot de passe doit avoir une longueur de 6 caractères, une majuscule, une minuscule et au moins un chiffre. Les contraintes restantes sont choisies par l'animateur.

Contraintes possibles :

- [A-Z] [a-z] [0-9] !?$
- [A-Z] [a-z] [0-9] !?$.-_
- [A-Z] [a-z] [0-9] !?$.-_@+



Diviser le tableau en deux, déterminer une somme, similaire pour les deux équipes mise de chaque côté du tableau (30 bitcoins par équipe par exemple), il s'agit du nombre de points que chaque équipe dispose pour jouer. Toujours de chaque côté du tableau tracer un nombre de tirets équivalent au nombre de caractères des mots de passe de chaque groupe (même concept que le pendu).



A son tour chaque équipe va pouvoir essayer de deviner une lettre du mot de passe de l'équipe adverse (toujours similaire au pendu), le nombre de tours est limité à 10 tours. A la fin des 10 tours l'équipe qui a le plus de bitcoins restant sur son compte gagne, si une équipe réussit à deviner le mot de passe entier elle vole la totalité de la somme restant sur le compte adverse.

L'équipe dont une lettre a été devinée se voit freezée (gelée) un bitcoin (représenté par un petit bâton au dessus de la somme) . Un bitcoin freezé est *toujours compris dans le total du compte* mais *ne peut être utilisé* pour faire une action.

Il existe 2 types d'actions que chaque équipe peut réaliser :

- Deviner une lettre au hasard (coûte 2 bitcoins à l'équipe qui effectue l'action).
- Utiliser le Brute Force* (coûte 3 bitcoins à l'équipe qui effectue l'action).

Le Brute Force se matérialise par un lancer de *dé* par un.e membre de l'équipe qui effectue l'action. Le

résultat affiché par le dés à six faces *doit être supérieur à 3*, si il l'est alors l'équipe obtient directement la lettre qu'elle essaye de deviner.

**Pour la définition, voir la partie définition ci-dessous*

4 Temps de partage

Une fois le jeu fini, les équipes dévoileront leur mot de passe (si ils n'ont pas été devinés) et expliqueront les diverses étapes par lesquelles ielles sont passé.e.s pour créer leurs mots de passe. Ielles pourront donner leur avis sur la méthode empruntée par l'équipe adverse.

Echanger avec les participant.e.s sur la méthodologie qu'ils ont choisie pour déterminer leurs mots de passe (et ce dont ielles vous ont fait part lors de l'étape 1). Leur donner des informations concernant la création d'un mot de passe : bien composer son mot de passe, comment stocker son mot de passe, quels sont les enjeux liés à la bonne protection de ses comptes et vous pouvez aussi parler rapidement du chiffrement des mots de passe (et faire part au public que ces notions pourront être abordées dans de futurs ateliers).

5 Définition

Brute Force : Le brute force est l'une des méthodes qui peut être utilisée pour découvrir le mot de passe du compte d'une personne. Cette méthode consiste à lancer un logiciel dit de *brute force*, qui va essayer toutes les combinaisons possibles (numérique et/ou alphanumérique et/ou caractères spéciaux). Il est judicieux lors de l'utilisation d'un logiciel comme celui-ci de définir des pré-sets ce qui réduira le nombre d'essais (car très chronophage), l'on peut définir une limite de caractères ou prédéfinir certaines combinaisons. Il est possible par exemple de baser une "attaque" de brute force sur des informations relatives à la personne (noms/prénoms de proches, dates de naissance, adresse etc..) auquel cas toutes les combinaisons possibles entre ces différentes informations seront essayées.