LES GARDIENS DU NUMÉRIQUE : LE JEU DE CARTES

Aide Animateur

Attention

Afin de pouvoir réaliser efficacement la session, il est important que l'animateur ait une bonne connaissance préalable du jeu de cartes et de ses règles. Il est fortement recommandé de prendre connaissance à l'avance du livret de règles, ou de jouer une partie si possible.

Introduction

Ce module pédagogique vise à sensibiliser les collégiens de la 6e à la 3e aux sujets des potentiels dangers pouvant être rencontrés sur internet. L'apprentissage prend la forme d'un jeu de cartes visant à introduire des concepts de manière ludique et amusante. Le jeu est introduit par l'animateur en début de partie, puis un débriefing est réalisé en fin de partie afin d'ancrer les notions importantes.

Déroulé de la session

Introduction de la partie  2'

L'introduction vise à accueillir les jeunes et à leur exposer la thématique de la session, à savoir : "apprendre à utiliser internet de manière sécurisée et responsable, en sachant prendre du recul, et se protéger des nombreux dangers (cyber-attaques, virus, vols de données, abus de confiance, fake news, cyberharcèlement…)."

Il s'agit également de rappeler que le jeu est "collaboratif" et que le groupe de participants jouent contre le paquet de cartes, qui représente la navigation sur internet, avec tous ces dangers.

Séance de jeu  20’ à 25’

La séance de jeu vise à introduire les concepts clé de la thématique en créant de l’engagement de la part des apprenants. L’objectif du jeu n’est pas de se substituer à une formation sur les dangers d’internet, mais simplement d’introduire, d’intéresser les participants, et d’amener de la curiosité ainsi que des pistes de réflexions.

Le jeu dure 20 à 25’ et se pratique par groupe de 3 à 4 participants.
Dans le cas où des groupes finissent avant la fin du temps, ils peuvent être invités à recommencer une partie.

Il est recommandé de démarrer une session de jeu par “un tour de chauffe” sous la supervision de l’animateur pour assurer la compréhension de la règle avant de commencer la partie.

Débriefing  10’ à 15’

À la suite de la séance de jeu, les participants seront amenés à revenir sur les éléments présentés au sein du jeu comme les différents risques, et les bonnes pratiques et astuces qui permettent de se protéger.

L’animateur peut organiser le débriefing de la manière suivante :

1- Demander aux participants leur score final et recueillir leurs avis sur ce qu’ils ont pensé du jeu

2- Recueillir et répondre aux éventuelles questions

3- Interroger les joueurs sur ce qu’ils ont retenu

4- Interroger les joueurs sur les menaces rencontrées sur internet et passer en revue les concepts clés (cf. définitions ci-après)

5- Interroger les joueurs sur les bonnes pratiques et astuces pour faire face aux menaces rencontrées sur internet (cf. bonnes pratiques et astuces ci-dessous)

Concepts clés

MENACES

Abus de confiance : Divers techniques pour abuser de la confiance des usagers existent sur internet. Ces escroqueries existent sous deux formes, les attaques directes (la personne malveillante vole un compte ou un mot de passe), ou indirectes ou la faille de sécurité vient de l'utilisateur (en cliquant sur un lien dangereux par exemple).

Hameçonnage : L'hameçonnage est une technique d'escroquerie tristement célèbre. Elle vise à pousser les utilisateurs à cliquer sur un lien en utilisant des techniques de manipulation, par exemple un mail "Très urgent ! à ouvrir tout de suite" imitant un mail de votre banque. Ensuite, vos données personnelles sont dérobées.

Récolteur de données : Un récolteur de données (comme le sont par exemple les « cookies ») est comme un espion numérique, qui récupère des informations sur votre identité et vos activités. Ces informations peuvent être utilisées pour analyser vos comportements, influencer vos choix, ou vous proposer des publicités ciblées.

Fake news (fausses actualités) / informations non sourcées : Sur les réseaux sociaux, n'importe qui peut partager ce qu'il souhaite. Parfois, on rencontre des publications qui visent à créer une actualité autour d'informations partielles ou erronées. Des informations mensongères peuvent ainsi être partagées avec des articles qui utilisent des données non sourcées et non validées par des experts. Cette méthode qui crée du flou dans la réflexion, peut être utilisée dans le but de tromper les lecteurs. Elle est fréquemment utilisée dans les périodes de débats (des élections ou la pandémie COVID par exemple).

Faux profil : Sur les réseaux sociaux, il est très simple de voler l'identité ou le profil numérique de quelqu'un. Ces vols permettent à des personnes mal intentionnées de créer de faux profils, imitant des célébrités ou des gens de votre entourage. L'objectif est de gagner la confiance des utilisateurs, souvent pour les escroquer.

Commentaires insultants : Régulièrement, des individus profitent de l'anonymat sur internet pour utiliser un langage violent et agressif, particulièrement sur les réseaux sociaux.

Cyberharcèlement / Photos compromettantes : Partager des photos ou des vidéos avec votre visage sur les réseaux sociaux est un risque certain. N'importe qui peut retrouver des photos de vous, en vacances ou faisant la fête avec vos amis par exemple.

Spam : Le spam définit le fait d'envoyer beaucoup de messages à une personne ou un groupe. Il peut être publicitaire, "malveillant", ou plus inconscient, par exemple quand on envoie plein de messages à un ami qui ne répond pas.

Virus : Les virus sont des programmes malveillants qui visent à infecter votre appareil pour causer des dégâts ou voler vos données personnelles. Ils existent sous diverses formes bien différentes.

Attaque de serveur "DDos" : L'attaque de serveur (DDos) est une technique de cyberattaque qui vise à saturer un serveur informatique avec un nombre élevé de demandes et de fichiers pour empêcher le serveur de fonctionner. Par exemple pour empêcher un diffuseur de vidéo en ligne (« streamer ») de réaliser son émission en direct (« live »).

Vol de contenu : Le vol de contenu est courant sur internet. Les créations artistiques de chacun des utilisateurs peuvent être volées par d'autres, qui en revendiquent la propriété (vol de dessin, photo, par exemple).

BONNES PRATIQUES & ASTUCES

Distinguer le vrai du faux : Croiser les sources est fondamental, que ce soit à propos d'articles, de photos… Notre cerveau adore les raccourcis, et nous avons tous tendance à agir (commentaires, partages) sous le coup des émotions. Il est important de vérifier les informations et données chiffrées (éditeur/auteur/date/ton…), de prendre du recul, et de ne pas croire trop rapidement ce qu'on peut lire. Il faut particulièrement être vigilant sur les réseaux sociaux car les algorithmes mettent en avant les publications ayant le plus fort engagement (likes, commentaires, republications), pouvant ainsi permettre à de fausses informations d'être très vite et très fortement relayées.

Contrôle des informations et partage responsable : En contrôlant les informations que l'on partage sur internet et les réseaux sociaux, on évite les risques de piratage et d'atteinte à sa réputation. Il est possible de privilégier les réseaux privés où les membres sont rigoureusement sélectionnés (famille, amis). Il faut également faire attention à ne pas donner de la visibilité à des contenus volés (textes, images, photos…) ou erronés, et à protéger ses propres créations via des signatures.

Signalement et soutien : Dans des situations de cyber-harcèlement, de photos compromettantes ou en présence de commentaires haineux/insultants, trois réponses à adopter sont importantes :

- Ne pas répondre aux messages pour ne pas surenchérir
- Signaler à la plateforme les utilisateurs adoptant de mauvais comportements
- Aider la victime en lui apportant son soutien

Accepter les cookies avec modération : En disant non aux cookies, ou en choisissant seulement ceux qui sont nécessaires, on garde un peu plus de contrôle sur notre vie privée et nos données personnelles.

Protection contre les virus et tentatives d'escroqueries : Pour se prémunir des attaques de virus, il est nécessaire d'installer un anti-virus mis à jour régulièrement. Il faut également ne pas cliquer sur les liens et pièces jointes associées aux messages douteux, dont on ne connait pas l'auteur, qui demandent de l'argent ou qui demandent de saisir ses codes confidentiels.

Les Gardiens du numérique, est une création de :

GROUPE VYV — mgen GROUPE VYV — MINISTÈRE DE L'ÉDUCATION NATIONALE ET DE LA JEUNESSE — CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS