



Le loup garou d'Internet

Contexte

73 %

des Français.e.s ont été confronté.e.s à des tentatives de phishing, avec une exposition accrue chez les jeunes adultes. Ces données soulignent l'importance de sensibiliser les plus jeunes aux risques d'escroqueries en ligne et de les éduquer aux bonnes pratiques de cybersécurité

(Source : étude IPSOS pour Cybermalveillance.gouv.fr, 2024)

Objectifs pédagogiques

À l'issue de cette activité, les participant.e.s seront plus en capacité de :

- Connaître et identifier certains dangers en ligne ;
- Analyser certains mécanismes de manipulation et de déstabilisation ;
- Exercer son esprit critique sur une situation donnée



Durée de la séance :
1h30



Equipe :
8 à 20 participant.e.s
1 à 2 animateur.rices



Matériel nécessaire :
ballons, chasubles, cartes rôles
à imprimer ou à réécrire

Déroulé

Introduction (5 minutes) :

Comme c'est la coutume dans le jeu du Loup-Garou, plantez le décor : " Etes-vous sûr.e.s de pouvoir compter sur vos coéquipier.e.s ? Qui est l'imposteur.e qui cherche à saboter son équipe Démasquez-les pendant les temps morts de ce match ! ". Sauf que dans cette version, le village ne dort pas, il joue au football ! Expliquez ensuite le principe du jeu décrit ci-dessous, et présentez les 3 rôles de "cyber-imposteur.e.s" avant de distribuer les cartes attribuant les rôles.

2) Distribution des rôles (5 minutes)

Organisez donc un match avec 2 équipes mais au sein de ces équipes, certain.e.s joueur.euse.s ont des rôles cachés : ce sont les cyber-imposteur.e.s. Les trois rôles sont les suivants :

- **Le/la scammer** : c'est traître qui agit contre l'intérêt de son équipe, comme en marquant contre son camp ou en faisant des fautes répétées qui pénalisent ses coéquipier.e.s.
- **Le/la cyberharceleur.se** : c'est un caméléon qui se montre opportuniste, il/elle joue normalement au début, puis dès qu'il y a des points ou bien une équipe qui semble avoir le dessus, il/elle joue de manière à la favoriser.
- **Le/la hacker** : c'est un.e saboteur.e agit de manière à déstabiliser son équipe et le jeu au global, par exemple en perturbant la communication sur le terrain, en jouant de façon imprévisible ou en faisant des scandales et de l'anti-jeu (perte de temps, simulations...).

Faites autant de cartes que de personnes sur le jeu, et glissez 1 cyber-imposteur.se toutes les 4 cartes. Veillez à ce que les 3 rôles soient représentés et à ce que le nombre de "loup" soient équilibré parmi les équipes.

3) Réalisation du jeu (10 minutes) :

Démarrez le match ! Il est interrompu soit toutes les 10 minutes (par exemple, libre à vous d'adapter ces temps de jeu), soit autant de fois qu'il y a de loup. Le temps d'interruption est de 5 minutes pour un temps d'échange en 3 temps :

- **Débat** : 4 minutes de discussions / débat avec les 2 équipes qui essayent de trouver les imposteur.e.s parmi elles/eux.
- **Vote** : A l'issue des 4 minutes, 1 minute avant la reprise du match est consacrée au vote à main levée d'élimination d'un.e cyber-imposteur.se. C'est la majorité qui l'emporte.
- **Élimination** : Quelque soit le rôle de la personne éliminée, elle **sort du jeu et devient consultant.e en cyber-imposture sur le bord du terrain** : elle cherche à déterminer qui sont les imposteur.e.s en observant le match et elle a le droit à 30 secondes de parole au début de chaque conseil d'élimination pour témoigner de son avis sur la situation. Cela permettra de garder tout le monde engagé.e dans le jeu !

Si tou.te.s les cyber-imposteur.se.s sont démasqué.e.s, ils/elles ont perdu le jeu !

4) Temps de bilan (10 minutes) :

Il s'agissait ici de montrer que les dangers en ligne nous entourent sans forcément que l'on n'y prête attention, mais avec un peu de bonnes volontés, on peut les débusquer ! Animez un temps d'échange autour de ces sujets, et rappelez quelques bonnes pratiques essentielles en ligne :

- **Être vigilant.e** sur les informations partagées : par exemple, ne pas divulguer ses coordonnées.
- **Être méfiant.e** sur les sollicitations reçues : les personnes qui nous contactent ne sont pas toujours celles qu'elles prétendent être et leurs intentions ne sont pas toujours sincères.
- **Ne jamais acheter seul.e** quelque chose sur Internet.
- Au moindre doute ou si un événement inhabituel survient, **en parler à un.e adulte** ou à une personne de confiance.

Pour aller plus loin, vous pouvez consulter les recommandations de [E-Enfance](#) ou le site cybermalveillance.gouv.fr.



Particuliers, entreprises, collectivités territoriales
Vous êtes victimes d'actes malveillants sur Internet ?

VIRUS PIRATAGE ARNAQUE CHANTAGE

RENDEZ-VOUS SUR WWW.CYBERMALVEILLANCE.GOUV.FR
POUR ÊTRE ASSISTÉ ET CONSEILLÉ

ASSISTANCE AUX VICTIMES D'ACTES DE CYBERMALVEILLANCE

INFORMATION ET SENSIBILISATION AUX RISQUES NUMÉRIQUES



Loyale



Loyale



Loyale



Loyale



Scammer

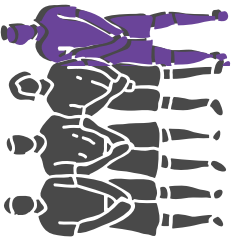


caméléon

Loyale



Hacker



traître

cyber-
harceleur.se



saboteur.se