STOP HACKERS

Déjoue les cyberattaques de tes amis et… de tes ennemis !

Cette activité est un jeu de rôle en débranché inspiré du jeu “Les Loups-garous de Thiercelieux” où les élèves sont répartis en équipes. Elle est destinée à un public de 10 à 12 ans. La thématique de cette activité est inspirée de la routine quotidienne des adolescents : des amis s’échangent des messages pour partager des contenus. Mais attention, les pirates guettent et sont une menace pour les amis. Qui sont les amis qui réussiront à échanger le plus de contenus ? Qui sont les pirates qui réussiront le plus d’attaques ?

Règles du jeu

Un set du jeu est composé de 6 amis, 3 techniciens et 1 routeur. Un set permet donc de faire jouer 10 élèves. Toutes les explications qui suivent sont fournies pour un set mais s'appliquent de la même manière si 20 ou 30 élèves participent (2 ou 3 sets à imprimer).

1. Matériel

Les amis ont

- un plateau représentant les smartphones des autres amis de son équipe et celui d'un destinateur inconnu
- des cartes "message" qui représentent des contenus qu'ils aiment (musique, jeu vidéo, photos, etc.)
- une carte "profil" qui définit son personnage (ce qu'il aime)
- une enveloppe pour envoyer les cartes "message"
- des étiquettes à placer sur les enveloppes pour dire à qui ils souhaitent envoyer un message et des trombones (ou autre système) pour les mettre et les retirer facilement
- un carnet ou une feuille pour écrire les codes

Les techniciens ont

- une fiche reprenant les instructions qu'ils devront suivre pendant la partie
- éventuellement des cartes "message"

Le routeur a

- un plateau représentant les smartphones des amis
- des cartes "publicité" qu'il devra envoyeraux amis.
- des étiquettes et trombones à placer sur les enveloppes pour dire à qui sont destinés les messages

2. Thème

Des amis s'envoient des messages pour partager sur des choses qu'ils aiment. Le routeur est chargé de transmettre ses messages entre les amis, aidé par ses techniciens. Mais attention, les pirates guettent …

3. Objectif de ce jeu

Proposition si on modifie sur base de notre dernière réunion :
Que la classe soit constituée d'une équipe ou de plusieurs, le jeu est une compétition entre les amis et les pirates. Les amis d'une même équipe vont tenter de s'envoyer un maximum de messages (carte "message") afin de cumuler les points. Les pirates mettent tout en œuvre pour piéger les amis. A chaque attaque réussie, les pirates remportent un point.
Les conditions de victoire sont explicitées dans le dossier pédagogique.

4. Mise en place

4.1. Les équipes et les rôles

Durant cette activité, les amis et les pirates vont s'affronter.

Les amis sont répartis dans la classe. Devant eux, ils ont un plateau de jeu représentant des smartphones, des cartes représentant des messages qu'ils pourront s'échanger, une carte "profil" qui définit sa personnalité et ce qu'il aime (à cacher), une feuille ou un carnet pour noter les codes et des enveloppes pour transmettre les cartes "message". Leur objectif est de s'envoyer des messages afin de cumuler des codes (notés sur les cartes "message") qui rapportent des points

Le·s routeur·s dispose·nt d'un plateau de jeu représentant les smartphones des amis et des cartes représentant des publicités. Leur objectif est de récupérer, trier et distribuer les messages entre les amis.

Le·s technicien·s dispose·nt d'une fiche contenant des instructions qu'ils devront suivre pour aider le routeur. Leur objectif est de suivre la mission qui leur a été donnée.

Les amis: Alice, Bob, Carole, David, Greg, Fanny

Le·s routeur·s	
Les techniciens : Eve, Oscar, Peggy	

5. Phases de jeu

A chaque tour de jeu :

- **Étape 1** → Les amis envoient un **message unique destiné à un ami** de leur équipe.

  Un message peut être constitué au maximum d'une carte "message" et d'une publicité/d'un concours/etc. S'ils ont reçu un message d'un autre ami, ils peuvent le transférer en plus également. Les cartes sont placées dans l'enveloppe du destinataire et celle-ci est déposée à l'avant du banc, pour être récupérée par le routeur. Une fois le message repris par le routeur, les amis peuvent en préparer un nouveau.

- **Étape 2** → Tel un facteur, le routeur passe près des amis et récupère les 6 enveloppes déposées sur le banc des amis. Il n'en récupère qu'une par ami même si les enveloppes s'accumulent trop vite. Il retourne à son plateau avec les enveloppes pour trier les messages.

  Lors du tri, le routeur ouvre une enveloppe et découvre, par exemple, un message d'Alice pour Bob. Il place ce message sur son plateau de jeu et plus précisément sur le smartphone de Bob. Il procède de la même manière pour les 5 autres messages. Il ajoute une publicité sur les smartphones de tous les amis. Ensuite, il réunit tous les messages adressés, par exemple, à Alice dans une enveloppe et ajoute l'étiquette adéquate (routeur pour Alice). Il procède de la même manière pour les 5 autres amis. Une fois l'opération de tri terminée, il passe à l'étape 3.

Pendant cette étape, les techniciens suivent les consignes qu'ils ont reçues. Ils ne peuvent mener qu'une tâche par tournée.

- **Étape 3** → Le routeur reprend sa tournée. Il dépose à chaque ami, par exemple Alice, l'enveloppe unique avec tous les messages qui lui sont adressés. Le routeur profite de ce passage pour récupérer les nouveaux messages préparés par les amis sur le coin du banc (étape 1).

  Les amis vont prendre connaissance du contenu et le trier sur leur plateau de jeu. Pour savoir quel ami a envoyé un message, il suffit de regarder la couleur de la carte (exemples : si c'est violet, c'est un message d'Alice; si la carte est grise, il s'agit d'un "autre destinataire").
  Les amis peuvent prendre connaissance des messages reçus. Ils doivent alors prendre une décision : noter ce code ou ne pas le noter. S'ils notent le code, cela signifie qu'ils réalisent l'action proposée ou qu'ils acceptent le message. S'ils ne notent pas le code, ils doivent alors écrire le code refusé et expliquer pourquoi ils ne souhaitent pas le garder.

6. La fin du jeu

Le jeu se termine lorsque le routeur a effectué au moins 7 tours (et maximum 10).

7. Conditions de victoires

Proposition avec nouveauté AMIS VS PIRATES
C'est l'équipe d'amis ou de pirates qui a le plus de points qui remporte la partie.
Pour rappel, sur chaque carte que les amis reçoivent, il y a un code. Les amis ont dû choisir de noter ces codes sur leur carnet ou pas. A la fin de la partie, les amis comptent le nombre de codes. 1 code écrit vaut 1 point.
Les pirates peuvent également gagner des points en réussissant les attaques menées vers les amis. 1 attaque réussie vaut 1 point.

Support pédagogique

---

1. Présentation

1.1. Objectifs de l'activité

Objectif général : comprendre les cyberattaques, en identifier les risques et les évaluer.
Objectifs d'apprentissage :

- Comprendre le fonctionnement des différentes menaces sur internet;
- Comprendre que les menaces sont mises en œuvre par des personnes (pas des machines) qui ont certaines intentions et comprendre la valeur des données qui sont volées ou endommagées[1];
- Identifier les conditions et le contexte social à partir desquels les menaces peuvent réussir (et devenir des attaques), ou échouer[2].

1.2. Durée de l'activité

Nous préconisons de prévoir 3 périodes de 50 minutes pour mener cette activité.

2. Précisions par rapport aux règles du jeu

Les techniciens/pirates

Comme vous aurez pu le remarquer, les élèves ne savent pas qui sont les pirates à la lecture des règles du jeu. C'est volontaire ! Le rôle de technicien est une couverture pour les pirates. Les amis ne les soupçonnent pas même s'ils savent que des pirates rôdent.
Après lecture des règles du jeu, il faudra expliquer aux techniciens le rôle qu'ils vont réellement jouer. Deux possibilités sont envisagées. Soit vous avez l'occasion de parler aux "techniciens" discrètement dans le couloir, soit vous distribuez une fiche avec les informations. Ils devront en prendre connaissance individuellement.

[1] Autrement dit, ce à quoi les pirates s'intéressent et pourquoi ils s'y intéressent.
[2] Le contexte peut rendre crédible les attaques, la personne qui est attaquée ne le sait pas nécessairement.

3. Phases de cette activité

3.1. Introduction

Vous allez présenter les règles et le matériel aux élèves.

Selon le nombre d'élèves, vous allez répartir les profils (amis, routeurs, pirates) et créer des équipes.

3.1.1. Composition des équipes

S'il y a 20 élèves (ou moins) dans la classe, vous devez créer deux équipes. Les équipes sont composées de cette manière[3] :

Nbre d'élèves	Amis	Routeurs	Techniciens = pirates
20	6 (x2)	1 (x2)	3 (x2)
19	5 et 6	1 (x2)	3 (x2)
18	5 (x2)	1 (x2)	3 (x2)
17	5 et 6	1 (x2)	2 (x2)
16	5 (x2)	1 (x2)	2 (x2)
15	4 et 5	1 (x2)	2 (x2)
14	4 (x2)	1 (x2)	2 (x2)
13	4 et 5	1 (x2)	1 (x2)
12	4 (x2)	1 (x2)	1 et 2
11	4 (x2)	1 (x2)	1 (x2)

S'il y a au moins 23 élèves dans la classe, vous devez créer 3 équipes. Reportez-vous au tableau pour 20 élèves.

Si vous avez 21 ou 22 élèves, vous pouvez imaginer une configuration de ce type :

Nbre d'élèves	Amis	Routeurs	Techniciens = pirates
22	6 (x2)	2 (x2)	3 (x2)
21	6 (x2)	1 et 2	3 (x2)

[3] Logique derrière ce tableau : Il faut toujours 1 routeur dans chaque équipe et au moins 4 amis qui s'envoient des messages. Le nombre de techniciens/pirates peut varier mais retirer un pirate c'est ne pas aborder un type de menace en ligne.

S'il y a moins de 10 élèves dans la classe, vous devez créer une seule équipe.

Nbre d'élèves	Amis	Routeur	Technicien(s) = pirate(s)
10	6	1	3
9	5	1	3
8	4	1	3
7	4	1	2
6	4	1	1

3.1.2. Disposition dans la classe

Les amis sont assis chacun à un banc et dispersés dans la classe. Pour éviter qu'ils communiquent autrement que par écrit, les amis d'un même groupe ne doivent pas se trouver assis l'un à côté de l'autre. Pour aider le routeur et les pirates à distinguer les équipes, une couleur ou un objet peut être associé à chaque groupe (badge, foulard, élastiques, etc.).
Les routeurs et les techniciens (pirates) d'une même équipe se placent sur un banc et attendent le début de la partie.Ils sont placés à l'arrière de la classe pour que les amis ne démasquent pas les "techniciens".

3.1.3. Conseils d'autres enseignants

Expliquer les règles du jeu

- Certains enseignants ont eu besoin d'un support de type diaporama, d'autres de mimer un tour pour que les élèves comprennent les différents rôles.

Matériel

- Si certains amis ne sont pas représentés (équipe réduite), n'hésitez pas à retirer ou barrer les informations inutiles.

3.2. Phases de jeu

<u>Quelques points d'attention</u>

- Rappelez aux amis qu'ils ont la possibilité de noter les codes ou pas. Lire la carte ne signifie pas qu'on doit noter le code. Ils peuvent découvrir le contenu et décider de ne pas noter le code.
- S'ils refusent de noter un code, ils doivent expliquer la raison. Vous disposerez de traces lors du débriefing.

- Il faut rappeler aux pirates qu'ils ne peuvent mener qu'une action par tournée du routeur. Si Eve veut en savoir plus sur les profils, elle doit cibler un ami à la fois.
-

Calculer les scores

A la fin de l'activité, il faudra calculer les points obtenus par les élèves.

Pour rappel, 1 code noté sur le carnet équivaut à 1 point, mais il se peut que l'élève ait noté un code d'un contenu piraté !

Pour retrouver ces codes piratés, il suffit de repérer les codes qui débutent par 2 (2xx-xxx). Il ne faut pas confondre avec les codes publicitaires qui commencent par 2 également mais ne dépassent jamais 200 (200-xxx).

3.3. Phase de débriefing

Afin de vous aider à mener ce débriefing, nous vous proposons une structure et une liste de questions.

3.3.1. Structure du débriefing

Temps de réaction :

- ➔ Les amis réagissent par rapport à leurs difficultés, leurs impressions, leurs craintes (ou pas) et à la manière dont ils ont perçu ou pas les menaces.
- ➔ Les élèves font le lien avec des situations vécues.
- ➔ Les routeurs peuvent alimenter la discussion avec leurs observations plus extérieures.

Temps de dévoilement :

- ➔ Les pirates se présentent, expliquent leurs intentions et les moyens qu'ils avaient à leur disposition.
- ➔ Ils expliquent les actions entreprises durant le jeu, réussies ou manquées.

3.3.2. Des points à aborder

En fonction des problématiques soulevées spontanément, plusieurs questions peuvent être abordées avec l'ensemble du groupe pour approfondir la discussion :

- ➔ Sur **les intentions des pirates**
- Est-ce que les amis ont compris ce qui intéressait les pirates, ce qu'ils voulaient ? Comment l'ont-ils compris ?
- Que veulent les pirates lorsqu'ils attaquent ? (nuire en endommageant des données ou du matériel, surveiller/espionner ou voler des données/de l'argent)

- ➔ Sur **la valeur des données**
- Quelles sont les données qui intéressent les pirates ?

- Comment on définit la valeur d'une donnée (pour les amis, pour les pirates) ?
    - Que peut faire Eve des données qu'elle a récoltées, par exemple ?
- Quelles sont les données qui ont le plus de valeur pour les pirates (données bancaires, données perso, photos, etc.) ?
    - Certaines données n'ont pas de valeur en soi, mais rassemblées avec d'autres, elles ont une grande valeur (ex.: les données personnelles récoltées en plusieurs fois pour établir le profil de quelqu'un, pouvant servir pour usurper une identité).
    - Quelles données peuvent servir à une arnaque, par exemple ?
- A quelles données ont-ils eu accès ?
- A quelles données doit-on être attentif sur internet ?
    - Qu'est-ce que je peux donner comme information, à qui et comment ?

➔ Sur **les manières d'attaquer, les menaces**

- Est-ce que vous avez identifié qu'il y avait différentes sortes de menaces, que les pirates attaquaient différemment ? Quelles menaces avez-vous identifiées ?
- Est-ce qu'il y a des menaces plus risquées que d'autres pour les amis ?
- Que peut faire un virus ? A quoi sert-il pour le pirate ?

➔ Sur la manière d'**identifier une menace**

- Comment vous êtes-vous rendu compte (ou pas) qu'il y avait une menace dans certains messages ?
- Comment les pirates ont-ils fait pour ne pas se faire remarquer ? Dans quels cas ça a marché (ou pas) ?
- Comment les pirates parviennent-ils à rendre crédibles leurs attaques dans le contexte d'échanges entre amis ?
- Pour ne pas se faire repérer, quelles sont les données qu'ils ont eu en leur possession, et comment les ont-ils eues ?
- Est-ce que vous avez fait attention à certaines informations que vous receviez ou donniez ? Comment ont-elles été utilisées par les pirates ?
- Comment certaines attaques ont réussi et d'autres pas ? Pourquoi ?
- Qu'est-ce que les amis ont fait (leurs actions) qui ont fait réussir certaines attaques (téléchargement, entrer en contact avec quelqu'un, partager un fichier, remplir un formulaire) ? Est-ce qu'il faut toujours une action d'un ami pour qu'une attaque soit réussie ?

➔ Sur la manière de **se protéger d'une menace**

- Que peut-on faire pour contrer une menace ?

- Est-ce qu'on peut se protéger de manière préventive (cryptage, antivirus, gestion de ses mots de passe, etc.) ?
- Est-ce que c'est toujours possible de se protéger ? Il n'y a pas de solution infaillible (ex: plus on crypte, plus il y a des moyens de décrypter)...
- Que faire si ce n'est pas possible de se protéger ? Comment gérer ses données de manière préventive ? Quelles informations met-on sur internet et sur sa machine ?
- Même s'il y a des risques, doit-on arrêter d'aller sur internet ? Il faut prendre en compte la réalité de chacun et vivre avec un risque acceptable...

3.3.3. Conseils des enseignants

- Les informations fusent au cours de ce débriefing, il est peut être intéressant de s'aider d'un support (carte mentale, notes au tableau) préparé à l'avance avec les questions clés ou à rédiger au moment même.
-

4. Et après ?

Cette activité peut être envisagée en complémentarité avec des outils éducatifs qui permettent d' :

- identifier concrètement les menaces : donner des indications techniques pour identifier une menace à partir d'une adresse mail, d'un lien vers un site, du nom d'un fichier à télécharger, d'une demande d'information, etc.
- apporter des solutions techniques : montrer comment protéger ses machines et ses données (mot de passe, antivirus, systèmes de cryptage, etc.)

En effet, ce dispositif aborde brièvement quelques thématiques que vous pourriez approfondir :

- L'identité numérique et les traces laissées sur internet;
- Le marketing et la publicité ciblée;
- Les big data et l'exploitation des données numériques;
- Les types de virus;
- La cryptographie.

<u>Ressources complémentaires</u>

School-IT est un projet de l'Université de Namur qui fournit aux enseignants des dispositifs d'éducation au numérique. Vous retrouverez des activités sur

- l'alphabétisation numérique
- l'intelligence artificielle

- la programmation
- etc.

Lien : https://school-it.info.unamur.be

Cybersimple : initiative issue d'une collaboration entre Google et Test-Achats qui "vise à promouvoir un Internet plus sûr et à sensibiliser les consommateurs à mieux se protéger face aux risques possibles sur le net".

Sur ce site vous aurez accès à

- des activités en ligne destinées aux enfants : "CyberHéros";
- des informations sur le sujet à destination des adultes.

Lien : https://www.cybersimple.be/fr/

Sur le site du **SPF Economie**, vous trouverez

- un test pour évaluer vos compétences numériques;
- des informations sur les stratégies mises en place pour le développement des compétences numériques.

Lien : https://economie.fgov.be/fr/themes/line/jeux-en-ligne/digital-duel/competences-numeriques