PARANO CHEZ LES NOOBS

LE JEU PÉDAGO-GEEK ET STRATÉ-GEEK DE PRÉVENTION DES USAGES À RISQUES DES NOUVELLES TECHNOLOGIES NUMÉRIQUES

LIVRET PEDAGO-GEEK

Douar Nevez
Centre de Soins, d'Accompagnement et de Prévention en Addictologie

Prévention 2.0

Région Bretagne

ars Agence Régionale de Santé Bretagne

Avec le soutien de la Région Bretagne et de l'Agence Régionale de Santé de Bretagne

Auteurs :
Laurent POMMEREUIL et Guillaume JEGOUSSE

Graphisme et illustrations :
Rémi Pommereuil - SIREN : 798 064 937
en partenariat avec les étudiants du lycée des métiers d'Art Bertrand Duguesclin (Brech)

Fabrication :

SOMMAIRE

6 ··· **Animation du jeu**
10 ··· **Piratage**
13 ··· **Vie publique/vie privée**
16 ··· **Cyber-harcèlement**
19 ··· **Usurpation d'identité**
22 ··· **Rencontres réelles**
24 ··· **Rapport filles / garçons**
26 ··· **Violence dans les média**
28 ··· **Pornographie**
31 ··· **Jeux Vidéo**
34 ··· **Parents : Parentalité et Internet**
37 ··· **Téléphone / Smartphone**
39 ··· **Réseaux sociaux en ligne**

Merci de vous être procuré le jeu « parano chez les noobs ».

La place du numérique dans notre société se développe à une allure exponentielle, en lien avec le développement d'Internet et l'amélioration constante des interfaces (ordinateur, téléphone, console). Les chiffres en la matière sont éloquents, c'est aujourd'hui tout un pan de l'économie mondiale qui est dédié au numérique.

Ces évolutions rapides modifient notre rapport au monde et aux autres personnes. Les contacts virtuels, le partage d'intérêts communs, le divertissement, l'information sont facilités. Nous devenons connectés en permanence à nos amis, à notre travail ou aux médias. Ces nouvelles technologies sont de formidables outils de jeux, de découverte et d'appréhension du monde.

Les différents acteurs de l'éducation (enseignants, animateurs, éducateurs…) ainsi que les parents sont parfois démunis face aux nouveaux problèmes liés à l'utilisation d'outils multimédia. La plupart d'entre eux ne sont actuellement pas préparés à échanger avec les adolescents sur les usages des jeux vidéo et des réseaux sociaux. En effet, un écart existe entre la connaissance de ces nouvelles technologies par les jeunes et les lacunes que certains parents ou éducateurs ont par rapport à l'utilisation de ces outils.

Ces dernières année ont vu l'explosion de nouvelles pratiques communautaires sur Internet (réseaux sociaux, blogs, messageries instantanées...) dont l'utilisation est peu encadrée et dont les outils de contrôle sont facilement contournés. Ce nouveau champ d'expression laissé aux plus jeunes amène parfois à des situations (incivilités, non-respect du droit à l'image, violences...) dont les conséquences peuvent avoir un impact néfaste sur la vie du jeune, de sa famille ou de son établissement scolaire.

L'objectif de parano chez les noobs est d'interroger notre relation au virtuel, de faire réfléchir les jeunes (ou les moins jeunes) aux risques existants et de les responsabiliser sur les actions possibles à mettre en place afin de réduire les risques. Nous avons choisi de proposer un jeu de société traditionnel plutôt qu'un serious game virtuel, afin de favoriser le débat d'une manière ludique. Le jeu devient une expérience agréable, dont on garde le souvenir plus longtemps qu'une action de prévention traditionnelle.

Les problématiques soulevés par les nouveaux médias sont nombreuses et touchent autant à l'Éducation qu'à l'Éthique. Certaines thématiques sont spécifiques (usurpation d'identité), quand d'autres sont plus transversales (réseaux sociaux). Une des idées fortes du jeu est de laisser choisir les thèmes de débat par les jeunes.

Ce livret pédago-geek vous permettra d'acquérir des bases de connaissance concernant les thématiques pouvant être abordées pendant le jeu « parano chez les noobs ». Nous espérons que vous passerez un aussi bon moment en animant ce jeu, que nous en avons eu en le construisant et en l'expérimentant sur des milliers d'élèves.

Guillaume JEGOUSSE
Laurent POMMEREUIL

Animation du jeu

Avant le jeu :

Nous vous conseillons de lire en premier lieu le livret de règles et de les connaitre.
Vous pouvez ensuite lire ce livret pédago-geek.

Durée du jeu :

Le nombre de tours dépend du nombre de joueurs et de la compétence (ou la chance) de telle ou telle catégorie de joueurs (noobs ou geeks).
La durée du jeu varie en fonction du nombre de joueurs, de la durée des échanges pendant le jeu et dans les phases de prévention. Nous conseillons aux meneurs de jeu de prévoir au minimum deux heures d'intervention par groupe.

Choix du type de jeu :

En fonction de l'âge et des compétences des joueurs, le meneur de jeu détermine si les cartes « appli » seront utilisées ou non. Le jeu sans appli a l'avantage d'être plus simple, moins contraignant en termes d'explications de règles, plus rapide mais perd en stratégie.

Jeu sans appli : convient à partir du collège (voire du CM2)
Jeu avec appli : convient à partir du lycée

Posture du meneur de jeu :

Le meneur de jeu est également animateur de prévention. Il alternera entre les phases d'animation de jeu pure, et les phases de débat avec les élèves. Ces phases de prévention ont lieu après la déconnexion, quand le meneur de jeu a expliqué tout ce qui s'est passé pendant la déconnexion (joueur éliminé par les geeks, rumeur, pouvoirs joués etc.). Il est essentiel d'aborder ces phases de prévention sans jugement des usages des jeunes. L'objectif est de les faire parler, et qu'ils trouvent eux même des réponses aux risques cités.

Objectifs de l'action de prévention :

- Permettre aux jeunes d'identifier les risques existants liés aux usages des NTIC, et les solutions concrètes pour s'en protéger
- Favoriser le bien-vivre-ensemble numérique et inciter les jeunes à prendre soin des autres
- Faire émerger la parole des jeunes sur leurs usages et valoriser les comportements sans risque
- Faire réfléchir les jeunes sur la place que prennent les NTIC dans leur vie

Choix de la thématique :

C'est le joueur éliminé par les geeks qui choisit la thématique. Vous projetez sur l'écran la liste de thèmes et il choisit. Vous cherchez alors la diapositive dans le diaporama qui correspond à cette thématique et lancez le débat.

Le débat de prévention :

Toutes les personnes présentes participent au débat de prévention (même si elles sont éliminées).
En fonction de la participation et des questionnements, ce mini-débat peut durer plus ou moins longtemps. Le temps de discussion sera généralement plus important sur des thématiques larges (réseaux sociaux, jeux vidéo…). Le diaporama est conçu de telle sorte que les lignes s'afficheront au fur et à mesure. Chaque diapositive est composée des éléments suivants :
Un chiffre ou une question pour lancer la réflexion : les élèves doivent essayer de deviner le lien entre le chiffre et la thématique, ou répondre à la question
Une question qui peut être posée au joueur éliminé. Nous utilisons parfois cette question pour faire un lien avec le jeu. En effet, si le joueur répond correctement à la question, vous pouvez lui donner le droit de donner la carte brigade numérique à qui il souhaite.
Des conseils de prévention. Ces conseils auront plus d'impact si vous les faites émerger par les jeunes au cours de l'échange. Vous les faites apparaitre ensuite pour une deuxième phase de mémorisation.
Le diaporama est un outil qui vous permet de garder une trame d'intervention en tête. Vous avez le choix de mener le débat de la manière dont vous voulez. N'éternisez tout de même pas le débat pour garder une dynamique de jeu (et avoir le temps de le finir !)
Après le débat de prévention, se lance le débat concernant le jeu, pendant lequel vous allez interroger les joueurs sur leurs ressentis en leur posant notamment cette question « Alors selon toi, qui sont les geeks autour de la table ? » et en incitant les personnes désignées à se défendre.

Principes généraux de prévention[1] :

A. OBJECTIFS DE LA PREVENTION
1. Agir sur les déterminants de santé pour lutter contre les inégalités sociales de santé
2. Développer des compétences personnelles (de vie) chez les jeunes
3. Développer des compétences d'adaptation sociale chez les jeunes
4. Développer les compétences sociales et civiques, l'autonomie et l'initiative des jeunes
5. Développer des stratégies de réduction des risques

B. MOBILISATION DES ACTEURS
6. Impliquer l'ensemble des partenaires
7. Impliquer les parents
8. Impliquer des jeunes formés à la prévention
9. Impliquer des intervenants compétents
10. S'appuyer sur les instances de santé et de citoyenneté

C. METHODES A PRIVILEGIER
11. Utiliser des modèles théoriques validés
12. Travailler dans la durée en cohérence avec le projet d'établissement
13. Intervenir précocement sur les questions de prévention
14. Favoriser un bon climat scolaire
15. Délivrer des messages positifs
16. Utiliser des méthodes interactives et pas uniquement la transmission d'information
17. Proposer des actions adaptées aux jeunes ayant des comportements à risque
18. Proscrire les stratégies d'appel à la peur et les témoignages de vie
19. Proscrire les propos moralisateurs

D. METHODOLOGIE DE PROJET
20. Bien connaitre la population des jeunes (connaissances, besoins, intérêts, entourage, lieux de vie…)
21. Evaluer les interventions

1. Source : AIRDDS, « stratégie de prévention des conduites addictives en milieu scolaire », 2012, http://www.cirdd-bretagne.fr/fileadmin/publications/Projets/Prevention_scolaire/PREVENTION_DES_CONDUITES_ADDICTIVES_synthese_des_recommandations.pdf

Après le jeu, l'importance de la conclusion :

Il est essentiel de garder un temps en fin d'intervention pour conclure. Ce temps d'échanges doit permettre d'évaluer ce que les jeunes gardent de l'intervention (logiquement ils vont aimer le jeu, il convient donc de les interroger sur l'aspect prévention.)

Pendant le jeu, vous avez surement pu identifier un ou des meneurs, un ou des manipulateurs, des stratégies d'attaque ou de défense efficaces et il est intéressant de s'appuyer sur cette expérience pour aborder la question des influences du groupe et les moyens d'éviter les influences négatives.

« Pendant la partie, certains d'entre vous ont-ils été manipulés ? Influencés ? ».Souvent, les jeunes répondent par la négative. Il est intéressant de leur expliquer qu'on est influencé tous les jours, par ses parents, ses professeurs, les médias et surtout ses amis ou connaissances. Cette influence peut être négative ou positive. La notion de libre-arbitre peut alors être expliquée, imagée et permettre de terminer l'intervention sur une ouverture intéressante en ce qui concerne leur liberté.

PIRATAGE

Définition :

Délit informatique qui consiste à s'approprier un concept logiciel en vue d'une exploitation ultérieure, à violer l'intégrité d'un système dans un but malveillant ou à copier des informations sans permission pour les utiliser, les diffuser ou les vendre.
Un virus informatique est un programme automate capable de se reproduire seul, à la base non malveillant, mais aujourd'hui souvent additionné de code malveillant (donc classifié comme logiciel malveillant), conçu pour se propager à d'autres ordinateurs en s'insérant dans des logiciels légitimes, appelés « hôtes ». Il peut perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre par tout moyen d'échange de données numériques comme les réseaux informatiques et les cédéroms, les clefs USB, etc.[1]

Contexte :

Le terme « hacker » est apparu dans les années 60 au sein du Massachusetts Institute of Technology (MIT). Des étudiants se surnomment ainsi après avoir démonté et modifié leurs maquettes pour améliorer les performances. Les virus naissent dans les années 1980.
Dans les années 1990, avec le développement d'internet un glissement s'opère vers la cybercriminalité et la « communauté » des hackers se divise. D'un côté les « black hat », aux activités souvent criminelles et de l'autre les « white hat » sans intention de nuire et surtout attachés à rendre public des failles de sécurité.
Dans les années 2000, on commence à parler d' « hacktivisme ». Le piratage informatique prend une dimension idéologique et militante (wikileaks, anonymous…), qui va atténuer les représentations négatives concernant les hackers.
Aujourd'hui, on estime souvent que les pirates sont des personnes très expérimentées. Mais l'accès aux techniques de piratage s'est démocratisé, facilitant leur propagation. Parallèlement, les personnes qui téléchargent illégalement peuvent être considérés comme des pirates informatiques.

Eléments statistiques :

Environ deux millions de virus existent sur Internet, et deux millions de codes malveillants supplémentaires sont créés chaque année.
Un tiers des internautes pratique le téléchargement illégal (via sites de Peer To Peer ou de téléchargement direct) ou le streaming de vidéos. Ce sont plus souvent les hommes qui téléchargent et les femmes qui pratiquent le streaming, et majoritairement des personnes entre 20 et 35 ans.
10% des utilisateurs de facebook ont déjà subi une tentative de piratage de compte.
55% des adolescents américains donnent des informations personnelles à des gens qu'ils ne connaissent pas ou peu.

Les différentes formes de piratage informatique[3] :

▪ **Le « social engineering »** : c'est une technique qui consiste à obtenir des informations de la part des utilisateurs par téléphone, courrier électronique, courrier traditionnel ou contact direct. Elle est basée sur l'utilisation de la force de persuasion et l'exploitation de la naïveté des utilisateurs en se faisant passer pour une personne de l'organisation : un technicien, par exemple un administrateur, etc. Cette technique est également appelée phishing et est couramment employée sur les réseaux sociaux après un piratage de compte. Néanmoins, cette pratique vise surtout les entreprises.

▪ **Le scam** : est une pratique frauduleuse d'origine africaine, consistant à extorquer des fonds à des internautes en leur faisant miroiter une somme d'argent dont ils pourraient toucher un pourcentage. L'arnaque du scam est classique : vous recevez un courrier électronique de la part du seul descendant d'un riche africain décédé il y a peu. Ce dernier a déposé plusieurs millions de dollars dans une compagnie de sécurité financière et votre interlocuteur a besoin d'un associé à l'étranger pour l'aider à transférer les fonds. Il est d'ailleurs prêt à vous reverser un pourcentage non négligeable si vous acceptez de lui fournir un compte pour faire transiter les fonds.

▪ **Le « Spoofing IP » ou usurpation d'adresse IP** : Cette technique repose sur le fait de remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine. Elle permet ainsi à un pirate d'envoyer des paquets (fichiers compressés) anonymement. Il ne s'agit pas pour autant d'un changement d'adresse IP, mais d'une mascarade de l'adresse IP au niveau des paquets émis.

▪ **Le « hijacking » ou « détournement de session »** : Le détournement de session est une technique consistant à intercepter une session TCP initiée entre deux machines afin de la détourner. Dans la mesure où le contrôle d'authentification s'effectue uniquement à l'ouverture de la session, un pirate réussissant cette attaque parvient à prendre possession de la connexion pendant toute la durée de la session.

2. http://fr.wikipedia.org/wiki/Virus_informatique
3. http://securiteinformartique.wordpress.com/2011/11/12/les-types-de-piratage/

Objectifs spécifiques du débat :

Faire prendre conscience aux élèves que les piratages peuvent généralement être évités avec des techniques simples.

Exemple de questions pouvant lancer le débat :

- Qu'est-ce qu'un virus ?
- Comment se protéger du piratage informatique ?
- Y a-t-il selon vous des pirates informatiques dans cette classe ? (rappel à la Loi concernant le téléchargement illégal)
- Qui possède un antivirus sur son téléphone ?

Conseils pouvant être donnés aux enfants :

- Toujours réfléchir avant de cliquer.
- Savoir identifier les publicités trompeuses.
- Installer un antivirus sur tous les appareils connectés, et en particulier sur son téléphone.
- Se méfier des applications sur téléphone, elles peuvent contenir des virus. Bien vérifier que l'éditeur de l'application est connu.
- Protéger ses comptes avec des mots de passe complexes (chiffres + lettres + caractères spéciaux) et avoir des mots de passe différents pour chaque site important (messagerie, réseaux sociaux…).
- Ne pas cliquer sur des e-mails provenant de destinataires inconnus.
- Stopper les programmes inconnus se téléchargeant tout seuls.

Pour reprendre le jeu :

On peut reprendre le jeu en parlant de la hackeuse ou de l'anonymous, et en abordant l'aspect éthique du piratage (droits d'auteurs par exemple).

Pour aller plus loin :

- Jean-François Pillou et Jean-Philippe Bay, tout sur la sécurité informatique, éditions Dunod, 2013, 256 pages
- Kevin Beaver, Combattre les hackeurs pour les nuls, éditions First interactive, 2014, 424 pages
- Frédéric Bardeau et Nicolas Danet, Anonymous : pirates informatiques ou altermondialistes numériques ?, Fyp éditions, 2011, 208 pages

VIE PUBLIQUE/VIE PRIVÉE

Définition :

La vie privée est la capacité, pour une personne ou pour un groupe, de s'isoler afin de se recentrer sur sa vie et de protéger ses intérêts. Les limites de la vie privée ainsi que ce qui est considéré comme privé diffèrent selon les groupes, les cultures et les individus, bien qu'il existe toujours un certain tronc commun.

Contexte :

La notion de vie privée et vie publique est très ancienne puisque Aristote en faisait déjà la distinction. La vie privée est inscrite dans la déclaration universelle des droits de l'homme de 1948. C'est une notion assez moderne dans son inscription dans le droit.
Internet est un formidable outil de partage à l'échelle mondiale. Cependant, son utilisation amène parfois à la violation de droits fondamentaux, comme la vie privée. Le problème est donc celui d'un équilibre entre sécurité et protection de la vie privée avec liberté sur Internet.
Paradoxalement, bien que les Français se montrent très attachés à la protection de leur vie privée, nombre d'entre eux s'exposent volontairement sur des sites. Il faut alors distinguer deux catégories de données personnelles collectées sur Internet : d'abord, les données confiées par les internautes aux services utilisés. Exemple : lors d'une inscription à un réseau social. Ensuite, les données collectées à notre insu par des services. Ainsi, le fait de s'exposer sur internet et plus précisément sur les médias sociaux favorise les risques de piratage, de moqueries, d'harcèlement ou de dévoilements publics d'informations privées.
Les nouvelles technologies numériques ont rendues plus floues les frontières entre vie publique et vie privée. Les émissions de téléréalité ont banalisé le fait de parler de soi et de se montrer entièrement. Parallèlement, les réseaux sociaux permettent à chacun de valoriser ses expériences et compétences, et d'en avoir un retour positif (puisque la touche « je n'aime pas » n'existe pas). Internet est aujourd'hui un outil utilisé dans le cadre de recrutement professionnel, ou d'enquêtes policières.

Eléments statistiques :

Chez les jeunes français de 16 à 25 ans[4] :
- L'usage des webcams est plus courant en France que la moyenne européenne (48% Vs 31%)
- Les enfants français rapportent plus de contacts sur les réseaux sociaux. 13% des 9-10 ans et 37% des 11-12 ans ont un profil sur un réseau social
- Les enfants français sont moins nombreux à préserver leur intimité sur les réseaux sociaux (34% Vs 43%)
- 43 % des enfants français ont déjà ajouté en amis des gens qu'ils ne connaissaient pas
- 12% des enfants français ont déjà envoyé une photo ou une vidéo à quelqu'un qu'ils ne connaissaient pas
- Le principal problème que les enfants rapportent avoir subi quant à leurs données personnelles est celui de l'utilisation non désirée par quelqu'un de leur mot de passe ou l'usurpation d'identité (6 %). Certains rapportent que des informations personnelles ont été utilisées d'une façon qu'ils n'ont pas aimée (3 %). Ces pourcentages sont légèrement inférieurs à la moyenne européenne

Objectifs spécifiques du débat :

- Faire prendre conscience aux jeunes que tout ce qui est mis sur Internet est potentiellement public et pas forcément effaçable
- Informer sur le droit à l'image

Exemple de questions pouvant lancer le débat :

- Quand peut-on poster une photo de quelqu'un sur les réseaux sociaux ?
- Est-ce que vous écririez sur Internet ce que vous aimiez quand vous aviez quatre ou cinq ans de moins ?
- Qui peut avoir accès à votre profil de réseau social ?
- Pourquoi doit-on trier les photos de nous qu'on met sur Internet ?
- Comment sait-on qu'on est sur un espace sécurisé sur internet ?

4. Extrait de l'étude EU kids online, london schools of economics and politics, 2012, http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx

Conseils pouvant être donnés aux enfants :

- Demander l'autorisation à la personne avant de publier une photo ou une vidéo d'elle
- Ne jamais donner d'informations personnelles à des inconnus, ou sur des espaces non sécurisés
- Toujours réfléchir avant de poster des photos ou vidéos compromettantes de soi

Pour reprendre le jeu :

On peut associer cette discussion aux compétences du moqueur (rumeurs) ou du maniaque (photos compromettantes) avant de lancer le jeu.

Pour aller plus loin :

- Traité de droit de la presse et des médias, sous la direction de Bernard Beignier, Bertrand de Lamy, Emmanuel Dreyer, V° La protection de la vie privée et de l'image des personnes, par Thomas Roussineau, Docteur en droit, Avocat au barreau de Paris, Litec, Paris, 2009
- La vie privée à l'ère du numérique, par Bénédicte Rey, Hermès Science Pub. : Lavoisier, 2012
- Économie des données personnelles et de la vie privée, Fabrice Rochelandet, Ed. La Découverte, Collection Repères, Paris, 2010

CYBER-HARCÈLEMENT

Définition :

Le **cyberharcèlement** est une forme de harcèlement conduite par divers canaux numériques (téléphones, réseaux sociaux…)

Contexte[5] :

Le cyberharcèlement est une forme récente de harcèlement. Quelques années auparavant, la fin des cours et le soir étaient des temps permettant d'apaiser les conflits de la journée. Aujourd'hui, avec le développement des réseaux sociaux, plus aucun temps de repos du conflit n'est permis. Le harcèlement n'est plus cantonné à la seule cour de récréation et aux moments où l'enfant est à l'école. L'ordinateur peut devenir un déversoir d'insultes et de menaces diverses et devient une arme utilisable par ceux qui ne peuvent pas se défendre physiquement ou socialement. De plus en plus d'adolescents utilisent ces interactions pour intimider et harceler les autres.
Les « croyances normatives approuvant le harcèlement » influent sur l'incidence de cyberharcèlement : plus le jeune croit qu'il est facile de harceler autrui, plus il ou elle se livrera à des violences par l'intermédiaire de chats, d'interventions indésirables sur les réseaux sociaux ou de publications de vidéos humiliantes. On observe que si le jeune harceleur perçoit que sa victime est peu soutenue par ses pairs, ses attaques seront d'autant plus féroces.

En outre, la distance physique avec la victime permet une démultiplication du nombre de harceleurs, de leurs attaques et de la force (psychologique) de celles-ci3.

- Il est moins important dans les interactions réelles d'être plus fort, intelligent, ou populaire que la victime pour se joindre à une entreprise de harcèlement.
- L'agresseur ne voit pas les réactions de souffrance de sa victime, ce qui court-circuite d'occasionnels passages à la compassion et l'empathie.
- La dépersonnalisation atteint non seulement la victime mais ses persécuteurs, qui ont tôt fait de se déresponsabiliser de leurs actes « virtuels ».
- Cette dépersonnalisation engendre une forme de paranoïa chez la victime, qui ne sait pas et ne peut savoir qui conspire dans l'anonymat des voies numériques.

5. http://fr.wikipedia.org/wiki/Cyberharc%C3%A8lement

Eléments statistiques[6]:

- 26 % des enfants (et 19 % à travers l'Europe) disent avoir été harcelés en ligne ou hors ligne, mais seuls 5 % disent que cela s'est passé sur Internet
- La victimation la plus courante est l'envoi de messages méchants[3] ou blessants (3 %), suivie par des messages postés en ligne (2 %) et d'autres contenus méchants en ligne (1 %). Seulement 1 % des enfants dit avoir été exclu socialement ou menacé en ligne
- 17 % des enfants disent avoir harcelé quelqu'un lors des douze derniers mois

Objectifs spécifiques du débat :

- Apprendre aux jeunes à réagir quand ils sont harcelés, et notamment d'en parler à un adulte
- Faire réfléchir les élèves sur le sentiment d'impunité pouvant exister quand on est à l'abri derrière son écran
- Rappeler la Loi
- Inviter les élèves à soutenir les victimes et à ne pas participer gratuitement au harcèlement, en partageant des photos, messages ou vidéos par exemple

Exemple de questions pouvant lancer le débat :

- Qu'est-ce que le cyberharcèlement ?
- Quel moyen numérique utilise-t-on le plus souvent pour harceler l'autre ?
- Que faire si on est harcelé ?
- Avez-vous déjà vu des personnes se faire harceler sur Internet et comment avez-vous réagi ?

6. Extrait de l'étude EU kids online, london schools of economics and politics, 2012, http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx

Conseils pouvant être donnés aux enfants :

▪ Essayer de se comporter devant son écran comme dans la vraie vie
▪ Faire réfléchir les jeunes sur le fait que nous n'avons pas tous les mêmes compétences, et qu'un message
▪ jugé sans importance pour quelqu'un, pourra être destructeur chez une personne plus faible
▪ Faire réfléchir aux chaînes de messages haineux, qu'il convient de ne pas partager
▪ Si on est harcelé :
- En parler à un adulte et envisager la possibilité d'un soutien extérieur (psychologue)
- Conserver les messages de harcèlement (copie d'écrans)
- Bloquer le harceleur (contacter l'opérateur téléphonique ou le fournisseur d'accès internet si besoin)
- En cas de harcèlement grave, porter plainte immédiatement

Pour reprendre le jeu :

Le maniaque symbolise bien le harcèlement. Vous pouvez demander aux élèves s'ils trouveraient normal que le maniaque puisse mettre le nez rouge au même joueur pendant tout le jeu.

Pour aller plus loin :

Site gouvernemental « agir contre le harcèlement à l'école » : http://www.agircontreleharcelementalecole.gouv.fr/quest-ce-que-le-harcelement/le-cyberharcelement/

USURPATION D'IDENTITÉ

Définition :

L'usurpation d'identité est le fait de prendre volontairement l'identité d'une autre personne vivante, généralement dans le but de réaliser des actions frauduleuses. Il existe également aujourd'hui des usurpations d'identité de personnes morales dans le but de réaliser des escroqueries (on appelle cela le « phishing » ou hameçonnage).

Contexte :

L'usurpation d'identité, bien que non-délimitée aux pratiques numériques, connait une expansion importante aujourd'hui, facilitée par ces nouveaux médias. L'usurpation d'identité débute toujours par la collecte de renseignements personnels sur la victime. Les renseignements personnels peuvent être le nom, le numéro de téléphone, la date de naissance, la filiation, l'adresse, le numéro d'assurance sociale, le numéro de carte de crédit, le mot de passe de carte de crédit ou de débit ou toute autre information permettant d'identifier la personne. La victime de l'usurpation d'identité reste vivante (sinon on parle de vol d'identité), et possède donc la faculté de défendre ses droits.

Les personnes souhaitant usurper une identité peuvent utiliser plusieurs techniques sur les NTIC :

▪ La subtilisation de mots de passe : il est possible de voler un mot de passe en regardant par-dessus l'épaule d'un individu qui écrit son mot de passe sur un clavier, en installant une caméra dans un endroit stratégique ou en utilisant un enregistreur de frappe.

▪ L'intrusion locale sur le navigateur : il est possible à un intrus de reprendre une session sur un site quand l'utilisateur a simplement fermé l'onglet où il opérait, en utilisant l'historique du navigateur. L'intrus local peut alors accéder aux informations du profil, les modifier, les détourner etc. et usurper l'identité de l'utilisateur légitime. L'usurpateur peut librement effectuer des transactions au détriment de l'utilisateur légitime.
L'écoute électronique : des fraudeurs peuvent placer des appareils d'écoute entre un terminal de validation de cartes de crédit et le réseau de communications pour capter les numéros de carte de crédit et les mots de passe des acheteurs.

▪ L'hameçonnage (ou phishing): il consiste à simuler des messages électroniques de compagnies légitimes qui demandent des informations personnelles au receveur ; évidemment, les réponses des répondeurs naïfs sont reçues par des fraudeurs qui utilisent ensuite ces informations pour frauder leurs victimes.

▪ Les escroqueries par téléphone : des fraudeurs se font passer pour des fonctionnaires, des enquêteurs ou des employés de compagnies légitimes pour soutirer des renseignements personnels.

Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende.

Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.[8]

Eléments statistiques :

6% des enfants français ont subi le fait que quelqu'un a utilisé leur mot de passe pour accéder à leurs informations ou a prétendu être eux.

Objectifs spécifiques du débat :

- Rappeler la Loi
- Faire prendre conscience aux jeunes qu'il est important de réfléchir avant de donner des informations personnelles sur Internet.
- Informer sur les techniques à mettre en place pour éviter l'usurpation d'identité

Exemple de questions pouvant lancer le débat :

- Qu'est-ce que l'usurpation d'identité ?
- Comment sait-on qu'un site est sécurisé ? (adresse en https et cadenas)
- Qui s'est déjà fait pirater son compte facebook ? Comment le pirate s'y est-il pris ? Comment avez-vous réagi ?

7. http://fr.wikipedia.org/wiki/Usurpation_d%27identit%C3%A9
8. Article 226-4-1. LOI n°2011-267 du 14 mars 2011 - art. 2

Exemple de questions pouvant lancer le débat :

- Qu'est-ce que l'usurpation d'identité ?
- Comment sait-on qu'un site est sécurisé ? (adresse en https et cadenas)
- Qui s'est déjà fait pirater son compte facebook ? Comment le pirate s'y est-il pris ? Comment avez-vous réagi ?

Conseils pouvant être donnés aux enfants :

- Toujours se déconnecter après être allé sur un site nécessitant une connexion (réseau social, adresse mail…)
- Ne jamais donner d'informations personnelles sur les réseaux sociaux ou sur un forum
- Ne jamais autoriser les sauvegardes de mots de passe pour se connecter plus rapidement. Il vaut mieux se déconnecter et retaper son mot de passe à chaque connexion.
- Se méfier quand un « ami » vous demande de faire telle ou telle action à sa place, le questionner précisément pour vérifier son identité
- Ne jamais donner son mot de passe, à qui que ce soit
- Ne jamais répondre à un mail provenant d'une entreprise qui demanderait des coordonnées bancaires ou des informations personnelles.

Pour reprendre le jeu :

Si vous jouez avec les applis, vous pouvez parler de la carte usurpation d'identité. Sinon, vous pouvez parler des geeks qui se font passer pour des noobs.

Pour aller plus loin :

- Guy de Felcourt, PDG de CPP FRANCE, auteur de Usurpation d'identité16, aux éditions du CNRS, Paris, 2011
- Olivier Iteanu, L'identité numérique en question, éditions Eyrolles, Paris 2008

RENCONTRES RÉELLES

Définition :

On appelle rencontres réelles, ou rencontres IRL, ou encore rencontres AFK (Away From Keyboard) une rencontre entre deux personnes ou un groupe de personnes rencontrées numériquement.

Contexte[5] :

Le développement d'Internet favorise la création de rencontres éloignées ou non de son lieu d'habitation. Il permet la rencontre en dehors des lieux de sociabilité existants (écoles, associations sportives…) et autorise les recherches ciblées en fonction de certains critères. Il existe différents moyens de rencontrer des personnes sur Internet et notamment :

- Les réseaux sociaux où l'on peut rencontrer les amis de ses amis ou des inconnus
- Les sites de rencontres, dont il existe une multitude de formes avec des critères de recherche géographiques, relatifs aux centres d'intérêt ou encore à la finalité de la rencontre souhaitée (sites de rencontre amicaux, amoureuses ou sexuelles).
- Les forums de discussion, où les personnes vont se rassembler généralement autour d'un intérêt
- Les jeux vidéo en ligne dont beaucoup favorisent les rencontres, voire même l'obligation de jouer avec d'autres pour avancer dans le jeu
- Les messageries instantanées
- Les chats en ligne via des applications ou des sites, par texte ou webcam
- Les roulettes de chat, où les personnes vont rencontrer des inconnus directement en webcam.

Ces possibilités de rencontres sont un formidable outil d'échanges. Néanmoins, ces espaces numériques de rencontres peuvent être infiltrés par des personnes mal intentionnées. D'autre part, les rencontres réelles se font en général assez rapidement après la rencontre numérique, sans prendre le temps de s'assurer de la bienveillance de son interlocuteur.
Il existe également des rencontres IRL collectives organisées pour se rencontrer entre joueurs ou utilisateurs de certains sites de rencontre.
De manière générale, les enfants ne communiquent pas beaucoup avec les adultes sur Internet, et ne les rencontrent donc pas dans la vie réelle. Les cas de pédophilie dont la prise de contact s'est faite sur Internet sont rares, bien que très médiatisés.

Eléments statistiques :

- 32 % des enfants, en France[6], ont communiqué en ligne avec un(e) inconnu(e)
- 12 % ont rencontré quelqu'un qu'ils avaient connu en ligne dans la vie réelle
- Les adolescents les plus âgés (13-16 ans) sont beaucoup plus nombreux que les plus jeunes à établir des contacts en ligne avec un(e) inconnu(e) et ils sont aussi plus susceptibles de rencontrer dans la vie réelle des personnes connues sur Internet[3]
- Les enfants des classes moyennes, en France, sont plus nombreux à dire avoir fait de nouvelles connaissances en ligne et de les avoir rencontrées en face à face.

Objectifs spécifiques du débat :

- Réduire les risques liés aux éventuelles rencontres réelles que l'enfant peut faire.

Exemple de questions pouvant lancer le débat :

- Comment peut-on savoir qui est vraiment celui avec qui on discute ?
- Qui utilise un pseudonyme ? A quoi ça sert ?

Conseils pouvant être donnés aux enfants :

- Parfois il est plus facile de se confier à des inconnus. Il faut particulièrement se méfier de ce que l'on peut dire à des inconnus
- Quand l'enfant décide de rencontrer quelqu'un :
  - Ne pas donner d'informations personnelles (adresse personnelle)
  - Venir au premier rendez-vous avec un adulte
  - S'il ne veut pas venir au rendez-vous avec un adulte, au moins prévenir
  - Toujours choisir un endroit public et passant, pour une première rencontre
  - Veiller à prendre son téléphone pour appeler en cas de problème

Pour reprendre le jeu :

Vous pouvez parler de l'anonymous pour évoquer l'anonymat sur Internet et la difficulté, voire l'impossibilité de connaitre l'identité réelle d'un pseudonyme numérique.

RAPPORT FILLES / GARÇONS

Contexte :

Le développement des nouvelles technologies a modifié les relations entre filles et garçons, entre hommes et femmes. On peut noter de manière non exhaustive :
- Les possibilités de rencontres multipliées
- Le lien à distance plus facilement maintenu
- L'accès à la pornographie ou la sexualité virtuelle
- La possibilité de communiquer plus facilement en « face à face ». Les jeunes nous disent souvent que les communications sont plus intéressantes quand l'autre est éloigné de son groupe d'appartenance.
- La facilité de harcèlement ou d'insultes

Internet est le reflet de la société dans son ensemble. Le sexisme y est présent, notamment dans le secteur des jeux vidéo. En effet, les filles sont très souvent moins bien perçues, voire insultées au sein des jeux en réseaux. Pour preuve, les compétitions de jeux vidéo ne sont toujours pas mixtes à l'heure actuelle.
Lorsque l'on interroge les filles d'une classe sur le harcèlement, elles répondent souvent qu'elles sont plus souvent harcelées en ligne que les garçons parce qu'elles sont plus faibles ou vulnérables. Bien souvent, elles ne savent pas pourquoi elles le pensent.

Eléments statistiques :

- Le nombre de jeunes ayant vu des images sexuelles en ligne augmente en âge (de 11 % pour les 9-10 ans à 39% pour les 15-16 ans)
- 19 % des jeunes ont reçu des messages sexuels en ligne provenant d'autres utilisateurs. Les filles sont plus perturbées que les garçons par ce genre de message
- Chez les adultes, 5,3 millions de français se connectent chaque mois sur un site de rencontre (un célibataire sur trois)

Objectifs spécifiques du débat :

- Faire prendre conscience aux filles qu'elles ne sont pas plus faibles ou plus vulnérables que les hommes, et qu'elles ont le choix d'agir
- Faire prendre conscience aux garçons que le sexisme est une discrimination punie par la loi, et que ce comportement ne plait pas aux filles

Exemple de questions pouvant lancer le débat :

- Pourquoi les filles sont-elles plus souvent harcelées que les garçons ?
- Qu'est-ce que le sexisme ? Pourquoi ça a lieu ?
- Est-ce que les filles préfèrent les machos ?

Conseils pouvant être donnés aux enfants :

- Inviter les filles à agir de manière collective dès qu'un harcèlement se produit
- Briser les chaînes de moqueries, harcèlement
- Agir sur Internet comme on agit dans la vie réelle

Pour reprendre le jeu :

La notion de sexisme dans les jeux vidéo peut être abordée en parlant de la gameuse.

VIOLENCE DANS LES MÉDIA

Définition :

Il est difficile de définir ce qu'est la violence tant elle est protéiforme et liée à des facteurs individuels. En effet, ce qui parait violent pour quelqu'un, ne l'est pas forcément pour l'autre. Selon l'OMS[9], la violence est l'utilisation intentionnelle de la force physique, de menaces à l'encontre des autres ou de soi-même, contre un groupe ou une communauté, qui risque fortement d'entraîner un traumatisme, des dommages psychologiques, des problèmes de développement ou un décès.

Contexte :

Les études concernant l'impact de la violence contenue dans les médias sont nombreuses mais présentent des résultats contradictoires et parfois des biais méthodologiques. Ces recherches se sont multipliées ces dernières années, et portent très souvent sur la télévision. Le développement d'Internet a entraîné une massification des visionnages de vidéo pouvant être violentes (violence physique, psychologique, pornographique…) et un accroissement des communications virtuelles (et notamment avec des inconnus) potentiellement violentes psychologiquement.
Les jeux vidéo ont été depuis leur création pointés du doigt concernant la violence contenue. Ils ont été souvent critiqués comme étant la cause possible de tueries de masse. Nous savons aujourd'hui que les jeux vidéo violents, pris isolément, ne sont pas un facteur de passage à l'acte violent. Cependant, il semble que la banalisation de la violence dans les jeux vidéo entraîne une inhibition des comportements de solidarité. En d'autres termes, plus on voit de violence, moins on aide celui qui subit la violence. Certaines études montrent que la violence contenue dans les média favorise le mimétisme et l'agressivité des enfants (actes et propos). D'autres études montrent à l'inverse que la violence contenue dans les jeux vidéo (à l'instar de nombre de jeux d'enfants : bagarres, cowboys et indiens…) permet de réfréner cette violence en agissant comme un exutoire (effet cathartique). Au final, il convient d'être très prudent sur cette question et d'avouer que les études actuelles ne permettent pas de conclusions scientifiques.
La violence psychologique sur Internet est très présente. L'exposition à des contenus inadaptés (pornographie, informations sans filtre, vidéos violentes, contacts avec des adultes malsains…) peut engendrer des phénomènes d'agressivité, d'incompréhension et de peur (cauchemars, terreurs nocturnes, difficultés d'endormissement, repli sur soi…) tant la propulsion dans l'âge adulte peut s'effectuer brusquement. D'autre part, la communication facilitée sur les réseaux sociaux ou les téléphones, sans en avoir acquis les compétences, peut engendrer des propos violents sans forcément que les jeunes aient conscience des conséquences psychologiques provoquées chez le destinataire.

Eléments statistiques :

- 19% des enfants de 11 à 12 ans ont déjà vu une image pornographique en ligne ou hors ligne
- 27% des jeunes de 9 à 17 ans qui ont vu des images sexuelles en ligne disent avoir été dérangés par cela
- A 13 ans et en moyenne, un enfant américain a déjà vu 100 000 actes de violence à la télévision, dont 8000 meurtres.

Objectifs spécifiques du débat :

- Faire comprendre aux jeunes qu'il est important pour se protéger de se conformer aux indications d'âge (télévision, jeux vidéo, vidéos en ligne, pornographie…)
- Expliquer que la notion de violence ressentie n'est pas la même pour tout le monde

Exemple de questions pouvant lancer le débat :

- Avez-vous déjà été confronté à des images violentes sur Internet sans le vouloir ?
- Avez-vous déjà eu peur avant de vous endormir après avoir regardé la télévision ?
- Qu'est-ce que la peur engendre chez vous ?

Conseils pouvant être donnés aux enfants :

- Se limiter aux indications d'âge présentes dans la signalétique jeunesse (télévision) et les normes PEGI (jeux vidéo)
- Inciter les jeunes à parler à un adulte de ce qui les a choqué, le plus vite possible, et ce même s'ils ont fait une bêtise (aller sur un site interdit, accepter un inconnu en ami…). Plus tôt le malaise est exprimé, moins il laissera de traces psychologiques
- Faire attention à leurs jeunes frère et sœur qui peuvent regarder leurs écrans
- Apprendre aux enfants à connaître leur peur et à regarder des programmes adaptés en fonction de celles-ci (certains enfants ont peur de l'eau par exemple, regarder « les dents de la mer » ne résoudra pas leur phobie)

9. Organisation Mondiale de la Santé – « Thèmes de santé – La violence »

Pour reprendre le jeu :

Vous pouvez parler de l'anonymous pour évoquer l'anonymat sur Internet et la difficulté, voire l'impossibilité de connaitre l'identité réelle d'un pseudonyme numérique.

Pour aller plus loin

- P. Lardellier (dir.), Violences médiatiques. Contenus, dispositifs, effets, L'Harmattan, 2003.
- M. Dagnaud, « Médias et violence. L'état du débat », Problèmes politiques et sociaux, n° 886, mars 2003.
- M-C Blandin, violence dans les media : quelles conséquences sur l'enfant et la société ?, Sénat, Rapport d'information n° 264 (2012-2013) fait au nom de la commission de la culture, de l'éducation et de la communication, déposé le 15 janvier 2013

PORNOGRAPHIE

Définition :

La pornographie est la représentation (sous forme d'écrits, de peintures, de spectacles, de photographies, de vidéo…) de pratiques obscènes, sans forcément de préoccupations artistiques, avec l'intention délibérée de provoquer l'excitation sexuelle du public auxquelles elles sont destinées. Le mot pornographie vient de pórnê signifiant « prostituée » et de gráphô, qui signifie « peindre », « écrire » ou « décrire ».

Contexte :

LLes nouvelles technologies ont permis le développement massif du visionnage de pornographie. Avant l'arrivée de ces nouveaux media, elle nécessitait un acte volontaire de la part de celui ou celle qui voulait y avoir accès, ce qui n'est plus le cas aujourd'hui. Avant l'arrivée de la photographie et de la vidéo, la pornographie faisait fonctionner l'imaginaire du spectateur et de l'auteur. Aujourd'hui, il est courant de tomber sur des images crues, forcément réalistes, sur Internet ou à la télévision, en voulant par exemple télécharger un épisode de série ou un film (ce que fait une majorité de jeunes).
L'âge moyen de la première relation sexuelle ne diminue pas en France, ce qui écarte le lien de causalité entre précocité d'accès à la pornographie, et précocité d'accès à la sexualité. Pour autant, la précocité de l'exposition à la pornographie, peut modifier la perception d'un acte sexuel. La pornographie représente souvent la femme comme soumise, pouvant être violentée, et s'adonnant souvent à des pratiques orales, ou annales. Les acteurs et actrices sont plus souvent choisis pour leurs qualités esthétiques que leurs talents d'acteur. Ceci peut amener les jeunes à avoir une vision déformée de la sexualité. Les garçons et les filles peuvent complexer par rapport à leurs corps, ils peuvent intégrer la fellation ou la sodomie, comme des pratiques obligées d'un rapport sexuel ou encore avoir du mal à différencier l'intime du public. C'est le cas notamment avec le développement d'applications photo ou vidéo, telles que snapchat®, qui permettent l'envoi de photos dénudées en faisant croire à son auteur qu'elles seront forcément supprimées.

Eléments statistiques :

- 11% des jeunes de 9 à 10 ans ont déjà vu une image sexuelle en ligne (19 % des 11-12 ans, 27 % des 13 – 14 ans, 40 % des 15 – 16 ans)
- Internet, puis la télévision sont les moyens d'accès à la pornographie les plus utilisés
- 1 % des sites Internet est consacré à la pornographie

Objectifs spécifiques du débat :

- Faire prendre conscience aux jeunes que la pornographie n'est pas la réalité

Exemple de questions pouvant lancer le débat :

Remarque : Impliquer les élèves sur cette thématique est difficile par le tabou qu'elle soulève. Il est particulièrement important d'utiliser l'humour et de ne stigmatiser personne pendant le débat. Il est également important de préciser que les propos jugeants ou moqueurs à destination entre élèves sont interdits.
- Comment sont présentées les femmes dans la pornographie ?
- Les actes montrés dans les films pornographiques sont-ils réels ?
- Pourquoi pensez-vous que les actrices pornographiques pratiquent-elles ce métier ?

Conseils pouvant être donnés aux enfants :

- La pornographie est interdite aux personnes mineures
- La pornographie est avant tout une industrie, destinée à gagner de l'argent. Les actes pornographiques présentés sont souvent différents d'une sexualité de couple classique. La plupart des réalisateurs de films pornographiques sont des hommes, qui font des films à destination d'autres hommes.
- Chacun peut disposer de son corps comme il le souhaite et personne n'est obligé d'effectuer des pratiques sexuelles qui ne lui plaisent pas
- Les actrices tournent dans des vidéo pour gagner de l'argent

Pour reprendre le jeu :

Le maniaque, en dévoilant des photos compromettantes, permet de discuter de l'envoi de photos intimes (sexting) pour reprendre le jeu.

Pour aller plus loin :

Une grande bibliographie est disponible sur Wikipedia : pornographie

JEUX VIDÉO

Définition :

« Un jeu vidéo est un jeu électronique qui implique une interaction humaine avec une interface utilisateur dans le but de générer un retour visuel sur un dispositif vidéo. Le joueur de jeu vidéo dispose de périphériques pour agir sur le jeu et percevoir les conséquences de ses actes sur l'environnement virtuel ».

Sur l'ensemble des différentes définitions des jeux vidéo que l'on peut trouver sur Internet ou dans les bibliothèques, cette définition du site coopératif Wikipédia est sans doute un peu complexe mais a le mérite d'englober l'ensemble de ce nouveau média et de ses évolutions.

Contexte :

Les jeux vidéo se sont démocratisés chez les particuliers au début des années 80 avec l'arrivée des premières consoles de salon et des ordinateurs personnels. Ce média particulier n'a cessé d'évoluer depuis et est aujourd'hui l'une des industries culturelles les plus lucratives avec le cinéma.

Les graphismes, la jouabilité et la diversité des jeux vidéos se développent constamment. On peut aujourd'hui jouer aux jeux vidéo sur tous les écrans disponibles (télévision, smartphones, tablettes, ordinateurs, consoles). Il existe différentes catégories de jeux vidéo (action / aventure, stratégie, simulation, jeux de rôle, sports…). Le développement d'Internet et des réseaux sociaux a modifié l'accessibilité aux jeux vidéo en ligne. Nombre de jeux à l'heure actuelle se jouent en ligne et favorisent un usage important par les mécanismes addictogènes mis en œuvre par les créateurs. Ainsi, la plupart des jeux créés pour les tablettes, les smartphones ou les réseaux sociaux présentent les caractéristiques suivantes :

- Se jouent en ligne (ce qui favorise la compétition entre joueurs)
- N'ont pas de fin
- Offrent des bonus si l'on se connecte régulièrement
- Favorisent la coopération entre joueurs (et donc le besoin de se connecter pour aider son équipe)
- Ne demandent pas de talent particulier (plus on joue, plus on est puissant)
- Se jouent en temps réel (une action sur le jeu nécessite plusieurs heures, voire plusieurs jours avant de s'effectuer ; on gagne des vies toutes les heures…)
- Permettent la création d'un avatar (qui nous ressemble souvent)

Ces caractéristiques addictogènes, inventées au départ dans les Jeux de Rôle Massivement Multijoueurs (MMORPG : comme world of warcraft® par exemple), sont présentes dans les jeux afin de pousser les joueurs à avoir recours à des achats pour augmenter l'avancement dans le jeu. C'est sur ce modèle que repose d'ailleurs l'efficience économique de ces jeux diffusé largement, souvent gratuitement.

L'usage excessif des jeux vidéo s'explique en partie par ces mécanismes. Le nombre d'heures passées à jouer n'est pas l'élément principal du diagnostic. Il est important de regarder si des conséquences négatives dans la vie de la personne se produisent, du fait de l'usage important des jeux (baisse des notes, moins d'amis, arrêt de l'activité de loisir, fatigue importante, agressivité, repli sur soi…). Bien souvent, les écrans sont un symptôme d'une difficulté éprouvée par la personne, et constituent un moyen efficace d'échapper à cette difficulté en s'immergeant dans le virtuel.

Eléments statistiques :

- L'âge moyen du joueur de jeu vidéo en France est de 35 ans, ce qui explique pourquoi le nombre de jeux réservé aux adultes est si important
- Parmi les joueurs de jeux vidéo, 50% sont des femmes
- En une dizaine d'années, les adolescents ont perdu en moyenne une heure de sommeil par nuit (la perte de sommeil est aussi présente chez les adultes dans une moindre mesure). Entre 18 et 24 ans, la durée de sommeil moyenne en semaine est de 5 h 40 par nuit !
- On estime qu'enlever les écrans au moins une heure avant le coucher permet d'augmenter la durée de sommeil de l'enfant et de l'adolescent d'une heure trente par nuit

Objectifs spécifiques du débat :

- Sensibiliser les jeunes aux risques associés à l'utilisation excessive des jeux vidéo : Désocialisation, manque de sommeil, baisse des résultats scolaires
- Développer un regard critique sur ces nouveaux médias : stéréotype sexiste, violence,

Exemple de questions pouvant lancer le débat :

- Qui, parmi vous, joue aux jeux vidéo. Et quels types de jeux préférez-vous ?
- Qu'est-ce qui vous fait aimer un jeu vidéo plus qu'un autre ?
- Quels sont les outils que vous privilégiez pour jouer aux jeux vidéo (consoles, ordi, mobiles) ?

Conseils pouvant être donnés aux enfants :

- Varier les types de jeux vidéo
- Privilégier les activités d'extérieurs lorsque c'est possible
- Faites attention à ce que peuvent voir vos petits frères et sœurs. Ne jouez pas à des jeux violents en leur présence.
- Limiter son temps de jeu. Respecter son besoin de sommeil
- Ne pas commencer plusieurs jeux présentant des caractéristiques addictogènes en même temps

Pour reprendre le jeu :

La gameuse et son marqueur nolife symbolisent la notion d'usage excessif des jeux vidéo. En privant sa victime de son vote, la gameuse représente le risque d'isolement social et l'impact du manque de sommeil sur la vie de tous les jours.
Parano chez les noobs est construit sur le paradoxe de parler de nouvelles technologie en utilisant un jeu basé sur l'utilisation de carte et le dialogue réel entre les joueurs. Vous pouvez souligner cet aspect et rappeler que les jeux de sociétés se développent beaucoup depuis plusieurs années et qu'il y en a pour tous les goûts.

Pour aller plus loin :

- Daniel Ichbiah, La Saga des Jeux Vidéo, Paris, Pix'n Love, 2009 (réimpr. 1997, 1998, 2004), 454 p
- Alain et Frédéric Le Diberder, L'Univers des jeux vidéo, 1998
- Tristan Donovan, Replay. The history of videogame, East Sussex, Yellow Ant, 2011, 501 p.
- S. Tisseron, qui a peur des jeux vidéo, Albin Michel, 2008, 176 p.

PARENTS : PARENTALITÉ ET INTERNET

Définition :

L'un des objectifs de Parano chez les Noobs est d'encourager les jeunes à développer avec leurs parents un dialogue autour de leurs usages des outils numériques. Et donc d'agir de manière indirecte sur le renforcement de la parentalité dans le cadre de l'éducation à l'usage des nouvelles technologies de l'information et de la communication.

La parentalité est un néologisme qui définit la fonction d'être parent dans ses aspects juridique, culturels, éducatifs, institutionnels. Selon la définition de 2004 du Centre de Recherche en Système de Santé de l'école de Santé Publique de Huy-Waremme, la parentalité désigne « l'ensemble des savoir-être et savoir-faire qui se déclinent au fil des situations quotidiennes en paroles, actes, partages, émotions et plaisirs, en reconnaissance de l'enfant, mais également en autorité, exigence, cohérence et continuité éducative ». Les actions de prévention à destination des parents en matière de réduction des risques à l'utilisation des NTIC s'inscrivent dans le renforcement de la parentalité par une forme d'éducation parentale telle que définie par Bernard Terrisse, professeur au Département des Sciences de l'Education à l'Université du Québec de Montréal, c'est-à-dire une actualisation des potentialités éducatives, par le développement du sentiment de compétences des parents et une meilleure utilisation des ressources de leur environnement.

Contexte :

Il est communément admis qu'il existe une fracture numérique générationnelle et culturelle qui constitue un clivage important sur les usages d'internet. Cette fracture est en partie liée à la cohabitation de deux générations dont l'une est née avec Internet et l'autre pas. D'une certaine manière, cette thématique du jeu, particulièrement transversale vise à réduire cette fracture numérique.

Eléments statistiques[10] :

- 90 % des parents effectuent au moins un acte de médiation parentale active des usages d'Internet (plus en direction des filles que des garçons). Cette médiation diminue au fur et à mesure de l'avance en âge de l'enfant (s'asseoir avec son enfant, expliquer ce qui est bien…)
- 98 % des parents effectuent au moins un acte de médiation parentale active concernant la sécurité (expliquer les sites sécurisés, suggestions concernant le comportement…)

- Lorsque l'enfant s'inscrit sur les réseaux sociaux, 98 % des parents restreignent l'accès à certains usages ou interdisent certains propos
- 40 % des parents d'enfants de 13 à 16 ans surveillent ce que font leurs enfants sur Internet (sites visités, propos sur les réseaux…)
- Ces actes de médiation parentale active sont jugés utiles par 50 % des enfants
- Cependant, 50 % des enfants ignorent les conseils de leurs parents

Objectifs spécifiques du débat :

- Inciter les jeunes à renforcer le dialogue sur leurs usages des nouvelles technologies avec leurs parents
- Rappeler le rôle protecteur et régulateur des parents
- Favoriser la diminution de la fracture numérique générationnelle en valorisant le rôle de l'enfant dans sa position d'apprenant potentiel de ses propres parents.

Exemple de questions pouvant lancer le débat :

- Qui, parmi vous, se considère plus expérimenté que ses parents sur Internet ?
- Qui, parmi vous, échange avec ses parents sur ce qu'il fait sur Internet ?
- Qui a déjà joué à des jeux vidéo avec ses parents ?
- Qui a déjà donné des conseils à ses parents sur l'utilisation d'internet, des mobiles ou des ordinateurs

Conseils pouvant être donnés aux enfants :

- Rappeler aux jeunes que les programmes de contrôles parentaux ont pour vocation première de les protéger non de les contrôler.
- Faire réfléchir les jeunes sur l'importance du dialogue en famille sur les questions ayant trait aux nouveaux médias numériques.
- En leur rappelant que leurs parents ne sont pas tous forcément nés avec internet, les placer aussi en situation d'experts capables d'apporter leurs apporter une meilleurs connaissance d'internet et de l'informatique.
- Insister sur le fait qu'en cas de problème sur internet, le premier réflexe des jeunes doit être d'en parler à un adulte en qui ils ont confiance.

10. Etude EU kids online, rapport pour la France, 2012

Pour reprendre le jeu :

L'application contrôle parental permet d'annuler la diffusion de photos compromettantes sur Internet par le maniaque. Si cette application a déjà été jouée, vous pouvez appuyer votre propos en revenant sur la situation de jeu qui a amené son utilisation. Sinon, vous pouvez rappeler aux joueurs à quel moment de la partie cette carte peut être utilisée.
L'animateur peut également inciter les joueurs à raconter leur partie le soir à leurs parents et ainsi d'amener un premier échange autour des nouvelles technologies et de leurs usages.

Pour aller plus loin :

- Etude EU kids online, rapport pour la France, médiation parentale
- S. Tisseron, du livre et des écrans, 2013, Manucius
- S. Tisseron, 3 – 6 – 9 – 12, apprivoiser les écrans et grandir, Erès, 2013,

TÉLÉPHONE / SMARTPHONE

Définition :

Un smartphone, ordiphone ou téléphone intelligent, est un téléphone mobile évolué disposant des fonctions d'un assistant numérique personnel, d'un appareil photo numérique et d'un ordinateur portable. La saisie des données se fait le plus souvent par le biais d'un écran tactile ou, plus rarement d'un clavier ou d'un stylet. Selon le principe d'un ordinateur, il peut exécuter divers logiciels/applications grâce à un système d'exploitation spécialement conçu pour mobiles, et donc en particulier fournir des fonctionnalités en plus de celles des téléphones mobiles classiques.

Il est possible de personnaliser son smartphone en y installant des applications additionnelles tel que des jeux ou des utilitaires via un magasin d'applications en ligne différent pour chaque système d'exploitation comme Google Play sur Android ou encore l'App Store sur iOS. Les smartphones ont besoin d'une connexion internet haut débit par l'intermédiaire d'un réseau de téléphonie mobile pour pouvoir utiliser le maximum de leur potentiel.

Contexte :

À partir de fin 2007 et du lancement de l'iPhone, le marché des smartphones s'étend considérablement jusqu'à dépasser en quelques années celui des téléphones mobiles « classiques ».

Eléments statistiques :

Sur l'année 2014, en France, il a été vendu plus de 18 millions de smartphones (soit plus de 15% par rapport à 2013). En fait, plus de trois mobiles vendus sur quatre sont désormais des mobiles « intelligents » et 30 millions de français disposent de téléphone connectés. Au niveau international, on constate que ce gigantesque marché est aux mains de trois multinationales qui cumulent 92,5% des ventes de systèmes d'exploitation pour mobiles, Microsoft, Google, Apple. Pour ce qui est de la vente des smartphones, trois marques se partagent les deux tiers du marché français.

De 11 à 14 ans, les jeunes s'équipent rapidement en mobiles : on passe ainsi de 30% à 80% de taux d'équipement en seulement 3 ans. A 15 ans, le taux de possession dépasse même celui de l'ensemble de la population française avec 92% des jeunes équipés, contre 82% chez les 25 ans et plus. Bref, les jeunes

et les mobiles en matière d'équipement, c'est une vraie rencontre !! A noter que les MVNO (Mobile Virtual Network Opérateur) comme Virgin mobile, Breizh mobile (si, si, ça existe !!), NRJ mobile… et les forfaits bloqués sont plus important chez les 11-14 ans.
Les jeunes vont utiliser principalement leurs smartphones pour envoyer des SMS et des MMS, pour jouer et consulter leurs profils sur les différents réseaux sociaux.

Objectifs spécifiques du débat :

- rappeler qu'un téléphone connecté est comme un ordinateur ou une tablette un appareil vulnérable au virus et piratage et qu'il nécessite comme tout outil numérique la mise en place de protection et de règles de conduites spécifiques à son utilisation

Exemple de questions pouvant lancer le débat :

- Qui, parmi, vous dispose d'un téléphone connecté à Internet ?
- Quels sont, selon vous, les risques associés à l'utilisation des téléphones portables connectés ?
- Combien de SMS pensez-vous envoyer par jour ?

Conseils pouvant être donnés aux enfants :

- Un téléphone connecté est aussi vulnérable aux virus et aux piratages qu'un ordinateur, il faut donc impérativement installer un anti-virus.
- Le mode Bluetooth facilite le piratage : penser à le désactiver après utilisation.
- Préserver son intimité et sa liberté, désactiver les options de géolocalisation
- Par précaution, se protéger des ondes :
- En évitant de dormir, avec le mobile près de sa tête. Si l'on utilise son smartphone comme réveil, vérifier si on peut l'éteindre tout en faisant fonctionner le réveil (la plupart disposent de cette fonctionnalité)
- Les ondes pourraient agir sur la fertilité, éviter donc de porter son téléphone dans la poche du pantalon !
- Privilégier l'utilisation du kit « mains-libres » pour appeler
- Ne pas répondre aux SMS dont on ne connait pas l'expéditeur, et ne pas télécharger les pièces jointes qui peuvent y être associées (risques de virus).
- Faire attention lorsque l'on télécharge une application (jeux en particulier) que celle-ci est bien gratuite.

Pour reprendre le jeu :

Aucune carte ne s'appuie précisément sur un outil. Les risques symbolisés par les geeks s'appliquent tout aussi bien aux tablettes, qu'aux ordinateurs et qu'aux mobiles. Ce que l'on constate, c'est que les jeunes sous-estiment les risques d'infection par des virus et de piratage des smartphones. Rappelez que les photos compromettantes, la publicité et les tentatives d'arnaques passent aussi par le biais des smartphones.

RÉSEAUX SOCIAUX EN LIGNE

Définition :

Initialement, un réseau social désigne un ensemble d'individus reliés entre eux par des interactions régulières. Le terme apparaît dès 1954 dans les écrits du sociologue John Arundel Barnes.
Dans « paranos chez les noobs », nous évoquons les réseaux sociaux numériques qui sont apparus avec l'évolution technologique et technique du web 2.0 comme un élément incontournable lorsqu'il s'agit d'évoquer les usages d'Internet.

Contexte[11] :

Le réseautage social existe depuis que les hommes sont constitués en société. Des groupes sociaux, organisés autour d'un thème fédérateur (religion, classe sociale, études, etc.), forment un type de réseautage informel : recommandation à un tiers, réunions organisées, etc. Le réseautage social peut prendre une forme plus organisée et institutionnelle, professionnelle ou «de loisir», payante ou gratuite. Ainsi les agences de rencontres offrent des services de réseautage social à caractère personnel tandis que les agences de chasseurs de têtes offrent des services de réseautage à caractère professionnel. Avec l'apparition d'Internet, le réseautage social a pris une nouvelle ampleur et ses formes et possibilités se sont multipliées.
Le premier site web de réseautage social fut Classmates.com, qui débuta ses activités en 1995. De nombreux autres réseaux sociaux lui ont emboité le pas, généralistes (facebook, twitter…) ou spécialisés (myspace, linkedin…). Un réseau social est orienté vers le web 2.0, c'est-à-dire qu'il permet à ses visiteurs d'être des participants actifs du réseau, et non plus de simples visiteurs de pages statiques.

11. Source : Wikipedia, réseautage social

Dans ces communautés, un premier ensemble de fondateurs envoie des messages invitant des membres de leur propre réseau personnel à joindre l'emplacement. Les nouveaux membres répètent le processus, accroissant le nombre de membres et de liens dans le réseau. Les emplacements offrent alors des dispositifs tels que les mises à jour automatiques de carnet d'adresses, la visualisation de profils personnels, la possibilité de former de nouveaux liens par des services d'introduction, et d'autres formes de raccordements sociaux en ligne.

La plupart des réseaux sociaux sur Internet sont publics, permettant à n'importe qui de s'y joindre. Les organismes, tels que de grandes entreprises, ont également accès à des programmes de réseautage sociaux privés, connus sous le nom de Enterprise Relationship Management

La constitution d'un réseau social peut être mise en relation avec la Pyramide des besoins de Maslow. Le regroupement d'un ensemble d'entités sociales est une résultante de besoins exprimés par l'individu lui-même. Ainsi, il est possible de mettre en évidence trois des besoins fondamentaux3 :

- L'accomplissement Personnel par l'expression de soi. Chaque utilisateur s'exprime sur sa fiche utilisateur, son profil, et l'enrichit de contenu. Il communique des informations personnelles qui permettent aux autres utilisateurs de le reconnaître, ou de le découvrir.
- La socialisation en éprouvant un besoin relationnel. Les utilisateurs peuvent entrer en relation entre eux directement ou par l'intermédiaire d'une connaissance commune; Cette relation est généralement matérialisée par une liste d'amis ou de contacts, publique ou privée. L'utilisateur peut aussi entrer en relation avec des marques, des artistes, des lieux, etc.
- L'estime des autres par l'intermédiaire du besoin de communiquer. L'utilisateur a à sa disposition une large variété d'outils pour communiquer (messagerie instantanée, dédicace/livre d'or sur le profil d'un contact, partage de contenus, forums). La communication peut-être enrichie selon les sites (invitation à des événements, partage d'agenda, etc.)

Ce monde virtuel permet donc nombres d'interactions entre internautes, constituant ainsi le réseautage social. La plupart des « amis » sur un réseau social sont des personnes présentes dans le cercle immédiat de l'utilisateur (environ 10% des contacts sont inconnus dans la vie réelle à 16 ans).

Eléments statistiques :

- 13 % des 9 -10 ans, 37% des 11 – 12 ans, 76 % des 13 – 14 ans et 90 % des 15 – 16 ans ont une activité sur au moins un réseau social
- Selon les dernières études européennes, 50% des jeunes publient sur Facebook des données privées visibles par tous sans vraiment s'en rendre compte
- Plus de 20% des enfants ont un profil complètement public (sans aucun paramétrage de confidentialité)

Objectifs spécifiques du débat :

Favoriser l'appropriation par les jeunes d'un usage responsable des réseaux sociaux, pour eux même et pour les autres.

Exemple de questions pouvant lancer le débat :

- Qui parmi vous dispose d'un compte Facebook ?
- Quels autres types de réseaux sociaux utilisez-vous et pourquoi ?
- Pourquoi selon vous le propriétaire de Facebook est particulièrement riche alors que ce réseau social est gratuit ?
- Selon vous, existe-t-il des risques à l'utilisation des réseaux sociaux ? Si oui lesquels ?

Conseils pouvant être donnés aux enfants :

- Vérifier régulièrement vos paramètres de confidentialité sur Facebook
  - Pas d'informations personnelles : Adresse, téléphone, Adresse mail personnelle…
  - Pas de photos compromettantes : Pour juger qu'une photo est compromettante, il suffit de l'imaginer vue par quelqu'un que l'on ne connait pas
  - Pas de message insultant, méprisant, haineux et pas de rumeurs

Pas de réseaux sociaux avant 13 ans, l'enfant n'étant pas prêt auparavant à différencier véritablement l'intime du public.

Pour reprendre le jeu :

Le moqueur illustre bien les potentialités offertes par les réseaux sociaux pour lancer des rumeurs sur les autres, de façon anonyme et gratuitement.

Pour aller plus loin :

- Romain Rissoan (2012), Les réseaux sociaux : Facebook, Twitter, LinkedIn, Viadeo - Comprendre et maîtriser ces nouveaux outils de communication, Eni, 2011
- Edelihan & Woodi (2011), L'avatar de l'homme sage, petit traité sur le réseau social numérique

Les applis ne peuvent être utilisées qu'une seule fois.

Le fake : Cette carte ne sert à rien du tout, si ce n'est qu'elle vous permet de faire croire aux autres que vous avez un pouvoir extrêment puissant. Enfin elle ne sert à rien quoi… *Appli à effet permanent (tant qu'on la possède).*

Brigade numérique : Le joueur qui détient cette carte a une voix qui compte double en cas d'égalité pendant un vote. *Appli à effet permanent.*

Contrôle parental : Annule l'effet chapeau sur le joueur voulu pendant toute la partie.
À utiliser en phase de connexion. *Appli à effet unique.*

Justice : Il permet d'enlever le marqueur « rumeur » de son choix. *À utiliser en phase de connexion.*

Usurpation d'identité : Lors de sa déconnexion définitive, le joueur possédant cette carte peut échanger sa carte personnage avec celle d'un autre joueur. *À utiliser une fois déconnecté définitivement.*

Hoax : Cette carte annule l'effet de la carte d'ursupation d'identité.
Elle ne peut s'appliquer qu'à soi même. *À utiliser juste après l'utilisation usurpation d'identité.*

Cheat code : le joueur qui a cette carte peut regarder les cartes d'un joueur.
À utiliser en phase de déconnexion en levant sa carte.

Modérateur : Cette carte permet d'annuler la capacité du gourou sur soi même. Le joueur désigné par le gourou et utilisant cette carte peut donc tout de même voter. *À utiliser en phase de connexion, uniquement sur soi-même.*

PEGI : Cette carte permet de réveiller le joueur endormi par la gameuse pendant un tour.
À utiliser en phase de connexion.

Bug : Cette carte entraine une perte de données (les joueurs rendent leurs cartes appli non utilisées au meneur). Une appli est distribuée à chaque joueur connecté. *À utiliser en phase de connexion.*

Voyeur : Pendant un tour, le joueur peut espionner secrètement pendant que les autres ont les yeux fermés, à ses risques et périls s'il se fait remarquer. *À utiliser en début de phase de déconnexion en levant sa carte.*

Signalement : En jouant cette carte, aucun geek ne peut agir pendant le tour suivant. Ils ne déconnectent personne, et ne peuvent pas utiliser leur capacité. *À utiliser en début de phase de déconnexion en levant sa carte.*

Liste des rumeurs utilisées par le moqueur

Voici une liste de rumeurs parmi lesquelles le moqueur peut choisir quand il désigne une de ses victimes. Quand le meneur appelle le moqueur, il projette une des cinq listes sur l'écran. Le moqueur, après avoir désigné sa victime choisit la rumeur en indiquant le chiffre avec ses doigts.

Le joueur désigné :

1
1. collectionne les rouleaux de papier toilette (vides)
2. a enlevé les petites roues de son vélo il y a deux mois
3. est toujours actif et a sa carte de membre du fan club de Dora l'exploratrice
4. mange les pistaches sans enlever la coque
5. mange ses crottes de nez

2
1. a pleuré quand il s'est coupé la main avec du papier
2. pense qu'une boite de nuit est une petite boite qu'on ouvre seulement la nuit
3. pense que les pokemon existent vraiment
4. est fan des nains de jardins et en possède 150
5. aime manger des tartines de paté – confiture

3
1. a un poster de T'choupi dans sa chambre
2. enfile son tutu dès qu'il rentre chez lui après l'école
3. ne loupe pas un épisode de la petite maison dans la prairie
4. écoute Justin Bieber
5. a une peur panique des télétubbies

4
1. est inscrit à un club de pâte à sel
2. son pseudo internet est bisoubisou56
3. pense que François Hollande vit aux Pays-Bas
4. croît encore au Père Noel
5. pense que Shakespeare est un jeu d'échecs en ligne

5
1. dort sous une couette imprimée avec des petits poney
2. dit encore « pestacle » au lieu de « spectacle », mais sans faire exprès
3. n'a pas compris le scénario du film « titanic »
4. pense qu'un cerveau est le petit du cerf
5. a pleuré devant Bambi la semaine dernière

Phases de jeu (adapter en fonction des cartes choisies et des éliminations de joueurs)

Phase 1 «VOUS ÊTES DÉCONNECTES ET FERMEZ TOUS LES YEUX»

1. Le meneur appelle l'**anonymous** qui ouvre les yeux et désigne un joueur du doigt. Le meneur montre la carte personnage de ce joueur à l'anonymous (et bouge les autres cartes des joueurs pour brouiller les pistes).
2. Le meneur demande au **moqueur** d'ouvrir les yeux et de désigner sa victime. Le meneur pose le marqueur correspondant devant la victime et fait choisir une rumeur au moqueur pour sa victime (voir liste des moqueries, page 11)
3. Le meneur demande l'**un après l'autre** à la **gameuse**, au **gourou** et à la **hackeuse** d'ouvrir les yeux. Il demande si ces personnages souhaitent utiliser leur pouvoir. Si oui, il exécute les pouvoirs des personnages (et pose les marqueurs correspondant).
4. Le meneur demande au **maniaque** d'ouvrir les yeux. Le maniaque choisit le joueur qui portera le chapeau pendant le tour suivant, puis referme les yeux. Le meneur place le chapeau sur la tête du noob désigné par le maniaque.
5. Le meneur demande à **tous les geeks** d'ouvrir les yeux. Ils se reconnaissent. Les geeks, dans le silence, choisissent ensemble le noob à déconnecter. Les geeks ferment les yeux.

Phase 2 «VOUS ÊTES CONNECTÉS ET OUVREZ TOUS LES YEUX»

6. **Tous les joueurs ouvrent les yeux**. Certains noobs découvrent les marqueurs placés devant eux. Le meneur de jeu projette sur l'écran le nom de la victime. La victime choisit un thème de prévention à aborder parmi ceux proposés (cf.livret pédago-geek). L'animateur projette la diapositive de prévention sur l'usage excessif et à risque des NTIC et lance le débat. Le joueur déconnecté tente de répondre à la question, avant de devoir se taire pour le reste de la partie, en continuant d'observer tout le monde. Fin du débat de prévention, le jeu reprend.
7. **Les joueurs sont invités à se prononcer** sur ce qui s'est passé pendant la nuit. **Le meneur de jeu incite chacun à parler** et à accuser d'autres joueurs, qui doivent se défendre. Après débat, le meneur demande **après un décompte jusqu'à trois de pointer leur doigt vers un autre joueur afin de le déconnecter**. Le joueur désigné à la majorité est déconnecté. En cas d'égalité, le vote du joueur qui a la carte brigade numérique compte double.
8. Les joueurs peuvent **utiliser une application** (ou juste après la déconnexion pour certaines cartes).
9. Le jeu se poursuit à partir de la phase 1.

Personnages

Les Geeks :

À chaque déconnexion, ils déconnectent un noob. Pendant la phase de connexion, le geek doit faire croire aux autres qu'il n'est qu'un simple noob.

La hackeuse : *Elle peut pirater l'ordinateur d'un personnage et connaitre son adresse IP.*
Une fois par partie, la hackeuse peut regarder les cartes appli et personnage d'un joueur.

Le maniaque : *Il adore dévoiler des photos compromettantes.*
Il peut mettre un chapeau sur la tête d'un autre personnage. À chaque déconnexion, il doit mettre le chapeau sur la tête d'un autre personnage. Cette capacité peut être contrée par la carte «contrôle parental».

La gameuse : *Elle joue toute la journée à World of Papierkraft.*
Elle dispose du marqueur « no life » qu'elle peut poser devant un joueur une fois par partie. Le noob ainsi désigné ne peut se connecter qu'une fois sur deux (il est trop fatigué et dort un jour sur deux). Le marqueur « no life » peut être enlevé par la carte « PEGI ».

Le moqueur : *« La rumeur est la fumée du bruit ».*
Il peut déposer un jeton rumeur devant un joueur à chaque fin de session et choisir une rumeur parmi la liste proposée en donnant le nombre avec ses doigts. S'il place une rumeur devant chaque joueur connecté (dont lui-même), il gagne la partie. Une rumeur peut être contrée par la carte « justice ».

Le gourou : *Le gourou aime manipuler sur Internet les âmes les plus faibles pour en faire ses fidèles serviteurs.* Une fois par partie, le gourou choisit un personnage qui sera manipulé pendant un tour. Le meneur pose alors le marqueur « n'écoute que ma voix » devant le joueur choisi. Au vote suivant, le vote de ce joueur manipulé se retournera contre lui-même.

Les noobs :

Les noobs n'ont aucun pouvoir particulier (en dehors des applis, et excepté l'anonymous).
À chaque connexion, ils votent pour déconnecter un joueur, en espérant que ce soit un geek.

L'anonymous : *Il a la capacité de s'introduire dans n'importe quel système informatique.*
Il peut regarder secrètement la carte personnage d'un joueur à chaque tour.

Animation du jeu

Le jeu est obligatoirement animé par un meneur de jeu.

Le meneur incarne Ursule de Saint Bidouille. En effet, en tant que propriétaire de l'Auberge de la Fesse de Bouc, c'est lui qui gère les connexions internet.

Préparation :

Désignation du joueur qui possèdera la carte « brigade numérique » :
Le meneur de jeu pose une question ou une devinette (exemple : « le premier qui devine ce que je dessine en ce moment au tableau », ou « Si Mario Bros mange un champignon magique par niveau, à partir de combien de niveaux peut-on dire qu'il est toxicomane ? » ou encore pour les élèves en informatique « dans quel protocole RFC est décrit le Webdav ? »). Le premier joueur qui répond correctement gagne cette carte. La carte brigade numérique sera ensuite donnée à un autre joueur :

- Par le joueur éliminé s'il répond correctement à une question posée pendant les débats de prévention (voir livret pédago-geek). Le joueur éliminé choisit alors le joueur qui aura la carte.
- Par le joueur éliminé qui la possédait et qui la donnera au joueur de son choix (si le joueur est éliminé et qu'il n'y a pas de débat à suivre).

Préparation des joueurs :
- Leur demander de préparer un papier avec leur prénom visible par vous.
- Leur demander d'enlever tout ce qu'il y a sur la table, excepté leur prénom.
- Leur demander d'enlever bracelets, manteaux, s'ils sont susceptibles de faire du bruit quand ils pointent du doigt.
- Leur demander d'éteindre leur téléphone portable.
- Leur rappeler que ce n'est qu'un jeu.
- Leur rappeler que la triche, « c'est super trop nul » (et surtout que ça gâche le plaisir des autres joueurs). Chaque joueur pris à tricher est automatiquement éliminé du jeu par le meneur du jeu (et ira sans doute en enfer).

Préparation des cartes

Conseils de répartition :

Nombre de joueurs	Nombre de Noobs	Anonymous	Maniac	Gourou	Hackeuse	Gameuse	Moqueur
8	5	▪	▪	▪			
9	6	▪	▪	▪			
10	6	▪	▪	▪	▪		
11	7	▪	▪	▪	▪		
12	8	▪	▪	▪	▪		
13	8	▪	▪	▪	▪	▪	
14	9	▪	▪	▪	▪	▪	
15	9	▪	▪	▪	▪	▪	▪
16	10	▪	▪	▪	▪	▪	▪

Il est possible de mettre plus ou moins de geeks, ces chiffres ne sont qu'indicatifs. Vous pouvez bien sur décider de jouer avec tel ou tel geek. Maniaque, gourou et hackeuse ont l'avantage de ne pas être trop compliqués à gérer.

Distribution des cartes :

Après s'être vu explicité les règles par le meneur de jeu (présentation du powerpoint spécifique), chaque joueur reçoit une carte personnage (et éventuellement une carte appli). Le meneur lit la page d'introduction et lance le jeu en lisant le passage suivant :

> Il est neuf heures du matin à Ardouère. Ursule Saint Bidouille ouvre les portes de la cyber-auberge. Tout le monde se presse pour y passer la journée. Vous êtes connectés et regardez votre/vos carte(s). Vous passez la journée sur Internet et en profitez pour envoyer des mails, effectuer des recherches, jouer, chatter…
> Il est 19h00 à Ardouère. Ursule sainte Bidouille ferme les portes de la cyber-auberge.
> Cependant, parmi vous, certains ont trouvé le moyen de prolonger leur connexion pour s'adonner à de sombres activités sur Internet.

“Ça y est !! On est connecté !! ” s’écria Ursule Saint Bidouille, tenancier de l’Auberge de la Fesse de Bouc, seul et unique lieu de rencontre de la Commune d’Ardouère, alors qu’il s’élançait dans la rue principale du bourg après avoir passé quarante huit heures sans dormir, perdu dans les fils et les codes de ses antiques ordinateurs.

Les quelques habitants alors présents évoquent encore avec émotion l’irruption d’Ursule, les traits tirés, son unique et dernière mèche de cheveux habituellement plaquée sur son crâne luisant pointant fièrement vers le ciel comme un point d’exclamation capillaire !

Ils lui répondirent par une ovation générale !! Ardouère était connecté !! Enfin, il pouvait rivaliser avec le village voisin de Sophtouère qui bénéficiait déjà d’une connexion au débit (de boissons) local.

L’ensemble des habitants se pressait déjà aux portes de l’auberge, chacun évoquant avec une excitation non dissimulée, ses envies pour sa première connexion sur Internet. Ardouère pouvait enfin entrer de plain-pied dans ce XXIe siècle numérique aux promesses de découvertes illimitées.

Ursule Saint Bidouille avait fait l’acquisition de plusieurs ordinateurs (et téléphones portables connectés au réseau 3Grammes) afin de transformer son auberge désuète mais néanmoins coquète, en un pôle technologique sans précédent dans l’histoire de la Commune. Il était sûr qu’une telle initiative lui rapporterait de l’argent et la notoriété nécessaire pour briguer le poste de Maire du village.

Hélas, il allait très vite découvrir que le monde numérique n’était pas uniquement pavé de bonnes intentions et que certains geeks devenaient vite mal attentionnés lorsqu’ils étaient connectés. Seuls les noobs pourront débusquer ces empêcheurs de surfer en rond afin que l’établissement conserve sa réputation sans faille.

But du jeu

La carte personnage qui sera distribuée à chaque joueur définira s’il est un noob, ou un geek.

- Les **Noobs** doivent déconnecter les **geeks.**
- Les **Geeks** doivent déconnecter les noobs, et ne pas se faire remarquer.

Phases de jeu :

1. Connexion : Tous les joueurs ont **les yeux ouverts**, débattent et votent pour éliminer un Geek présumé (ils le déconnectent).

2. Déconnexion : Tous les joueurs ont **les yeux fermés**.

3. Pendant la phase de déconnexion, **Les Geeks ouvrent les yeux**, utilisent leur pouvoir et votent pour éliminer un Noob.

4. Eventuellement **Prévention** : Le meneur de jeu anime un débat sur un thème en lien avec les risques numériques (à partir d’une diapositive de prévention fournie avec le jeu). Le débat de prévention a lieu en début de phase de connexion. Le joueur éliminé par les geeks choisit le thème qu’il souhaite parmi ceux proposés (voir liste des thèmes de prévention) et doit répondre à une question de la diapositive.

5. Fin du jeu : Chaque joueur déconnecté par les autres joueurs est éliminé définitivement du jeu. Il garde toujours les yeux ouverts mais n’a plus le droit de parler. Le jeu se termine lorsqu’il ne reste plus qu’un ou plusieurs Geeks (et tous les Geeks gagnent) ou plus qu’un ou plusieurs Noobs (et tous les Noobs gagnent).

Cas particuliers :

- Si au dernier tour de connexion, il ne reste qu’un Noob et qu’un Geek, c’est le Geek qui l’emporte (c’est injuste mais c’est comme ça).
- Si le moqueur (voir liste des personnages, page 9) a déposé un marqueur « rumeur » devant tous les joueurs encore connectés (dont lui-même), il gagne la partie tout seul.

Auteurs :
Laurent POMMEREUIL et Guillaume JEGOUSSE

Graphisme et illustrations :
Rémi Pommereuil - SIREN : 798 064 937
en partenariat avec les étudiants du lycée des métiers d'Art Bertrand Duguesclin (Brech)

Fabrication :

SOMMAIRE

5 **But du jeu**
Phases de jeu
Cas particuliers

6 **Animation du jeu**
Préparation

7 **Préparation des cartes**
Conseils de répartition
Distribution des cartes

8 **Phases de jeu**
Phase 1
Phase 2

9 **Personnages**
Les Geeks
Les noobs

10 **Les applis**

11 **Liste des rumeurs utilisées par le moqueur**

PARANO CHEZ LES NOOBS

LE JEU PÉDAGO-GEEK ET STRATÉ-GEEK DE PRÉVENTION DES USAGES À RISQUES DES NOUVELLES TECHNOLOGIES NUMÉRIQUES

LIVRET DE RÈGLES

Douar Nevez
Centre de Soins, d'Accompagnement et de Prévention en Addictologie

Prévention 2.0

Région Bretagne

ars Agence Régionale de Santé Bretagne

Avec le soutien de la Région Bretagne et de l'Agence Régionale de Santé de Bretagne