Épisode 13 – « Spam Attack»

Ta boîte aux lettres est privée mais des intrus peuvent y glisser.

Préambule

Les spams, quelle plaie ! Ces messages électroniques non sollicités envoyés en masse à de nombreux contacts, en général à des fins commerciales, peuvent avoir différentes causes. Autrefois apanage des services de messagerie, les spams sont désormais également très répandus sous forme de textos qui viennent polluer les téléphones portables.

Parfois, ils proviennent de bases de données qui ont été collectées légalement, avec l'accord inattentif des personnes, par des sociétés peu scrupuleuses qui les ont revendues ou louées (légalement ou pas). Dans d'autres cas, ils résultent de l'introduction de programmes malveillants, qui volent le carnet d'adresses d'utilisateurs.

Souvent, il suffit d'un formulaire rempli imprudemment pour que votre boite aux lettres devienne la cible de messages publicitaires ou problématiques (contenus choquants, escroqueries, lettres en chaîne, etc.) Gare à qui mord à l'hameçon !

Protection de ses données ou de son ordinateur, dans les deux cas pour éviter les soucis, il faut en connaître les causes. Etre un internaute responsable mais aussi curieux, créatif n'est pas inné, cela s'apprend… Posséder certains savoir-faire ne dispense pas de tout savoir, de toute prudence ou de tout savoir-vivre. Internet n'échappe pas à la règle.

.

Objectifs généraux

- Savoir se protéger des contenus indésirables non sollicités
- Apprendre à protéger ses données personnelles
- Développer son esprit critique

Objectifs spécifiques

- Agir avec prudence (ne pas répondre aux messages non sollicités)
- Signaler les spams
- Naviguer en protégeant ses données personnelles
- Mettre en place des logiciels anti-spams

Domaines du B2i abordés

- Domaine 2 : adopter une attitude responsable
- Domaine 5 : communiquer, échanger

Thèmes abordés

- Spams, messages indésirables
- Techniques de phishing
- Logiciels de protection (anti-virus, pare-feu, anti-spyware, filtre anti-spam)

Ressource utilisée

- Épisode Vinz et Lou sur Internet « Spam attacks » (2 minutes)

Versions disponibles

- Versions accessibles : langue des signes française (LSF), langage français parlé complété (LPC), sous-titrage, audio-description
- Version anglaise

Durée de l'atelier

- Entre 30 minutes et 1 heure

Modalité

- Atelier en mode collectif

Matériel nécessaire

- Un ordinateur connecté
- Un vidéoprojecteur ou TNI

DÉROULEMENT DE L'ATELIER

1 Faire émerger les représentations / la parole

Avant de lancer l'atelier, rappeler les règles de prise de parole :

- **On écoute** les autres, tout le monde doit pouvoir prendre la parole.
- **On respecte** les limites de la liberté d'expression : pas de propos injurieux, pas de moqueries. Chacun a le droit de formuler ses impressions, ses pensées, ses ressentis et ses questions en étant respecté.
- **On s'engage à ne pas répéter** les propos échangés pendant l'atelier, en particulier ceux qui auraient trait à la vie privée.

Exemples de questions, partir des représentations et connaissances des enfants :

- Connaissez-vous toujours les auteurs des mails que vous recevez ?
- Faut-il se méfier lorsqu'on ne connait pas l'auteur d'un message ? Ou lorsque les messages sont rédigés dans une langue étrangère ?
- Y-a-t-il des contenus dont il faut se méfier ?
- Qu'appelle-t-on un spam ?
- Quelle est la bonne attitude à adopter quand on en reçoit ?

Quelques conseils

- Ces questions, non-exhaustives, ont pour objectif de **faire émerger les représentations** des enfants. Les inviter à **s'exprimer spontanément** permet de faire un premier état des lieux de leurs idées et ressentis.
- Pour comparer et voir l'évolution des représentations des enfants au cours de l'atelier, **noter quelques-unes de leurs réponses** au tableau afin de pouvoir les réutiliser en fin d'atelier et permettre un retour réflexif.

2 Projeter le dessin animé et analyser le scénario

- Projeter au groupe le dessin animé une première fois pour un visionnage collectif.
- Décrypter ensemble le scénario du dessin animé à l'aide du tableau ci-dessous.

Quelques conseils

- Après un **premier visionnage** et des questions succinctes sur la **compréhension globale** de l'épisode (« Que se passe-t-il ? Qui sont les personnages ? Que font-ils ? »), un **second visionnage** peut être fait avant l'étape plus précise de **décryptage** afin de développer une **meilleure perception des détails et des étapes** de l'épisode, mais aussi d'éclairer d'éventuelles **incompréhensions**.
- Faire le **lien entre le scénario et le vécu des enfants** permet de déclencher la parole et de confronter ces situations avec leur quotidien : « Et toi, est-ce que tu as déjà entendu des histoires comme ça ? », « Qu'as-tu ressenti ? », « Qu'aurais-tu aimé faire à la place de tel ou tel personnage ? ».

Dans les coulisses du scénario

Problématiques abordées	Éléments du scénario	Questions associées	Analyse
Spam, courrier indésirable	Vinz reçoit un message d'un inconnu, en anglais, lui vantant une pilule « miracle » pour développer ses muscles et sa pilosité. Il s'empresse d'y répondre, pour en savoir plus.	Vinz connaît-il l'auteur du message? Comment celui-ci connaît-il l'adresse de Vinz ?	Les spams sont des courriers indésirables, d'auteurs inconnus, envoyés massivement à de nombreuses personnes. Les adresses mails des destinataires ont été obtenues de façon déloyale (contrairement aux messages publicitaires). Souvent les spams sont écrits en anglais ou dans un mauvais français, ce qui explique que Vinz ait tant de mal comprendre le message.
Escroquerie, technique de phishing	Après ce premier message, Vinz n'arrête pas de recevoir de nouveaux messages, toujours en anglais, vantant différentes pilules, ou autres procédés pour augmenter son QI, bronzer sans soleil, etc. Bob, le met en garde. Ce sont des spams ; maintenant que Vinz a confirmé son adresse en répondant à l'un des messages, sa boite aux lettres risque en être saturée.…	Que cherchent à faire les auteurs de ces spams ? Pourquoi entrent-ils en contact avec Vinz ?	Souvent, comme ceux-ci, les spams cherchent à vendre quelque chose : des médicaments, des produits financiers, des services olé olé, des logiciels piratés. Des spams d'escrocs peuvent aussi promettre un enrichissement rapide ou jouer sur votre corde sensible pour vous faire donner de l'argent La technique que l'on appelle phishing (hameçonnage), consiste à se faire passer pour quelqu'un d'autre, une banque par exemple et à demander de saisir ses codes confidentiels. Enfin certains spams sont utilisés pour diffuser des virus ou faire de la propagande.
Filtre anti-spams, anti-virus	C'est au tour de Lou de recevoir un spam, l'invitant à se marier avec un poilonours ! Cette fois, Vinz est averti. Il la prévient du danger.	Quels sont les messages qui doivent nous alerter ? Les spams peuvent-ils provenir d'un ami ? Comment faire quand sa boite aux lettres est saturée de spams ?	Attention à ne pas confondre messages publicitaires, newsletters que vous avez consenti à recevoir et spams. C'est le contenu, peu probable, alléchant, agressif d'un message qui peut vous alerter. Le fait qu'un message provienne d'un ami n'est pas une garantie, sa boite mail a pu être piratée et des spams envoyés à son nom à tous ses contacts à son insu. Si votre boite aux lettres est

			saturée de spams, un logiciel de filtrage anti-spam qui triera automatiquement votre courrier est une solution. Avec un bon anti-virus, pour éviter d'autres désagréments !

3 Proposition d'activité

Repasser le dessin animé après ce travail de décryptage. Les enfants pourront ainsi avoir le plaisir de regarder l'épisode sous un nouveau jour. Puis, proposer-leur cette activité :

Objectifs

- Aborder **les techniques de spam** et d'escroquerie sur Internet
- Amener les enfants à **faire preuve de discernement**
- Apprendre à **se protéger efficacement**

Déroulé de l'activité

- Proposer la lecture de différents spams et analyser ce qui les différencie de messages publicitaires émanant d'enseignes ayant pignon sur rue.
- Insister sur le fait qu'il est toujours possible de se désabonner d'une newsletter (la loi oblige à ce que la procédure de désabonnement soit visible sur le message).
- Lors de petits jeux de rôle, tester la naïveté des enfants, en leur montrant différents mails frauduleux, auxquels il ne faut pas répondre…
- Les informer des risques de cybercriminalité (usurpation d'identité, adultes cherchant à entrer en contact avec des enfants, escroqueries diverses) et des lois en matière de protection de la personne et de la vie privée.

Quelques conseils

- Lors du temps d'échange, **noter au tableau** quelques-unes des **idées des enfants** permettra de leur donner des **pistes de réflexion** et des **exemples** pour la suite de l'activité.
- Si nécessaire, préciser à nouveau qu'il n'est **pas question d'évaluation**. Chacun a le **droit de se tromper** et d'avoir son propre avis. Toutes les idées sont les bienvenues et seront discutées ensuite ensemble.
- Le travail en binôme favorise les **interactions** entre les enfants. Elle leur permet d'**échanger leurs points de vue**, de **comparer leurs réponses** et de **coopérer pour apprendre ensemble**. Un peu comme sur un site d'apprentissage collaboratif

Jouer à l'activité interactive associée

Défi «Spam Attack», activité interactive pour apprendre à faire preuve de discernement (un message d'un inconnu ventant un produit miracle, un message inhabituel émanant de votre banque, prudence !).

4 Les messages clés à retenir

En fin d'atelier, en reprenant leurs représentations initiales, demander aux enfants ce qu'ils ont retenu, si leurs représentations ont évolué au cours de l'atelier, ce qu'ils pensent maintenant, ce qui a changé pour eux. Cette étape peut se faire aussi bien à l'oral qu'à l'écrit.
Il est également possible de distribuer aux enfants cette courte liste de messages clés à retenir, à coller dans leur cahier, par exemple.

- Bien réfléchir avant de communiquer votre adresse sur Internet et **bien regarder les petites cases à cocher** !
- **Pour signaler un spam reçu** sur votre téléphone portable, **composer le 33 700**
- **Pour éviter de recevoir des SMS** de la part d'une société, **envoyez le mot STOP** au numéro qui a envoyé le message (ce service ne fonctionne pas avec la plupart des numéros à 5 chiffres)
- **Ne jamais répondre à un spam** : cela validerait l'existence de votre adresse.
- **Réserver l'adresse électronique** attribuée par votre fournisseur **d'accès à vos relations privées.**
- **Créer au moins une boite email auprès d'un prestataire gratuit** ; cette dernière sera réservée aux échanges sur forums, aux commandes sur des sites commerciaux, etc. Il sera toujours possible de la supprimer si elle venait à être inondée de spams.
- **Protéger votre ordinateur avec un antivirus à jour et un pare-feu ;** cela évitera entre autre qu'il ne devienne l'un de ces « PC Zombies » contrôlé à votre insu par un spammeur qui l'utilise pour ses envois.
- Quand le mal est fait (ce qui est rapide), il ne vous reste plus qu'à installer sur votre machine **un logiciel dit anti-spam** qui fera le tri dans vos messages en les pré-classant.
- Enfin, réfléchir avant de se fâcher avec un ami en l'accusant de vous avoir envoyé un spam, **c'est peut-être lui la victime** ! Alors informez-le !

5 Autres ressources Tralalere disponibles

SERIE VINZ ET LOU SUR INTERNET

- **Episode « Remplir ou ne pas remplir un formulaire »** sur les risques liés à la divulgation des données personnelles.
- **Episode « Mon ordinateur a attrapé un virus»** sur les différents moyens d'être contaminé par un virus informatique.

PORTAIL www.InternetSansCrainte.fr
Et en particulier l'espace 7-12, l'espace enseignants et la plateforme d'auto-formation.