Institut National Universitaire Champollion

Rapport de projet tutoré

Sensibilisation sur les réseaux sociaux et la cybercriminalité

Réalisé au collège les Roussillous à Saint Pierre de Lages

31570

Rapport rédigé par ROCA Vincent

Sommaire

I. Présentation du projet tutoré

Ce projet consiste à la prévention et à la formation des jeunes envers les risques d'internet.

Le projet est réalisé dans l'établissement du collège Les Roussillous à Saint pierre de Lages 31570.

Des appels téléphoniques ont été échangés et un rendez vous a été pris pour mettre en place l'intervention. Il a été décidé que cette intervention se ferait avec des classes de 5èmes.

Les interventions ont lieu le Jeudi 13 décembre et le vendredi 14 décembre. Chacune des trois interventions durent une heure.

L'intervention se fera sous forme de diaporama et présentera les risques des réseaux sociaux (Demande de l'établissement car programme déjà en cours dans celui-ci), la cybercriminalité et comment protéger ses données personnelles sur les réseaux sociaux et contre la cybercriminalité.

II. Explication du projet tutoré

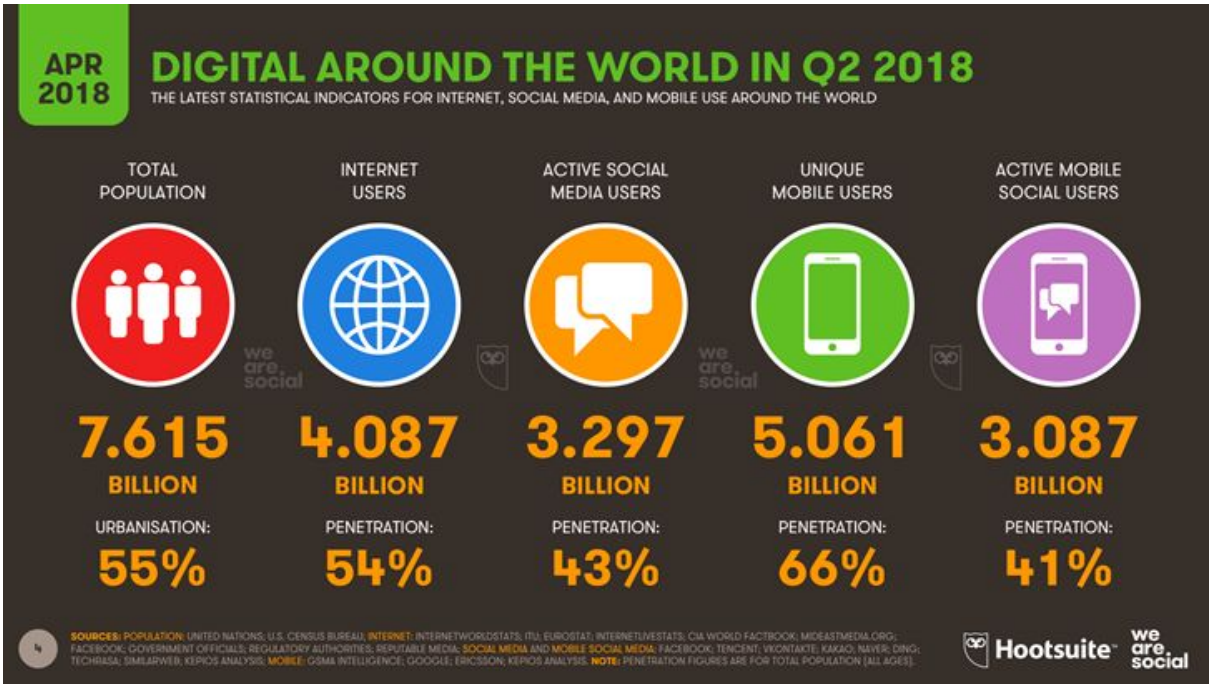
A) Le danger des réseaux sociaux

a) Quelques chiffres

La première partie du diaporama est consacrée aux risques des réseaux sociaux envers les jeunes.

Premièrement, une présentation globale des réseaux sociaux est réalisée grâce à des chiffres et la présentation de différents réseaux sociaux.

Cette présentation des chiffres permet de faire prendre conscience aux élèves que la population de l'internet et surtout des réseaux sociaux est énorme et que les risques et dangers sont présents.



Exemple : Environ 3 milliard d'utilisateurs sur les réseaux sociaux en Avril 2018.

Source : Wearesocial.com

b) Différents réseaux sociaux

La présentation des différents réseaux sociaux montrent aux élèves qu'il existe une multitude de réseaux sociaux avec toutes formes de contenus (Vidéo, Photo, Commentaire..).

c) Vidéo de prévention

Deuxièmement, une présentation via une vidéo qui montre les risques de ne pas protéger ses données sur le réseau social Facebook.

Il s’agit d’un homme se faisant passer pour un voyant mais qui n’utilise que les données Facebook de chaque personne afin de leur prouver qu’ils ne sont pas protéger. Cette campagne de prévention a été réalisé en Belgique.

Encore une fois, cela permet de prouver aux élèves que si nous ne protégeons pas nos comptes Facebook ou autres, il est très facile d’en savoir plus sur nous et notre vie privée.

Source : https://www.dailymotion.com/video/xx06es

d) Accessibilités des commentaires et des photos

Ensuite, une slide sur le risque d'accessibilité des commentaires et des photos. En effet, il est important de faire comprendre aux élèves que laisser ses photos accessibles peuvent être un poids pour leur futur.

De plus, la CNIL a montré que chez les jeunes plus de 86% postent des photos et identifient les personnes présentes sur la photo.

Les élèves doivent aussi savoir qu’il faut demander l’avis des personnes avant de poster une photo d’elles, publier des photos adaptées au réseau social et utiliser les outils d'identification à bon escient.

Si les photos ou bien les commentaires sont accessibles facilement, ils pourront être utilisés contre eux plus tard dans le monde professionnel ou même dans le monde de l’éducation.

e) La cyberdépendance

Quatrièmement, nous évoquons la cyberdépendance qui peut nuire chez les plus jeunes.

En effet, les élèves peuvent devenir dépendant à ses réseaux sociaux et cette dépendance peut amener à un échec scolaire.

Pour cela, nous nous appuyons sur des auteurs tels que Block en 2007 et Beard et Wolf en 2001 qui disent qu'il y a quatre composantes à considérer :

- L'utilisation excessive
- L'état de manque
- La tolérance
- Les conséquences négatives

En ce qui concerne la cyberdépendance, le test de Kimberley Young "Internet Addiction Test" permet de savoir si nous sommes cyberdépendant ou non. Il est composé de 20 questions où chaque réponse sont notées sur une échelle de 0 à 5.

La cyberdépendance amène aussi à des symptômes physique et comportementaux.

Symptômes physiques :

- Yeux secs
- Maux de tête
- Troubles du sommeil
- Alimentation irrégulière
- Hygiène dégradée

Symptômes comportementaux :

- Refus de modifier ses habitudes
- Agressivité
- Fatigue nerveuse
- Sentiment de honte

L'addiction aux réseaux sociaux peuvent amener à un échec scolaire.

f) Risques d'insultes et de harcèlements

Prévenir sur les risques d'insultes et de harcèlements me paraissait important car la tranche d'âge des élèves sur laquelle j'interviens est propice à être touchée par le harcèlement ou les insultes via les réseaux sociaux.

D'après le site *Internet sans crainte*, les personnes les plus touchées sont les jeunes de 12 à 15 ans.

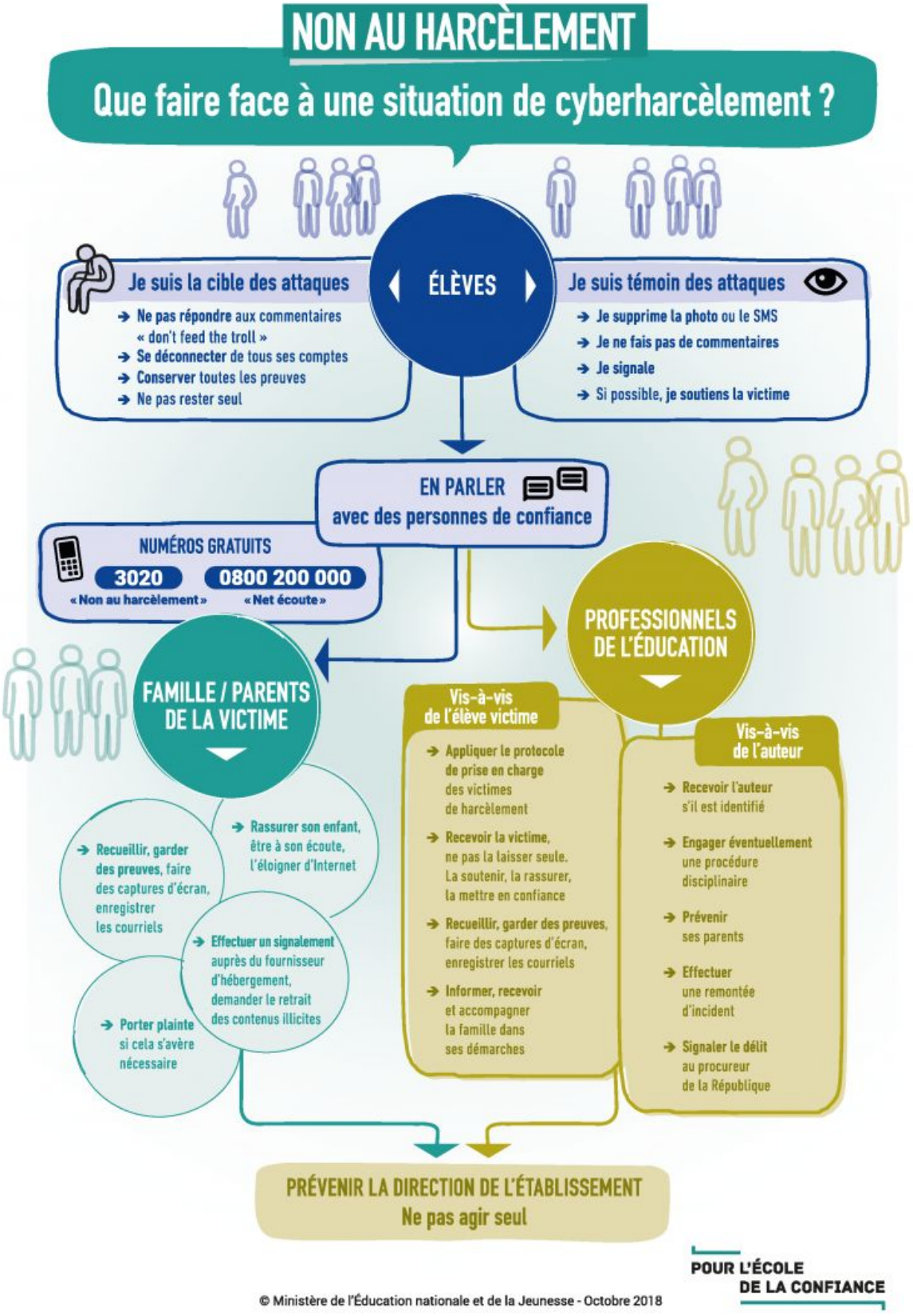
A cause des réseaux sociaux, le cyber harcèlement augmente. Il est donc important de sensibiliser les jeunes et leur apprendre comment réagir face à cet harcèlement.

La plupart des jeunes victimes de cyber harcèlement préfèrent ne pas en parler car ils ont honte d'en parler et se referme sur eux-mêmes.

Pourtant, lorsque quelqu'un est victime de cyberharcèlement, le seul remède est la discussion.

Il est important que la victime parle afin de ne pas rentrer dans une spirale négative.

Le ministère de l'education nationale à créer le schéma suivant afin de réagir face au cyberharcèlement.


NON AU HARCÈLEMENT
Que faire face à une situation de cyberharcèlement ?
ÉLÈVES
Je suis la cible des attaques
Ne pas répondre aux commentaires « don't feed the troll »
Se déconnecter de tous ses comptes
Conserver toutes les preuves
Ne pas rester seul
Je suis témoin des attaques
Je supprime la photo ou le SMS
Je ne fais pas de commentaires
Je signale
Si possible, je soutiens la victime
EN PARLER avec des personnes de confiance
NUMÉROS GRATUITS
3020 « Non au harcèlement »
0800 200 000 « Net écoute »
FAMILLE / PARENTS DE LA VICTIME
Recueillir, garder des preuves, faire des captures d'écran, enregistrer les courriels
Rassurer son enfant, être à son écoute, l'éloigner d'Internet
Effectuer un signalement auprès du fournisseur d'hébergement, demander le retrait des contenus illicites
Porter plainte si cela s'avère nécessaire
PROFESSIONNELS DE L'ÉDUCATION
Vis-à-vis de l'élève victime
Appliquer le protocole de prise en charge des victimes de harcèlement
Recevoir la victime, ne pas la laisser seule. La soutenir, la rassurer, la mettre en confiance
Recueillir, garder des preuves, faire des captures d'écran, enregistrer les courriels
Informer, recevoir et accompagner la famille dans ses démarches
Vis-à-vis de l'auteur
Recevoir l'auteur s'il est identifié
Engager éventuellement une procédure disciplinaire
Prévenir ses parents
Effectuer une remontée d'incident
Signaler le délit au procureur de la République
PRÉVENIR LA DIRECTION DE L'ÉTABLISSEMENT
Ne pas agir seul
POUR L'ÉCOLE DE LA CONFIANCE
© Ministère de l'Éducation nationale et de la Jeunesse - Octobre 2018

B) La cybercriminalité

Sensibiliser les élèves à la cybercriminalité est important car les nouvelles technologies sont de plus en plus présentes aujourd'hui dans nos vies. Il est donc possible que dans leur futurs études ou métiers, les élèves soient confrontés à cette cybercriminalité.

La cybercriminalité c'est l'ensemble des activités illégales effectuées par l'intermédiaire d'Internet.

Une multitude d'attaques de cybercriminalité sont possibles mais les plus connues sont le cheval de troie, le "phishing" et le "ransomware".

Faire connaître ces techniques à des élèves de 5èmes est important car ils pourront se protéger en conséquences quand il seront confrontés à ceux-ci dans leur vie.
Nous allons étudier les trois attaques et apprendre comment les éviter.

Le cheval de troie

Le cheval de troie permet :

- De supprimer l'ensemble du système
- Le vol de données bancaires
- Le suivi de l'utilisateur
- Effectuer un DDos (Dénie de service)
- Installer un serveur FTP
- Désactiver les antivirus
- Blocage aux site web essentiels et ressources liées à la sécurité
- Connexion internet dégradées

D’après le site *Le Blog du Hackeur,* voici quelques outils pour éviter un cheval de troie :

- Installer un antivirus et un pare feu
- Ne laisser personne accéder à votre ordinateur sans votre présence
- Faire attention aux sites piégés
- Méfiance avant de cliquer sur un programme

Pour faire comprendre de façon ludique aux élèves qu’est ce que le cheval de troie, je m’appuie sur une vidéo réalisé par Hack Academy.

Source : https://www.youtube.com/watch?v=SLeebIMR6H4

Le Phishing

D’après le site du gouvernement, le phishing a pour objectif d’usurper une identité afin d’obtenir des renseignement personnels et des identifiants bancaires pour en faire un usage criminel.

Comment cela fonctionne-t-il ?

Premièrement le cybercriminel se fait passer pour une personne de confiance et diffuse un mail frauduleux à une grande listes de contacts. Le mail demande aux destinataires de mettre à jour leurs informations personnelles sur un site falsifié vers lequel ils sont redirigés

De plus, le nombre important de destinataires dans la liste augmente la confiance envers le message diffusé.

En inscrivant ces informations sur le site falsifié, le cybercriminel a accès à celles-ci. Il pourra donc avoir accès à des informations comme les informations bancaire, financières…

Comment prévenir face au Phishing :

- Ne pas avoir confiance au nom de l'expéditeur de l'email. Si vous avez un doute, alors contacter l'expéditeur via un autre biais
- Se méfier des pièces jointes
- Ne jamais répondre par mail à une demande d'information confidentielle
- Faire attention à la qualité du français dans le mail (Orthographe)

Pour faire comprendre de façon ludique aux élèves qu'est ce que le phishing, je m'appuie sur une vidéo réalisé par Hack Academy

Source : https://www.youtube.com/watch?v=RupAsjOSuOc

Le ransomware

Et enfin, le Ransomware, dont l'objectif est de chiffrer des données puis demander à leur propriétaire de l'argent contre une clé qui permettra de les déchiffrer

Tout d'abord, le cybercriminel envoie un mail qui contient des pièces jointes ou des liens piégés qui demande de payer une facture rapidement par exemple.

Lorsque la victime clic, le logiciel est directement téléchargé et commence à chiffrer les données personnelles.

Ensuite, dès lors que les fichiers sont devenus cryptés et inaccessibles, un message de rançon s'affiche en demandant de l'argent contre une clé de décryptage.

Attention, ce n'est pas parce que vous payez la rançon que vos données vous seront redonnées.

Comment prévenir face au Ransomware?

- Ne pas avoir confiance dans le nom de l'expéditeur
- Se méfier des pièce jointes et des liens
- Effectuer des sauvegardes régulièrement
- Mettre à jour régulièrement tous vos principaux logiciels

Je m'appuierai encore une fois sur une vidéo venant du site du gouvernement.

Source : https://www.youtube.com/watch?v=i2SRKqILdh0

Comment réagir si on est victime de Ransomware et/ou de Phishing ?

Si vous êtes victime de cyberattaque, il faut déposer plainte vers la Police ou la Gendarmerie Nationale en se munissant de :

- Références des transferts d'argents effectués
- Référence des personnes contactées : email, pseudo ect..
- Numéro de votre carte bancaire
- Autre renseignement pour identifier l'escroc

C) Comment se protéger vis à vis des réseaux sociaux ainsi que des pirates de l'internet ?

Le fait de sensibiliser, de former les élèves de 5èmes à se protéger est important car en vue de l'évolution des nouvelles technologies, il est très probable qu'ils soient confronter à celles-ci dans leur futur.

Former tôt les jeunes à ces nouvelles technologies peut être intéressant en vue de les protéger eux même ou même leur entreprise.

C'est pourquoi j'ai voulu leur apprendre les bases de la sécurité informatique afin d'avoir un minimum de sécurité sur leurs appareils et ceux de l'établissement

Pour cela je vais d'abord parler des réseaux sociaux les plus "connus" et utilisés par les jeunes. Et ensuite, je développerai la sécurité de leurs appareils en dehors des réseaux sociaux.

Les réseaux sociaux :

Avant tout, il y a en général 4 type de données collectées sur les réseaux sociaux.

Les informations de votre profil, les traces de votre activité, l'activité silencieuse et la géolocalisation.

Pour éviter le vols de ses données, chacun des réseaux sociaux ont mis en place leur politique de sécurité avec des paramètres de confidentialité.

Facebook :

Facebook est le réseaux social le plus attaqué. Mais il est possible de bien sécuriser votre compte ainsi que ses informations.

Une rubrique "Privacy basics" est disponible sur facebook avec le message suivant : "C'est vous qui décidez qui peut voir ce que vous publiez sur Facebook".
Cette rubrique permet d'apprendre aux utilisateurs comment se protéger sous forme de slides, de présentation.

Pour apprendre à se protéger sur Facebook vous accès à :

- Contrôle de ce que vous publiez sur Facebook
- Gestion des interactions et de l'impact des autres sur votre contenu
- Personnalisation de ce que l'on veut voir
- Protection de votre compte
- Contrôler les publicités visibles

Instagram :

Instagram est l'un des réseaux les plus utilisé par les jeunes de nos jours. Il permet le partage de photos et vidéos.

A l'image de Facebook, Instagram à une rubrique intitulée "Confidentialité et Sécurité". Cette rubrique permet d'apprendre comment protéger ses données personnelles. Dans celle ci on y retrouve :

- Contrôle de sa visibilité
- Résolution des abus et blocages des personnes
- Partage des photos en sécurité
- Signalement des comptes piraté, usurpation d'identité, abus...

Pour le moment il existe peu de paramètre pour sécuriser au maximum son compte mais il est possible de passer le profil en privée. Le fait d'avoir un compte privée nous permet d'accepter que les personnes que l'on connaît mais aussi d'éviter que tout le monde puisse voir le contenu de votre compte.

<u>Snapchat :</u>

Snapchat est très utilisé chez les jeunes collégiens. Il existe quelques astuces afin de protéger son compte.

- Masquer son numéro de téléphone
- Utiliser un pseudo et pas son nom et prénom
- Autoriser seulement ses amis à voir ses story
- Activer l'authentification par sms

Le réseau social snapchat est dangereux car souvent les jeunes pensent que les photos envoyées sont éphémères mais tout ce qui est envoyé sur le net est enregistré. Comme les jeunes pensent que les photos sont éphémères, ils ont tendance à envoyer des photos à caractères sexuels par exemple en pensant qu'ils ne risquent rien.

Twitter :

Twitter est un réseau social qui n'était pas trop utilisé par les jeunes auparavant mais qui augmente maintenant.

Le problème de twitter c'est que votre twit sera visible dans le monde entier quoi qu'il arrive. C'est pourquoi il est d'autant plus important de savoir sécuriser ses données sur Twitter.

La politique de confidentialité de Twitter est très transparente envers la sécurité et la protection de votre compte.

Cependant il y a une autre rubrique "Twitter en tout sécurité ! Les bases" où l'on peut trouver les informations suivantes :

- Protection de votre compte
- Evaluation des liens sur Twitter et éviter l'hameçonnage "phishing"

Ensuite, la rubrique "Protection de vos données personnelles" permet :

- Le contrôle des informations partagées
- Les conseils de sécurité destinés aux professeurs, aux parents et adolescents

Se protéger face à la cybercriminalité

Etant en face d'élèves de 5ème je préfère rester sur les bases de la sécurisation de leurs appareils et ne pas rentrer dans les détails afin de ne pas les perdre.

En faisant des recherches sur la protection face a la cybercriminalité, je me suis aperçu que la plupart des résultats étaient des sites d'assurances qui accompagne les clients.

Je me suis appuyer sur le site de l'assurance "La mobilière" qui propose quelques conseils de bases tels que :

- Installer un logiciel antivirus et le mettre à jour régulièrement
- Sauvegarder régulièrement ses données sur des supports externes
- Installer seulement des programmes venant de sources sûres
- Ne cliquez pas sur les pièces jointes suspectes
- Jamais donner des informations personnelles sur le net
- Choisir différents mots de passe pour chaque site et avec des caractères spéciaux
- Vérifiez régulièrement ses relevés bancaires
- Triez et choisir ses amis sur les réseaux sociaux
- Bloquer ou dénoncer les auteurs de cybercriminalité

III. Questionnaire

Afin de savoir si mon intervention a été fructueuse et si les élèves étaient déjà conscient des risques de l'internet, j'ai créé ce questionnaire pour en savoir plus.

1. De quel sexe êtes vous ?

2. Etes vous sur les réseaux sociaux ?

3. Si oui, le(s)quel(s) ?

4. Combien de fois par jour allez vous sur les réseaux sociaux ?

5. Vos comptes sont-il sécurisés ?

6. Avez vous déjà lu la politique de sécurité de chaque réseau social?

7. Qu'est ce que la cybercriminalité ?

8. Qu'est ce que le Phishing ?

9. Qu'est ce que le Ransomware ?

10. Qu'est ce qu'un cheval de troie ?

L’analyse des réponses se fera à l’oral devant le jury.

Bibliographie :

Image chiffre Internautes - *Wearesocial.com*

Cartographie Réseaux sociaux - *IUT Bordeaux*

Vidéo de présentation - *https://www.dailymotion.com/video/xx06es*

Non au harcèlement - *Ministère de l'éducation*

Cheval de troie - *Le blog du hackeur*

Cheval de troie vidéo - *https://www.youtube.com/watch?v=SLeebIMR6H4*

Le phishing - *Site du gouvernement*

Le phishing vidéo - *https://www.youtube.com/watch?v=RupAsjOSuOc*

Le ransomware - *Site du gouvernement*

Le ransomware vidéo -*https://www.youtube.com/watch?v=i2SRKqILdh0*

Annexes :


LES DANGERS DES RÉSEAUX SOCIAUX ET LA CYBERCRIMINALITÉ


SOMMAIRE
I. Les dangers des réseaux sociaux
II. La cybercriminalité
III. Comment se protéger sur internet ?
IV. Questionnaire

I. LES DANGERS DES RÉSEAUX SOCIAUX

Les chiffres :

- 4 milliard d'internautes
- 3 milliard d'utilisateurs de réseaux sociaux
- 432 millions le nombre de pirates (2016)

I. LES DANGERS DES RÉSEAUX SOCIAUX

- Accessibilité des commentaires et photos

I. LES DANGERS DES RÉSEAUX SOCIAUX

- La cyberdépendance :
  - Utilisation excessive
  - Etat de manque
  - Tolérance
  - Conséquences négatives

I. LES DANGERS DES RÉSEAUX SOCIAUX

Risques d'etre insulté ou harcelé

QUE FAIRE ???

II. LA CYBERCRIMINALITÉ

- Infraction à la loi sur internet
- Quels types d'infractions ?

II. LA CYBERCRIMINALITÉ

- Les attaques des cybercriminels

II. LA CYBERCRIMINALITÉ

- Phishing
- Ransomware

III. COMMENT SE PROTÉGER ?

Pour vous protéger:

- limitez-vous à publier les informations que vous pourriez raconter à un inconnu rencontré dans la rue.
- restreignez l'accès aux informations que vous publiez en utilisant les paramètres de confidentialité.
- acceptez les invitations d'«amitié», uniquement des personnes que vous connaissez vraiment dans la vie réelle.
- armez-vous de bon sens lorsque vous recevez des messages d'une personne que vous ne connaissez pas.
- n'ouvrez pas les liens (documents, photos, vidéos, etc.) provenant de source douteuse et vérifiez-les toujours avant de cliquer dessus.
- utilisez des mots de passe forts et différents pour chaque compte/service.
- assurez-vous que vos programmes informatiques sont parfaitement à jour (navigateur, système d'exploitation, antivirus, etc.).

- Sur les réseaux sociaux

III. COMMENT SE PROTÉGER ?

1. Installez un logiciel antivirus sur votre ordinateur et mettez-le à jour régulièrement ainsi que votre système d'exploitation.
2. Sauvegardez régulièrement les données importantes sur un support externe (sauvegardes).
3. N'installez que des programmes qui viennent d'une source sûre.
4. Ne cliquez pas sur les pièces jointes suspectes et n'ouvrez aucun lien.
5. Ne transmettez aucune information personnelle à des personnes que vous ne connaissez pas.
6. Choisissez des mots de passe et gardez vos données d'accès confidentielles.
7. Vérifiez régulièrement vos relevés bancaires et relevés de carte de crédit.
8. Regardez à deux fois quels sont vos amis sur les réseaux sociaux.
9. Utilisez les paramètres de confidentialité des réseaux sociaux afin que tous vos contenus ne soient pas accessibles au public et n'acceptez que des contacts que vous connaissez également dans la vie hors ligne.
10. Prenez des mesures si vous remarquez que quelqu'un est victime de cyberintimidation : Bloquez ou dénoncez les auteurs et prenez des captures d'écran.

- Protection basique sur les appareils


IV. QUESTIONNAIRE
Question