Chat/forums

Mandat	Les élèves discutent des dangers liés aux réseaux sociaux sur la base d'un article de journal. Les élèves conçoivent un jeu de rôle, au cours duquel différentes personnes mentionnées dans l'article prennent la parole. Les élèves réfléchissent à la discussion en rédigeant un manuel sur le comportement à adopter sur un forum de chat/un réseau social, ainsi que sur les informations que l'on peut divulguer et celles qu'il vaut mieux ne pas communiquer.
Objectif	• Les élèves identifient les dangers liés aux réseaux sociaux. • Les élèves peuvent se mettre à la place de différentes personnes mentionnées dans l'article présenté et formuler leurs réflexions. • Les élèves peuvent réfléchir aux connaissances acquises et les formuler dans un texte qu'ils rédigent eux-mêmes.
Lien avec le programme scolaire	• Les élèves peuvent communiquer à l'aide des médias tout en respectant certaines règles de sécurité et de conduite. (MI.1.4c)
Matériel	• Article de journal «De faux-amis très actifs sur Facebook» (en allemand uniquement) • Feuille de travail «chat/forums»
Forme de travail	Ensemble de la classe/travail individuel
Temps imparti	45 minutes

Informations complémentaires:

- Article servant de base à la discussion: Perte d'emploi suite à un commentaire raciste sur Facebook
  https://www.les-crises.fr/liker-sur-facebook-peut-vous-couter-votre-emploi/
  https://references.lesoir.be/article/11-facons-de-se-faire-virer-a-cause-de-facebook/
- Article servant de base à la discussion: Sextortion, chantage sur le chat vidéo.
  https://francoischarlet.ch/2014/sextorsion-ou-chantage-sexuel-par-video-comment-ca-se-passe-et-que-faire/ (avec vidéo)
  https://www.skppsc.ch/fr/sextorsion-images-compromettantes-reseaux-sociaux-et-chantage-un-cocktail-dangereusement-epice/

Réseaux sociaux

Discussion

Lis l'article de journal ci-dessous et discute avec ton voisin ou ta voisine de table d'autres dangers auxquels il est possible de s'exposer sur les réseaux sociaux.
Ecrivez vos constatations en quelques mots sur les lignes suivant l'article.
Résous ensuite les deux exercices consécutifs sur les dangers et les risques des réseaux sociaux.

https://www.tagesanzeiger.ch/zuerich/verbrechen-und-unfaelle/auf-facebook-sind-falsche-freunde-aktiv/story/10875168 (en allemand uniquement - traduction ci-dessous)

De faux-amis très actifs sur Facebook

Des escrocs utilisent la plateforme de médias sociaux pour soutirer de l'argent. Les plaintes s'accumulent auprès de la police zurichoise.

Les pirates informatiques copient des profils Facebook et envoient de nouvelles invitations à devenir amis.

Photo: Keystone

Stefan Hohler
Journaliste du domaine policier @tagesanzeiger09.05.2017

«Si vous recevez une invitation à devenir amis de la part d'une personne qui porte le même nom que moi, et qui vous demande votre numéro de téléphone: ce n'est pas moi!» Aujourd'hui, il ne s'écoule pas un jour sans qu'un utilisateur Facebook envoie ce message d'avertissement ou un message de ce type.

Les pirates informatiques copient les profils Facebook et envoient des invitations à devenir amis aux connaissances du titulaire initial du profil. Dans un deuxième temps, ils demandent à leurs victimes leur numéro de téléphone mobile et un code SMS leur permettant d'effectuer des achats directement décomptés sur la facture du téléphone mobile.

Recrudescence des cas

Selon Michael Walker, porte-parole de la police, le phénomène est apparu pour la première fois à l'automne 2015. Au début, les escroqueries étaient des cas individuels, mais cette tendance a fortement augmenté. Rien que sur les deux premiers mois de cette année, près de 50 plaintes ont été déposées. La tendance est à la hausse.

Les sommes escroquées sont généralement peu élevées. Les arnaqueurs créeraient un compte auprès d'un fournisseur en ligne permettant de payer par facture de téléphone mobile. Les montants ne sont portés au débit de la facture que si cette facture a été confirmée par le code envoyé ou si le numéro de téléphone mobile la confirme activement.

La police cantonale de Zurich constate désormais une recrudescence des plaintes de ce genre. «A l'heure actuelle, nous recevons deux à trois plaintes de ce type par semaine», déclare la porte-parole de la police cantonale Carmen Suber. Une enquête est en cours, mais il n'y a pas encore eu d'arrestation. La difficulté est liée au fait que les malfaiteurs peuvent agir de l'étranger ou au niveau international.

Contrôler chaque invitation à devenir amis

Surber recommande de ne pas donner son propre numéro de téléphone mobile. Par ailleurs, il ne faut jamais transmettre de code PIN reçu par SMS ni confirmer de code PIN inconnu.

Par mesure de sécurité, les utilisateurs de Facebook peuvent protéger leur vie privée et n'autoriser les accès qu'à leurs amis avec les réglages correspondants. «Chaque demande d'ajout à sa liste d'amis doit être soigneusement contrôlée, et il convient surtout de vérifier si l'on n'a pas déjà accepté la personne dans la liste d'amis», explique Surber.

Un journaliste des journaux de quartier et courriers locaux zurichois de la «Lokalinfo» a également goûté à la piraterie informatique – à ses dépens. Il a accepté une invitation à devenir amis et a reçu peu de temps après un message privé par la messagerie instantanée de Facebook. «Donne-moi ton numéro de mobile.» Ceci fiat, la sollicitation suivante ne s'est pas fait attendre: «Tu vas recevoir un code par SMS, peux-tu me le transmettre?» Ce qu'il a fait, pensant qu'il s'agissait d'une collègue de la rédaction.

Ce n'est que plus tard que le journaliste constate que les pirates informatiques ont acheté une console de jeu pour 100 francs sur une boutique en ligne étrangère. «Le montant a été imputé à ma facture de téléphone mobile par un fournisseur tiers.» Il a porté plainte auprès de la police et a informé **Swisscom**. Celle-ci a fait preuve de compréhension et n'a pas débité le montant.

«Si ce type de cas touche une facture Swisscom, nous recommandons aux clients de nous contacter», nous a répondu la porte-parole de Swisscom Sabrina Hubacher. En cas d'escroquerie, Swisscom renonce au paiement des fournisseurs tiers. Ceux-ci doivent alors réclamer eux-mêmes l'argent. Hubacher recommande tout de même de poster un commentaire sur **Facebook** quant au profil piraté et de porter plainte auprès de la police.

(Tages-Anzeiger)

Créé le: 09.05.2017, 14h51

1. **Les dangers et les risques des réseaux sociaux:**

.....

.....

.....

.....

.....

2. **Réfléchis à ce que les personnes de l'article pourraient raconter dans une interview. Comment se sont-ils mis dans cette situation? Quels étaient leurs motifs? Qu'en pensent-elles a posteriori? Comment se sentent-elles après les «faits»? A quelles conséquences doivent-elles s'attendre?**

La victime:	*Le malfaiteur:*

La police:

Tu trouveras d'autres informations sur les dangers liés aux réseaux sociaux sur le site:

Jeunes et médias, Réseaux sociaux, Opportunités et risques
https://www.jeunesetmedias.ch/fr/opportunites-et-risques/reseaux-sociaux.html

3. **Rédige un manuel dans lequel tu expliques à un jeune comment se comporter sur les réseaux sociaux ou ce que l'on peut y divulguer et ce qu'il vaut mieux garder pour soi.**
   Pour t'aider, tu peux utiliser le lien suivant:
   https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/Internet_und_Computer/services-en-ligne/medias-sociaux/observations-concernant-les-sites-de-reseautage-social.html
   (Préposé fédéral à la protection des données et à la transparence, Réseaux sociaux, «Recommandations aux utilisateurs»)

Comment utiliser les réseaux sociaux en toute sécurité:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Source d'images: Handwerk-Magazin.de
https://img.handwerk-magazin.de/files/smthumbnaildata/392x/5/1/4/6/3/1/Fotolia_44298834_kbuntuFotolia.com_social_media.jpg

Solutions possibles:

1. **Les dangers et les risques des réseaux sociaux:**

- *La sensibilisation insuffisante à l'accessibilité de commentaires, photos, etc. pour d'autres utilisateurs, et aux dangers connexes d'utilisation abusive de donnée. Une fois sur la Toile, les photos peuvent pour ainsi dire plus être supprimées.*
- *Cyberdépendance*
- *Distraction pendant les devoirs lorsque les jeunes les font à l'ordinateur tout en étant connectés à un réseau social.*
- *Contacts non sollicités et agressions sexuelles: les pédosexuels peuvent prendre contact avec des victimes potentielles par les réseaux sociaux.*
- *Etre ridiculisé, offensé ou harcelé par d'autres «utilisateurs» (cybermobbing)*

(Source: https://www.jeunesetmedias.ch/fr/opportunites-et-risques/reseaux-sociaux.html)

Autres possibilités:

- *Obtenir, subtiliser des données afin de les utiliser de manière abusive ou de les publier.*
- *Chantage basé sur des informations, des images ou des vidéos mises en ligne par la victime, ou subtilisées par l'extorqueur (que la victime en soit consciente ou non)*
- *Les informations données sur les réseaux sociaux peuvent être utilisées pour des attaques de phishing.*

2. **Réfléchis à ce que les personnes de l'article pourraient raconter dans une interview. Comment se sont-ils mis dans cette situation? Quels étaient leurs motifs? Qu'en pensent-elles a posteriori? Comment se sentent-elles après les «faits»? A quelles conséquences doivent-elles s'attendre?**

Solutions individuelles des élèves

Réflexions possibles:
La victime: n'a pas réfléchi aux conséquences, était naïve. Peut être par la suite déçue, honteuse, furieuse, etc. Les données qui sont transmises sur la Toile ou ont été subtilisées peuvent parfois s'y retrouver ultérieurement. Des conséquences ultérieures ne sont donc pas exclues, si les données sont transmises ou revendues.
Le malfaiteur: peut avoir différents motifs (pauvreté, cupidité, plaisir de faire souffrir autrui, etc.), peut se sentir fort, voire supérieur, après son acte, peut éventuellement le regretter par la suite. Il n'a peut-être pas réfléchi aux conséquences de son acte. S'il est pris, il doit s'attendre à une poursuite pénale.

Le policier: est actif dès qu'une plainte est déposée. Peut sans doute se mettre à la place de la personne lésée. Doit tenter d'élucider le cas et de trouver le responsable (malfaiteur). Peut être frustré si ce genre de cas se répète et que ses enquêtes n'apportent pas les résultats escomptés.

3. **Rédige un manuel dans lequel tu expliques à un jeune comment se comporter sur les réseaux sociaux ou ce que l'on peut y divulguer et ce qu'il vaut mieux garder pour soi.**

Solutions individuelles des élèves
Comparaison éventuelle aux informations du site:
https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/Internet_und_Computer/services-en-ligne/medias-sociaux/observations-concernant-les-sites-de-reseautage-social.html (Préposé fédéral à la protection des données et à la transparence, Réseaux sociaux, «Recommandations aux utilisateurs»)