Chat/Foren

Arbeitsauftrag	Die SuS diskutieren anhand eines Zeitungsartikels über Gefahren von sozialen Netzwerken. Die SuS entwerfen ein Rollenspiel, bei welchem verschiedene Personen aus dem Artikel zur Sprache kommen sollen. Die SuS reflektieren die Diskussion, indem sie eine Anleitung darüber schreiben, wie man sich in einem Chat/sozialen Netzwerk verhalten soll und welche Informationen man preisgeben darf bzw. lieber nicht preisgeben sollte.
Ziel	• SuS erkennen die Gefahren und Risiken von sozialen Netzwerken. • SuS können sich in verschiedene Personen aus dem abgedruckten Artikel hineinversetzen und deren Überlegungen formulieren. • SuS können ihre Erkenntnisse anhand eines selbst formulierten Textes reflektieren und in Worte fassen.
Lehrplanbezug	• SuS können mittels Medien kommunizieren und dabei die Sicherheits- und Verhaltensregeln befolgen. (MI.1.4c)
Material	• Zeitungsartikel «Auf Facebook sind falsche Freunde aktiv» • Arbeitsblatt «Chat/Foren»
Sozialform	Plenum/Einzelarbeit
Zeit	45 Minuten

Zusätzliche Informationen:

- Hintergrundartikel: Jobverlust nach rassistischem Facebook-Kommentar http://www.watson.ch/Digital/International/680621549-Das-sagt-der-Junge--der-wegen-eines-rassistischen-Kommentars-auf-Facebook-seine-Stelle-verlor
- Hintergrundartikel: Sextortion, Erpressung im Videochat. https://www.nzz.ch/panorama/aktuelle-themen/erpressung-im-videochat-st-galler-polizei-warnt-vor-sextortion-ld.92278

Soziale Netzwerke

Diskussion

Lies den unten stehenden Zeitungsartikel und diskutiere anschliessend mit deiner Banknachbarin, deinem Banknachbarn, welchen anderen Gefahren man sich in sozialen Netzwerken aussetzen kann.
Schreibt eure Erkenntnisse in Stichworten auf die Linien nach dem Artikel.
Löse anschliessend die beiden Folgeaufträge zu den Gefahren und Risiken von sozialen Netzwerken.

https://www.tagesanzeiger.ch/zuerich/verbrechen-und-unfaelle/auf-facebook-sind-falsche-freunde-aktiv/story/10875168

Auf Facebook sind falsche Freunde aktiv

Betrüger nutzen die Social-Media-Plattform, um Geld abzuzocken. Bei der Zürcher Polizei häufen sich die Anzeigen.

Die Hacker kopieren Facebook-Profile und verschicken erneute Freundschaftsanfragen.

Bild: Keystone

Stefan Hohler
Polizeireporter @tagesanzeiger09.05.2017

«Falls ihr gerade Freundschaftsanfragen bekommt von jemandem, der so heisst wie ich, und der dann eure Telefonnummer erchattet: Das bin nicht ich!» Derzeit vergeht kaum ein Tag, ohne dass ein Facebook-User solche oder ähnliche Warnungen verschickt.

Hacker kopieren bestehende Facebook-Profile und verschicken Freundschaftsanfragen an die Bekannten des ursprünglichen Inhabers. In einem zweiten Schritt werden die Opfer nach ihrer Handynummer und einem SMS-Code gefragt, mit denen die Hacker danach Einkäufe tätigen können, die dem Opfer direkt auf der Handyrechnung belastet werden.

Starke Zunahme der Fälle

In Zürich ist das Phänomen laut Michael Walker, Sprecher der Stadtpolizei, erstmals im Herbst 2015 aufgetaucht. Anfänglich seien die Betrügereien noch vereinzelt gewesen, jetzt hätten sie aber stark zugenommen. Allein in den ersten beiden Monaten dieses Jahres seien rund 50 Anzeigen eingereicht worden. Tendenz steigend.

Die ertrogenen Summen seien im Allgemeinen niedrig. Die Betrüger würden im Internet bei Online-Anbietern ein Konto einrichten, wo die Rechnungen über Handynummern bezahlten werden. Die Rechnung werde nur belastet, wenn man sie entweder mit dem zugesandten Code oder mit der Handynummer aktiv bestätige, sagt Walker.

Auch die Kantonspolizei Zürich muss sich inzwischen häufiger mit solchen Anzeigen befassen. «Wir erhalten derzeit wöchentlich zwei bis drei davon», sagt Kapo-Sprecherin Carmen Suber. Man sei am Ermitteln, zu Verhaftungen sei es aber noch nicht gekommen. Die Schwierigkeit liege darin, dass die Täter auch aus dem Ausland agieren oder international tätig sein könnten.

Jede Freundschaftsanfrage überprüfen

Surber empfiehlt, die eigene Handynummer nicht bekannt zu geben. Zudem sollen keine per SMS erhaltenen PIN-Codes weitergeschickt und/oder keine unbekannten SMS bestätigt werden.

Als Sicherheitsvorkehrungen könne auf der Facebook-Seite unter Einstellungen die Privatsphäre geschützt und Zugriffe nur für Freunde erlaubt werden. «Jede Freundschaftsanfrage soll genau geprüft werden, insbesondere, ob man nicht schon mit der Person befreundet ist», sagt Surber.

Auch ein Journalist der Zürcher Quartier- und Lokalzeitungen «Lokalinfo» machte Bekanntschaft mit den Hackern. Er nahm eine Freundschaftsanfrage an und erhielt kurz darauf eine private Nachricht über den Facebook-Messenger. «Gib mir bitte kurz deine Handynummer.» Nachdem er die Nummer bekannt gab, folgte die nächste Aufforderung: «Du erhältst gleich einen Code per SMS, kannst du mir diesen angeben?» Auch diesen Code leitete er an die vermeintliche Redaktionskollegin weiter.

Erst später stellte der Journalist fest, dass die Hacker auf seine Rechnung Guthaben für eine Spielkonsole für 100 Franken in einem ausländischen Onlineshop gekauft haben. «Der Betrag wurde über einen sogenannten Drittanbieter auf meiner Handyrechnung belastet.» Er erstattete Anzeige bei der Polizei und informierte die **Swisscom**. Diese zeigte sich entgegenkommend und belastete den Betrag nicht.

«Betrifft ein solcher Fall eine Swisscom-Abrechnung, so empfehlen wir den Kunden, sich bei uns zu melden», sagt Swisscom-Sprecherin Sabrina Hubacher auf Anfrage. Die Swisscom verzichte im Betrugsfall auf die Auszahlung an Drittanbieter. Diese müssen die Gelder danach selbst einfordern. Hubacher empfiehlt trotzdem eine Meldung bei **Facebook** über das gehackte Profil und eine Anzeige bei der Polizei.

(Tages-Anzeiger)

Erstellt: 09.05.2017, 14:51 Uhr

1. **Gefahren und Risiken im Umgang mit sozialen Netzwerken:**

.....

.....

.....

.....

.....

2. **Überlege dir, was die beteiligten Personen aus dem Artikel in einem Interview aussagen würden. Warum sind sie in diese Situation geraten? Was waren ihre Beweggründe? Wie denken sie im Nachhinein darüber? Wie fühlen sie sich nach der «Tat»? Welche Folgen müssen sie erwarten?**

Das Opfer:

Die Täter:

Die Polizei:

Weitere Informationen zu den Gefahren im Umgang mit sozialen Netzwerken findest du unter:

Jugend und Medien, soziale Netzwerke, Chancen und Gefahren
http://www.jugendundmedien.ch/chancen-und-gefahren/soziale-netzwerke.html

3. **Verfasse eine Anleitung, in welcher du einem Jugendlichen erklärst, wie man sich in sozialen Netzwerken verhalten soll bzw. was man über sich preisgeben soll und was nicht.**
   Als Hilfe kannst du folgenden Link verwenden:
   https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/onlinedienste/soziale-medien/erlaeuterungen-zu-sozialen-netzwerken.html
   (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, soziale Netzwerke, «Empfehlungen an die Benutzerinnen und Benutzer»)

So nutzt du soziale Netzwerke sicher:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

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

Lösungsvorschläge:

1. Gefahren und Risiken im Umgang mit sozialen Netzwerken:

- *Fehlendes Bewusstsein über die Zugänglichkeit von Kommentaren, Fotos etc. für andere und damit verbunden die Gefahr von Datenmissbrauch. Einmal im Netz zirkulierende Bilder können kaum mehr gelöscht werden.*
- *Online-Sucht*
- *Ablenkung von den Hausaufgaben, wenn Jugendliche diese am Computer machen und gleichzeitig im sozialen Netzwerk eingeloggt sind*
- *Unerwünschte Kontakte und sexuelle Übergriffe: Pädosexuelle können über soziale Netzwerke Kontakt mit potenziellen Opfern aufnehmen.*
- *von anderen «Usern» blossgestellt, beleidigt oder belästigt werden (Cybermobbing)*

(Quelle: http://www.jugendundmedien.ch/chancen-und-gefahren/soziale-netzwerke.html)

Weitere Möglichkeiten:

- *Erschleichen, Abgreifen von Daten, welche dann missbräuchlich verwendet oder veröffentlicht werden können*
- *Erpressung aufgrund von Informationen, Bildern oder Videos, welche vom Opfer ins Netz gestellt oder vom Erpresser abgegriffen wurden (mit oder ohne Wissen des Opfers)*
- *Informationen aus sozialen Netzwerken können für Phishing-Attacken verwendet werden.*

2. Überlege dir, was die beteiligten Personen aus dem Artikel in einem Interview aussagen würden. Warum sind sie in diese Situation geraten? Was waren ihre Beweggründe? Wie denken sie im Nachhinein darüber? Wie fühlen sie sich nach der «Tat»? Welche Folgen müssen sie erwarten?

individuelle Lösungen der SuS

Mögliche Überlegungen:
Opfer: Dachte nicht über Konsequenzen nach, war blauäugig, naiv. Ist im Nachhinein evtl. enttäuscht, beschämt, wütend etc. Daten, die im Netz landen oder abgegriffen wurden, sind evtl. auch später noch im Netz auffindbar. Spätere Konsequenzen sind also nicht ausgeschlossen, falls die Daten weitergegeben oder verkauft wurden.
Täter: Motive können unterschiedlich sein (Armut, Gewinnsucht, Freude am Leid anderer etc.), man kann sich nach der Tat zuerst stark und überlegen fühlen, evtl. kommt später Reue dazu, vielleicht wurden die Auswirkungen der Tat gar nicht bedacht. Bei Auffliegen der Tat muss mit Strafverfolgung gerechnet werden.

Polizist: Wird aktiv, sobald Strafantrag gestellt wird. Kann sich wahrscheinlich in die geschädigte Person hineinversetzen. Muss versuchen, die Tat aufzuklären und Verantwortliche (Täter) zu finden. Allenfalls frustriert, falls öfters solche Fälle gemeldet werden und seine Ermittlungen nicht die gewünschten Erfolge bringen.

3. **Verfasse eine Anleitung, in welcher du einem Jugendlichen erklärst, wie man sich in sozialen Netzwerken verhalten soll bzw. was man über sich preisgeben soll und was nicht.**

individuelle Lösungen der SuS
kann mit den Verhaltensregeln auf:
https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/onlinedienste/soziale-medien/erlaeuterungen-zu-sozialen-netzwerken.html (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, Soziale Netzwerke, «Empfehlungen an die Benutzerinnen und Benutzer») verglichen werden