Arbeitsblatt: Täter und Opfer im Internet

Aufgabe 1
Nenne jeweils drei Beispiele, wie du im Internet zum Opfer oder zum Täter werden kannst.

Opfer	Täter
Verletzung deiner Persönlichkeitsrechte	Verletzung von Persönlichkeitsrechten (z. B. ungefragte Veröffentlichung von Porträtaufnahmen)
Identitätsdiebstahl (Account kopieren und mit falschem Namen posten)	Verletzung von Urheberrechten (illegale Downloads, illegales Uploading, unberechtigte Nutzung von lizenzrechtlich geschützten Medien)
Cybermobbing (wenn jemand dich über das Internet mobbt)	Cybermobbing (Beleidigung, üble Nachrede usw.)

Aufgabe 2
Recherchiere die jeweiligen Paragraphen im Strafgesetzbuch (StGB), die für Vergehen im Internet relevant sind. Was bedeuten sie?
§ 202a Ausspähen von Daten
§ 202b Abfangen von Daten
§ 263a Computerbetrug
§ 303a Datenveränderung
§ 303b Computersabotage

Aufgabe 3
Was könnt ihr daheim an eurem Computer und an eurem Smartphone dafür tun, nicht Opfer von Cybercrime zu werden? Nenne drei Beispiele.

Maßnahmen gegen Cybercrime:
- Zwei-Faktor-Authentifizierung einschalten, wo es möglich ist
- nur https-Verbindungen nutzen
- Smartphone immer mit Passwort versehen, keine Fingermuster
- Smartphone-Ortung einschalten
- in sozialen Netzwerken nur Sachen posten, die auch öffentlich gemacht werden könnten
- keine Mails von unbekannten Absendern öffnen
- keine zweifelhaften Websites aufsuchen (z. B. Kinostreaming-Plattformen)
- Virenscanner (vor allem bei Windows und Android) verwenden

Arbeitsblatt: Cybermobbing bis Volksverhetzung

Aufgabe 1
Welche verschiedenen Formen von Cybermobbing gibt es? Nenne einige davon und recherchiere, welche Straftaten dies sein könnten.

- Flaming (Beleidigung, Beschimpfung)
- Harassment (Belästigung)
- Denigration (Anschwärzen, Gerüchte verbreiten)
- Impersonation (Auftreten unter falscher Identität)
- Outing (Bloßstellen)
- Exklusion (Ausschluss, Ausgrenzung)
- Cyberstalking (fortwährende Belästigung und Verfolgung)
- Cyberthreats (offene Androhung von Gewalt)

Bedrohung, Beleidigung, üble Nachrede, Verleumdung, außerdem eventuell Computerbetrug/-sabotage usw.

Aufgabe 2
Wer könnte im Fall von Cybermobbing helfen? Erstellt eine Liste möglicher Ansprechpartner/innen. Ihr könnt auch Websites recherchieren, die bei Cybermobbing helfen.

Ansprechpartner/innen:

- Eltern
- Lehrer/in
- Vertrauenslehrer/in
- Schulsozialarbeiter/in
- (Schul-)Psycholog/in
- Streitschlicher/in, Mediator/in
- Freund/in
- Online-Beratungsstellen

Websites:
- Nummer gegen Kummer
- klicksafe.de
- handysektor.de
- mediaculture online
- Internet ABC
- Polizeiliche Kriminalprävention
- Juuuport

Aufgabe 3
Im Netz versuchen rechtsradikale Gruppierungen, ihre menschenfeindliche Propaganda zu verbreiten. Da eindeutige Symbole wie das Hakenkreuz in Deutschland verboten sind, gibt es vermehrt Versuche, diese Symbole zu „codieren“. Sind dir im Internet schon einmal solche Codes begegnet? Du kannst auf der Website www.dasversteckspiel.de diese Codes anschauen und die jeweilige Bedeutung nachlesen. Sucht euch jeweils eine dieser Beschreibungen aus und stellt sie den anderen vor.

Beispiele

Thorshammer
In der Bildsprache der extremen Rechten, insbesondere ihrer Musikbands, ist der Gott Thor die reinigende Kraft. Er soll mit seinem Thorshammer „das deutsche Volk vom verderbenden Ungeziefer reinigen“.

18
18 steht für Adolf Hitler.
Die Zahlenkombination findet sich beispielsweise in den Namen der Organisation Combat 18 und der Band Sturm 18.

CONSDAPLE
Die Marke Consdaple ist bei Neonazis aufgrund der im Wort enthaltenen Buchstabenkombination NSDAP beliebt.

Arbeitsblatt: Betrug und Jugendschutz im Netz

Aufgabe 1
Wie könnt ihr euch vor Betrügern im Internet am besten schützen, zum Beispiel bei eBay-Käufen oder Webshops?
- Trusted Shops nutzen
- eBay-Treuhandservice nutzen
- nicht vorab überweisen
- Angebot sehr genau durchlesen
- gesundes Misstrauen entwickeln
- Vorsicht bei besonders günstigen Angeboten

Aufgabe 2
Hattet ihr schon einmal eine Phishing-E-Mail in eurer Mailbox? Oder Bekannte von euch? Oder habt ihr per WhatsApp eine Kettenmail erhalten? Diskutiert darüber, warum die Leute so etwas weiterleiten. Woran habt ihr erkannt, dass es sich um eine falsche Nachricht gehandelt hat?
- anderer Absender als üblich
- unglaubwürdige Story bei Kettenmails
- meistens schlechtes Deutsch bei Spam- und Phishing-Mails
- Anhänge sind meistens als Zipdateien mitgeliefert

Aufgabe 3
Ist es für euch okay, wenn Kinder und Jugendliche Spiele spielen, die nicht für ihr Alter freigegeben sind? Wie denkt ihr darüber?
Wer setzt die Altersfreigaben bei Computerspielen fest, und wie arbeiten diese Leute?
Bewusstsein schaffen für die Notwendigkeit von Altersfreigaben. Die Arbeit der USK kennenlernen.

Aufgabe 4
Was könnt ihr tun, wenn ihr über strafrechtlich relevante Inhalte im Internet stolpert?
- Eltern informieren
- Lehrer informieren
- Polizei informieren, evtl. auch über die Internetwache

Arbeitsblatt: Darknet und Verschwörungstheorien

Aufgabe 1
Was genau ist das sogenannte Darknet und was ist der Unterschied zum WWW (World Wide Web) und zum sogenannten Deep Web?
Das Darknet ist ein abgeschlossener Bereich des WWW, der nur mit einem bestimmten Browser (dem TOR-Browser) erreicht werden kann. Darknet-Seiten haben immer die Endung .onion und sind ein anonymisierter Teil des WWW. Das Deep Web ist der Teil des Internets, der nicht zum WWW gehört.

Aufgabe 2
Gibt es auch eine mögliche positive Nutzung des Darknets (TOR-Netzwerk)? Wie denkt ihr darüber? In welcher legalen Situation wäre es sinnvoll, das Internet anonym nutzen zu können?
- für Journalisten und deren Informanten
- bei Anzeige von Verbrechen und Straftaten in Firmen oder Organisationen
- für oppositionelle Politiker in autoritären Staaten

Aufgabe 3
Terroristische Gruppierungen versuchen vor allem über das Internet, junge Menschen anzusprechen. Seien es islamistische oder rechtsextreme Gruppierungen, alle nutzen soziale Netzwerke, um ihre menschenverachtenden Botschaften zu verteilen. Oft nutzen sie Verschwörungstheorien und Falschmeldungen, um Angst zu erzeugen und die öffentlich-rechtlichen Medien abzuwerten. Welche dieser Theorien kennt ihr? Recherchiert nach diesen Verschwörungstheorien und auch nach Seiten, die darüber aufklären und Falschmeldungen entlarven. Diskutiert über euer eigenes Verhalten in sozialen Netzwerken. Was teilt ihr, was teilt ihr nicht? Überprüft ihr die Posts, bevor ihr sie teilt?
- http://de.verschwoerungstheorien.wikia.com/wiki/Verschw%C3%B6rungstheorien_Wiki
- http://de.verschwoerungstheorien.wikia.com/wiki/Liste_der_Verschw%C3%B6rungen

Aufklärungsseiten:
- http://www.mimikama.at/ (Zuerst denken, dann klicken)
- http://www.hoaxsearch.com/
- https://hoax-info.tubit.tu-berlin.de/hoax/hoaxlist.shtml

Arbeitsblatt: Soziale Netzwerke und Passwörter

Aufgabe 1
Welche sozialen Netzwerke nutzt du? Schaue dir die AGB von WhatsApp, Instagram und Snapchat an. Wie gehen diese mit deinen Daten um?
- WhatsApp ist end-to-end-verschlüsselt, die Inhalte können von WhatsApp und dem Mutterkonzern Facebook nicht ausgelesen und archiviert werden.
- Aber die Metadaten (wer wann mit wem kommuniziert) können nicht verschlüsselt werden.
- Bei Instagram werden die Nutzerdaten von Facebook eingesehen und Profile angelegt bzw. Werbung geschaltet.
- Snapchat speichert die Bilder zentral.

Aufgabe 2
Schaue dir die Privatsphäre-Einstellungen der jeweiligen sozialen Netzwerke an und versuche, diese so einzustellen, dass möglichst nur wenige deine Daten zu Gesicht bekommen (z. B. nur Familie und Freunde). Nutze gegebenenfalls Tipps und Tricks zu Privatsphäre-Einstellungen, die es auf Seiten wie Klicksafe oder Handysektor gibt.
Ziel ist, Bewusstsein für Privatsphäre zu schaffen und die Einstellungsmöglichkeiten der sozialen Netzwerke kennenzulernen.

Aufgabe 3
Passwörter sind das A und O für eine sichere Internetnutzung. Tauscht euch aus, wie ihr mit euren Passwörtern umgeht. Habt ihr sie schon einmal weitergegeben? Ändert ihr sie regelmäßig?
Wie sehen sichere Passwörter oder sogenannte Passphrasen aus? Wie kann man sich gute und starke Passwörter einfach merken? Recherchiere dazu, zum Beispiel auf klicksafe.de.
Teste Passwort-Generatoren aus und lasse dir eine Liste mit Passwörtern erzeugen. Du kannst auch Passwort-Tresore recherchieren und einen davon ausprobieren.
Bewusstsein für sichere Passwörter schaffen
- sichere Passwörter: http://www.klicksafe.de/themen/datenschutz/privatsphaere/wie-sollte-ein-sicheres-passwort-aussehen/

- Passwort-Generatoren, zum Beispiel http://www.gaijin.at/olspwgen.php
    Ilenatoga357
    Uvovebade542
    Ikinehiku917
    Urupuwuwo396
    Emutuvuwe597