

Einführung Datenschutz

Arbeitsauftrag	<ul style="list-style-type: none"> • Vergleichen der Standard-Einstellungen in sozialen Netzwerken • Probleme mit Datenschutz thematisieren (evtl. auch unter Einbezug des Informationsdossiers, insbesondere Kap. 1 «Was ist Datenschutz?») • Schwierigkeiten in der Zukunft durch unvorsichtiges Umgehen mit Daten erkennen • Zusatzblatt: «Das gebe ich von mir preis!» Schnelle SuS können sich anhand des Arbeitsblattes überlegen, welche Daten sie mit wem teilen würden. <p>Die anschliessende Diskussion kann in Partnerarbeit, Gruppenarbeit oder im Plenum geführt werden.</p>
Ziel	<ul style="list-style-type: none"> • Die SuS überlegen sich, was sie in sozialen Netzwerken veröffentlichen (wollen) und inwiefern sie Handlungsspielraum bei den persönlichen Einstellungen besitzen. • Die SuS können die Risiken unverschlüsselter Datenübermittlung und -speicherung abschätzen.
Lehrplanbezug	<ul style="list-style-type: none"> • MI.2.3n: «Die SuS können die Risiken unverschlüsselter Datenübermittlung und -speicherung abschätzen.»
Material	<ul style="list-style-type: none"> • Auftragsblatt «Diskussion – besonders schützenswerte Daten» • Screenshots «Privatsphäre-Einstellungen» • Arbeitsblatt «Tabelle»
Sozialform	Einzelarbeit/Partnerarbeit/Plenum
Zeit	60 Minuten

Zusätzliche Informationen:

- Durch die Abgabe der Screenshots, auf welchen die Privatsphäre-Einstellungen in verschiedenen sozialen Netzwerken abgebildet sind, können die SuS unterschiedliche Einstellungsvarianten vergleichen und beurteilen. Dies empfiehlt sich, da viele Jugendliche sich (zu) wenig mit diesen Einstellungen auseinandersetzen und deshalb nur bedingt Auskunft über die eigenen Einstellungen geben können. Wenn man die Grundeinstellungen nicht selber anpasst, geben die Onlinedienste und Apps meistens mehr Daten preis als für deren Funktion nötig ist (z. B. Zugriff auf Adressbuch, Standortdaten).
- Um die verwendeten Begriffe zu erläutern, kann das Dossier «Datenschutz», welches zur Lektionsreihe gehört, beigezogen werden (z. B. soziales Netzwerk, Cloud).

Einführung Datenschutz

- **Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)**
Erläuterungen zu sozialen Netzwerken
https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/onlinedienste/soziale-medien/erlaeuterungen-zu-sozialen-netzwerken.html



Wie sicher ist dein Account?



Diskussion

Vergleiche mit deiner Banknachbarin, deinem Banknachbarn, ob und wie sich die Privatsphäre-Einstellungen in euren sozialen Netzwerken unterscheiden. Nehmt dazu die Screenshots auf den nächsten Seiten zur Hilfe.

Beispiele: Instagram, google+, Snapchat, Facebook, kik etc.

- Könnt ihr **Unterschiede** feststellen?
(Privatsphäre, Sicherheit, Freundschaftsanfragen, Benachrichtigungen etc.)
- Diskutiert ausserdem, was sich ändert, wenn ihr **andere Profileinstellungen** vornehmt.
- Gibt es Einstellungen, die **unbedingt** vorgenommen werden sollten?
- Was lässt sich **nicht ändern**?

→ Notiert eure Erkenntnisse auf den unten stehenden Linien:

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....



Wusstest du?

SNS sind meistens gratis, aber sie sind keine gemeinnützigen Einrichtungen. Es findet ein «Handel» statt: Dienstleistungen für Benutzerinnen und Benutzer im Tausch gegen deren Daten.

www.jugendundmedien.ch
Interessante Hinweise und Tipps zu sozialen Netzwerken und den empfohlenen Sicherheitseinstellungen.



Bildquelle: Wepushbuttons
<https://wepushbuttons.com.au/wp-content/uploads/2013/04/social-media-list.jpg>



Beispiel 1: Facebook-Privatsphäre-Einstellungen (Stand April 2018)

Privatsphäre-Einstellungen und Werkzeuge

Wer kann meine Inhalte sehen?	Wer kann deine zukünftigen Beiträge sehen?	Freunde	Bearbeiten
	Überprüfe alle deine Beiträge und Inhalte, in denen du markiert bist		Aktivitätenprotokoll verwenden
	Möchtest du die Zielgruppe für Beiträge einschränken, die du mit Freunden von Freunden oder öffentlich geteilt hast?		Vergangene Beiträge einschränken
Wer kann mich kontaktieren?	Wer kann dir Freundschaftsanfragen senden?	Alle	Bearbeiten
	Wessen Nachrichten sollen in meinem Postfach gefiltert werden?	Einfaches Filtern	Bearbeiten
Wer kann nach mir suchen?	Wer kann mithilfe der von dir zur Verfügung gestellten E-Mail-Adresse nach dir suchen?	Freunde	Bearbeiten
	Wer kann mithilfe der von dir zur Verfügung gestellten Telefonnummer nach dir suchen?	Alle	Bearbeiten
	Möchtest du, dass andere Suchmaschinen einen Link zu deiner Chronik enthalten?	Ja	Bearbeiten

Beispiel 2: Twitter-Privatsphäre-Einstellungen (Stand April 2018)

Privatsphäre

Foto-Markierungen

- Jedem erlauben, mich in Fotos zu markieren
- Nur Leuten, denen ich folge, erlauben, mich in Fotos zu markieren
- Niemandem erlauben, mich in Fotos zu markieren

Tweet-Sicherheit

- Meine Tweets schützen

Wenn ausgewählt, werden nur von Dir bestätigte Personen Deine Tweets erhalten. Deine zukünftigen Tweets werden nicht öffentlich sichtbar sein. Frühere Tweets können an verschiedenen Stellen noch sichtbar sein. **Mehr erfahren.**

Standort twittern

- Meinen Tweets einen Standort hinzufügen

Wenn Du mit einem Standort twitterst, speichert Twitter diesen Standort. Du kannst vor jedem Tweet den Standort ein- oder ausschalten. **Mehr erfahren**

Alle Standortinformationen löschen

Das wird alle Standortinformationen vorheriger Tweets löschen. Dies könnte bis zu 30 Minuten dauern.

Feststellbarkeit

- Erlaube anderen, mich mithilfe meiner E-Mail-Adresse zu finden

Adressbuch

Deine Kontakte verwalten

Kontakte, die Du aus Deinem Adressbuch auf Twitter hochgeladen hast.

Das Feature, mit welchem Du Twitter basierend auf Deinen Besuchen anderer Webseiten personalisieren kannst, steht Dir nicht zur Verfügung.

Gesponsert Inhalt

- Anzeigen maßschneidern basierend auf von Weropartnern geteilten Informationen

Auf diese Weise kann Twitter Werbeanzeigen über Dinge anzeigen, an denen Du bereits Interesse gezeigt hast. **Erfahre** mehr darüber, wie es funktioniert, sowie über zusätzliche Datenschutzmöglichkeiten.

Twitter für Teams

- Jedem erlauben, mich zu dessen Team hinzuzufügen
- Nur jenen, denen ich folge, erlauben, mich zu deren Team hinzuzufügen
- Nicht jedem erlauben, mich zu dessen Team hinzuzufügen

Organisationen können jeden dazu einladen, von ihrem Account zu twittern, indem die Team-Funktion in TweetDeck genutzt wird. **Mehr erfahren.**

Änderungen speichern



Das gebe ich von mir preis!



Aufgabe

Kreuze in der Tabelle unten an, welche Informationen du an welche Personengruppe weitergeben würdest.

Setze ein (+) für «ja», ein (-) für «nein» und ein (?), wenn du dir nicht sicher bist.

	Familie	Kolleginnen /Kollegen	Chef, Lehrperson	Follower auf Instagram	Fremde auf der Strasse	Unbekannte im Chat
Alter, Geschlecht						
Blutgruppe						
Angaben über Geschwister, Familienmitglieder						
Lohn, Arbeitsstelle						
Fotos von meinem Freund/ meiner Freundin und mir						
Geschäftskontakte						
Kontaktliste aus meinem Handy						
meine Handynummer						
meine E-Mail-Adresse						
meine Wohnadresse						
mein Pin-Code für mein Handy oder meinen Laptop						
Bild von meinem Gesicht						
Bild von meinem Körper (mit Kleidern)						
Bild von meinem nackten Körper						
mein Kontostand						



	Familie	Kolleginnen /Kollegen	Chef, Lehrperson	Follower auf Instagram	Fremde auf der Strasse	Unbekannte im Chat
Informationen zu meinem Tagesablauf						
Persönliches, das ich von einer Freundin/einem Freund erfahren habe.						
Passwort für mein Konto in einem sozialen Netzwerk (z. B. Instagram, Facebook)						
meine sexuelle Orientierung						

Vergleiche anschliessend deine Kreuze mit einer Mitschülerin, einem Mitschüler.

Wo gibt es Unterschiede?

Wo seid ihr euch einig?

Welche Daten gebe ich in einem sozialen Netzwerk preis?

.....

.....

.....

.....

.....

.....



Weitere Infos zum Thema:

Schau genau: Falsche Identitäten im Chat (Stadtpolizei Zürich)

http://www.schaugenau.ch/de/belaestigungenn#!falsche_identitaeten

EDOEB: Datenübermittlung von Whatsapp an Facebook

https://www.edoeb.admin.ch/edoeb/de/home/aktuell/aktuell_news/datenuebermittlung-von-whatsapp-an-facebook.html



- Situation 6** *Freundschaftsanfrage von einem Unbekannten sollte man nicht einfach annehmen, weil man nicht sicher sein kann, dass diese Person nicht unlautere Absichten hat. Ausser sich selber kann man dadurch auch andere in unangenehme oder auch gefährliche Situationen bringen. Philipp muss davon ausgehen, dass sämtliche Inhalte, welche er in Zukunft mit seinen «Freunden» teilt, auch von dieser Person gesehen werden und von ihr verwendet, bearbeitet oder veröffentlicht werden.*
- Situation 7** *Da Banken nie per SMS oder E-Mail Zugangsdaten anfordern, muss davon ausgegangen werden, dass sich eine unbefugte Person die Bankdaten von Corinne erschleichen will. Gibt Corinne tatsächlich ihre Bankdaten weiter, droht ihr ein finanzieller Schaden. Deshalb darf man nie Anhänge in solchen Mails öffnen oder auf Links klicken.*
- Situation 8** *Da Francesco sein Handy nicht verschlüsselt hat, kann ein allfälliger Finder auf sämtliche Daten, Apps und Inhalte des Mobiltelefons zugreifen. Dies kann dazu führen, dass private und sensible Inhalte (Fotos, Videos, Nachrichten etc.) abgegriffen werden oder Francescos Accounts dazu genutzt werden, Kontakte herauszufiltern, Personen unter falschem Namen zu kontaktieren etc.*

Zu den strafrechtlichen Konsequenzen im Bereich Datenschutz siehe «Bilder und Bildrechte (2.7)» sowie «Konkrete Gefahren und rechtliche Folgen (2.4)» und «Smartphones (2.5)» im Informationsdossier «Datenschutz» zu dieser Lektionsreihe.

Zusatzblatt «Das gebe ich von mir preis!

→ *individuelle Lösungen der SuS*

Was ist Datenschutz?

Arbeitsauftrag	<ul style="list-style-type: none"> Die Lehrperson stellt anhand einer PowerPoint-Präsentation die Themen Datenschutz, Privatsphäre, Überwachung und Big Data vor. Die SuS füllen währenddessen das Arbeitsblatt aus, um ihr Wissen zu vertiefen und festzuhalten. anschliessend gemeinsame Besprechung des Gehörten und Festgehaltenen
Ziel	<ul style="list-style-type: none"> Die SuS vertiefen und erweitern ihr Wissen zu den Themen Datenschutz, Privatsphäre, Überwachung und Big Data. Die SuS können Informationen und Positionen zu aktuellen gesellschaftlichen Herausforderungen und Konflikten bezüglich Interesse und Wahrheitsgehalt hinterfragen (z. B. Schutz und Verwendung von Daten).
Lehrplanbezug	<ul style="list-style-type: none"> ERG.1.2d
Material	<ul style="list-style-type: none"> PowerPoint-Präsentation «Datenschutz» Arbeitsblatt «Datenschutz»
Sozialform	Einzelarbeit, Plenum
Zeit	30 Minuten

Zusätzliche Informationen:

- Weiterführende Informationen zu Themen rund um den Datenschutz finden sich im Informationsdossier «Datenschutz», welches zu dieser Lektionsreihe gehört. Gegebenenfalls können den SuS Auszüge daraus abgegeben werden, um ihnen unbekannte Begriffe näherzubringen (z. Bsp. 1.2. Begriffe).
- Zusätzliche Hintergrundinformationen:
 - Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz.html> umfassende Informationen rund um den Datenschutz, gegliedert in verschiedene Themenfelder



Was ist Datenschutz?



Aufgabe

Deine Lehrperson hat dir mit der PowerPoint-Präsentation das Thema «Datenschutz» nähergebracht. Versuche nun mit den gehörten Informationen die nachfolgenden Fragen und Aufgaben zu lösen.

Ergänze die folgenden Satzanfänge, sodass sie mit dem Gehörten übereinstimmen:

Datenschutz ist ...

.....

Das Ziel des Datenschutzes ist ...

.....

Besonders «schützenswerte Daten» sind zum Beispiel ...

.....

Probleme beim Datenschutz kann es geben, wenn ...

.....

«Privatsphäre» heisst ...

.....

Der Staat darf nur überwachen, wenn ...

.....

Gib zu jeder Situation einen kurzen Kommentar ab, ob der Datenschutz verletzt worden ist.

- Als du am Morgen die Zeitung öffnest, traust du deinen Augen nicht: Bei einem Artikel zu einer Party am Wochenende befindet sich ein Foto von dir mit einer Bierflasche in der Hand. Du wusstest nicht, dass du fotografiert wirst und der Fotograf hat dich auch danach nicht angesprochen.

.....



- Du bist auf dem Säntis und genießt die Aussicht. Hinter dir schiessen einige Touristen Selfies von sich. Du bist dir sicher, dass du auch im Hintergrund zu sehen bist. Ohne dich anzusprechen, fahren die Touristen mit der nächsten Gondel talwärts.
-
- Dein Sportverein lanciert eine neue Internetseite. Darauf findet sich auch die Rubrik «Geburtstagskinder». Jeden Tag werden diejenigen Vereinsmitglieder aufgelistet, welche ihren Geburtstag feiern. So zum Beispiel: «Wir gratulieren heute Stefan Müller aus unserer U19-Mannschaft zum 16. Geburtstag.»
-



Wenn du dich genauer über den Datenschutz und das Strafrecht im Bereich des Datenschutzes informieren möchtest, findest du unter

<https://www.edoeb.admin.ch/>

wichtige Informationen.



Bildquelle: Legal Tribune Online (<https://www.lto.de/recht/hintergruende/h/bag-urteil-8azr101013-datenschutz-arbeitnehmer-einwilligung/>)



Lösungsvorschläge

Datenschutz ist...

der Schutz der Privatsphäre und Persönlichkeit der Menschen, deren Daten bearbeitet werden.

Das Ziel des Datenschutzes ist ...

so viele Daten wie nötig, so wenig Daten wie möglich zu sammeln. Oder mit anderen Worten:

Personendaten so zu bearbeiten, dass die Privatsphäre der Betroffenen möglichst wenig tangiert wird.

Besonders «schützenswerte Daten» sind zum Beispiel ...

- *die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten;*
- *die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit.*
- *Massnahmen der sozialen Hilfe;*
- *administrative oder strafrechtliche Verfolgung und Sanktionen.*

Probleme beim Datenschutz kann es geben, wenn ...

Daten bearbeitet oder veröffentlicht werden, ohne dass die betroffene Person eingewilligt hat.

Schutz der «Privatsphäre» heisst ...

dass Daten, die mit unserer Person zu tun haben, geschützt werden.

Definition Wikipedia: Privatsphäre bezeichnet den nichtöffentlichen Bereich, in dem ein Mensch unbehelligt von äusseren Einflüssen sein Recht auf freie Entfaltung der Persönlichkeit wahrnimmt. Das Recht auf Privatsphäre gilt als Menschenrecht und ist in allen modernen Demokratien verankert. Dieses Recht kann aufgrund des öffentlichen Interesses an einer Person oder zu Zwecken der Strafverfolgung eingeschränkt werden.

Der Staat darf nur überwachen, wenn ...

... ein Gesetz ihn dazu ermächtigt;

... das öffentliche Interesse an der Überwachung höher zu werten ist als das Interesse des Einzelnen an seiner Privatsphäre.

Gib zu jeder Situation einen kurzen Kommentar ab, ob der Datenschutz verletzt worden ist.

- Als du am Morgen die Zeitung öffnest, traust du deinen Augen nicht: Bei einem Artikel zu einer Party am Wochenende befindet sich ein Foto von dir mit einer Bierflasche in der Hand. Du wusstest nicht, dass du fotografiert wirst und der Fotograf hat dich auch danach nicht angesprochen.

Was ist Datenschutz?



Wenn Informationen über Menschen gesammelt und bearbeitet werden, ist deren Persönlichkeit davon betroffen.

Diese Betroffenheit kann stark oder schwach sein, positive oder negative Reaktionen hervorrufen.

(Botschaft zum Bundesgesetz über den Datenschutz)

Kennst du selbst solche negativen Beispiele?

Beispiel 1: Soziale Netzwerke sammeln Daten, um ihre Nutzer mit gezielter (unerwünschter) Werbung versorgen zu können.

Beispiel 2: Fotos von dir werden, ohne dass du es willst, veröffentlicht (z. B. im Internet).

Beispiel 3: Deine Kontaktinformationen, welche du bei einem Wettbewerb angegeben hast, werden an interessierte Firmen weiterverkauft.

Was ist Datenschutz?



Ziel des Datenschutzes:

Der Datenschutz setzt sich zum Ziel, der Datenbearbeitung **Leitplanken** zu setzen.

Die **Entfaltung der Persönlichkeit** soll nicht durch unnötige und unerwünschte Informationstätigkeiten beeinträchtigt werden.



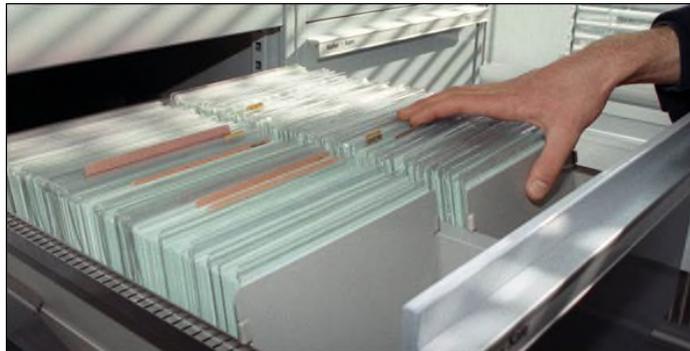
Bildquelle: Pixabay, www.pixabay.com

Was ist Datenschutz?



Grundsätze des Datenschutzes:

- So viele Daten wie nötig und so wenig Daten wie möglich sammeln und bearbeiten.
- Jeder Mensch hat das Recht, Einsicht in die Daten zu erhalten, welche über ihn erfasst werden!
- Der Einzelne hat das Recht, Informationen über ihn berichtigen (korrigieren) oder löschen zu lassen oder zu verlangen, dass der Informationsbearbeiter sie nicht weitergeben darf.



Bildquelle: 20 Minuten, www.20min.ch

Was ist Datenschutz?



Was sind «besonders schützenswerte» Daten?

Im Datenschutzgesetz (DSG) wird im Artikel 3 Folgendes ausgeführt:

- die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten
- die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit
- Massnahmen der sozialen Hilfe
- administrative oder strafrechtliche Verfolgung und Sanktionen

Auch biometrische Daten gelten als besonders schützenswert, werden im heutigen Gesetz aber noch nicht erwähnt.

Was ist Datenschutz?



Was macht Daten besonders schützenswert?

Personendaten oder personenbezogene Daten verraten viel über uns und sind deshalb kostbar.

Für Unternehmen bedeuten sie bares Geld, und sie können von anderen missbraucht werden (z. B. Weiterverkauf von Kundendaten, Weitergabe von Adressdaten)

Schützen wir unsere Daten, heisst das **Privatsphäre, Anonymität und mehr Sicherheit** für uns. Einfach unbezahlbar!

In den folgenden beiden Beispielen wird aufgezeigt, inwiefern im täglichen Leben Probleme und Überschneidungen beim Datenschutz auftreten können.

Was ist Datenschutz?



Beispiel 1: Google Street View

Google fotografiert mit dem Google-Auto die Strassen und Gebäude auf der ganzen Welt und verknüpft diese Bilder mit der Strassenkarte.



Was ist Datenschutz?



Datenschutzproblem:

Die Aufnahmen **können für Personen nachteilig sein**, z. B. für eine Person, welche eine Drogenberatungsstelle betritt oder eine psychiatrische Klinik und dabei abgelichtet wird.

Google hat **keine Einwilligung** von den einzelnen Personen, dass sie die Aufnahmen veröffentlichen dürfen.

Deshalb müssen alle **Personen, Autoschilder und Privatbereiche unkenntlich** gemacht werden, um so die Persönlichkeitsrechte des einzelnen Menschen zu schützen.

Was ist Datenschutz?



Beispiel 2:

Erfassen von Personendaten für Werbezwecke

Nino bestellt gerne im Internet Kleider und elektronische Hilfsmittel.

Dabei hat er verschiedene Informationen über sich angegeben.

Diese Informationen wurden nun zu Verkaufs- und Werbezwecken an weitere Internetportale und Werbeagenturen weitergegeben.

Datenschutzproblem:

Unternehmen, die Daten erheben, müssen klar ausweisen, für welchen Zweck diese Daten erhoben werden. Die Person, welche die Personendaten von sich preisgibt, muss kennzeichnen können, dass sie mit der Weitervergabe einverstanden ist.



Bildquelle: BZ Berlin

http://www.bz-berlin.de/data/uploads/2017/02/83159111_1486646630-768x432.jpg

Was ist Datenschutz?



Privatsphäre

Privatsphäre bezeichnet den nichtöffentlichen Raum, in welchem ein Mensch unbehelligt von äusseren Einflüssen sein Recht auf freie Entfaltung wahrnimmt.

(<https://de.wikipedia.org/wiki/Privatsph%C3%A4re>)

Nicht alle Informationen über uns und unser Leben gehen jeden etwas an, oder?

Dementsprechend ist es wichtig, die eigene Privatsphäre zu schützen und die Privatsphäre anderer zu respektieren.



Bildquelle: Bundesministerium für Forschung und Bildung

https://static1.bmbfcluster.de/2/3/3/4_c76fda0ed54d014/2334meg_4e6cb79899f70b9.jpg



Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDOB
Préposé fédéral à la protection des données et à la transparence PFPDT
Incaricato federale della protezione dei dati e della trasparenza IFPDT
Incumbens federal per la protecciuin da datas e per la trasparenza IFPDT



Was ist Datenschutz?



Überwachung

Tagtäglich werden Daten von uns gesammelt. Geschieht dies mit der Absicht, ein **Profil** zu erstellen, spricht man auch von **Überwachung**.

So kann beispielsweise auch der Staat Personen überwachen, um festzustellen, ob diese eine Verbindung zu extremistischen oder terroristischen Gruppierungen haben.

Was ist Datenschutz?



Bei der Überwachung von Personen gilt ...

1. das Legalitätsprinzip:

Staatliches Handeln muss in **einem Gesetz vorgesehen** sein (z. B. Strafprozessrecht, Nachrichtendienstgesetz).

2. das Prinzip der Verhältnismässigkeit:

Es muss abgewogen werden, was höher einzuschätzen ist:

- das **Interesse der betroffenen Person** an ihrer Privatsphäre
- das **Interesse des Staates und der Öffentlichkeit** an der Überwachung

Was ist Datenschutz?



Beispiel:

Der Lehrmeister von F. vermutet, dass er während der Arbeit zu viel privat im Internet surft. Insbesondere soll er oft in sozialen Netzwerken wie Instagram und Snapchat verweilen und die Arbeit dadurch vernachlässigen.

Der Lehrmeister hat nun einerseits ein **Interesse, den Computer von F. zu überwachen** und seine Internetaktivitäten festzuhalten. Andererseits hat F. ein **Interesse an seiner Privatsphäre** und er möchte vermutlich nicht, dass sein Vorgesetzter alles weiss, was er im Internet macht.

Bildquelle: ZDF

<https://www.zdf.de/nachrichten/heute-sendungen/videos/ueberwachung-kuendigung-100.html>



Was ist Datenschutz?



Lösungsvorschlag zum Beispiel:

Auch wenn der Lehrmeister den Verdacht hegt, dass F. während der Arbeitszeit privat im Internet surft, darf er ihn **nicht** überwachen.

- Es gibt keine gesetzliche Grundlage dazu, weshalb das **Legalitätsprinzip** eine Überwachung nicht zulässt.
- Ausserdem besteht kein übergeordnetes Interesse vonseiten der Öffentlichkeit oder des Staates an einer Überwachung (**Prinzip der Verhältnismässigkeit**).

Bildquelle: ZDF

<https://www.zdf.de/nachrichten/heute-sendungen/videos/ueberwachung-kuendigung-100.html>



Was ist Datenschutz?



Auftrag

Löse nun das Arbeitsblatt «Was ist Datenschutz?» (Lektion 2)

Besprich deine Lösungen mit deiner Banknachbarin, deinem Banknachbarn.

Anschliessend wird das Blatt im Klassenrahmen besprochen.



Bildquelle: Pixabay, www.pixabay.com

Soziale Netzwerke

Arbeitsauftrag	<ul style="list-style-type: none"> Die SuS gestalten ein Plakat nach bestimmten Kriterien über ein soziales Netzwerk (z. B. Instagram, Snapchat, Pinterest, Facebook, Twitter etc.) Die SuS erarbeiten die Kriterien für ein sicheres Passwort und entwerfen ein eigenes, sehr sicheres Passwort. Dieses kann anschliessend auf www.passwortcheck.ch getestet werden.
Ziel	<ul style="list-style-type: none"> Die SuS können Verflechtungen und Wechselwirkungen zwischen physischer Umwelt, medialen und virtuellen Lebensräumen erkennen und für das eigene Verhalten einbeziehen (z. B. soziale Netzwerke und ihre Konsequenzen im realen Leben). Die SuS kennen die Kriterien für sichere Passwörter.
Lehrplanbezug	<ul style="list-style-type: none"> MI.1.1e
Material	<ul style="list-style-type: none"> Plakatpapier, White Board oder Flipchart Computer mit Internetzugang, alternativ Tablets oder Handys
Sozialform	Gruppenarbeit / Einzelarbeit
Zeit	30 Minuten

Zusätzliche Informationen:

- Für die Bearbeitung des Gruppenauftrages zu den sozialen Netzwerken empfiehlt es sich, in der Klasse abzuklären, welche Netzwerke von den SuS tatsächlich genutzt werden.
- Es kann für die SuS durchaus auch interessant sein, «fremde» soziale Netzwerke zu untersuchen und Unterschiede zu den von ihnen genutzten zu finden.
- Statistiken zur Social-Media-Nutzung:
<https://de.statista.com/themen/1842/soziale-netzwerke/>
 Die hier aufgelisteten Statistiken können als Einstieg gebraucht werden, um den SuS das Ausmass und die Bedeutung der sozialen Netzwerke weltweit aufzuzeigen.



Soziale Netzwerke



Recherche

Gestaltet in Dreiergruppen ein Plakat, auf welchem ihr ein soziales Netzwerk vorstellt.

Zur Auswahl stehen:

Snapchat, Instagram, Facebook, Twitter, Pinterest, Myspace, Tumblr, Flickr

Auf dem Plakat sollen folgende Informationen dargestellt werden:

- ✓ Was ist der Zweck des sozialen Netzwerkes? Was kann man als Nutzer machen?
- ✓ Wie viele Nutzer hat das soziale Netzwerk in der Schweiz? Wie viele weltweit?
- ✓ Wem gehört das soziale Netzwerk? Welche Person(en)/Firma steckt dahinter?
- ✓ Wie kann man sich mit anderen Nutzern verbinden? Wie kann man in Kontakt treten?
- ✓ Welche Inhalte können mit anderen Nutzern geteilt werden?
- ✓ Wie viele Schülerinnen und Schüler in der Klasse nutzen dieses soziale Netzwerk?
- ✓ Was geschieht mit den Daten, wenn sie einmal hochgeladen wurden?
- ✓ Kann man seinen Account auch wieder löschen? Was geschieht dann mit den Daten?
- ✓ Zusätzliche interessante Informationen zu eurem sozialen Netzwerk

Sammelt die Informationen zuerst auf einem Notizblatt und ordnet sie anschliessend.
Gestaltet danach euer Plakat.



Hilfreiche Links bei der Suche nach Informationen:

<https://alike.ch/soziale-netzwerke-in-der-schweiz-die-liste/>

<https://hosting.1und1.de/digitalguide/online-marketing/social-media/die-wichtigsten-social-media-plattformen/>

Bildquelle: Sputnik Deutschland

<https://de.sputniknews.com/politik/20161217313803946-deutschland-sozialnetze-fake-news-strafen/>



Lösungsvorschläge

Arbeitsblatt «Soziale Netzwerke»

individuelle Lösungen der SuS, je nach gewähltem Netzwerk

Sollten innerhalb der Klasse noch weitere Netzwerke genutzt werden, können diese in der Auswahlliste ergänzt werden.

Arbeitsblatt «Sichere Passwörter»

Kriterien für ein sicheres Passwort

Notiere in der unten stehenden Liste, welche Kriterien ein sicheres Passwort gemäss www.passwortcheck.ch erfüllen muss.

<i>Grossbuchstaben</i>	<i>Kleinbuchstaben</i>
<i>Zahlen</i>	<i>Sonderzeichen</i>
<i>Länge des Passwortes</i>	<i>Zeichen im Wörterbuch</i>
<i>ein anderes Passwort für jeden Account</i>	<i>nie «Passwort» oder «12345» benutzen</i>
<i>keine Kombinationen, die mit der eigenen Person zu tun haben</i>	<i>keine Wörter aus dem Lexikon</i>
<i>Tipp: Denk dir einen Satz aus und gestalte aus den Anfangsbuchstaben ein Passwort (z. B. Ich kenne 23 oder 24 Personen aus meiner Klasse persönlich = Ik23o24PamKp)</i>	

Anregung, wie die Aufgabe gelöst werden könnte

Für die Bearbeitung beider Arbeitsblätter ist ein Zugang zum **Internet** notwendig.

Zum einen, um Informationen über das gewählte soziale Netzwerk zu sammeln, zum anderen, um das eigene und das kreierte Passwort zu kontrollieren und die Hinweise für ein sicheres Passwort nachzuschlagen.

Da die SuS nur kurze Eingaben tätigen müssen, kann ggf. auch mit Tablets oder Mobiltelefonen gearbeitet werden.

Chat/Foren

Arbeitsauftrag	<p>Die SuS diskutieren anhand eines Zeitungsartikels über Gefahren von sozialen Netzwerken.</p> <p>Die SuS entwerfen ein Rollenspiel, bei welchem verschiedene Personen aus dem Artikel zur Sprache kommen sollen.</p> <p>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.</p>
Ziel	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • SuS können mittels Medien kommunizieren und dabei die Sicherheits- und Verhaltensregeln befolgen. (MI.1.4c)
Material	<ul style="list-style-type: none"> • 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 [@tagesanzeiger](#) 09.05.2017



«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.



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>



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 Aufhängen 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

Cybermobbing

Arbeitsauftrag	<ul style="list-style-type: none"> • SuS tauschen sich in Kleingruppen über Erfahrungen mit Cybermobbing aus. • SuS informieren sich mithilfe der Merkblätter zum Thema Cybermobbing. • SuS gestalten ein Rollenspiel, in dem sie eine Situation und deren Lösung darstellen. • LP zeigt rechtliche Konsequenzen auf.
Ziel	<ul style="list-style-type: none"> • Die SuS reflektieren ihre Kenntnisse über Cybermobbing und vertiefen diese mithilfe der Informationen auf den zur Verfügung gestellten Unterlagen. • Die SuS kennen die rechtlichen Folgen von Cybermobbing.
Lehrplanbezug	<ul style="list-style-type: none"> • SuS können Folgen medialer und virtueller Handlungen erkennen und benennen (z. B. Identitätsbildung, Beziehungspflege, Cybermobbing). MI.1.1c
Material	<ul style="list-style-type: none"> • Arbeitsblatt «Cybermobbing» • Ein Computer oder Tablet pro Gruppe, alternativ: ausgedruckte Informationen der Webseiten.
Sozialform	Gruppenarbeit/Einzelarbeit/Plenum
Zeit	45 Minuten

In Zusammenarbeit mit **EDÖB** und **Jugend und Medien**

Zusätzliche Informationen:

- Die Informationen der Webseiten, welche auf dem Arbeitsblatt aufgeführt wurden, können den SuS auch in ausgedruckter Form abgegeben werden. Andernfalls können die SuS mithilfe von Computern oder Tablets die Informationen direkt auf den Homepages abrufen.
- Die rechtlichen Konsequenzen können den SuS mündlich durch die Lehrperson vermittelt werden. Dabei hilft die Broschüre von der Schweizerischen Kriminalprävention SKP «Cybermobbing – alles, was Recht ist» <https://www.skppsc.ch/de/wp-content/uploads/sites/2/2016/12/rechtcybermobbing.pdf> Wichtig ist dabei, darauf hinzuweisen, dass bei Beschimpfung, übler Nachrede, Verleumdung etc. neben den strafrechtlichen Konsequenzen auch zivilrechtlich gegen Täter vorgegangen werden kann. So kann dem Opfer ein Schadenersatz oder Genugtuung zugesprochen werden. Ebenso besteht das Recht auf Berichtigung falscher Inhalte, welches beim «Verursacher» eingefordert werden kann. Empfohlen wird deshalb, in konkreten Situationen zuerst das Gespräch mit dem «Verursacher» zu suchen (eventuell unter Einbezug einer Vermittlungsperson, z. B. Lehrperson) und diesen aufzufordern, die Persönlichkeitsverletzung zu beheben bzw. den Schaden wiedergutzumachen.



Cybermobbing

Diskussion



**Diskutiert in der Gruppe eure Erfahrungen mit Cybermobbing.
Wann spricht man von Cybermobbing?
Kennt ihr jemanden, dem dies widerfahren ist?
Wie kommt es zu Cybermobbing? Was sind Auslöser?
Wie fühlen sich die betroffenen Personen?
Was kann man tun, wenn man selber zum Opfer von Cybermobbing wird?**

Recherche



**Informiert euch anhand der unten aufgeführten Merkblätter und Webseiten über das Thema Cybermobbing.
Haltet die wichtigsten Erkenntnisse schriftlich fest.**

Seite der EU zu Cyberbullying
<http://keepcontrol.eu/?lang=d>

Seite der Europäischen Union zum Thema «Cybermobbing»
<http://www.klicksafe.de/themen/kommunizieren/cyber-mobbing/>

Cybermobbing, Games, Smartphones und Co.? Medienkompetenz – Tipps im sicheren Umgang mit digitalen Medien. Broschüre der nationalen Plattform «Jugend und Medien» (Seite 23)
https://www.jugendundmedien.ch/fileadmin/user_upload/Angebote/FAQ_Medienkompetenz_dt_2015_Web.pdf

Das halte ich fest:



Aufgabe

**Überlegt euch in der Gruppe selber eine Situation, in welcher es zu Cybermobbing kommt.
Spielt der Klasse anschliessend die Situation vor.**

Vorgaben für das Rollenspiel:

Personen

- Täter (mehrere)
- Opfer
- Mitläufer
- evtl. Eltern
- evtl. Lehrperson
- evtl. weitere Personen

Ablauf

- Vorgeschichte (Wie kommt es zu der Cybermobbing-Situation?)
- Ablauf des Cybermobbings (Was geschieht? Wer macht was?)
- Auflösung (Wie wird die Situation gelöst? Wie verhalten sich Täter und Opfer?)



Rechtliche Konsequenzen von Cybermobbing:

Jugend und Medien «Alles, was Recht ist»

http://www.jugendundmedien.ch/fileadmin/user_upload/2_Chancen_und_Gefahren/Cybermobbing_AlleswasRechtist_DE_10055.pdf

Bildquelle: Epochtimes.de
http://www.epochtimes.de/assets/uploads/2015/03/Cyber_Mobbing_Illu_Christian_Schlierkamp-640x427.jpg

Smartphones

Arbeitsauftrag	<ul style="list-style-type: none"> • SuS informieren sich, welche Daten in einem Smartphone anfallen. • SuS recherchieren anhand des Arbeitsblattes, wie sie ihre Daten auf dem Smartphone möglichst sicher schützen können. • SuS präsentieren ihre Lösungen der Klasse.
Ziel	<ul style="list-style-type: none"> • Die SuS können erklären, welche Daten auf einem Smartphone anfallen. • Die SuS kennen die Möglichkeiten, mit welchen sie ihre Daten auf dem Smartphone sicher schützen können.
Lehrplanbezug	<ul style="list-style-type: none"> • SuS können alleine und in Arbeitsteams mit medialen Möglichkeiten experimentieren und sich darüber austauschen. (MI.1.3h)
Material	<ul style="list-style-type: none"> • ein Computer pro Gruppe • Arbeitsblatt «Smartphones» • Smartphones der SuS
Sozialform	Plenum/Gruppenarbeit
Zeit	20 Minuten

Zusätzliche Informationen:

- Innerhalb der Gruppenarbeit sollen die SuS auch Zeit zum Recherchieren und Suchen haben. Dabei können auch weitere Webseiten hinzugezogen werden.
- 10 goldene Regeln zum Thema «Smartphone Sicherheit» (PC-Magazin.de)
<http://www.pc-magazin.de/bildergalerie/smartphone-sicherheit-tipps-galerie-3197166-118531977.html>



Diskussion



Diskutiert in eurer Gruppe, welche Massnahmen ihr treffen könnt, um die Daten in eurem Smartphone besser zu schützen. Dabei könnt ihr auch die Links unten verwenden, um zusätzliche Informationen zu erhalten.

Links

- Sicher unterwegs (Bluewin):
<https://www.bluewin.ch/de/digital/redaktion/2017/17-02/mit-diesen-apps-wird-das-smartphone-sicherer.html>
- Sicherheit: Wie schütze ich das Smartphone (Klicksafe.de):
<http://www.klicksafe.de/themen/kommunizieren/smartphones/sicherheit-wie-schuetze-ich-das-smartphone/>
- Apps und Datenschutz (Klicksafe.de):
<http://www.klicksafe.de/themen/kommunizieren/apps/apps-datenschutz/>
- Smartphone sicher (Handysektor.de)
<https://www.handysektor.de/hacker-sicherheit/smartphone-sicher.html>
- Diebstahlschutz (Handysektor.de)
<https://www.handysektor.de/hacker-sicherheit/diebstahlschutz.html>
- Privatsphäre auf dem Smartphone (Androidpit.de)
<https://www.androidpit.de/tipps-sicherheit-datenschutz-smartphone>
- eigene gefundene Webseiten



Lösungsvorschläge:

- 1. Durchsuche dein Smartphone und schreibe alle Daten über dich und andere Personen, welche sich darauf finden, in die unten stehenden Kärtchen.**

Die ausgeschnittenen Kärtchen mit den gefundenen Daten können in einer Auslegeordnung auf einem Tisch oder an der Wandtafel bzw. einem White Board oder einer Pinnwand gesammelt und gruppiert werden. So erhalten die SuS einen Überblick über die Vielfalt der abgespeicherten Daten.

- 2. Schreibt die fünf wichtigsten Regeln für den Schutz eurer Daten im Smartphone in die unten stehende Liste. Präsentiert diese anschliessend der Klasse.**

individuelle Lösungen der SuS

Tipps rund um das Thema Smartphone und Sicherheit finden sich auch im Informationsdossier, welches zu dieser Lektionsreihe gehört, im entsprechenden Kapitel.

Ausserdem findet man bei PC-Magazin.de 10 goldene Regeln, welche mit Screenshots in einer Galerie präsentiert werden. Diese könnten auch via Beamer mit den Lösungen der SuS verglichen werden.

<http://www.pc-magazin.de/bildergalerie/smartphone-sicherheit-tipps-galerie-3197166-118531974.html>

Tipps:

- nicht mehr benutzte Apps deinstallieren*
- Berechtigungen der Apps überprüfen und einschränken; nur Funktionen aktiviert lassen, die man tatsächlich braucht (benötigt z. B. eine App Zugriff auf Standortdaten oder persönliche Kontakte?)*

Konkrete Situationen

Arbeitsauftrag	<ul style="list-style-type: none"> • SuS spielen das «Cyber-Game» in Vierer- oder Fünfergruppen. • Die Anzahl der zu spielenden Situationen wird von der LP festgelegt. • Anschliessend werden die umstrittensten Situationen in der Klasse diskutiert.
Ziel	<ul style="list-style-type: none"> • SuS können bisher Gelerntes reflektieren und im Spiel konkret anwenden. • SuS diskutieren die Situationen in der Gruppe und können ihre Meinungen begründen.
Lehrplanbezug	<ul style="list-style-type: none"> • SuS können Chancen und Risiken der Mediennutzung benennen und Konsequenzen für das eigene Verhalten ziehen (z. B. Vernetzung, Kommunikation, Cybermobbing, Schuldenfalle, Suchtpotenzial). (MI.1.1e)
Material	<ul style="list-style-type: none"> • Spielanleitung «Cyber-Game» • Aktionskarten «Cyber-Game»
Sozialform	Plenum oder Gruppenarbeit
Zeit	fünf Minuten pro Aktionskarte

Zusätzliche Informationen:

- Zusätzlich können auch die Online-Situationen von www.thewebsters.ch verwendet werden, um die Aktionskarten zu ergänzen.
- Auf www.webfail.at finden sich weitere witzige «Fails», also peinliche oder zum Nachdenken anregende Internet-Beiträge. Einige standen den in diesem Spiel verwendeten Karten Modell, auch wenn sie leicht verändert wurden. Es finden sich aber haufenweise Posts, Einträge, Dialoge etc., die zum Schmunzeln anregen oder zu denken geben. Diese können als Grundlage für Diskussionen oder als Einstieg in die Lektion verwendet werden.



Cyber-Game



Aufgabe

Lest die Informationen zum Cyber-Spiel durch und spielt das Spiel in Vierer- oder Fünfergruppen.

Spielanleitung

Das Spiel besteht aus verschiedenen Aktionskarten, die eine konkrete Situation beschreiben oder einen Post darstellen. Wer am Zug ist und eine Karte vom Stapel nimmt, muss die Frage(n) möglichst genau beantworten und seine Antwort gut erklären und begründen.

Die Mitspieler beobachten und beurteilen die Ausführungen des Spielers, der am Zug ist.

Anschliessend werden die Ausführungen von den Mitspielern bewertet. Die Punktvergabe muss begründet werden können.

Punkte

- 3 Punkte Die Äusserungen des Spielers am Zug sind ausführlich und können von den Mitspielern nicht ergänzt werden.
- 2 Punkte Die Äusserungen des Spielers am Zug sind ausführlich. Es finden sich aber zusätzliche Gedanken.
- 1 Punkt Die Äusserungen des Spielers am Zug sind zwar korrekt, werden aber nicht begründet oder sind lückenhaft.
- 0 Punkte Die Mitspieler sind sich einig, dass die Ausführungen des Spielers am Zug falsch sind.

Spielende

Nach einigen Runden (die Rundenzahl wird vorher bestimmt) werden die Punkte zusammengezählt. Der Gewinner hat die Aufgabe, die drei umstrittensten Karten innerhalb der Gruppe zu bestimmen.



Diskussion

Die umstrittensten Karten jeder Gruppe werden in der Klasse diskutiert.



Link / Video

Auf www.thewebsters.ch findest du weitere Situationen und Geschichten rund um das Internet und seine Gefahren.



Aktionskarte
9



Nina
Kann mir jemand einen Gefallen tun? Bin gerade in den USA und sollte eine wichtige E-Mail von meinem neuen Vermieter erhalten. Der wollte mir einen neuen Vertrag schicken und weiss nicht, dass ich weg bin. Kann ihm jemand antworten, dass ich erst in 3 Wochen zurückkomme? DANKE!
Gefällt mir Kommentieren Gestern um 22:00

Mike Klar, kann ich machen.
Gefällt mir Kommentieren Gestern um 22:00

Nina Super, vielen Dank. Meine E-Mail Adresse ist nina.supergirl@mail.ch, mein Passwort ist nina445. Der Vermieter heisst Paul S.
Gefällt mir Kommentieren Gestern um 22:00

Was ist problematisch an dieser Situation?
Was muss Nina nun befürchten?
Erkläre und begründe deine Antwort.

Aktionskarte
10



Du erhältst folgende E-Mail:

*Sehr geehrter Paypal-Kunde
Wir führen zurzeit regelmässig anfallende Wartungsarbeiten an unserem Sicherheitssystem durch. Ihr Konto wurde nach dem Zufallsprinzip für diese Arbeiten ausgewählt. Sie werden dafür durch mehrere Webseiten geführt, auf denen Sie Ihre Angaben bestätigen müssen.
Bitte bestätigen Sie Ihre Kontoangaben, indem Sie die entsprechenden Daten auf einer der folgenden Seiten eingeben. Rufen Sie dazu folgende Webseite auf:
<https://www.paypal.com/cgi-bin/webscr?=login.run>
Bitte bestätigen Sie die Kontoangaben möglichst bald, um eine Unterbrechung des Services zu vermeiden.
Sollten Sie Ihr Konto nicht aktualisieren, wird die Nutzung dieses Services eingeschränkt.*

*Vielen Dank!
Ihr Paypal-Team*

Was ist problematisch an dieser Situation?
Wie reagierst du auf die E-Mail?
Erkläre und begründe deine Antwort.

Aktionskarte
11



Dein bester Freund zeigt dir auf seinem Handy ein paar neue Youtube-Videos.

Das letzte Video zeigt, wie zwei ältere Schüler einen jüngeren bedrängen, ihn schlagen und mit den Füssen nach ihm treten.

Was ist das Problem am Verhalten deines Freundes?
Wie reagierst du?
Erkläre und begründe deine Antwort.

Aktionskarte
12



Du erhältst folgende E-Mail:

*Was ist besser als ein 400Eur Willkommens-Bonus? Ein bis zu 400EUR Einzahlungs-Bonus, der auf Ihrem Konto gutgeschrieben wird!
Neue Spieler sind nur Sekunden von der Action entfernt, wenn sie sich im Virtual Vegas Players Club anmelden. Eröffnen Sie einfach Ihr neues Konto, machen Sie Ihre ersten Einzahlungen und Sie werden das Geld sofort sehen!
Mit bis zu 400 EUR Geld vom Haus zu spielen gibt Ihnen die Freiheit, die erstaunlichen neuen Spiele und die genialen Live Dealer Erlebnisse auf unserer Webseite zu entdecken. Probieren Sie etwas, was Sie vorher noch nie gespielt haben, oder geniessen Sie einfach die vielen alten Favoriten, die wir anbieten.
Wir verschenken Geld, also schnappen Sie es sich! Registrieren Sie sich noch heute unter:
<http://www.web-vegasvip.ne/de>*

Was ist problematisch an dieser E-Mail?
Wie reagierst du auf die Nachricht?
Erkläre und begründe deine Antwort.



Lösungsvorschläge zu den Aktionskarten

1. *Fotos, auf denen jemand allzu leicht bekleidet ist, sind dann heikel, wenn sie ins Internet gestellt werden und zwar unabhängig davon, ob deine Freundin das Hochladen akzeptiert oder nicht. Bilder von dir beim Tennis spielen und in der Landschaft sind an sich unproblematisch, solange sich nicht andere Personen darauf befinden. Eine Gefahr kann das Hochladen von Urlaubsfotos dann darstellen, wenn sie unmittelbar hochgeladen werden und auf eine längere Abwesenheit schliessen lassen. Einbrecher könnten erfahren, dass du nicht zu Hause bist. Gib nicht unbedacht zu viele Informationen preis.*
2. *Du veröffentlichst erstens, dass du eine Woche lang in der Regel alleine zu Hause bist; sozusagen eine Einladung für Menschen mit krimineller Neigung. Ausserdem gibst du deine Abwesenheit bekannt. Einbrecher könnten erfahren, dass du nicht zu Hause bist. Gib nicht unbedacht zu viele Informationen preis.*
3. *Dies ist ein klarer Fall von Cyber-Mobbing: Erstelle Bildschirmfotos als Beweis. Eine angemessene Reaktion muss gut überlegt sein, da sie auch Konsequenzen für dich haben kann. Trotzdem – in so einem Fall solltest du Zivilcourage zeigen: Wende dich an eine Vertrauensperson und – je nach Schwere des Falls – an die Polizei. Hast du Angst vor einer Reaktion deines Mitschülers, kannst du die Behörden auch anonym kontaktieren.*
4. *E-Mails können heute leicht gefälscht werden, die Adressen sehen dann so aus, als ob sie von Bekannten stammen. Wenn du der Sache misstraust, solltest du unbedingt darauf verzichten, auf den Link zu klicken. Viren, Trojaner oder andere «Malware» könnten sich auf deinem Computer einnisten. Am besten fragst du deinen Freund, ob er dir die E-Mail wirklich geschickt hat.*
5. *Adi hat sich unerlaubterweise Zugang zu einem fremden Netzwerk verschafft. Dies stellt eine Straftat dar. Fab hat Adi zur Weiterverbreitung gestohlener Daten aufgefordert. Auch das kann juristische Folgen haben. Ein klärendes Gespräch mit einer Aufforderung zur Wiedergutmachung dürfte das Minimum sein. Je nach Beziehung zu den beiden kann das Verhalten der beiden auch juristische Folgen haben. Der Nachbar muss sein Verhalten bezüglich Passwörtern überprüfen und in Zukunft sichere verwenden. Ausserdem müsste er genaue Informationen einholen, welche Daten ihm abhandengekommen sind.*
6. *Alle Personen, die auf den Bildern erkennbar sind, muss Ines um Erlaubnis bitten. Eine Gefahr kann das Hochladen von Urlaubsfotos dann darstellen, wenn sie unmittelbar hochgeladen werden und auf eine längere Abwesenheit schliessen lassen. Einbrecher könnten erfahren, dass Ines und die anderen auf dem Bild erkennbaren Personen nicht zu Hause sind. Gib nicht unbedacht zu viele Informationen preis.*
7. *Pauls Fehler ist offensichtlich: Er hat sein Handy seinem Bruder überlassen. Geräte, die eine solche Konzentration an persönlichen Daten aufweisen, überlässt man am besten niemandem. Mara hat wohl etwas vorschnell reagiert und sich nicht an die Netiquette gehalten. Emotionale und sehr private Äusserungen haben in sozialen Netzwerken nichts zu suchen.*
8. *Alice verstösst gegen «goldene Regeln» im Chat: Man soll sich nicht mit Menschen aus einem Chat treffen, schon gar nicht alleine. Ausserdem soll man misstrauisch sein, weil die anonymisierte Kommunikation im Chat Täuschungen fördert. Und wenn man den Chatpartner trotzdem treffen will, ist es klar, dass man das Gegenüber nicht anlügen sollte ... Eine Erklärung hätte vor einem Treffen abgegeben werden müssen.*
9. *Persönliche Informationen wie E-Mail-Adressen, insbesondere in Verbindung mit dem dazugehörigen Passwort, gehören nicht in die Öffentlichkeit und somit auch nicht auf Facebook oder ein anderes soziales Netzwerk. Jede Person, welche Ninas Meldungen ansehen kann, hat nun die Möglichkeit, sich in ihren E-Mail-Account einzuloggen. Sollten noch weitere Dienste mit dieser E-Mail-Adresse verknüpft sein, können auch diese missbraucht werden. Falls Nina ihre Meldungen nicht nur für Freunde, sondern für alle Nutzer von Facebook zugänglich gemacht hat, ist der Kreis der möglichen Drittpersonen, welche auf ihr Konto zugreifen könnten, um ein Vielfaches grösser.*
10. *Die E-Mail erscheint echt, weil sie auf den ersten Blick vertrauenswürdige Links enthält. Ein seriöses Finanzinstitut verlangt keine derartigen Aktionen von Kunden. Der elektronische Briefverkehr kann relativ einfach gefälscht werden (Banken und andere Finanzinstitute sind von Phishing-Attacken besonders betroffen). Bei E-Mails, die die Finanzen betreffen, gilt es generell, sehr vorsichtig zu sein und sich abzusichern, bei Unsicherheit z. B. mit einem klärenden*



Telefonat. Verdächtige Links sollten auf keinen Fall angeklickt und angehängte Dateien nicht geöffnet werden. Dadurch können Viren, Trojaner oder andere «Malware» auf deinen Computer gelangen.

- 11. Dein Freund verbreitet Gewalt-Videos. Distanziere dich davon. Handelt es sich bei den Schülern auf dem Video um Leute aus deinem Umfeld, musst du das Gespräch mit einer Vertrauensperson suchen. Cyber-Gewalt ist keine Bagatelle!*
- 12. Mit einem unglaublich gut klingenden Angebot will man dich dazu bringen, auf einen Link zu klicken. Solche E-Mails – die übrigens oft in schlechtem Deutsch verfasst sind, was aber nicht heisst, dass es nicht auch «fehlerfreie» Spam-Mails gibt – müssen gelöscht werden, am besten ungeöffnet, wenn man sie schon im Betreff als Spam identifiziert. Niemals unbekannte Links anklicken. Meist – aber nicht immer – passieren solche Nachrichten den Spam-Filter nicht und sie landen im Spam-Ordner. Wahrscheinlich müsstest du dich auch fragen, ob du jemandem deine E-Mail-Adresse gegeben hast, ob du auf problematischen, unseriösen Webseiten surfst und ob du dein Surf-Verhalten überdenken musst. Lösche auf jeden Fall zwischendurch die Cookies in deinem Web-Browser.*
- 13. Sandro, Domi und Nina verletzen die Würde ihres Lehrers. Sie stellen ihn bloss, indem sie – natürlich ohne Einwilligung – Fotos von ihm ins Netz stellen. (Allfällige) Freundschaft in Ehren: Wer hier nur zuschaut, macht sich mitschuldig. Erstelle ein Bildschirmfoto und sprich mit einer Vertrauensperson über das weitere Vorgehen. Informiere deinen Lehrer.*
- 14. Entschuldige dich in aller Form bei deinem Lehrer. Versichere ihm, dass dies ein einmaliger Ausrutscher war und nicht wieder vorkommen wird. Der Lehrer fühlt sich berechtigterweise belogen und verliert ein gewisses Mass an Vertrauen in dich. Es gilt, Prioritäten zu setzen: Man kann nicht krank sein und nicht zur Schule erscheinen, aber Zeit zum Feiern haben.*
- 15. Wird Daves Passwort geknackt, läuft er – die sehr wahrscheinliche – Gefahr, dass alle seine Konten manipuliert werden. Er verliert die Kontrolle, nicht nur über die Konten, sondern über sämtliche Daten, die auf den betroffenen Plattformen hinterlegt wurden. Dave muss in Zukunft sichere und unterschiedliche Passwörter verwenden.*
- 16. Mit diesem Hinweis öffnet Selim Einbrechern fast eigenhändig Tür und Tor ... Derartige Informationen öffentlich zu machen, ist fahrlässig. Sie gehören nicht ins Netz. Ansonsten weiss jedermann, dass das Haus/die Wohnung zwei Wochen lang leer steht.*
- 17. Jemand ist in das Konto von Pauline eingedrungen (z. B. indem er das Passwort ausfindig gemacht hat) und hat ihr Passwort geändert. Tipp: Keine einfachen Passwörter wie 123456, Namen von Personen, Haustieren etc. verwenden, die sich z. B. auf dem Facebook-Profil finden können.*