Einführung Datenschutz

Arbeitsauftrag	• 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. Die anschliessende Diskussion kann in Partnerarbeit, Gruppenarbeit oder im Plenum geführt werden.
Ziel	• 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	• MI.2.3n: «Die SuS können die Risiken unverschlüsselter Datenübermittlung und -speicherung abschätzen.»
Material	• Auftragsblatt «Diskussion – besonders schützenswerte Daten» • Screenshots «Privatsphäre-Einstellungen» • Arbeitsblatt «Tabelle»
Sozialform	Einzelarbeit/Partnerarbeit/Plenum
Zeit	60 Minuten

Zusätzliche Informationen:

- Durch die Abgabe der Printscreens, 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.

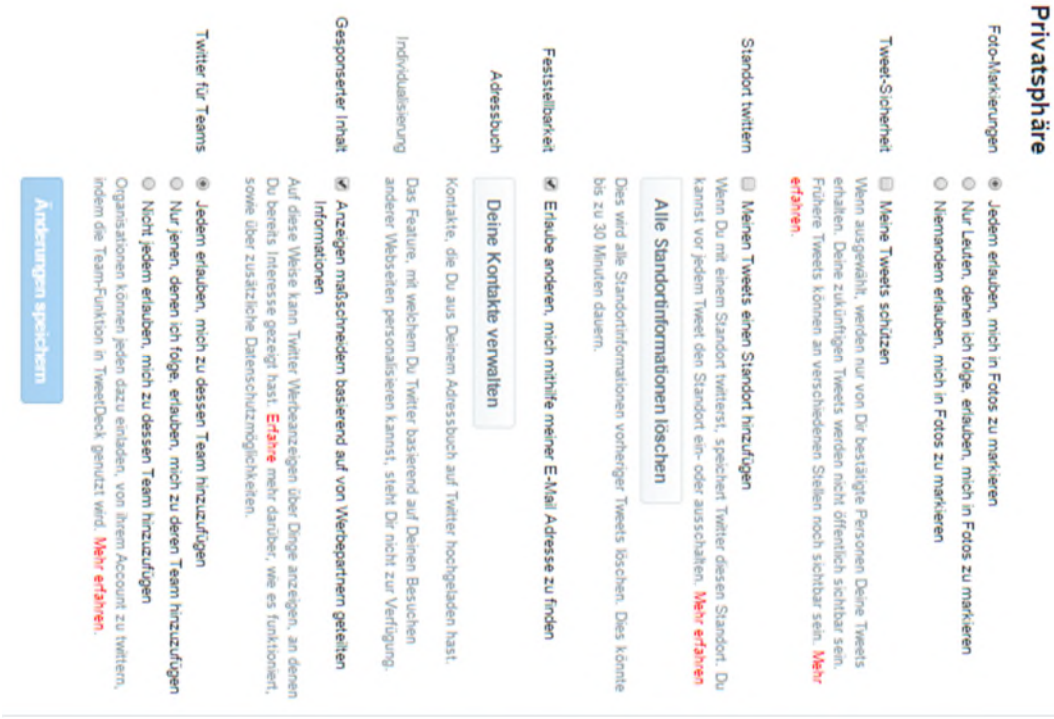
Bildquelle: Wepushbuttons
https://wepushbuttons.com.au/wp-content/uploads/2013/04/social-media-list.jpg

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

Privatsphäre-Einstellungen und Werkzeuge

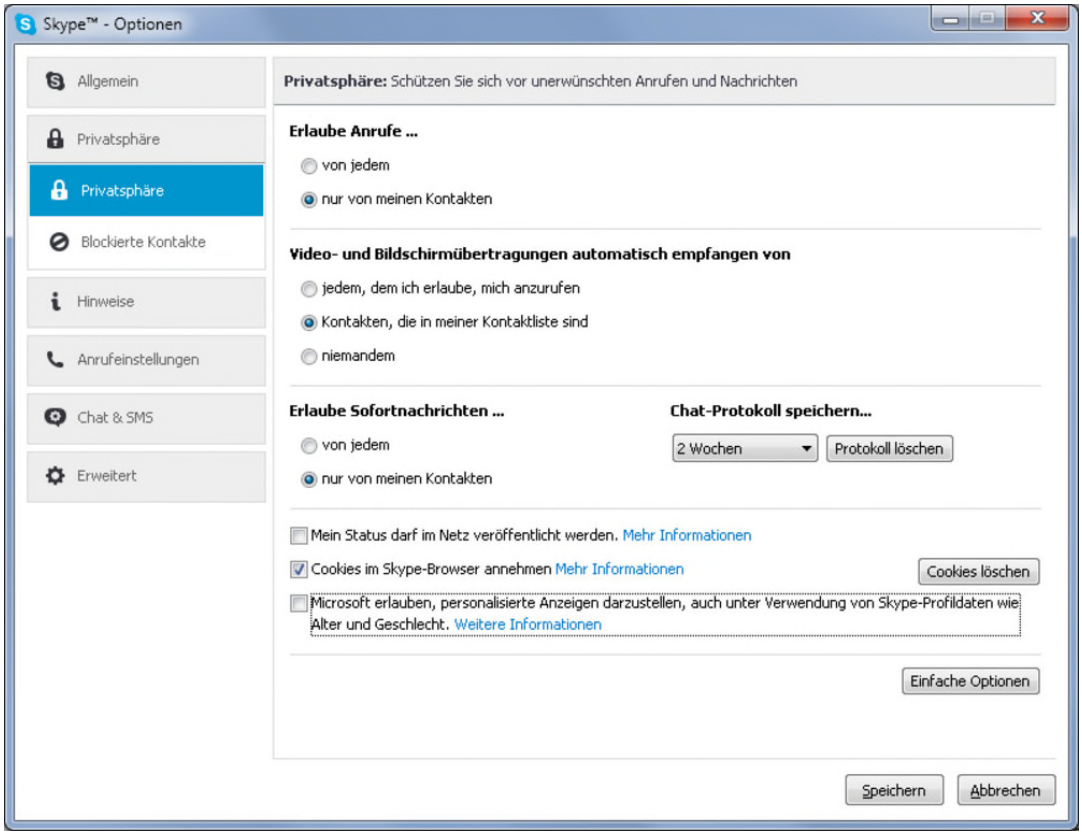
Wer kann meine Inhalte sehen?	Wer kann deine zukünftigen Beiträge sehen?	**Freunde**	Bearbeiten
	Überprüfe alle deine Beiträge und Inhalte, in denen du markiert bist		Aktivitätenprotokoll verwenden
	Möchtest du die Zielgruppe für Beiträge einschränken, die du mit Freunden von Freunden oder öffentlich 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)



Beispiel 3: Snapchat-Privatsphäre-Einstellungen (Stand April 2018)

Beispiel 4: Skype-Privatsphäre-Einstellungen (Stand April 2018)



Wenn Daten in falsche Hände geraten …

Aufgabe
Wähle eine der folgenden Situationen aus und überlege dir, was anschliessend passieren könnte.
Notiere in Stichworten, wie die Fortsetzung deiner Meinung nach aussehen könnte.

1. Eine Schülerin schickt private Bilder in einen Gruppenchat. Diese zeigen sie im Ausgang, wo sie Alkohol trinkt, ausgelassen feiert und raucht.
2. Stephan ändert sein Profilbild. Auf dem Bild posiert er in der Umkleide des Fitnessstudios, im Hintergrund sieht man einen jungen Mann, der sich gerade umzieht.
3. Lea und ihr Freund tauschen gerne Bilder per Chat miteinander aus. Auf einigen Bildern sind beide unbekleidet. Nach einiger Zeit trennen sich die beiden im Streit.
4. Michael speichert seine Zugangsdaten für seine sozialen Netzwerke, sein Online-Konto und seinen E-Mail-Account in einer Cloud. Die Betreiber der Cloud haben ihren Standort allerdings nicht in der Schweiz und unterstehen damit auch nicht dem Schweizer Datenschutzgesetz.
5. Michelle nimmt während der Schule unbemerkt Fotos von ihren Mitschülerinnen und Mitschülern und ihrem Lehrer auf. Diese lädt sie anschliessend auf Instagram.
6. Philipp erhält eine Freundschaftsanfrage von einer unbekannten Person auf Instagram. Er nimmt diese an, obwohl er nicht weiss, wer sich hinter dem Profil versteckt.
7. Corinne erhält von einer unbekannten Nummer eine SMS mit der Aufforderung, ihre Bankdaten für eine Überprüfung anzugeben. Als Absender steht am Schluss der Nachricht «Ihre Bank».
8. Francesco hat ein neues Handy. Er überträgt die Inhalte seines alten Mobiltelefons auf das neue, vergisst aber, ein Passwort einzurichten. Einen Tag später lässt er das Handy im Bus liegen.

Fortsetzung …

……

……

……

……

……

Kannst du dir weitere Beispiele vorstellen, in welchen persönliche Daten in falsche Hände geraten und welche Probleme damit ausgelöst werden könnten?

……

……

……

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/belaestigungen#!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

Lösungsvorschläge

Arbeitsblatt «Wie sicher ist dein Account?»

➔ **individuelle Lösungen der Schülerinnen und Schüler**

Wichtig ist der Hinweis darauf, dass bei einigen sozialen Netzwerken die Privatsphäre-Einstellungen aktiv geändert werden müssen. So ist zum Beispiel bei Instagram das Profil grundsätzlich für jeden zugänglich. Will man es nur Freunden (Follower) zugänglich machen, muss man dies in den Privatsphäre-Einstellungen selber anpassen.
Siehe auch:
http://praxistipps.chip.de/privatsphaere-fuer-instagram-einstellen-so-klappts_12050

Arbeitsblatt «Wenn Daten in falsche Hände geraten …»

Mögliche Fortsetzungen und Diskussionsansätze:

Situation 1 *Die Fotos können aus dem Gruppenchat theoretisch an alle möglichen Personen verschickt und sogar im Internet publiziert werden. Dies kann beispielsweise zu Problemen mit den Eltern, mit dem Lehrbetrieb etc. führen.*

Situation 2 *Das Profilbild von Stephan ist, je nach Privatsphäre-Einstellung, für den anderen Benutzer sichtbar. Da Stephan eine weitere Person ohne ausdrückliche Einwilligung auf dem Bild abgelichtet und das Bild veröffentlicht hat, könnten sich daraus neben zivilrechtlichen auch strafrechtliche Konsequenzen ergeben. Dies insbesondere, da die andere Person beim Umziehen fotografiert wurde.*

Situation 3 *Sowohl Lea als auch ihr Ex-Freund haben keine Kontrolle darüber, was nach der Trennung mit den Bildern, welche sie sich gegenseitig geschickt haben, geschieht. Zum einen können die Bilder weiterverschickt und veröffentlicht werden, was sicher nicht im Sinne der fotografierten Person ist. Zum anderen verstossen sie gegen das Datenschutzgesetz und verletzen die Privatsphäre der anderen Person widerrechtlich und machen sich unter Umständen sogar strafbar, wenn sie die Bilder ohne die Einwilligung des anderen weiterverschicken oder veröffentlichen.*

Situation 4 *Da Michael seine Daten in einer ausländischen Cloud gespeichert hat, kann er nicht sicher sein, dass diese Daten auch nach schweizerischem Standard gesichert sind. Da es sich um vertrauliche Daten und Passwörter handelt, könnte Michael durch ein Abgreifen der Daten durch Unbefugte grosser Schaden entstehen.*

Situation 5 *Michelle nimmt die Bilder ohne Einwilligung der abgelichteten Personen auf und veröffentlicht diese anschliessend. Dadurch drohen ihr zivilrechtliche Konsequenzen.*

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*