

MEDIEN SICHER NUTZEN – NEUES UNTERRICHTSKONZEPT DER VERBRAUCHERZENTRALE RHEINLAND-PFALZ E.V.

Social Communitys – sicher vernetzt

Kontakt:

Verbraucherzentrale Rheinland-Pfalz e.V.
Telekommunikation und Digitale Medien
Seppel-Glückert-Passage 10
55116 Mainz

E-Mailadresse: telekommunikation@vz-rlp.de

Stand: Mai 2017

Inhalt

| | |
|--|----|
| Legende | 4 |
| 1 Soziale Netzwerke..... | 5 |
| 1.1 Sachinformation | 5 |
| 1.1.1 Soziale Netzwerke – wie ist die Lage? | 5 |
| 1.1.2 Wie unterscheiden sich die Anwendungen? | 6 |
| 1.1.3 Welche Bedeutung haben Daten?..... | 7 |
| 1.1.4 Wie öffentlich bin ich? | 8 |
| 1.1.5 Wie steht es mit Urheber- und Persönlichkeitsrechten in sozialen Netzwerken?..... | 9 |
| 1.1.6 Was bedeutet Datensparsamkeit?..... | 9 |
| 1.1.7 Was sind Privatsphäreinstellungen?..... | 10 |
| 1.1.8 Was sollte man über WhatsApp wissen?..... | 10 |
| 1.1.9 Datensicherheit: Wie wichtig sind gute Passwörter?..... | 11 |
| 1.1.10 Links und Materialien | 12 |
| 1.1.11 Mögliche Verknüpfung mit anderen Themen | 13 |
| 1.2 Erarbeitungsphase Schwerpunkt: Soziale Netzwerke und Instant Messenger..... | 13 |
| 1.2.1 Handyampel..... | 15 |
| 1.2.2 Clevere Netzwerker..... | 15 |
| 1.2.3 Was verrate ich von mir?..... | 16 |
| 1.2.4 Öffentlich oder privat? | 16 |
| 1.2.5 Unterrichtsgespräch: Das Netz vergisst nicht | 17 |
| 1.2.6 Check dein Profil, bevor es andere tun..... | 18 |
| 1.2.7 PC-Übung Ego-Googeln | 18 |
| 1.2.8 Unterrichtsgespräch WhatsApp-Statistik | 19 |
| 1.2.9 Sicheres Passwort..... | 20 |
| 1.2.10 PC-Übung Passwortprüfer (Fortsetzung von „Sicheres Passwort“) | 20 |
| 1.2.11 WhatsApp, Instagram & Co.: sicher in sozialen Netzwerken | 22 |

| | | |
|-------|--|----|
| 1.3 | Materialien | 23 |
| 1.3.1 | Handyampel..... | 24 |
| 1.3.2 | Arbeitsblatt Clevere Netzwerker (Kurzversion) | 25 |
| 1.3.3 | Arbeitsblatt Clevere Netzwerker (Langversion)..... | 26 |
| 1.3.4 | Vorlage Was verrate ich von mir?..... | 28 |
| 1.3.5 | Öffentlich oder privat? | 29 |
| 1.3.6 | Arbeitsblatt Sicheres Passwort..... | 34 |
| 1.3.7 | WhatsApp, Instagram & Co.: sicher in sozialen Netzwerken | 37 |

Legende

einfach (etwa Klassenstufe 4 und 5): ❶ ❷ ❸

mittel (etwa Klassenstufe 6 und 7): ❶ ❷ ❸

schwer (etwa Klassenstufe 7+): ❶ ❷ ❸

sprachlich leichter zugänglich: 👁

weiterführend (zur weiteren Beschäftigung mit dem Thema oder zur Binnendifferenzierung während des Unterrichts): 📖

externer Link: ➡

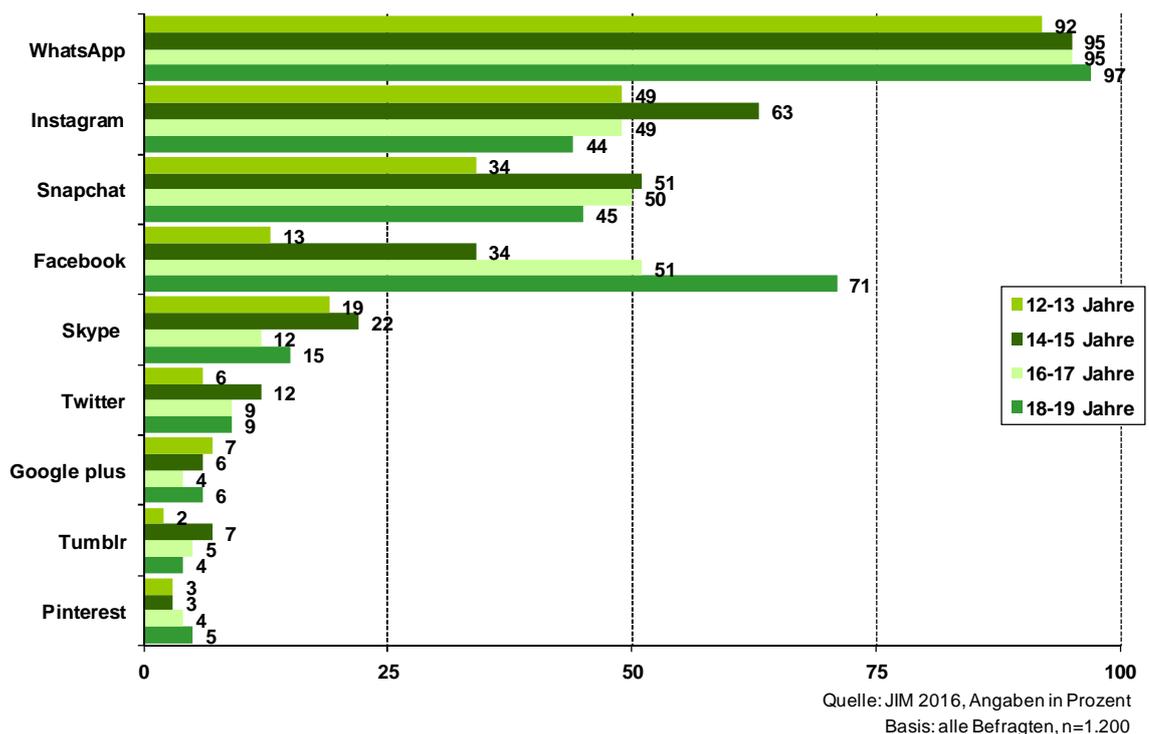
1 Soziale Netzwerke

1.1 Sachinformation

1.1.1 Soziale Netzwerke – wie ist die Lage?

Soziale Netzwerke – oft auch als Social Networks oder Social Communities bezeichnet – sind ein virtueller Ort des Austauschs und der Freundschaftspflege und ein wesentlicher Faktor der Internetnutzung. Möchte man WhatsApp in diese Gruppe einordnen, so ist der zu Facebook gehörende Dienst absoluter Spitzenreiter: Laut JIM-Studie 2016¹ nutzen 95 Prozent aller Zwölf- bis 19-Jährigen mindestens mehrmals pro Woche **WhatsApp**. 89 Prozent geben an, es täglich zu tun. Dahinter folgen mit etwas Abstand **Instagram**, **Snapchat** und **Facebook**. Die Dienste Twitter, Google plus, Tumblr oder Pinterest spielen eine weniger große Rolle.

Aktivitäten im Internet – Schwerpunkt: Kommunikation 2016
- täglich/mehrmals pro Woche -



Diese große Relevanz im Alltag von Kindern und Jugendlichen macht deutlich, wie wichtig eine Beschäftigung mit dem Thema ist. Denn ein kompetenter Umgang mit diesen Anwendungen bedeutet – fernab von reinen Bedienungsaspekten – zu wissen, wie man sich in solchen virtuellen Gemeinschaften souverän und sicher bewegt; und dazu gehört das Wissen um Risiken und Gefahren.

¹ Medienpädagogischer Forschungsverbund Südwest (Herausgeber): JIM 2016. Jugend, Information, (Multi-)Media. Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland. Stuttgart, 2016.

1.1.2 Wie unterscheiden sich die Anwendungen?

WhatsApp ist genau genommen kein soziales Netzwerk, sondern ein sogenannter Instant Messenger, der das Versenden unter anderem von Textnachrichten, Bildern, Videos und Sprachnachrichten ermöglicht. In erster Linie geht es hier also um Eins-zu-eins-Kommunikation von Smartphone zu Smartphone. Allerdings gibt es auch die Möglichkeit, sich in Gruppen mit mehreren WhatsApp-Nutzern auszutauschen. 95 Prozent der Zwölf bis 19-Jährigen nennen WhatsApp als eine ihrer drei Lieblingsapps auf dem Smartphone (JIM-Studie 2016, S. 30). Bei den Sechs- bis Siebenjährigen nutzen bereits 27 Prozent den Instant Messenger (KIM-Studie 2016², 35).

Anfang des Jahres 2014 übernahm Facebook den Dienst für eine Summe von 19 Milliarden US-Dollar (Quelle: ➔ www.heise.de; Stand: 2014). Mittlerweile ist die App für den Nutzer kostenlos (Stand: März 2017).

WhatsApp ist immer wieder aufgrund von Datenschutz- und Sicherheitsbedenken in der Kritik (siehe z.B. ➔ netzpolitik.org; Stand: September 2016). So hat der Dienst im August 2016 Schlagzeilen gemacht, da er sich in geänderten Nutzungs- und Datenschutzbestimmungen die Möglichkeit eingeräumt hat, Daten seiner Nutzer an Facebook weiterzugeben. Der Verbraucherzentrale Bundesverband klagt nun gegen das Unternehmen. (➔ www.verbraucherzentrale.de; Stand: Januar: 2017)

In dieser Aktualisierung der Nutzungsbedingungen wurde auch das Nutzungsalter von 16 auf 13 Jahre gesenkt. Allerdings mit der Einschränkung: „bzw. so alt, wie es in deinem Land erforderlich ist, damit du berechtigt bist, unsere Dienste ohne elterliche Zustimmung zu nutzen“ (➔ [Nutzungsbedingungen WhatsApp](#); Stand: März 2017). Mehr zu dieser Diskussion gibt auf der ➔ [Seite von Klicksafe](#) (Direktlink).

Mehr zu WhatsApp auf ➔ Klicksafe.de.

Instagram ist der Name für eine App und gleichzeitig für die dahinter stehende Community. Der Fokus liegt hier auf der Veröffentlichung von Bild- und Videodateien. Über die App können Fotos und Videos aufgenommen, mit Filtern versehen und anderen Nutzern zugänglich gemacht werden.

Seit 2012 gehört der Dienst zu Facebook. Laut eigenen Angaben hatte das Unternehmen im Dezember 2016 600 Millionen Nutzer. 51 Prozent der Jugendlichen nutzen regelmäßig Instagram; täglich sind es 39 Prozent (JIM-Studie 2016; S. 31), allerdings sind darunter mehr Mädchen als Jungen. Die Registrierung und Nutzung von Instagram ist kostenlos. In den ➔ [Nutzungsbedingungen von Instagram](#) (Stand: März 2017) heißt es: „Du musst mindestens 13 Jahre alt sein, um den Dienst zu nutzen.“

Wie es bei sozialen Netzwerken üblich ist, wird eine Profilseite angelegt, auch ein „Abonnieren“ der Bilder von Freunden ist möglich. Die Voreinstellungen an der App sind öffentlich. Will man dies ändern, muss man selbst aktiv werden und die Privatsphäreinstellungen anpassen.

Mehr zu Instagram auf ➔ Klicksafe.de.

² Medienpädagogischer Forschungsverbund Südwest (Herausgeber): KIM 2016. Kindheit, Internet, Medien. Basisstudie zum Medienumgang 6- bis 13-Jähriger in Deutschland. Stuttgart, 2017.

Snapchat ist, ähnlich wie WhatsApp, ein Instant Messenger zur direkten Kommunikation. Mit der App lassen sich Bild- und Videonachrichten verschicken. Das Besondere der App ist, dass man die Sichtbarkeit der verschickten Nachrichten bestimmen kann: Ein Bild ist beispielsweise nur für wenige Sekunden sichtbar, bevor es sich von selbst löscht.

Diese Tatsache hat der App auch den Ruf einer Sexting-App eingebracht, da Jugendliche die vermeintliche Sicherheit des „Selbstzerstörungsmechanismus“ nutzten, um Inhalte mit erotischem oder freizügigem Inhalt zu versenden. Allerdings ist es technisch durchaus möglich, durch Screenshots Bilder auch dauerhaft zu speichern oder gelöschte Nachrichten wiederherzustellen.

Snapchat liegt in der Nutzungshäufigkeit bei Jugendlichen kurz hinter Instagram; laut Zahlen der JIM-Studie 2016 (S. 31) nutzen 45 Prozent der Zwölf- bis 19-Jährigen die App regelmäßig, 35 Prozent sogar täglich. Die App ist kostenlos; eine Registrierung ist laut Snapchat-➔ [Nutzungsbedingungen](#) (Stand: März 2017) nur für Personen über 13 Jahren erlaubt.

Die App Snapchat wurde im Jahr 2011 vom Unternehmen Snap Inc. gegründet. Die Übernahme-Angebote von Facebook wurden bislang abgelehnt.

Mehr zu Snapchat auf ➔ www.klicksafe.de.

Facebook ist im Vergleich zu den anderen Diensten fast schon ein Urgestein. Seit seiner Gründung im Jahr 2004 durch Mark Zuckerberg versteht es sich als soziales Netzwerk, das dazu dient, mit Personen aus dem realen Bekanntenkreis in Austausch zu treten. Mehr als eine Milliarde Menschen weltweit nutzen diesen Dienst.

Bei Jugendlichen verliert Facebook allerdings an Beliebtheit, vor allem bei den jüngeren Nutzern sind Apps wie Instagram und Snapchat wesentlich beliebter. Bei den 18- bis 19-Jährigen wird Facebook aber nach wie vor genutzt (JIM-Studie 2016, S. 31).

Facebook lässt sich kostenlos im Browser oder per App nutzen; um sich zu registrieren, muss man mindestens 13 Jahre alt sein. Nutzer unter 18 Jahren haben einen Minderjährigen-Account mit restriktiveren Privatsphäre-Einstellungen.

Bei Facebook erstellt man eine Profilseite über sich selbst; wer die Sichtbarkeit seiner Informationen und Inhalte beschränken will, muss dies in den Privatsphäre-Einstellungen tun.

Kritisiert wird das gleichnamige Unternehmen hinter dem sozialen Netzwerk immer wieder wegen undurchsichtiger Datenschutzregelungen. In jüngster Zeit richtete sich die Kritik auch gegen Facebooks Umgang mit sogenannten Fake News.

Mehr zu Facebook auf ➔ www.klicksafe.de.

1.1.3 Welche Bedeutung haben Daten?

All die genannten Dienste sind für die Nutzerinnen und Nutzer kostenlos, dennoch verdienen die dahinterstehenden Unternehmen Geld damit. Das kalifornische Unternehmen Facebook beispielsweise macht seinen Umsatz durch Werbung und virtuelle Güter; im Jahr 2016

betrug der Gesamtumsatz 27,6 Milliarden Euro (Quelle: ➔ youngdata.de, Stand: März 2017). Obwohl es manchmal anders wirkt, ist man als Nutzer oder Nutzerin nicht Kunde dieser Unternehmen, sondern das Produkt, das vermarktet wird. Je mehr über mich bekannt ist, je mehr Daten ein Unternehmen über mich gesammelt hat, umso passendere Werbung kann es mir präsentieren. Und je gezielter die Werbung, desto größer der Gewinn. Gleiches gilt für Google und andere Unternehmen. Daten sind die Währung, mit der wir im Internet bezahlen.

Auf Youngdata.de finden sich weitere Informationen beispielsweise zu ➔ [Facebook](#) und ➔ [Google](#).

1.1.4 Wie öffentlich bin ich?

Sich im Internet zu präsentieren und mit anderen zu kommunizieren übt eine große Faszination auf Jung und Alt aus. Es gibt viele Gründe, sich in sozialen Netzwerken zu beteiligen. Gerade für Kinder und Jugendliche werden viele Entwicklungsschritte auch digital begangen: Wer bin ich und wie möchte ich von anderen gesehen werden? Wie viele Freunde habe ich? Wie reagieren andere auf mich? Solche Fragen der Selbstfindung und Identitätsbildung lassen sich auch über soziale Netzwerke bearbeiten.

Gerade jüngere Nutzer sehen sich vor allem in Interaktion mit ihren Freunden und Bekannten. Dass aber je nach Einstellungen theoretisch die ganze Welt mitlesen kann, ist oft nicht präsent; schon gar nicht bewusst sind die Risiken, die damit verbunden sind.

Es gilt also, ein Bewusstsein dafür zu schaffen, was Privatsphäre und Öffentlichkeit konkret bedeuten, welche Bedeutung Daten für verschiedene Personen und Gruppen haben und welche Folgen die unachtsame Preisgabe von Informationen haben können.

Zum einen ist das natürlich die wirtschaftliche Verwertung von Daten, beispielsweise zu Werbezwecken wie dem Anzeigen von personalisierter Werbung. Zum anderen spielen aber auch Bild- und Persönlichkeitsrechte von anderen Personen eine Rolle.

In vielen sozialen Netzwerken gibt es Privatsphäreinstellungen, in denen man die Sichtbarkeit von Informationen und eingestellten Beiträgen anpassen kann. Oftmals ist voreingestellt, dass Informationen öffentlich sind; der Nutzer oder die Nutzerin muss selbst aktiv werden, um es zu ändern.

Problematisch ist auch, wenn Kinder und Jugendliche ein falsches Alter angeben: Bei Facebook beispielsweise haben 13- bis 17-Jährige spezielle Minderjährigen-Accounts mit strengeren Privatsphäreinstellungen. Wird ein Nutzer (für Facebook) 18, ändern sich diese Einstellungen automatisch in eine weniger restriktive Form (➔ [Hilfeseite Facebook](#)). Mit einem falschen Alter können nicht nur unter 13-Jährige in Facebook aktiv sein, sondern es können sich auch die Einstellungen ändern, ohne dass der Nutzer oder die Nutzerin auch wirklich volljährig wird. Eine wirksame Alterskontrolle gibt es bei den meisten sozialen Netzwerken nicht.

1.1.5 Wie steht es mit Urheber- und Persönlichkeitsrechten in sozialen Netzwerken?

Bilder spielen eine große Rolle in sozialen Netzwerken. Entweder passiv genutzt, indem man sich Bilder und Videos anschaut, oder aktiv, indem der Nutzer oder die Nutzerin selbst Bilder und Videos einstellt und teilt. Dabei kommt Persönlichkeits- und Urheberrechten eine wichtige Bedeutung zu (s. Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**).

Bilder, die ich nicht selbst gemacht habe, darf ich in der Regel nicht ohne Zustimmung des Urhebers bzw. Rechteinhabers veröffentlichen. In welchen Kontexten eine Veröffentlichung vorliegt, ist nicht immer eindeutig zu beantworten. Ein öffentliches Facebook- oder Instagram-Profil zählt aber mit Sicherheit dazu.

Auch bei selbst erstellten Bildern muss man vor der Veröffentlichung prüfen, ob alle Abgebildeten damit einverstanden sind. Bei unter 18-Jährigen müssen genau genommen auch die Eltern zustimmen. Dies gilt in dieser Form nicht für Personen des öffentlichen Interesses, für Versammlungen oder wenn Menschen auf einem Bild lediglich Beiwerk sind (z. B. Touristen vor dem Mainzer Dom).

1.1.6 Was bedeutet Datensparsamkeit?

Unter Datensparsamkeit versteht man, möglichst wenige Daten über sich und andere preiszugeben. Nicht bei jeder Registrierung ist es nötig, auch wirklich die eigene Adresse einzugeben. Auch bei Bildern sollte darauf geachtet werden, was online gestellt wird („Think before you post“), denn es gilt der Satz: „Das Internet vergisst nichts“: Je nach Nutzungsbedingungen eines Dienst werden dem Anbieter weitgehende Nutzungsrechte eingeräumt; auch privat lassen sich online gestellte Bilder vervielfältigen und weiterverbreiten.

In den Facebook-AGB steht beispielsweise „Für Inhalte, die durch Rechte am geistigen Eigentum geschützt sind, wie Fotos und Videos (IP-Inhalte), erteilst du uns ausdrücklich nachfolgende Genehmigung, vorbehaltlich deiner Einstellungen für Privatsphäre und Apps: Du gewährst uns eine nicht-exklusive, übertragbare, unterlizenzierbare, gebührenfreie, weltweite Lizenz für die Nutzung jedweder IP-Inhalte, die du auf bzw. im Zusammenhang mit Facebook postest (IP-Lizenz). Diese IP-Lizenz endet, wenn du deine IP-Inhalte oder dein Konto löschst; es sei denn, deine Inhalte wurden mit anderen geteilt und diese haben die Inhalte nicht gelöscht.“ (Quelle: ➔ [Facebook-AGB](#), Stand: 15.05.2017)

Auch Personalabteilungen haben ein Interesse daran, den Bewerber oder die Bewerberin schon vorab „kennenzulernen“. Gibt es öffentlich verfügbare Informationen im Internet über diese Person? Was lässt sich über sie herausfinden? (Auf die Spitze treibt diesen Sachverhalt ein Video von ➔ [netzdurchblick.de](#), das auch im Unterricht eingesetzt werden kann.

Ein Grundsatz sollte also sein, nur Dinge hochzuladen, die man auch fremden Menschen zeigen würde. Privatsphäreinstellungen sollten möglichst restriktiv genutzt werden; auch mit Pseudonymen zu arbeiten und nicht den echten Namen zu verwenden, ist im Sinne der Datensparsamkeit wünschenswert.

Weitere Datenschutztipps gibt es auf dem Jugendportal der unabhängigen Datenschutzbehörden des Bundes und der Länder sowie des Kantons Zürich:

➔ www.youngdata.de

Ein ➔ [Video vom Internet ABC](#) führt in die Thematik Datenschutz ein.

1.1.7 Was sind Privatsphäreinstellungen?

Die meisten Dienste und Anwendungen bieten auf ihren Seiten sogenannte Privatsphäreinstellungen. Hier lässt sich einstellen, wer welche Inhalte sehen darf. So gibt es beispielsweise bei Facebook oder Instagram die technische Möglichkeit, einzuschränken, wer das eigene Profil und die geposteten Inhalte sehen darf. Bei Facebook sind das beispielsweise „Freunde“, bei Instagram nur zugelassene „Follower“. Wer (und vor allem wie viele) diese Personen jeweils sind, liegt natürlich in der Hand des Nutzers bzw. der Nutzerin.

Bei WhatsApp lässt sich in den Privatsphäreinstellungen der „Zuletzt online“-Status ausschalten. Auch die Sichtbarkeit der Profilbilder lässt sich hier einschränken.

Weitere Tipps und Infos zu Privatsphäreinstellungen bei den jeweiligen Diensten:

- WhatsApp (➔ www.klicksafe.de)
- Instagram (➔ www.klicksafe.de und ➔ www.handysektor.de)
- Snapchat (➔ www.handysektor.de)
- Facebook (➔ www.klicksafe.de)

1.1.8 Was sollte man über WhatsApp wissen?

Die Zahlen sprechen für sich: Mehr als eine Milliarde Menschen weltweit nutzen den Instant Messenger WhatsApp. Der Dienst ist kostenlos und bietet eine ganze Reihe von verschiedenen Funktionen.

Gleichzeitig ist die Anwendung, die seit 2014 zu Facebook gehört, immer wieder in der Kritik. Zuletzt machte Facebook Ende August 2016 Schlagzeilen durch die Ankündigung, zukünftig die Telefonnummern der Nutzer an Facebook weiterzugeben. Auch wenn dieser Datenaustausch aufgrund der Proteste vorerst eingestellt wurde, vom Tisch ist diese Debatte noch nicht. Anfang 2017 hat der Verbraucherzentrale Bundesverband Klage gegen WhatsApp eingereicht.

Eine Ende-zu-Ende-Verschlüsselung ist mittlerweile in WhatsApp enthalten, allerdings weiß der Messengerdienst trotzdem sehr genau, wann wer mit wem in Kontakt ist. Diese sogenannten Metadaten sind für das Unternehmen sehr aufschlussreich.

Damit man seine Freunde in der WhatsApp-Kontaktliste findet, muss das Adressbuch des Smartphones an Server von WhatsApp Inc. weitergeleitet werden. Somit hat das Unternehmen die Daten von allen im Adressbuch gespeicherten Personen, selbst wenn diese vielleicht gar kein WhatsApp haben. Dies hat mit Datenverantwortung für andere zu tun, und ist auch im Hinblick auf deutsches Datenschutzrecht rechtlich schwierig.

Nutzt man WhatsApp, muss man sich bewusst sein, dass man vermarktet wird. Und dass die Tatsache, dass der Dienst kostenlos ist, nicht bedeutet, dass das Unternehmen Facebook kein Geld damit verdient. Im Gegenteil: Die Übernahmesumme in Milliardenhöhe zeigt, dass WhatsApp (bzw. die damit verfügbaren Daten) als sehr wertvoll angesehen wurde.

Es gibt eine Reihe von Programmen, die ähnlich wie WhatsApp funktionieren und ➔ [ernstzunehmende Alternativen](#) darstellen.

Abseits vom Datenschutz spielen auch Kettenbriefe und Spam im WhatsApp eine Rolle. Mit dem Hinweis auf vermeintliche Gutscheine oder neue WhatsApp-Funktionen wird zum Anklicken eines Links verleitet. Hier verstecken sich oft dubiose Gewinnspiele, im schlechtesten Fall fängt man sich Schädlinge ein oder tappt in eine ➔ [Abofalle](#) (siehe Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**).

Instant Messenger spielen in der Kommunikation für Jugendliche sowie in Familien eine große Rolle. Der Druck, ständig erreichbar zu sein und antworten zu müssen, kann eine enorme Belastung ausüben, wie im ➔ [Video von Handysektor](#) dargestellt wird.

Die Lesebestätigung in WhatsApp sowie der Zuletzt-online-Status können ausgeschaltet werden. Wie das geht, zeigt ➔ [schau-hin.info](#).

Einen Überblick, wie viele Nachrichten man mit WhatsApp verschickt und erhalten hat, findet sich unter Einstellungen > Datennutzung > Netzwerk-Nutzung.

Mehr zum Thema WhatsApp auf ➔ [schau-hin.info](#), auf ➔ [youngdata.de](#) sowie auf ➔ [handysektor.de](#).

1.1.9 Datensicherheit: Wie wichtig sind gute Passwörter?

„1800 Minecraft-Passwörter aufgetaucht“, „68 Millionen Dropbox-Passwörter gestohlen“, „Spotify-Nutzer sollten ihr Passwort ändern“. Solche und ähnliche Meldungen finden sich immer wieder in den Medien. Passwörter sind die Schlüssel für Internetdienste und schützen persönliche Daten, die man einem Anbieter anvertraut hat, vor fremden Zugriffen. Bei jeder Registrierung muss man sich eins ausdenken, je mehr man im Internet aktiv ist, desto mehr Passwörter hat man auch. Und merken sollte man sie sich auch am besten alle noch. Kein Wunder, dass eins der weltweit am häufigsten verwendeten Passwörter „123456“ lautet, aber weit entfernt davon ist, Schutz zu bieten. Denn nach wie vor ist ein schlecht gewähltes Passwort eine der am meisten genutzten Sicherheitslücken im Internet. Eingesetzt werden zum Passwortknacken meist Programme, die automatisch und in Sekundenschnelle beliebte (Pass-)Wörter, Wörterbucheinträge und Zahlenkombinationen testen.

Wie sieht es ein sicheres Passwort aus? Und wie kann man sich auch solche sicheren Passwörter merken?

Die Seite ➔ [www.youngdata.de](#) gibt Informationen und Hintergrundwissen rund um sichere Passwörter. Hier ist auch der empfehlenswerte Film „Unknackbar, aber einfach zu merken – Passwörter einfach erklärt“ verlinkt.

Ein sicheres Passwort sollte:

- mindestens zwölf Stellen lang sein (besser sogar 20)
- aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (&, %, \$, #, ?, ! etc.) bestehen
- nicht in einem Wörterbuch zu finden sein
- nicht zur eigene Person gehören (Geburtsdaten etc.)
- keine Zahlen- oder Buchstabenfolge sein (123456..., ABCDEF...)

Um sich solche kryptischen Passwörter zu merken, empfiehlt es sich, mit Tricks zu arbeiten: Man denkt sich einen Satz aus und verwendet nur die Anfangsbuchstaben dieses Satzes als Passwort.

Ich **h**abe **d**rei **H**aubtiere: **e**inen **H**und **u**nd **z**wei **G**oldfische.

IhdH:eHuzG.

Aus dem „und“ wird ein „+“-Zeichen; die Zahlen werden als Ziffer dargestellt. (Satzzeichen werden ebenfalls übernommen.)

Also: **Ih3H:1H+2G.**

Der Satz ist leichter zu merken als die Zahlenfolge.

Auf der Seite ➔ www.checkdeinpasswort.de lässt sich prüfen, wie sicher ein Passwort ist. Je länger das Passwort, desto schwerer knackbar ist es natürlich.

Weitere Informationen: ➔ www.verbraucherzentrale.de und ➔ www.bsi-fuer-buerger.de;
Stand: März 2017

Eine andere Methode, sichere Passwörter zu erstellen, ist ➔ [mit einem Passwort-Schlüssel](#) zu arbeiten.

1.1.10 Links und Materialien

Die EU-Initiative Klicksafe stellt eine Reihe von Materialien zum Thema bereit. Zu einzelnen Anwendungen wie Snapchat, YouNow, Youtube etc. gibt es Leitfäden, wie genau beispielsweise Privatsphäreinstellungen vorgenommen werden können. ➔ Baustein 3 des Lehrerhandbuch beschäftigt sich u.a. mit dem Thema Kommunikation via WhatsApp und Co. Z. B. zum Thema ➔ Instagram findet sich ein Flyer für SuS; auch zum Thema ➔ Privatsphäre aus medienethischer Perspektive finden sich verschiedene Materialien.

➔ www.klicksafe.de/materialien

Auf Handysektor.de können verschiedene Apps und ihre Vor- und Nachteile nachgelesen werden.

➔ www.handysektor.de

Das Thema Datenschutz wird auf der Jugendseite der unabhängigen Datenschutzbehörden des Bundes und der Länder sowie des Kantons Zürich behandelt, auch bezogen

➔ www.youngdata.de

auf verschiedene Social-Media- und Instant-Messenger-Anwendungen.

Die Initiative „SCHAU HIN! Was Dein Kind mit Medien macht“ richtet sich primär an Eltern. Hier gibt es ebenfalls u.a. Informationen zu sozialen Netzwerken.

➔ www.schau-hin.info

Im Materialkompass Verbraucherbildung des Verbraucherzentrale Bundesverband finden sich eine Reihe von ausführlich bewerteten Unterrichtseinheiten zum Thema. Am besten das gewünschte Stichwort in das Suchfeld eingeben.

➔ www.verbraucherbildung.de

1.1.11 Mögliche Verknüpfung mit anderen Themen

Online-Werbung: Soziale Netzwerke sind in der Regel kostenlos. Trotzdem wird damit Geld verdient. Wie funktioniert das? Was sind die Geschäftsmodelle von sozialen Netzwerken? Auch auf das Thema personenbezogene Werbung kann hier eingegeben werden.

Urheber- und Persönlichkeitsrechte: Bilder spielen eine große Rolle bei Sozialen Netzwerken. Doch dabei gilt es einiges zu beachten: Fremde Bilder dürfen nicht einfach verwendet, Abgebildete müssen gefragt werden. Dieser Themenbereich kann von Sozialen Netzwerken ausgehend gut thematisiert werden.

WhatsApp, Instagram, Snapchat: Eine Beschäftigung mit einzelnen Diensten bietet sich an, da diese mittlerweile eine große Rolle im Alltag von Kindern und Jugendlichen spielen. Sich beispielsweise die Privatsphäreinstellungen genauer anzuschauen, kann sinnvoll sein. Voraussetzung ist natürlich, dass die SuS die entsprechende Anwendung bereits zum großen Teil nutzen.

Smartphones und Apps: Soziale Netzwerke werden verstärkt auf Smartphones genutzt, Dienste wie Snapchat und WhatsApp fast ausschließlich mobil. Von diesem Aspekt ausgehend können Apps und ihre Nachteile thematisiert werden (Berechtigungen, Werbung etc.).

1.2 Erarbeitungsphase Schwerpunkt: Soziale Netzwerke und Instant Messenger: WhatsApp, Snapchat und Co.

Ziele:

- Die SuS wissen, was Soziale Netzwerke und Instant Messenger sind.
- Die SuS haben den Begriff der Öffentlichkeit reflektiert.
- Die SuS kennen Geschäftsmodelle solcher kostenloser Dienste.
- Die SuS wissen, dass die kostenlose Dienste oft mit ihren Daten bezahlen.
- Die SuS sind für die Bedeutung von Daten sensibilisiert.
Die SuS kennen den Begriff der Datensparsamkeit.

- Die SuS wissen, dass sie Privatsphäreinstellungen in sozialen Netzwerken vornehmen können.
- Die SuS kennen die Bedeutung von Bildern für soziale Netzwerke und Instant Messenger.
- Die SuS sind sensibilisiert für rechtliche Aspekte rund um das Thema Fotos.

- Die SuS wissen, in welchen Situationen Fotografieren erlaubt ist und in welchen nicht.
- Die SuS wissen, dass die Fotos nur mit Erlaubnis der abgebildeten Person veröffentlichen/ins Internet stellen dürfen (Recht am eigenen Bild).
- Die SuS wissen, wie sie vorgehen können, wenn ihr Recht am eigenen Bild verletzt wurde.
- Die SuS kennen Ausnahmen zum Recht am eigenen Bild.
- Die SuS wissen, was das Urheberrecht ist.

Zu Methoden zu diesen Lernzielen siehe Schwerpunkt Urheberrechtsverletzungen.

- Die SuS wissen um die Problematik verschickter Bilder bei WhatsApp.
- Die SuS wissen um die Problematik ins Internet gestellter Bilder.
- Die SuS wissen, wohin sie sich bei Problemfällen wenden können.

| | Methode | Zeit (Min.) | Arbeits- und Sozialform/ Methode | Medien/ Material |
|-------------|--|-------------|---|--|
| ①②③👁 | 01_Handyampel | 10 | Einzelarbeit, anschl. Plenum | Arbeitsblatt in Schüleranzahl |
| ①②③ | 02_Clevere Netzwerker | 10–20 | Partnerarbeit, Aufgreifen im Plenum | Arbeitsblatt in Kurz- oder Langversion in Schüleranzahl |
| ①②③👁 | 03_Was verrate ich von mir? | 10 | Plenum | Tafel, Kreide oder ähnliche Visualisierungsmöglichkeit, alternativ Kopiervorlage |
| ①②③ | 04_Öffentlich oder privat | 15–20 | Gruppenarbeit | Kopiervorlagen in Gruppenanzahl, Kleber, Scheren |
| ①②③👁 | 05_Unterrichtsgespräch: Das Netz vergisst nichts | 15 | Plenum | Präsentationsmöglichkeit für Web-Video |
| ①②③👁 | 06_Check dein Profil, bevor es andere tun | 15 | Plenum | Präsentationsmöglichkeit für Web-Video |
| ①②③👁 (👁) | 07_PC-Übung Ego-Googeln | 20 (+15) | PC-Partner- oder Einzelarbeit (zus. Plenum) | PCs mit Internetzugang |
| ①②③👁 | 08_Unterrichtsgespräch WhatsApp-Statistik | 10 | Plenum, Unterrichtsgespräch | Eigene Smartphones der SuS |
| ①②③ | 09_Sicheres Passwort | 20 | Einzel- oder Gruppenarbeit, Plenum, Unterrichtsgespräch | Für Einzel- oder Gruppenarbeit Arbeitsblatt |

| | Methode | Zeit (Min.) | Arbeits- und Sozialform/ Methode | Medien/ Material |
|------|--|-------------|---|---|
| ①②③👁 | 10_PC_Übung Passwortprüfer (Fortsetzung von „Sicheres Passwort“) | 15 | Einzel- oder Partnerarbeit | PCs mit Internetzugang |
| ①②③👁 | 11_WhatsApp, Instagram & Co.: sicher in sozialen Netzwerken | 10 | Einzelarbeit, Plenum, Unterrichtsgespräch | Arbeitsblatt in Schüleranzahl (oder an der Tafel für Plenumsarbeit) |

1.2.1 Handyampel

Dauer: ca. 10 Minuten

Ziel: Einstieg ins Thema Messenger, Sensibilisierung für Nachrichteninhalte

Schwierigkeit: ①②③

Material: Arbeitsblatt

Technik: ohne

Sozialform: Einzelarbeit, Aufgreifen im Plenum

Umsetzung: Jede Schülerin und jeder Schüler erhält eine Handyampel. Anhand der Beispielnachrichten sollen alle für sich entscheiden, welche Nachricht sie okay bzw. nicht okay finden. Gemeinsam werden danach die Ergebnisse besprochen.

Hinweis: Das Arbeitsblatt kann generell als Einstieg ins Thema WhatsApp/Instant Messaging dienen, außerdem können Aspekte wie Persönlichkeitsrechte (Recht am eigenen Bild) oder auch Cybermobbing herausgegriffen werden.

1.2.2 Clevere Netzwerker

Dauer: 10–20 Minuten

Ziel: Einstieg ins Thema, Sensibilisierung für Daten

Schwierigkeit: ①②③

Material: entweder Arbeitsblatt Clevere Netzwerker (Kurzversion) oder Arbeitsblatt Clevere Netzwerker (Langversion) in Schüleranzahl

Technik: ohne

Sozialform: Partnerarbeit, Aufgreifen im Plenum

Umsetzung: Jede Schülerin und jeder Schüler erhält einen Fragebogen, den er oder sie gemeinsam mit der Sitznachbarin oder dem Sitznachbarn ausfüllen soll. Anschließend wird im Unterrichtsgespräch über die preisgegebenen Daten

gesprochen. Welche dieser Daten könnten problemlos an der Schuleingangstür aufgehängt werden, welche nicht? Kann man anhand dieser Informationen herausfinden, um welchen Schüler oder welche Schülerin es sich handelt? Im Anschluss kann die Brücke zu sozialen Netzwerken geschlagen werden: Wenn diese Informationen z.B. bei Facebook preisgegeben werden, weiß Facebook eine ganze Menge über eine Person. Und mithilfe dieser Informationen kann auch sehr gezielt Werbung gemacht werden, die sich an den jeweiligen Interessen orientiert.

Hinweis: Die Fragebögen können auch eingesammelt und gemischt werden. Zwei bis vier Kinder ziehen jeweils einen Zettel und lesen die Antworten vor. Können die SuS herausfinden, zu wem die Beschreibung passt? Diese Übung eignet sich auch für jüngere Kinder.

Kernbotschaft: Sei sparsam mit deinen Daten!

1.2.3 Was verrate ich von mir?

Dauer: ca. 10 Minuten

Ziel: Einstieg ins Thema, Sensibilisierung für Daten

Schwierigkeit: ❶❷❸

Material: Tafel, Kreide oder andere Visualisierungsmöglichkeit, alternativ Kopiervorlage

Technik: ohne

Sozialform: Plenum

Umsetzung: Was können andere von mir wissen? Was behalte ich lieber für mich selbst? Die Antworten auf diese Brainstorming-Fragen werden an der Tafel gesammelt. Die Angaben, die andere wissen dürfen, werden dabei in die Sprechblase geschrieben. Die anderen kommen in den Menschen.

Hinweis: Entweder die Referentin/der Referent sammelt die Meldungen der SuS und notiert diese. Oder die SuS kommen an die Tafel und schreiben ihre Angaben auf. Die SuS können auch erst für sich selbst (oder in Gruppen) die Figur des Menschen (siehe Vorlage 1.3.4) beschriften, im Plenum werden einzelne Aspekte herausgegriffen und diskutiert.

Kernbotschaft: Daten sind nicht gleich Daten.

1.2.4 Öffentlich oder privat?

Dauer: ca. 15–20 Minuten

Ziel: Vertiefung des Themas, Sensibilisierung für Daten, Datenpreisgaben differenzieren lernen, Privatsphäreinstellungen kennenlernen

- Schwierigkeit: ① ② ③
- Material: Vorlage → Öffentlich oder privat? ausgedruckt in Gruppenanzahl, Kleber, Scheren
- Technik: ohne
- Sozialform: Gruppenarbeit
- Umsetzung: Daten sind unterschiedlich sensibel. In Kleingruppen diskutieren die SuS, welche Daten für alle sichtbar sein können und welche eher privat sind. Dafür schneiden sie die einzelnen „Daten“ auf dem Arbeitsblatt aus und kleben sie in die entsprechende Sprechblase. Die Ergebnisse der Gruppen müssen nicht zwangsläufig verglichen werden, da Gruppen unterschiedlicher Meinung sein können; eine anschließende Diskussion im Plenum ist aber wünschenswert. Hier kann man beispielsweise über Privatsphäreinstellungen sprechen, die aktiv vom Nutzer oder der Nutzerin vorgenommen werden müssen und die z.T. recht versteckt sein können.
- Hinweise: Die Übung kann auch mit der gesamten Gruppe im Plenum gemacht werden. Als Schnellabfrage und Einstieg in eine Diskussion kann auch mit farbigen Moderationskarten (Ampelabfrage) gearbeitet werden. Der Referent/die Referentin nennt Beispiele für Daten, die SuS bewerten mit farbigen Moderationskarten (rot = privat/problematisch, gelb = kommt darauf an/unsicher, grün = öffentlich/unproblematisch), ob diese Daten für alle sichtbar/zugänglich sein dürfen oder nicht. Daran anknüpfend kann dann auf Privatsphäreinstellungen in sozialen Netzwerken eingegangen werden.
- Kernbotschaft: Privatsphäreinstellungen nutzen!
- Diese Übung ist angelehnt an Arbeitsblätter aus dem Zusatzmodul „Ich bin öffentlich ganz privat“ von Klicksafe.

1.2.5 Unterrichtsgespräch: Das Netz vergisst nicht

- Dauer: ca. 15 Minuten (ja nach Diskussion)
- Ziel: Vertiefung des Themas, Sensibilisierung für die Langlebigkeit von Informationen im Netz, Überleitung zum Thema Privatsphäreinstellungen
- Schwierigkeit: ① ② ③
- Material: ohne
- Technik: Präsentationmöglichkeit für Video „Date“ (→ [Online-Zugriff](#))
- Sozialform: Plenum
- Alternative: Check dein Profil, bevor es andere tun.
- Umsetzung: Gemeinsam wird das Video „Date“ von Watchyourweb angeschaut. Anschließend wird eine Diskussion über den Satz „Das Netz vergisst nicht“

geführt.

Welches Problem hat der Junge in dem Film? Inwiefern könnte das wirklich passieren? Wie kann man das verhindern?

Hinweis: Der Film kann vor dem „webman-Kommentar“ am Ende gestoppt werden (also bei der Szene mit der Plakatwand). Am besten stellt man zunächst einmal ein paar Fragen zum Verständnis des Films. Vielleicht ist nicht allen klar geworden, dass auf den Plakaten verschiedene Ex-Freundinnen des Jungen zu sehen sind. Ggf. kann man den Film abschließend auch noch mal anschauen.

Diese Übung ist angelehnt an Material der Verbraucherzentrale Nordrhein-Westfalen.

Kernbotschaft: „Einmal ins Internet gestellt Daten können noch lange bestehen bleiben.“

1.2.6 Check dein Profil, bevor es andere tun

Dauer: ca. 15 Minuten (je nach Diskussion)

Ziel: Vertiefung des Themas, Sensibilisierung für die Langlebigkeit von Informationen im Netz, Überleitung zum Thema Privatsphäreinstellungen

Schwierigkeit: ① ② ③

Material: ohne

Technik: Präsentationmöglichkeit für Video „Check dein Profil, bevor es andere tun“ (➔ [Online-Zugriff z.B. via Netzdurchblick](#))

Sozialform: Plenum

Alternative: Das Netz vergisst nicht

Umsetzung: Gemeinsam wird das Video „Check dein Profil, bevor es andere tun“ angeschaut. Anschließend wird eine Diskussion über den Satz „Das Netz vergisst nicht“ geführt. Welches Problem hat der junge Mann in dem Film? Inwiefern könnte das wirklich passieren? Wie kann man das verhindern? Inwiefern ist das Profil im Netz für Arbeitgeber interessant?

Hinweis: Es bietet sich an, erst einige Fragen zum Film zu stellen und ihn zusammenfassen zu lassen. Sofern nicht allen der eigentliche Witz des Films klar geworden sein sollte (nämlich, dass der Bewerber in dem Video sich selbst, also sein Online-Profil trifft), kann man den Film abschließend auch noch mal zeigen.

Kernbotschaft: „Informationen über mich im Netz können auch für andere interessant sein.“

1.2.7 PC-Übung Ego-Googeln

Dauer: ca. 20 Minuten (+15 Minuten Diskussion)

- Ziel:** Vertiefung des Themas, Sensibilisierung für die Langlebigkeit von Informationen im Netz, Bewusstsein für eigene Daten im Netz
- Schwierigkeit:** ① ② ③
- Material:** ohne
- Technik:** PCs mit Internetzugang
- Sozialform:** Einzel- oder Gruppenarbeit am PC, anschließende Diskussion im Plenum
- Umsetzung:** „Was weiß das Internet über euch?“ Einzeln oder in Gruppen suchen die SuS in Suchmaschinen nach ihrem Namen. Dabei können verschiedene Eingabemöglichkeiten ausprobiert werden (Vor- und Nachname in Anführungszeichen, zusätzliche Eingabe des Ortes). „Notiert, was ihr findet.“
- Hinweise:** Treffer aus Sozialen Netzwerken sind ebenso möglich wie Presseartikel zu Schul-, Sport- und Vereinsaktivitäten. Um diese Ergebnisse zu sortieren und einschätzen zu lernen (gerade bei jüngeren SuS), bietet sich eine Diskussion im Anschluss an. Ggf. sollte auch auf Privatsphäreinstellungen zu sprechen gekommen werden, auch die Rolle von Pseudonymen sowie Persönlichkeits- und Urheberrechte können hier thematisiert werden.
- Diese Übung eignet sich insbesondere bei Klassen, in denen viele SuS in Sozialen Netzwerken aktiv sind. Wichtig ist, deutlich zu machen, dass es nicht darum geht, besonders viel oder wenig über sich zu finden, sondern dass man die öffentlich zugänglichen Informationen kennt und damit einverstanden ist (Stichwort: Identitätsmanagement)
- Kernbotschaft:** „Ich weiß, was das Netz über mich weiß!“

1.2.8 Unterrichtsgespräch WhatsApp-Statistik

- Dauer:** ca. 10 Minuten
- Ziel:** Einstieg ins Thema, Sensibilisierung für die Menge an verschickten Nachrichten
- Schwierigkeit:** ① ② ③
- Material:** ohne
- Technik:** eigene Smartphones der SuS
- Sozialform:** Unterrichtsgespräch
- Umsetzung:** Wie viele WhatsApp-Nachrichten bekommt ihr pro Tag? Wie viele schreibt ihr? Nach ersten Schätzungen sollen die SuS an ihren eigenen Geräten nachschauen, was die WhatsApp-Statistik sagt. Dazu öffnen sie WhatsApp und tippen auf das Menü (rechts, drei Punkte). Unter „Datennutzung“ und

„Netzwerk-Nutzung“ findet sich unter anderem die Anzahl der gesendeten und empfangenen Nachrichten.

Hinweis: Diese Methode ist nur sinnvoll, wenn in der Klasse auch WhatsApp genutzt wird (vorher abfragen). Vor der Übung sollten Nutzungsregeln für die eigenen Smartphones in der Unterrichtssituation festgelegt werden.

1.2.9 Sicheres Passwort

Dauer: ca. 20 Minuten

Ziel: Sensibilisierung für die Bedeutung von sicheren Passwörtern

Schwierigkeit: ❶❷❸

Material: ggf. Arbeitsblatt

Technik: ohne

Sozialform: Unterrichtsgespräch, Einzel- oder Gruppenarbeit

Umsetzung: Zunächst wird in einem Unterrichtsgespräch auf die Bedeutung von Passwörtern im Internet eingegangen. Wie viele Passwörter haben die SuS? Für welche Dienste? Warum braucht man Passwörter? Wie sieht es sicheres Passwort aus? Entweder kann mit dem Arbeitsblatt gearbeitet werden (für ältere SuS empfiehlt sich der Profi-Tipp), oder die Referentin/der Referent schreibt die wichtigsten Kriterien eines sicheren Passworts an die Tafel. Dann wird das Passwort „MHdh3;3EhmH“ angeschrieben. Ist das ein sicheres Passwort? Warum? Wie kann man es sich merken? Hinter diesem Passwort stecken die Anfangsbuchstaben (und Satzzeichen) von „Mein Hut der hat 3 Ecken, 3 Ecken hat mein Hut“. Können die SuS eigene sichere Passwörter bilden? Diese können in der Übung „Passwortprüfer“ getestet werden.

Wichtig ist der Hinweis, dass bei Hacker-Angriffen mit automatisierten Programmen gearbeitet wird, die in Sekundenschnelle verschiedene Listen durchgehen. Deshalb sollte man keine „sinnvollen“ Wörter verwenden, also keine, die ich Wörterbüchern zu finden sein könnten, und keine gängigen Zahlenkombinationen wie Geburtsdaten etc. Auch die Kombination aus beidem ist nicht sicher.

1.2.10 PC-Übung Passwortprüfer (Fortsetzung von „Sicheres Passwort“)

Dauer: ca. 15 Minuten

Ziel: Sensibilisierung für die Bedeutung von sicheren Passwörtern

Schwierigkeit: ❶❷❸

Material: ohne

- Technik: PCs mit Internetzugang
- Sozialform: Einzel- oder Partnerarbeit
- Umsetzung: Mit einer in der Übung „Sicheres Passwort“ gelernten Methode sollen sich die SuS ein sicheres Passwort erstellen. Dieses notieren sie sich zunächst und geben es auf der Internetseite ➔ www.checkdeinpasswort.de ein. Wie sicher ist es? In einer abschließenden Plenumsrunde kann besprochen werden, was gut, was weniger gut funktioniert hat.
- Hinweise: Natürlich können auch auf der Seite live noch weitere Passwörter getestet werden. Vorher sollte aber der Arbeitsauftrag klar sein, um allzu wilde Tipps zu vermeiden.

1.2.11 WhatsApp, Instagram & Co.: sicher in sozialen Netzwerken

Dauer: ca. 10 Minuten

Ziel: Ergebnissicherung

Schwierigkeit: ❶❷❸

Material: Arbeitsblatt

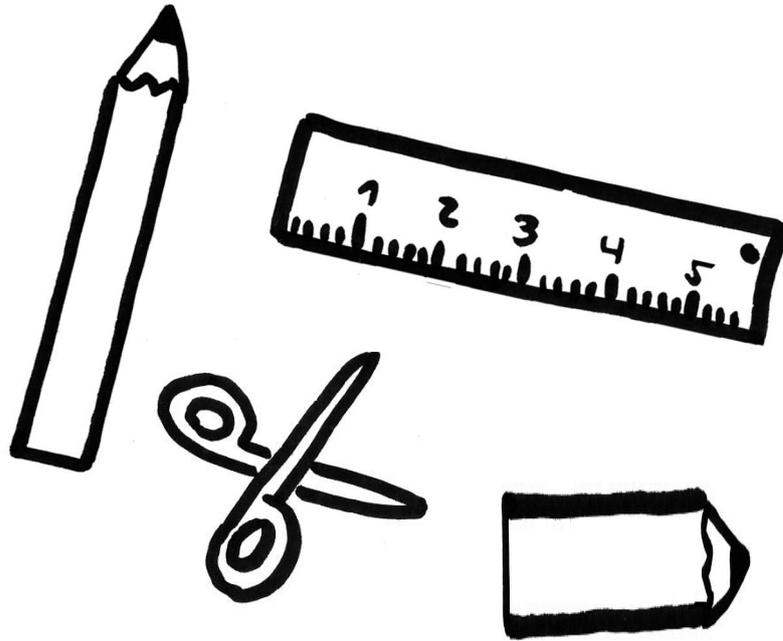
Technik: ohne

Sozialform: Unterrichtsgespräch, Einzelarbeit

Umsetzung: Zum Abschluss des Schwerpunkts soziale Netzwerke werden in einem kurzen Unterrichtsgespräch Tipps zur Nutzung gesammelt. Für sich halten die SuS ihre Tipps auf einem Arbeitsblatt fest, das sie mit nach Hause nehmen.

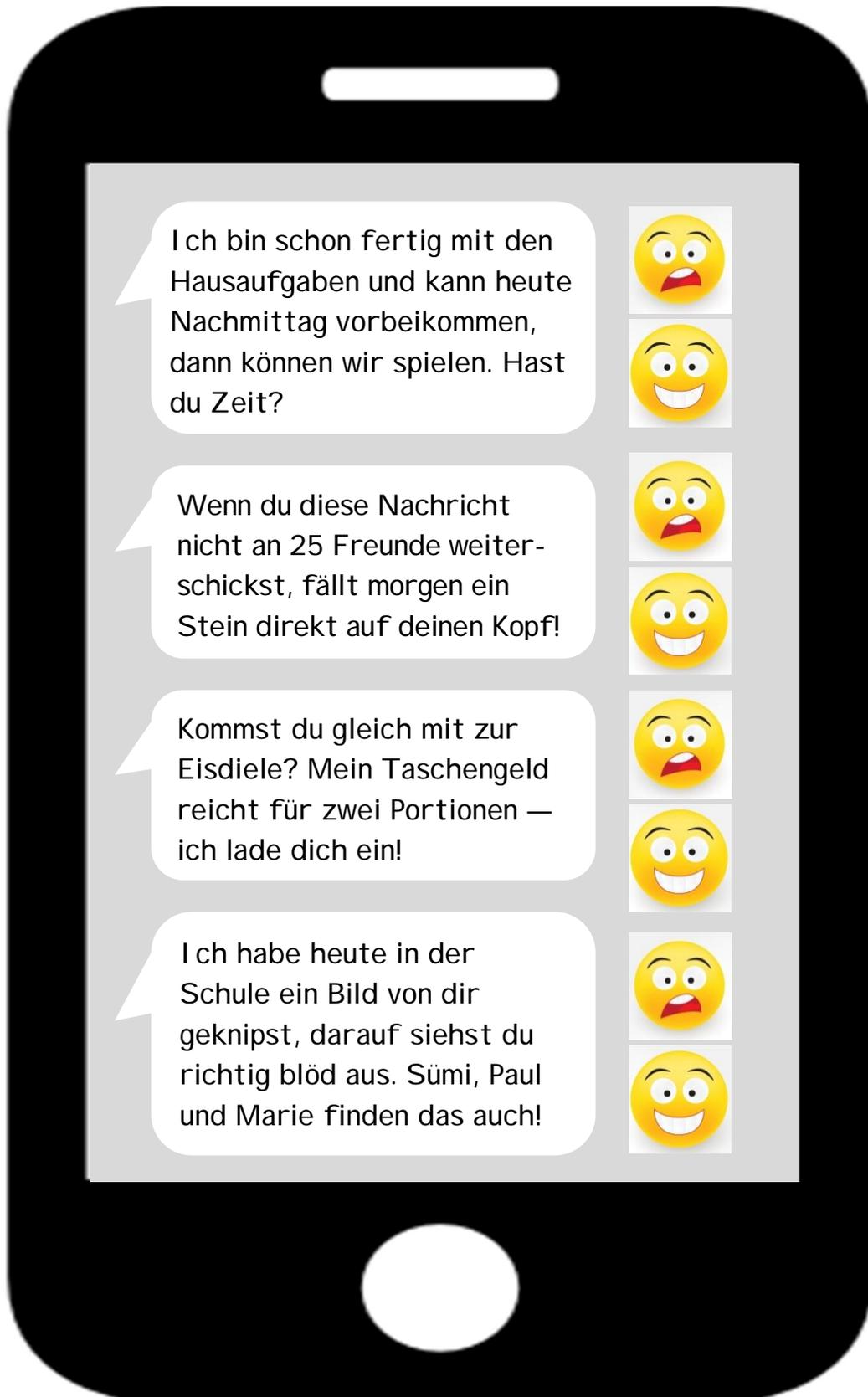
Hinweis: Die Sammlung von Tipps kann auch gemeinsam an der Tafel erfolgen.

1.3 Materialien



1.3.1 Handyampel

Was denkst du, wenn dir jemand diese Nachrichten auf dein Handy sendet?
Welches Emoticon trifft deine Stimmung?



1.3.2 Arbeitsblatt Clevere Netzwerker (Kurzversion)

Kennst du deinen Sitznachbarn/deine Sitznachbarin?

Wie lautet der Vorname deines Sitznachbarn/deiner Sitznachbarin?

Kreuze an:

| | | | |
|------------------------------------|--------------------------------------|--|-----------------------------------|
| Ist er/sie ein Junge oder Mädchen? | <input type="checkbox"/> Junge | <input type="checkbox"/> Mädchen | |
| In welche Schule geht er/sie? | <input type="checkbox"/> Grundschule | <input type="checkbox"/> weiterführende Schule | |
| Welche Hobbys hat er/sie? | <input type="checkbox"/> Sport | <input type="checkbox"/> Musik | <input type="checkbox"/> Freunde |
| | <input type="checkbox"/> Shoppen | <input type="checkbox"/> Lesen | <input type="checkbox"/> Computer |
| Was ist sein/ihr Lieblingsfach? | <input type="checkbox"/> Deutsch | <input type="checkbox"/> Kunst | <input type="checkbox"/> Mathe |
| | <input type="checkbox"/> Sport | <input type="checkbox"/> Musik | <input type="checkbox"/> Englisch |

Kennst du deinen Sitznachbarn/deine Sitznachbarin?

Wie lautet der Vorname deines Sitznachbarn/deiner Sitznachbarin?

Kreuze an:

| | | | |
|------------------------------------|--------------------------------------|--|-----------------------------------|
| Ist er/sie ein Junge oder Mädchen? | <input type="checkbox"/> Junge | <input type="checkbox"/> Mädchen | |
| In welche Schule geht er/sie? | <input type="checkbox"/> Grundschule | <input type="checkbox"/> weiterführende Schule | |
| Welche Hobbys hat er/sie? | <input type="checkbox"/> Sport | <input type="checkbox"/> Musik | <input type="checkbox"/> Freunde |
| | <input type="checkbox"/> Shoppen | <input type="checkbox"/> Lesen | <input type="checkbox"/> Computer |
| Was ist sein/ihr Lieblingsfach? | <input type="checkbox"/> Deutsch | <input type="checkbox"/> Kunst | <input type="checkbox"/> Mathe |
| | <input type="checkbox"/> Sport | <input type="checkbox"/> Musik | <input type="checkbox"/> Englisch |

1.3.3 Arbeitsblatt Clevere Netzwerker (Langversion)

Kennst du deinen Sitznachbarn/deine Sitznachbarin?

Wie lautet der Vorname

deines Sitznachbarn/deiner Sitznachbarin?

Kreuze an:

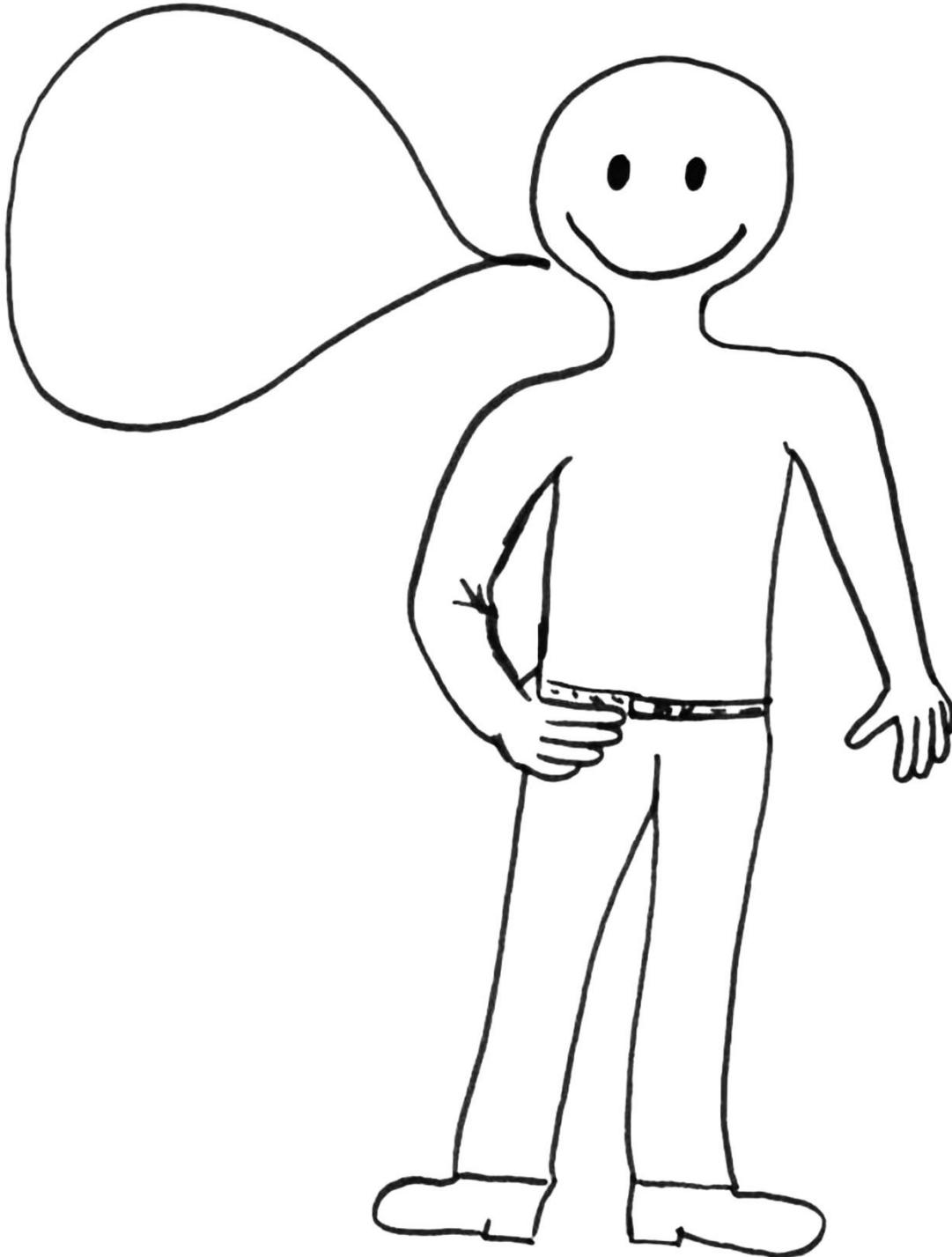
| | | | |
|--------------------------------------|--------------------------------------|--|--|
| Ist er/sie ein Junge oder Mädchen? | <input type="checkbox"/> Junge | <input type="checkbox"/> Mädchen | |
| In welche Schule geht er/sie? | <input type="checkbox"/> Grundschule | <input type="checkbox"/> weiterführende Schule | |
| Wie kommt er/sie zur Schule | <input type="checkbox"/> zu Fuß | <input type="checkbox"/> die Eltern fahren | <input type="checkbox"/> mit dem Fahrrad |
| | <input type="checkbox"/> mit dem Bus | <input type="checkbox"/> mit dem Roller | |
| Welche Hobbys hat er/sie? | <input type="checkbox"/> Sport | <input type="checkbox"/> Musik | <input type="checkbox"/> Freunde |
| | <input type="checkbox"/> Shoppen | <input type="checkbox"/> Lesen | <input type="checkbox"/> Computer |
| Was ist sein/ihr Lieblingsfach? | <input type="checkbox"/> Deutsch | <input type="checkbox"/> Kunst | <input type="checkbox"/> Mathe |
| | <input type="checkbox"/> Sport | <input type="checkbox"/> Musik | <input type="checkbox"/> Englisch |
| Was isst er/sie am liebsten? | <input type="checkbox"/> Pizza | <input type="checkbox"/> Döner | <input type="checkbox"/> Spaghetti |
| | <input type="checkbox"/> Hamburger | <input type="checkbox"/> Pfannkuchen | <input type="checkbox"/> Eis |
| Kennst du seine/ihre Telefonnummer? | <input type="checkbox"/> ja | <input type="checkbox"/> nein | |
| Wie lautet seine/ihre Telefonnummer? | | | |
| Wie alt ist er/sie? | | | |

Frage deinen Sitznachbarn/deine Sitznachbarin, wem du das Infoblatt über sie/ihn geben darfst.

| | | | | |
|--|----|--------------------------|------|--------------------------|
| Seinen/ihren Eltern? | ja | <input type="checkbox"/> | nein | <input type="checkbox"/> |
| Dem besten Freund/der besten Freundin? | ja | <input type="checkbox"/> | nein | <input type="checkbox"/> |
| Einer Nachbarin? | ja | <input type="checkbox"/> | nein | <input type="checkbox"/> |
| Einem Lehrer? | ja | <input type="checkbox"/> | nein | <input type="checkbox"/> |
| Dem Schuldirektor? | ja | <input type="checkbox"/> | nein | <input type="checkbox"/> |
| Einem Jungen aus der 8. Klasse? | ja | <input type="checkbox"/> | nein | <input type="checkbox"/> |
| Dem Busfahrer? | ja | <input type="checkbox"/> | nein | <input type="checkbox"/> |
| An der Schuleingangstür aufhängen? | ja | <input type="checkbox"/> | nein | <input type="checkbox"/> |
| Bilde die Summe der „Jas“ und „Neins“. | ja | | nein | |

1.3.4 Vorlage Was verrate ich von mir?

Was verrate ich von mir?



1.3.5 Öffentlich oder privat?

Was ist öffentlich, was privat?

Unten stehen viele Beispiele für sogenannte personenbezogene Daten. Welche davon dürfen alle wissen (öffentlich), welche wollt ihr lieber für euch behalten (privat)? Wo seid ihr euch uneinig?

Schneidet die „Daten“ aus und klebt sie in die entsprechende Sprechblase.



mein Vorname

wo mein
Taschengeld liegt

in wen ich
verliebt bin

mein Nachname

mein neuester
Lieblingfilm

wovor ich Angst habe

Farbe meiner
Unterwäsche

welchen Lehrer ich blöd finde

meine Telefonnummer

meine Handynummer

ob ich Pickel habe

Namen meiner Eltern

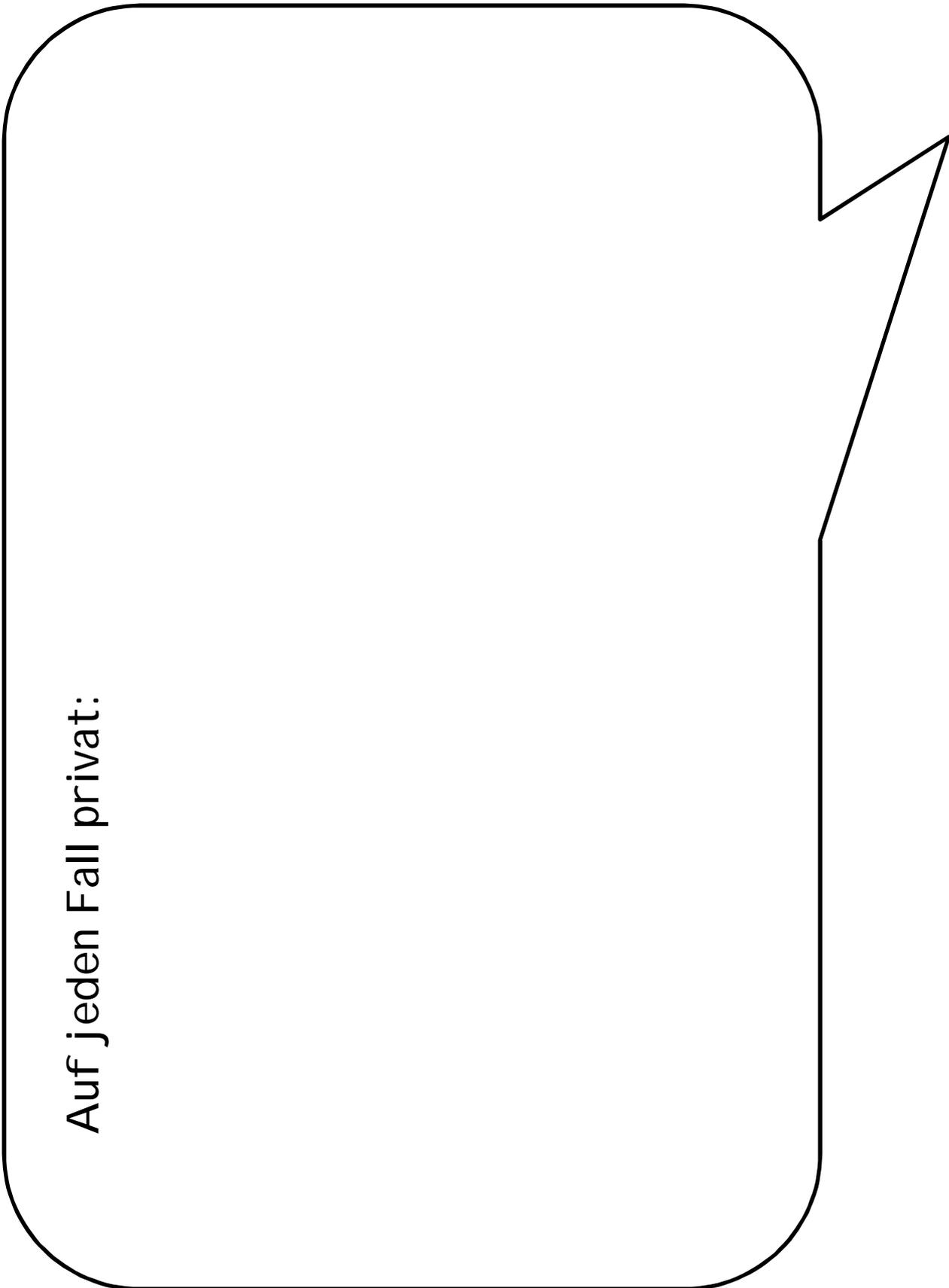
wo ich wohne

mein
Geburtsdatum

wer mein bester
Freund ist

wie oft ich mir die
Zähne putze

Öffentlich / für alle:



Auf jeden Fall privat:

Nicht eindeutig:

Für Freunde:

1.3.6 Arbeitsblatt Sicheres Passwort

1. Könnt ihr diese Passwörter entschlüsseln?

| Gesuchtes Wort: | Suchhilfen: | Lösung: |
|-----------------|--------------------|---------|
| g _ h _ _ m | versteckt | |
| P _ _ s _ _ _ t | sichert den Zugang | |
| _ 2 _ _ _ 6 | Zahlenfolge | |
| h _ _ l _ | Begrüßung | |

Diese Passwörter zählen zu den beliebtesten Passwörtern in Deutschland. Mit solchen Passwörtern macht man es Hackern ganz schön leicht.

Ein sicheres Passwort sollte so aussehen:

- mindestens 8 Stellen lang – je länger, desto besser!
- Mischung Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen
- möglichst keine Namen, Geburtsdaten oder normale Wörter nutzen

Außerdem gilt:

- für jeden Account ein anderes Passwort wählen!
- Passwörter geheim halten und nicht weitersagen!
- Passwörter regelmäßig ändern!

Auflösung:
geheim, Passwort, 123456, hallo

So erstellt ihr ein sicheres Passwort in nur 3 Schritten:

1. Denkt euch einen Satz mit mindestens acht Wörtern (besser zwölf!) und am besten noch einem Zahlwort aus. Zum Beispiel: „Ich habe 1 dicken, roten Kater, der 15 Jahre alt ist und viel frisst.“

Jetzt ihr:

2. Markiert oben alle Anfangsbuchstaben, Satzzeichen und Zahlen in diesem Satz.

Also so: „Ich habe 1 dicken, roten Kater, der 15 Jahre alt ist und viel frisst.“

3. Schreibt die Anfangsbuchstaben und Satzzeichen ab:

Also so: Ih1d,rK,d15Jaiuvf.

*Fertig ist euer Passwort.
Ihr müsst euch nur noch
den Satz merken!*



Wie gut ein solches Passwort ist, könnt ihr auf der Seite www.checkdeinpasswort.de testen.

Quellen:

Schlüssel: Ciker-Free-Vector-Images, Pixabay.com; Lizenz: [CC0](https://creativecommons.org/licenses/by-nc-sa/4.0/) ,

Schloss: OpenClipart-Vectors, Pixabay.com; Lizenz: [CC0](https://creativecommons.org/licenses/by-nc-sa/4.0/)

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2017

Soweit nicht anders gekennzeichnet, steht diese Publikation unter [CC-BY-NC-SA](https://creativecommons.org/licenses/by-nc-sa/4.0/).

Arbeitsblatt sicheres Passwort – Profitipp

Schon mal was von einem Passwortschlüssel gehört? Mit dem erstellt man sichere Passwörter.

So geht's:

Schritt 1: geheimes Wort ausdenken

Schritt 2: mithilfe des Schlüssels das geheime Wort „verschlüsseln“

Schritt 3: fertig – Passwort nutzen!

So musst du dir nur ein Wort merken. Hast du den Schlüssel dabei, kannst du das Passwort immer wieder erstellen.

| | | | | | | | | | | | |
|--------------|---|---|---|-----|-----|-----|-----|-----|------|-----|------|
| S | g | # | 8 | s | n | ? | F | e | j | 6 | 4 |
| Startzeichen | | | | ABC | DEF | GHI | JKL | MNO | PQRS | TUV | WXYZ |

Aus dem Wort „Computer“ wird dann also das Passwort „seej66nj“. Davor kommen noch die vier Startzeichen, die immer gleich bleiben.

Das Passwort lautet also: Sg#8seej66nj

Und jetzt du: Wie lautet das Passwort mit dem geheimen Wort „Sommerferien“?

Und wie mit deinem eigenen, ausgedachten Passwort?

Wichtig: Den Schlüssel kannst du dir notieren oder aufschreiben und immer bei dir haben. Das geheime Wort solltest du aber niemandem verraten!

Auflösung:
Sg#8seej66nj

1.3.7 WhatsApp, Instagram & Co.: sicher in sozialen Netzwerken

Wie sollte man sich in sozialen Diensten wie WhatsApp und Instagram verhalten? Formuliere Tipps und schreibe sie in die Sprechblasen.

Benutze sichere
Passwörter!

Sei sparsam
mit deinen
Daten!

