Verbraucherzentrale
Rheinland-Pfalz

Medien sicher nutzen
Modul 4

Soziale Netzwerke

Medien sicher nutzen

Gefördert durch das
Ministerium für Familie, Frauen, Kultur
und Integration (MFFKI)

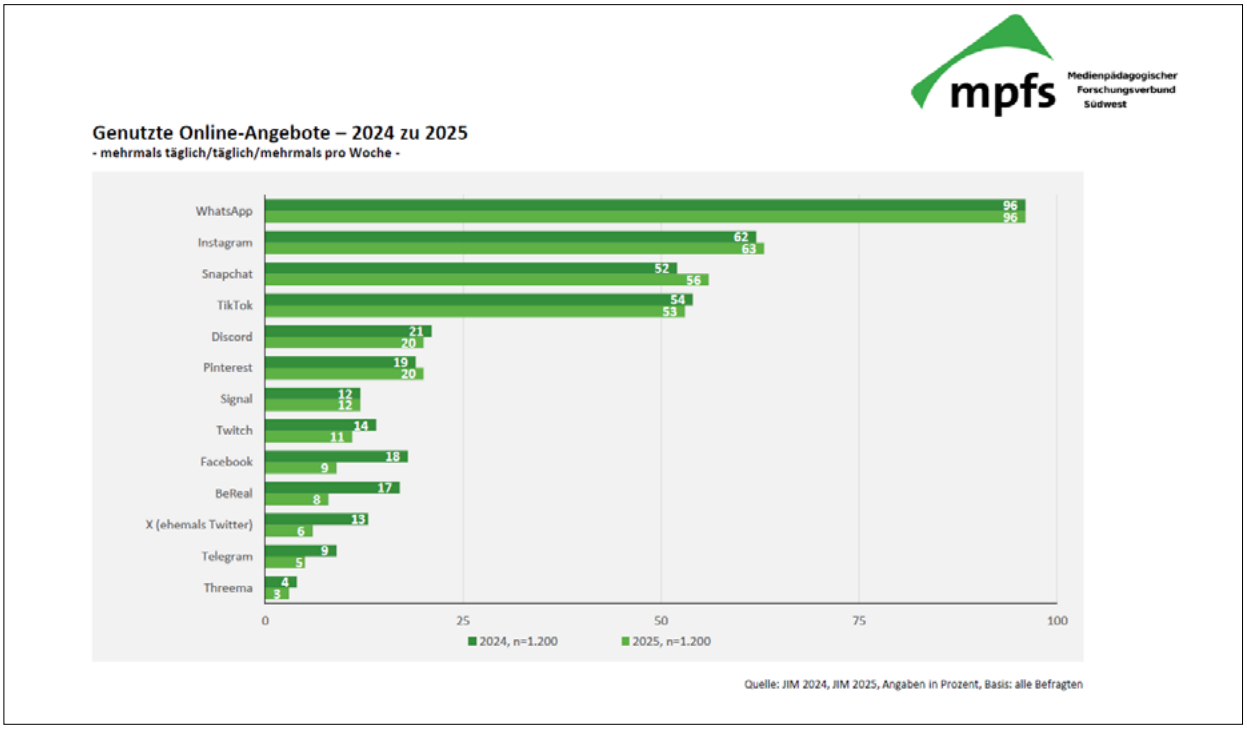
RheinlandPfalz
MINISTERIUM FÜR
FAMILIE, FRAUEN, KULTUR
UND INTEGRATION

Die Materialien stehen auch auf Schulcampus,
dem Bildungsserver Rheinland-Pfalz.
https://www.schulcampus-rlp.de

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

1. Sachinformationen

Soziale Netzwerke – oft auch als „Social Networks“ oder „Social Communitys“ bezeichnet – sind ein virtueller Ort des Austauschs und der Freundschaftspflege und damit ein wesentlicher Antrieb für die Internetnutzung. Möchte man WhatsApp in diese Gruppe einordnen, so ist der zu Meta (ehemals Facebook) gehörende Dienst absoluter Spitzenreiter: Laut JIM-Studie 2025[1] nutzen 96 Prozent aller Zwölf- bis 19-Jährigen mindestens mehrmals pro Woche **WhatsApp**. Dahinter folgen mit etwas Abstand **Instagram, Snapchat und TikTok.** Alternative Messanger wie Signal oder Threema spielen nur eine Untergeordnete Rolle, das Urgestein Facebook ebenfalls.



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 2025. Jugend, Information, Medien. Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland. Stuttgart, 2025 (Link: https://mpfs.de/app/uploads/2025/11/JIM_2025_PDF_barrierearm.pdf).

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

1.1 Wie unterscheiden sich die Anwendungen?

WhatsApp

WhatsApp, das zum Meta-Konzern gehört, ist momentan der weltweit größte Kurznachrichtendienst. Der Name der App ist an den englischen Ausdruck „What's up?“ („Was ist los?“, „Was geht?“) angelehnt und wird durch das Kürzel „App“ (englisch „application“ = „Anwendung“) ergänzt. Dabei ist WhatsApp genauer betrachtet kein soziales Netzwerk, sondern ein sogenannter Instant-Messaging-Dienst, welcher das Versenden von Textnachrichten, Bildern und Videos sowie Sprach- und Videonachrichten ermöglicht. Klassische Telefongespräche über das Internet sowie Videochats sind ebenfalls möglich und insbesondere bei Kindern und Jugendlichen sehr beliebt. Die Inhalte der Nachrichten können dabei nicht nur an eine einzelne Person, sondern auch an mehrere Teilnehmende gleichzeitig gerichtet sein.

96 Prozent nutzen WhatsApp mehrmals in der Woche, 93 Prozent sogar mehrmals täglich.

Im Jahr 2014 übernahm der damals noch als Facebook firmierende Konzern den Dienst für eine Summe von 19 Milliarden US-Dollar.[3] Für die Nutzer:innen ist die App kostenlos und zeigt auch keine „nervenden“ Werbeanzeigen. Zu den Vorteilen gehört zudem eine sogenannte „Ende-zu-Ende-Verschlüsselung“, welche die Weiterleitung der jeweiligen Nachrichten absichern soll.

Trotz der großen Beliebtheit und der offensichtlichen Vorzüge sollte man WhatsApp nur vorsichtig nutzen. Bereits mit der Installation der App gibt man die Weitergabe sämtlicher Kontakte frei, wenn man dies nicht aktiv in den App-Berechtigungen untersagt, sprich wegklickt. Tut man dies nicht, werden geteilte Kontakte unverschlüsselt an einen amerikanischen Server von WhatsApp Inc. weitergeleitet und dort abgespeichert. Besonders problematisch ist, dass sich WhatsApp dabei nicht auf die Daten der WhatsApp-Nutzer:innen beschränkt, sondern alle Daten kopiert. Folglich werden auch Daten von Personen, welche kein WhatsApp nutzen beziehungsweise den Messenger nicht einmal installiert haben, weitergeleitet – obwohl sie WhatsApp keine Erlaubnis zur Weiterleitung ihrer Daten erteilt haben.

WhatsApp ist aufgrund von Datenschutz- und Sicherheitsbedenken immer wieder in der Kritik.[4] Beispielsweise machte die App im August 2021 dadurch Schlagzeilen, dass ihre geänderten Nutzungs- und Datenschutzbestimmungen die Möglichkeit einräumten, Daten ihrer Nutzer:innen an Facebook weiterzugeben. Somit benutzt Facebook beziehungsweise Meta WhatsApp, um weitere Daten über seine Nutzer:innen zu sammeln, welche diese von sich preisgeben. Die App analysiert dabei nicht nur die Inhalte, sondern auch das vollständige Nutzungsverhalten, das heißt, wie oft, wie lange und mit wem Informationen geteilt wurden.

[2] JIM-Studie 2025, S. 33

[3] https://www.heise.de/newsticker/meldung/Facebook-kauft-WhatsApp-2118920.html, Stand: 2014.

[4] https://netzpolitik.org/2016/abschied-von-whatsapp-fuenf-gute-gruende-fuer-den-messenger-wechsel/, Stand: 09/2016.

Am 25. Mai 2018 trat die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union in Kraft. Sie beschäftigt sich unter anderem damit, was Unternehmen wie zum Beispiel Meta mit den Daten ihrer Kund:innen machen dürfen – besonders, wenn sie jünger als 16 Jahre alt sind. In den aktuellen Nutzungsbedingungen wurde 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“.[5]

Wollen jüngere Kinder den Dienst nutzen, muss eine Einwilligung der Eltern vorliegen. Neue Nutzer:innen müssen ihr Alter bestätigen. Eine Kontrolle gibt es jedoch nicht. Wer die App auf seinem Handy installiert und das Gerät verifiziert, kann sie auch nutzen.

Mehr zu WhatsApp auf:

- https://www.bmfsfj.de/blob/137194/57c29c845962dafe83aea3417e04b6ef/schau-hin-medienratgeber-digital-aufwachsen-data.pdf
- https://www.futurebiz.de/?s=whatsap
- https://www.handysektor.de/artikel/fake-news-via-whatsapp-kennst-du-den-doppelpfeil
- https://www.handysektor.de/artikel/10-goldene-regeln-fuer-den-gruppenchat-in-whatsapp
- https://www.klicksafe.de/themen/kommunizieren/whatsapp/#s|whatsapp

[5] https://www.whatsapp.com/legal/terms-of-service-eea, Stand: 07/2023.

Instagram
Instagram ermöglicht es seinen Nutzer:innen, Bilder und Videos mit Menschen aus aller Welt zu teilen. Hierbei hat der Dienst als einer der ersten den sogenannten „Feed“ populär gemacht. Im Feed werden Bild- und Videoinhalte auf dem eigenen Profil in Endlosschleife dauerhaft einsehbar gepostet – quasi wie ein Nachrichtenkanal. So entstand das Phänomen, dass Nutzer:innen sich teilweise nur schwer von der App lösen, da sie unentwegt wie in einer Suchtspirale von neuem Inhalt zu neuem Inhalt geleitet werden und aus Angst, etwas zu verpassen, sich schwertun, diesen Kreislauf zu durchbrechen.[6] Neben dem Feed lassen sich eigene Inhalte auch mit einer Sichtbarkeitszeit von 24 Stunden in eine sogenannte „Story“ laden. Das Format „IGTV“ (= Instagram TV) ermöglicht das dauerhafte Hochladen von bis zu 60-minütigen Videos. In den jeweiligen Bild- und Videodateien, Storys und IGTV-Beiträgen findet man stets die Inhalte der Personen, denen man folgt. Diese können dann „geliked“ werden. Die eigenen Profile sind entweder für alle sichtbar auf „öffentlich“ gestellt, oder sie sind „privat“. Private Profile sind nur für diejenigen sichtbar, denen man erlaubt hat, dem eigenen Feed zu folgen. Unter den in ihren Feeds geposteten Beiträgen können sich Instagram-Nutzer:innen öffentlich austauschen.

Auf einen Story-Post kann mit unterschiedlichen Smileys oder mit dem Versenden einer Nachricht reagiert werden. Die App bietet zudem die Möglichkeit, selbst aufgenommene Bilder vor dem Veröffentlichen zu bearbeiten und mit Filtern zu belegen – eine Funktion, die von vielen Nutzer:innen zwar gerne und häufig eingesetzt wird und dennoch in der Kritik steht, da sie die Wirklichkeit verfälscht. Gegenwärtig gibt es daher zwei gegenläufige Trends: Solche Nutzer:innen, die die App auch weiterhin nutzen, um ihre Bilder beziehungsweise sich selbst darauf zu verschönern, und solche, die darauf bewusst verzichten, um ihr „wirkliches Ich“ zu zeigen.

Instagram wird auch von zahlreichen prominenten Musiker:innen, Sportler:innen und Schauspieler:innen genutzt. Diese teilen alltägliche Situationen und stellen durch ihre Fotos und Videos eine persönliche Nähe zu ihren Follower:innen her. Dies führt stellenweise zu einer Form der übertriebenen Selbstdarstellung – wie zum Beispiel bei den beiden „Selfie-Vollprofis“ Kim Kardashian mit über 362 Millionen Follower:innen (Stand: Juli 2023) und Christiano Ronaldo mit 595 Millionen Follower:innen (Stand: Juli 2023). Geprägt wird Instagram von zahlreichen weiteren sogenannten Influencer:innen (englisch „to influence“ = „beeinflussen“): Diese nutzen ihre große Followerschaft und damit verbundene Reichweite über die App, um mit Werbung Geld zu verdienen.

Seit 2012 gehört der Dienst ebenfalls zu Meta. Laut eigenen Angaben hatte das Unternehmen im Juni 2018 die Grenze von einer Milliarde Nutzer:innen durchbrochen. 63 Prozent der deutschen Jugendlichen nutzen Instagram mehrmals in der Woche (2024: 62 Prozent, 2021: 58 Prozent)[7].

[6] https://www.zdf.de/nachrichten/panorama/soziale-medien-jugendliche-sucht-100.html, Stand: 15.03.2023.

[7] JIM-Studie 2025, S. 30 und JIM-Studie 2021, S. 37.

Die Registrierung und Nutzung von Instagram ist kostenlos. In den Nutzungsbedingungen von Instagram heißt es: „Du musst mindestens 13 Jahre alt sein, um den Dienst zu nutzen.“[8]

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

Mehr zu Instagram auf:

- https://www.futurebiz.de/?s=instagram
- https://www.handysektor.de/artikel/instagram-einstellen
- https://www.handysektor.de/artikel/dein-vertrag-mit-instagram
- https://www.klicksafe.de/themen/kommunizieren/soziale-netzwerke/instagram/was-ist-instagram/#s|instagram

Snapchat
Die App Snapchat ist bei Kindern und Jugendlichen ebenfalls beliebt. Laut JIM-Studie 2025 nutzen 56 Prozent der befragten Jugendlichen Snapchat mindestens mehrmals pro Woche, im Vorjahr waren es 52 Prozent.[9]

Bei Snapchat handelt es sich um eine Kombination aus einem Messengerdienst und einer Foto/Video-Community. Mit Snapchat können Videos und Fotos mit kleinen Kurznachrichten erstellt und vor dem Versenden durch verschiedene Filter, Emojis oder Spezialeffekte kreativ gestaltet werden.

Das Besondere der App ist dabei, 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“ nutzen, 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. Auch Zusatzprogramme, welche eine langfristige Speicherung solcher Bilder ermöglichen, übertragen diese teilweise auf ihre eigenen Server, die gehackt werden können. Außerdem speichert sowohl das Smartphone der Sender:innen als auch das Smartphone der Empfänger:innen Daten in „temporären“ Verzeichnissen, die sich möglicherweise ebenfalls auslesen lassen. Nur weil

[8] https://about.instagram.com/de-de/blog/announcements/continuing-to-make-instagram-safer-for-the-youngest-members-of-our-community, Stand: 03/2021.

[9] JIM-Studie 2025, S. 32

Snapchat das Bild nicht mehr öffnet, heißt das also nicht, dass man dieses Bild nicht über ein anderes Programm weitherhin öffnen und bearbeiten kann.

Die zwei wichtigsten Funktionen bei Snapchat sind das „Snappen“ und das „Chatten“:

a) Snappen
Bei Snapchat können Fotos und Videos („Snaps“) mit Filtern, Text und Emojis versehen, heruntergeladen und auf anderen Netzwerken wie Instagram oder Facebook geteilt werden. In der App verschwinden diese Snaps innerhalb von bis zu zehn Sekunden. Werden Bilder zum „Story“ genannten Profil hinzugefügt, sind sie bis zu 24 Stunden sichtbar.

b) Chatten
Bei Snapchat können sich Nutzer:innen direkt anrufen, kurze Videobotschaften, Nachrichten, Fotos und Sticker schicken. Auch Gruppenchats mit bis zu 16 Teilnehmenden sind möglich. Snapchat wird dadurch auch zum Messenger. Mit Freundschafts-Emojis bewertet die App den Austausch zwischen zwei Menschen. Besonders das Flammensymbol (oder: „Snapstreak“) weckt den Ehrgeiz der Nutzer:innen, denn es bedeutet, dass zwei Freund:innen mindestens drei Tage am Stück jeweils innerhalb von 24 Stunden Snaps ausgetauscht haben; die Zahl neben der Flamme dokumentiert die Anzahl der Tage mit regelmäßigem Kontakt.

Mehr zu Snapchat auf:

- https://www.handysektor.de/artikel/dein-vertrag-mit-snapchat
- https://www.handysektor.de/artikel/snapchat-einstellen
- https://www.futurebiz.de/artikel/snapchat-statistiken-nutzerzahlen
- https://www.klicksafe.de/apps/snapchat/#s|snapchat

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

Facebook
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 3 Milliarden Menschen weltweit nutzen diesen Dienst.[10]

Das Alter der Facebook-Nutzer hat sich allerdings nach oben verschoben, unter Jugendlichen spielt das Netzwerk keine große Rolle mehr. Manche haben noch ein Konto, allerdings bedeutet ein Facebook-Konto nicht zwangsläufig die Nutzung der Plattform selbst, sondern kann auch zum Verknüpfen mit anderen Plattformen und digitalen Spielen verwendet werden.[11]

Das soziale Netzwerk Facebook lässt sich kostenlos im Browser oder per App nutzen; um sich zu registrieren, muss man mindestens 13 Jahre alt sein. Nutzer:innen 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 Meta, das Unternehmen hinter dem sozialen Netzwerk, immer wieder wegen undurchsichtiger Datenschutzregelungen. In jüngster Zeit richtete sich die Kritik auch gegen Metas Umgang mit sogenannten Fake News.

Mehr zu Facebook:
https://www.klicksafe.de/facebook

TikTok
Die Video-App TikTok erfreut sich bei Kindern und Jugendlichen weltweit großer Beliebtheit. Ihre Nutzungszahlen steigen täglich. TikTok entstand aus der beliebten App musical.ly, einer App, in der sogenannte LipSync-Videos erstellt und veröffentlicht werden konnten. In diesen Videos konnten die Nutzer:innen vorgegebene Lippenbewegungen synchron zur vorgegebenen Musik nachahmen. Auch kleinere Choreografien wurden zur Nachahmung bereitgestellt. Die App gab ihren Nutzer:innen dadurch die Möglichkeit, sich wie ein Popstar zu fühlen beziehungsweise ihren Stars nachzueifern. Mit zusätzlichen Videoeffekten konnten schnell kurze (15 bis 60 Sekunden lange), professionelle Videos erstellt werden. Wie bei den anderen Apps auch konnten andere Nutzer:innen durch „Likes“ und Kommentare auf die veröffentlichten Videos reagieren. Mittlerweile gibt es bei TikTok alle Arten von Videos, die sich zum Beispiel mit Themen wie Beauty, Comedy, Politik oder Bildung beschäftigen, und das Format der Kurzvideos hat sich als Social-Media-Standard einen Namen gemacht und wird auch von anderen Diensten übernommen (bei Instagram etwa in Form der „Reels“).

[10] https://de.statista.com/statistik/daten/studie/181086/umfrage/die-weltweit-groessten-social-networks-nach-anzahl-der-user / Stand: 2026

[11] JIM-Studie 2025, S. 34

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

So beliebt die App bei ihren Nutzer:innen ist, umso kritischer sollte sie betrachtet werden. Hier ist zuerst einmal ihre Zugehörigkeit zum chinesischen Konzern ByteDance zu berücksichtigen. Dies legt zumindest die Vermutung nahe, dass die Daten der Nutzer:innen der chinesischen Regierung zugespielt werden könnten. Auch in den USA gibt es seit 2018 mit dem sogenannten Cloud Act eine gesetzliche Regelung, die es US-Behörden ermöglicht, auf Daten von US-Diensten auch im Ausland zuzugreifen. Wie häufig derartige Zugriffe passieren, lässt sich schwer sagen, es verdeutlicht jedoch allein die Möglichkeit, wie wichtig es ist, die Sicherheitseinstellungen anzupassen und die jeweiligen Informationen vor ihrer Veröffentlichung genau zu prüfen.

Zu den weiteren Herausforderungen beim Umgang mit TikTok zählen die möglichen In-App-Käufe. Beispielsweise können Nutzer:innen beim Streamen der Videos virtuelle Geschenke kaufen, um in einem Livestream zusätzlich aufzufallen.[12] Deshalb ist es wichtig, In-App-Käufe einzugrenzen beziehungsweise eine Drittanbietersperre einzurichten, um mögliche Abofallen auszuschließen.

Zusätzlich versuchen viele Nutzer:innen, mit besonders freizügigen Darstellungen Aufmerksamkeit, Likes und neue Follower:innen zu gewinnen. Dies birgt ähnliche Gefahren, wie wir sie bereits bei Snapchat oder Instagram kennengelernt haben. Die Möglichkeit, diese Videos zu kontrollieren, ist nicht gegeben. Eine Verbreitung im Internet lässt sich kaum verhindern.

Auch Themen wie Hatespeech, Cybermobbing, Fake News und die Verbreitung rechtsradikaler Inhalte spielen eine große Rolle. Es kam sogar zu Fällen von digitalen Hexenjagden, die in reale und tragische Gewaltverbrechen unter Teenagern wie dem sogenannten Fall Louise [13] mündeten oder zu Lynchjustiz-Aufrufen nach Falschnachrichten.[14] Deshalb hat TikTok mittlerweile Jugendschutzfilter, private Profile und eingeschränkte Kontaktfunktionen nachgerüstet.

Mehr zu TikTok auf:

- https://www.klicksafe.de/tiktok
- https://www.schau-hin.info/grundlagen/tiktok-das-steckt-hinter-der-trend-app
- https://www.internet-abc.de/eltern/kinder-und-tiktok/

[12] https://www.klicksafe.de/news/was-macht-mein-kind-eigentlich-bei-tiktok, Stand 09/2023

[13] https://www.wa.de/nordrhein-westfalen/luise-freundeberg-fall-taeterinnen-tiktok-namen-videos-bilder-polizei-nutzer-warnung-hetzjagd-92150127.html

[14] https://www.sueddeutsche.de/panorama/indien-sie-pruegeln-menschen-tot-weil-sie-fake-news-gelesen-haben-1.4037146

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

1.2 Welche Bedeutung haben Daten?

All die genannten Dienste sind für die Nutzer:innen kostenlos, dennoch verdienen die dahinterstehenden Unternehmen natürlich Geld damit. Das kalifornische Unternehmen Meta (Facebook, Instagram und Whatsapp) beispielsweise macht seinen Umsatz durch Werbung und virtuelle Güter: Hier lag der Gesamtumsatz im Jahr 2024 bei rund 164 Milliarden US-Dollar.[15]

Werbung spielt in sozialen Netzwerken also eine Bedeutung!

Dies gilt einerseits für die Diensteanbieter selbst, die sich regelmäßig durch die Werbeeinnahmen finanzieren, da die Dienste den Nutzer:innen kostenfrei zur Verfügung stehen. Dementsprechend wird das Nutzungsverhalten gezielt ausgewertet, um Nutzer:innen möglichst interessenentsprechende und damit teurer vermarktbare Werbung personalisiert anzubieten. Obwohl es manchmal anders wirkt, ist man als Nutzer:in nicht Kunde oder Kundin dieser Unternehmen, sondern im Gegenteil 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 Onlineunternehmen. Daten sind die Währung, mit der wir im Internet bezahlen.

Andererseits träumen auch immer mehr gerade jüngere Nutzer:innen davon, selbst gefeierte Influencer:innen zu werden und ihren Lebensunterhalt mit Social-Media-Postings zu bestreiten. Leider gelingt dies nur einer verschwindenden Minderheit, während die Mehrzahl sich für Kleinstbeträge vor der Kamera abrackert[16] und im Zweifelsfall noch Gefahr läuft, abgemahnt zu werden, wenn vergessen wird, einen Werbepost auch als solchen zu kennzeichnen.[17]

Mehr über Daten, Facebook, Google und Co. auf:

- www.youngdata.de
- www.klicksafe.de
- www.schau-hin.info
- www.lmz-bw.de

[15] https://de.wikipedia.org/wiki/Meta_Platforms#Finanzen, Stand 2026

[16] https://www.businessinsider.de/wirtschaft/umfrage-zeigt-wie-viel-influencer-verdienen-nur-4-prozent-koennen-von-ihren-accounts-leben/

[17] https://www.verbraucherzentrale.de/wissen/digitale-welt/soziale-netzwerke/influencerin-oder-nicht-wann-ein-beitrag-in-social-media-werbung-ist-39954

1.3 Wie öffentlich bin ich?

Sich im Internet zu präsentieren und mit anderen zu kommunizieren, übt eine große Faszination auf jüngere und ältere Menschen aus. Es gibt vielfältige Gründe, sich an der Kommunikation in den 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 Freund:innen habe ich?“
- „Wie reagieren andere auf mich?“

Solche Fragen der Selbstfindung und Identitätsbildung finden mehr und mehr in sozialen Netzwerken statt. Gerade jüngere Nutzer:innen interagieren hier mit ihren Freund:innen und Bekannten, suchen und finden Gleichgesinnte und können sich zu nahezu jedem Thema umfassend informieren. Doch die unterschiedlichen Angebote bergen auch zahlreiche Risiken: Die jeweiligen Profileinstellungen entscheiden darüber, ob Informationen öffentlich sichtbar sind, das heißt, ob diese von allen Nutzer:innen eingesehen werden können. Die Tragweite solcher offenen Einstellungen ist vielen nicht bewusst. Auch die damit verbundenen Risiken und möglichen Konsequenzen sind den meisten nicht bekannt oder sie werden ignoriert. Folglich verhalten sich Nutzer:innen häufig zu sorglos und riskieren mit der Weitergabe persönlicher Informationen negative Reaktionen, wie zum Beispiel die ungewollte Verbreitung eines persönliches Bildes oder beleidigende Kommentare durch fremde Personen.

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 nach sich ziehen kann. Zum einen ist das natürlich die wirtschaftliche Verwertung von Daten, beispielsweise zu Werbezwecken wie der Anzeige personalisierter Werbung. Zum anderen spielen aber auch Bild- und Persönlichkeitsrechte von anderen Personen eine Rolle.

In vielen sozialen Netzwerken gibt es Privatsphäre-Einstellungen, in denen man die Sichtbarkeit von Informationen und eingestellten Beiträgen anpassen kann. Oftmals ist voreingestellt, dass die Informationen erst einmal öffentlich einsehbar sind. Folglich müssen Nutzer:innen selbst aktiv werden, um die eigenen Einstellungen anzupassen und auf „privat“ zu stellen.

Problematisch wird es auch, wenn Kinder und Jugendliche ein falsches Alter angeben: Bei Facebook beispielsweise haben 13- bis 17-Jährige spezielle Minderjährigen-Accounts mit strengeren Privatsphäre-Einstellungen. Wird ein:e Nutzer:in (für Facebook) 18, ändern sich diese Einstellungen automatisch in eine weniger restriktive Form (siehe Facebook-Hilfeseite). Mit einem falschen Alter können nicht nur Jugendliche unter 13 Jahren in Facebook aktiv sein, sondern es können

sich auch Einstellungen ändern, ohne dass der Nutzer oder die Nutzerin auch wirklich volljährig wird. Eine wirksame Alterskontrolle gibt es bei den meisten sozialen Netzwerken nicht.

1.4 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 selbst Bilder und Videos eingestellt und geteilt werden. Dabei kommt Persönlichkeits- und Urheberrechten eine wichtige Bedeutung zu (siehe Modul 3, „Urheber- und Persönlichkeitsrechte im Internet“).

Bilder, die ich nicht selbst gemacht habe, darf ich in der Regel nicht ohne Zustimmung der Person veröffentlichen, bei der die Urheber- beziehungsweise Inhaberrechte liegen. 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 (zum Beispiel Tourist:innen vor dem Mainzer Dom).

1.5 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“, also „Denk nach, bevor du etwas postest“), denn es gilt der Satz:

„Das Internet vergisst nichts.“

Je nach Nutzungsbedingungen eines Dienstes werden dem Anbieter weitgehende Nutzungsrechte eingeräumt; auch privat lassen sich online gestellte Bilder vervielfältigen und weiterverbreiten.

In den Instagram- und Facebook-AGB steht beispielsweise:

„Insbesondere wenn du Inhalte, die durch geistige Eigentumsrechte geschützt sind (wie Fotos oder Videos), auf oder in Verbindung mit unseren Produkten teilst, postest oder hochlädst, räumst du uns eine nicht-ausschließliche, übertragbare, unterlizenzierbare und weltweite Lizenz ein, deine Inhalte (gemäß deinen Privatsphäre- und App-Einstellungen) zu hosten, zu verwen-

den, zu verbreiten, zu modifizieren, auszuführen, zu kopieren, öffentlich vorzuführen oder anzuzeigen, zu übersetzen und abgeleitete Werke davon zu erstellen. Diese Lizenz dient nur dem Zweck, dir unsere Produkte bereitzustellen. Das bedeutet beispielsweise, dass du uns, wenn du ein Foto auf Facebook teilst, die Berechtigung erteilst, es zu speichern, zu kopieren und mit anderen zu teilen (wiederum im Einklang mit deinen Einstellungen). Dies können z. B. Meta-Produkte oder Dienstleister sein, die diese von dir genutzten Produkte und Dienste unterstützen."[18]

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[19], das auch im Unterricht eingesetzt werden kann.

Ein Grundsatz sollte also sein, nur Dinge hochzuladen, die man auch fremden Menschen zeigen würde. Die Privatsphäre-Einstellungen sollten die Freigabe der eigenen Informationen deutlich begrenzen und lediglich einer ausgewählten Gruppe anderer Nutzer:innen zugänglich gemacht werden. Zusätzlich erscheint es sinnvoll, den wirklichen Namen nicht für ein privates Profil zu verwenden. Stattdessen sollte ein Pseudonym gewählt werden, um zum Beispiel die Auffindbarkeit über eine Suchmaschine zu vermeiden.

Weitere Datenschutztipps gibt es hier:

- www.youngdata.de
- www.klicksafe.de
- www.schau-hin.info
- www.lmz-bw.de

[18] https://de-de.facebook.com/legal/terms, Stand: 20.10.2022.

[19] https://www.youtube.com/watch?v=n1TroNdzbWg, Stand: 18.07.2023.

1.6 Was sind Privatsphäre-Einstellungen?

Die meisten Dienste und Anwendungen bieten auf ihren Seiten sogenannte Privatsphäre-Einstellungen. Hier lässt sich einstellen, wer welche Inhalte sehen darf. So gibt es beispielsweise bei TikTok oder Instagram die technische Möglichkeit, einzuschränken, wem das eigene Profil und die geposteten Inhalte angezeigt werden. Bei TikTok 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 beziehungsweise der Nutzerin.

Bei WhatsApp kann in den Privatsphäre-Einstellungen der „Zuletzt online“-Status ausgeschaltet werden. Auch die Sichtbarkeit der Profilbilder lässt sich hier einschränken.

Weitere Tipps und Infos zu Privatsphäre-Einstellungen bei den jeweiligen Diensten:

- WhatsApp: https://www.klicksafe.de/whatsapp
- Instagram: https://www.klicksafe.de/instagram und https://www.handysektor.de/apps-upps/daumen-hoch/detailansicht/article/mehr-kontrolle-ueber-dein-instagram-profil.html
- Snapchat: https://handysektor.de/snapchat
- https://www.klicksafe.de/tiktok

1.7 Was sollte man über WhatsApp noch 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 Meta (ehemals Facebook) gehört, immer wieder in der Kritik. So machte Facebook Ende August 2016 Schlagzeilen durch die Ankündigung, zukünftig die Telefonnummern der Nutzer:innen von WhatsApp 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. Diese Klage wurde schlussendlich nach etlichen Jahren und Instanzen 2022 vor dem Europäischen Gerichtshof EuGH (C-40/17) erfolgreich beendet.[20]

[20] https://www.verbraucherzentrale.nrw/wissen/digitale-welt/datenschutz/eughurteil-likebutton-von-facebook-nur-mit-info-an-nutzer-12029, Stand: 10.08.2022

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 Freund:innen 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 nutzen. Dies hat mit Datenverantwortung für andere zu tun und ist auch im Hinblick auf deutsches Datenschutzrecht schwierig.[21]

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 Meta kein Geld damit verdient. Im Gegenteil: Die Übernahmesumme in Milliardenhöhe zeigt, dass WhatsApp (beziehungsweise die damit verfügbaren Daten) als sehr wertvoll angesehen wurde.

Abseits des Datenschutzes spielen auch Kettenbriefe und Spam in WhatsApp eine Rolle. Mit dem Hinweis auf vermeintliche Gutscheine oder neue WhatsApp-Funktionen wird zum Anklicken eines Links verleitet. Dahinter verstecken sich oft dubiose Gewinnspiele, im schlechtesten Fall fängt man sich Schädlinge ein oder tappt in eine Abofalle (siehe auch Modul 2, „Smartphones, Apps und Games“, Kapitel, 1.2 „Wie finanzieren sich kostenlose Apps?“).

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 (https://www.handysektor.de/mediathek/videos/erklaervideo-whatsapp-stress.html) dargestellt wird.

Die Lesebestätigung in WhatsApp sowie der „Zuletzt online“-Status können ausgeschaltet werden. Wie das geht, zeigt www.schau-hin.info.

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

Mehr zum Thema WhatsApp auf:

- www.schau-hin.info
- www.youngdata.de
- www.handysektor.de

[21] https://www.lto.de/recht/hintergruende/h/ag-bad-hersfeld-beschluss-f12017easo-whatsapp-nutzung-kontakte-eltern-kontrolle-kinder-bis-volljaherigkeit/, Stand 12.09.2023

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

1.8 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 aktiver man im Internet ist, desto mehr Passwörter hat man also. 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 ein sicheres Passwort aus? Und wie kann man sich solche sicheren Passwörter auch merken?

Die Seite www.youngdata.de gibt Informationen und Hintergrundwissen rund um sichere Passwörter.

Ein sicheres Passwort sollte:

- **mindestens zwölf Stellen lang sein (besser sogar 20),**
- **aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (&, %, $, #, ?, ! und so weiter) bestehen,**
- **nicht in einem Wörterbuch zu finden sein,**
- **nicht auf die eigene Person hindeuten (Geburtsdaten und Ähnliches) sowie**
- **keine Zahlen- oder Buchstabenfolge sein (123456 ..., ABCDEF ...).**

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

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**austiere**: 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 Zeichenfolge.

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

Außerdem sollte man regelmäßig auf der Seite des Hasso Plattner Instituts mit dem Identity Leak Checker[22] oder auf der Seite des australischen Sicherheitsforschers Troy Hunt[23] prüfen, ob die eigenen Accounts geleakt wurden und auf dem internationalen Datenschwarzmarkt zum Kauf angeboten werden – dann gilt es, schleunigst die Zugangsdaten zu ändern und besonders gefährdete Dienste mittels Zwei-Faktor-Authentifizierung abzusichern.

Tipp: Immer mehr Internetbrowser bieten eine automatisierte Überwachung der eigenen Accounts auf Datenlecks an, wie etwa dem Firefox Monitor[24]

Mehr zum Thema Passwörter findet sich im „Medien sicher nutzen“-Modul 5, „Daten- und Accountsicherheit“, Kapitel 6.2, „Sichere Passwörter“.

[22] https://sec.hpi.de/ilc/search?lang=de

[23] https://haveibeenpwned.com/

[24] https://monitor.firefox.com/

2. Links und weiterführende Informationen

Die EU-Initiative klicksafe stellt eine Reihe von Materialien zum Thema bereit. Zu einzelnen Anwendungen wie Snapchat oder YouTube gibt es Leitfäden, wie genau beispielsweise Privatsphäre-Einstellungen vorgenommen werden können. Auch zum Thema Privatsphäre aus medienethischer Perspektive finden sich verschiedene Materialien.	www.klicksafe.de/materialien
Auf Handysektor.de können die Vor- und Nachteile verschiedener Apps 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 auf verschiedene Social-Media- und Instant-Messenger-Anwendungen.	www.youngdata.de
Die Initiative „SCHAU HIN! Was Dein Kind mit Medien macht“ richtet sich primär an Eltern. Hier gibt es ebenfalls Informationen zu sozialen Netzwerken.	www.schau-hin.info
Im Materialkompass Verbraucherbildung des Verbraucherzentrale Bundesverbands finden sich eine Reihe von geprüften Unterrichtseinheiten zum Thema. Am besten das gewünschte Stichwort in das Suchfeld eingeben.	https://www.verbraucher-bildung.de/materialkompass

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

2.1 Mögliche Verknüpfung mit anderen Themen

Onlinewerbung: 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 eingegangen werden. Geschäftsmodelle und Onlinewerbung werden in „Medien sicher nutzen“ – Modul 2 behandelt.

Urheber- und Persönlichkeitsrechte: Bilder spielen eine große Rolle in 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. Urheber- und Persönlichkeitsrechte werden in „Medien sicher nutzen“ - Modul 3 behandelt.

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 Privatsphäre-Einstellungen 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 und so weiter).

3. 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 kostenlosen Dienste.
- Die SuS wissen, dass sie 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 Privatsphäre-Einstellungen 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 sie die Fotos nur mit Erlaubnis der abgebildeten Personen 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.

- 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 in Problemfällen wenden können.

Methoden zu den Lernzielen im Kasten finden sich im „Medien sicher nutzen“-Modul 3, „Urheber- und Persönlichkeitsrecht“ .

	Methode	Zeit (Minuten)	Arbeits- und Sozialform/Methode	Medien/ Material
1 2 3	01 Handyampel	10	Einzelarbeit, anschließend Plenum	Arbeitsblatt „Handyampel“ in Anzahl der SuS
1 2 3	02 Clevere Netzwerker:innen	10–20	Partnerarbeit, Aufgreifen im Plenum	Arbeitsblatt „Clevere Netzwerker:innen“ in Kurz- oder Langversion in Anzahl der SuS
1 2 3	03 Was verrate ich von mir?	10	Plenum	Tafel, Kreide oder ähnliche Visualisierungsmöglichkeit, alternativ Kopiervorlage „Was verrate ich von mir?“
1 2 3	04 Öffentlich oder privat?	15–20	Gruppenarbeit	Kopiervorlage „Öffentlich oder privat?“ in Gruppenanzahl, Kleber, Scheren
1 2 3	05 Unterrichtsgespräch „Das Netz vergisst nichts“	15	Plenum	Präsentationsmöglichkeit für Webvideo
1 2 3	06 Check dein Profil, bevor es andere tun	15	Plenum	Präsentationsmöglichkeit für Webvideo
1 2 3	07 PC-Übung „Ego-Googeln“	20 (+ 15)	PC-Partner- oder Einzelarbeit (zusätzlich Plenum)	PCs mit Internetzugang
1 2 3	08 Unterrichtsgespräch „WhatsApp-Statistik“	10	Plenum, Unterrichtsgespräch	eigene Smartphones der SuS
1 2 3	09 Sicheres Passwort	20	Einzel- oder Gruppenarbeit, Plenum, Unterrichtsgespräch	für Einzel- oder Gruppenarbeit Arbeitsblatt „Sicheres Passwort“

	Methode	Zeit (Minuten)	Arbeits- und Sozial-form/Methode	Medien/ Material
1 2 3	10 PC_Übung „Passwortprüfer“ (Fortsetzung von „Sicheres Passwort“)	15	Einzel- oder Partnerarbeit	PCs mit Internetzugang
1 2 3	11 WhatsApp, Instagram und Co.: sicher in sozialen Netzwerken	10	Einzelarbeit, Plenum, Unterrichtsgespräch	Arbeitsblatt „Whats-App, Instagram und Co.: sicher in sozialen Netz-werken“ in Anzahl der SuS (oder an der Tafel für Plenumsarbeit)

Anmerkung: Allgemeine Informationen zum Thema Soziale Netzwerke finden sich in der PowerPoint-Präsentation „Digitale Lebenswelten“. Darüber hinaus gibt es Präsentationen zu Instagram, Tiktok und Snapchat.

Hinweise:

①②③ Schwierigkeitsstufen der jeweiligen Methoden. Zutreffendes ist rot gefüllt.
sprachlich leicht zugänglich
Onlinematerial
SuS: Schülerinnen und Schüler

3.1 Handyampel

Dauer:	circa 10 Minuten
Ziel:	Einstieg ins Thema Messenger, Sensibilisierung für Nachrichteninhalte
Schwierigkeit:	1 2 3
Material:	Arbeitsblatt „Handyampel“
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 beziehungsweise nicht okay finden. Gemeinsam werden danach die Ergebnisse besprochen.
Hinweise:	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.

3.2 Clevere Netzwerker:innen

Dauer:	10–20 Minuten
Ziel:	Einstieg ins Thema, Sensibilisierung für Daten
Schwierigkeit:	1 2 3
Material:	entweder Arbeitsblatt „Clevere Netzwerker:innen“ (Kurzversion) oder Arbeitsblatt „Clevere Netzwerker:innen“ (Langversion) in Anzahl der SuS
Technik:	ohne
Sozialform:	Partnerarbeit, Aufgreifen im Plenum
Umsetzung:	Jede Schülerin und jeder Schüler erhält einen Fragebogen, den sie oder er 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 zum Beispiel 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 SuS 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!

3.3 Was verrate ich von mir?

Dauer:	circa 10 Minuten
Ziel:	Einstieg ins Thema, Sensibilisierung für Daten
Schwierigkeit:	1 2 3
Material:	Tafel, Kreide oder andere Visualisierungsmöglichkeit, alternativ Kopiervorlage „Was verrate ich von mir?“
Technik:	ohne
Sozialform:	Plenum
Umsetzung:	Was können andere von mir wissen? Was behalte ich lieber für mich? Die Antworten auf diese Brainstorming-Fragen werden an der Tafel gesammelt. Die Angaben, die andere kennen dürfen, werden dabei in die Sprechblase geschrieben. Die anderen kommen in den Menschen.
Hinweis:	Entweder sammelt die referierende Person 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 Kopiervorlage „Was verrate ich von mir?“) beschriften, im Plenum werden einzelne Aspekte herausgegriffen und diskutiert.
Kernbotschaft:	Daten sind nicht gleich Daten.

3.4 Öffentlich oder privat?

Dauer:	circa 15–20 Minuten
Ziel:	Vertiefung des Themas, Sensibilisierung für Daten, Datenpreisgaben differenzieren lernen, Privatsphäre-Einstellungen kennenlernen
Schwierigkeit:	❶❷③
Material:	Kopiervorlage „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“ vom 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 Privatsphäre-Einstellungen sprechen, die aktiv von den Nutzer:innen vorgenommen werden müssen und die zum Teil 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. Die referierende Person 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 Privatsphäre-Einstellungen in sozialen Netzwerken eingegangen werden.
Kernbotschaft:	Privatsphäre-Einstellungen nutzen!

Diese Übung ist angelehnt an einen Arbeitsauftrag im (mittlerweile nicht mehr verfügbaren) Zusatzmodul „Ich bin öffentlich ganz privat“ von klicksafe.

3.5 UnterrichtsgespräcH „Das Netz vergisst nicht“

Dauer:	circa 15 Minuten (ja nach Diskussion)
Ziel:	Vertiefung des Themas, Sensibilisierung für die Langlebigkeit von Informationen im Netz, Überleitung zum Thema Privatsphäre-Einstellungen
Schwierigkeit:	① ② ③
Material:	ohne
Technik:	Präsentationmöglichkeit für Video „Date“ (http://www.watchyourweb.de/p3548375992_450.html#film_anschauen)
Sozialform:	Plenum
Alternative:	Video „Check dein Profil, bevor es andere tun“ (https://www.youtube.com/watch?v=n1TroNdzbWg)
Umsetzung:	Gemeinsam wird das Video „Date“ von Watchyourweb angeschaut. Anschließend wird eine Diskussion über den Satz „Das Netz vergisst nicht“ geführt. Mögliche Fragen: Welches Problem hat der Junge in dem Film? Inwiefern könnte das wirklich passieren? Wie kann man das verhindern?
Hinweise:	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. Gegebenenfalls kann man den Film abschließend auch noch mal anschauen. Diese Übung ist angelehnt an Material der Verbraucherzentrale Nordrhein-Westfalen.
Kernbotschaft:	Einmal ins Internet gestellte Daten können noch lange bestehen bleiben.

3.6 Check dein Profil, bevor es andere tun

Dauer:	circa 15 Minuten (je nach Diskussion)
Ziel:	Vertiefung des Themas, Sensibilisierung für die Langlebigkeit von Informationen im Netz, Überleitung zum Thema Privatsphäre-Einstellungen
Schwierigkeit:	① ② ③
Material:	ohne
Technik:	Präsentationmöglichkeit für Video „Check dein Profil, bevor es andere tun“ (https://www.youtube.com/watch?v=n1TroNdzbWg)
Sozialform:	Plenum
Alternative:	Unterrichtsgespräch „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. Mögliche Fragen: Welches Problem hat der junge Mann in dem Film? Könnte das wirklich passieren? Wie kann man das verhindern? Inwiefern ist das Profil im Netz für Arbeitgeber:innen 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 Onlineprofil trifft), kann man den Film abschließend auch noch mal zeigen.
Kernbotschaft:	Informationen über mich im Netz können auch für andere interessant sein.

3.7 PC-Übung „Ego-Googeln“

Dauer:	10–15 Minuten (+ 5 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 Internetzugriff (wahlweise auch Smartphones)
Sozialform: im Plenum	Einzel- oder Gruppenarbeit am PC/Smartphone, anschließende Diskussion
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). Die SuS sollten dabei ihr „analoges Profil“ und ihr „digitales/virtuelles Profil“ googeln. **Auftrag: „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. Gegebenenfalls sollte die Sprache auf Privatsphäre-Einstellungen kommen, 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). Hier kann man den SuS auch zeigen, wie sich Bilder aus der Google-Suche entfernen lassen.
Kernbotschaft:	Ich weiß, was das Netz über mich weiß!

3.8 Unterrichtsgespräch „WhatsApp-Statistik“

Dauer:	circa 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 gehen in die Einstellungen. Unter „Speicher und Daten“ 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.

3.9 Sicheres Passwort

Dauer:	circa 20 Minuten
Ziel:	Sensibilisierung für die Bedeutung von sicheren Passwörtern
Schwierigkeit:	1 2 3
Material:	gegebenenfalls → Arbeitsblatt „Sicheres Passwort“
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 ein sicheres Passwort aus? Entweder kann mit dem Arbeitsblatt gearbeitet werden (für ältere SuS empfiehlt sich der Profitipp), oder die referierende Person schreibt die wichtigsten Kriterien eines sicheren Passworts an die Tafel. Dann wird das Passwort „MH,dh3E;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 Hackerangriffen mit automatisierten Programmen gearbeitet wird, die in Sekundenschnelle verschiedene Listen durchgehen. Deshalb sollte man keine „sinnvollen“ Wörter verwenden, also keine, die in Wörterbüchern zu finden sein könnten, und keine gängigen Zahlenkombinationen wie Geburtsdaten und Ähnliches. Auch die Kombination aus beidem ist nicht sicher.

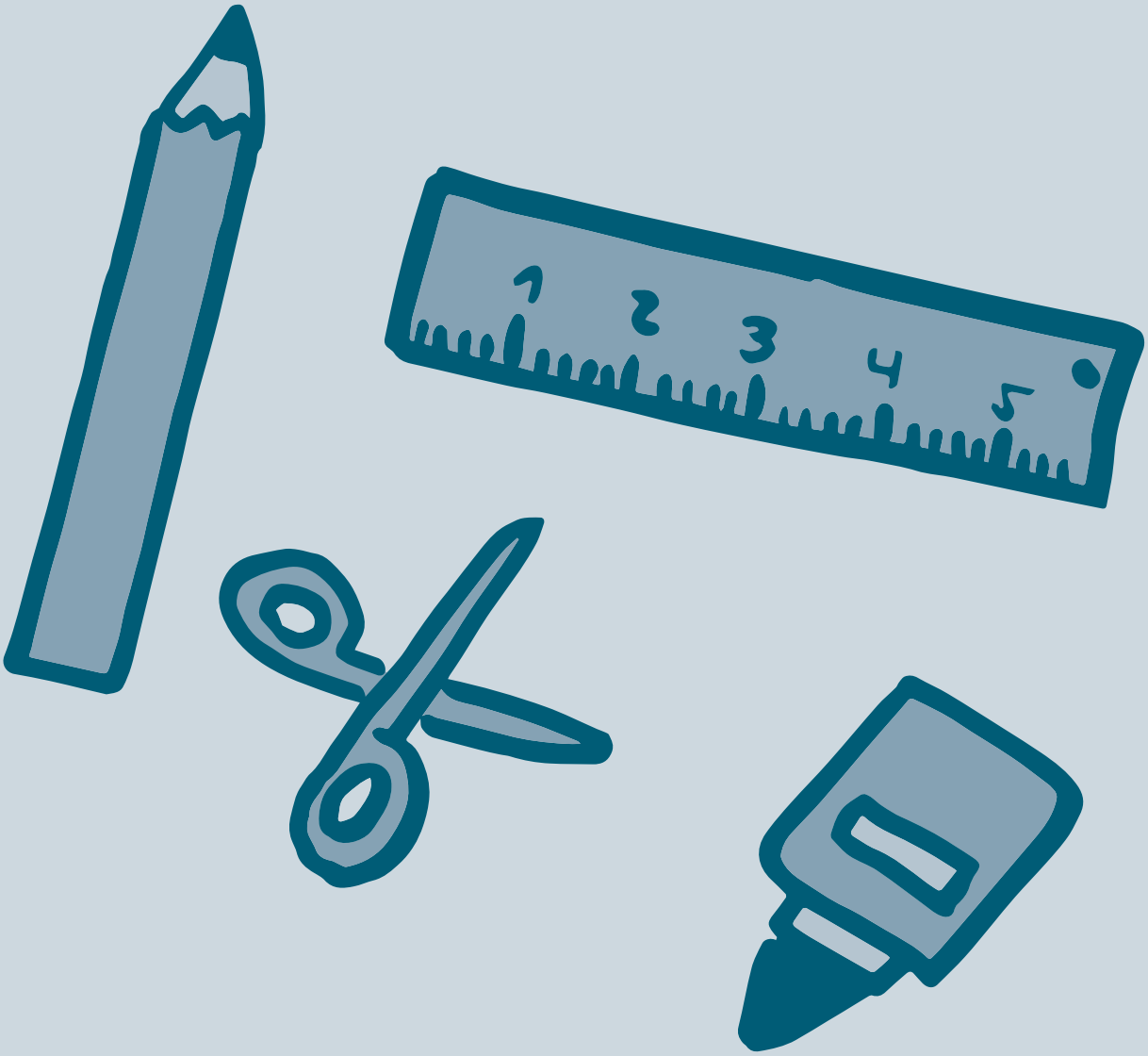
3.10 PC-Übung „Passwortprüfer“ (Fortsetzung von „Sicheres Passwort“)

Dauer:	circa 15 Minuten
Ziel:	Sensibilisierung für die Bedeutung von sicheren Passwörtern
Schwierigkeit:	1 2 3
Material:	ohne
Technik:	PCs mit Internetzugriff
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 auf der Seite live noch weitere Passwörter getestet werden. Vorher sollte aber der Arbeitsauftrag klar sein, um allzu wildes Tippen zu vermeiden.

3.11 WhatsApp, Instagram und Co.: sicher in sozialen Netzwerken

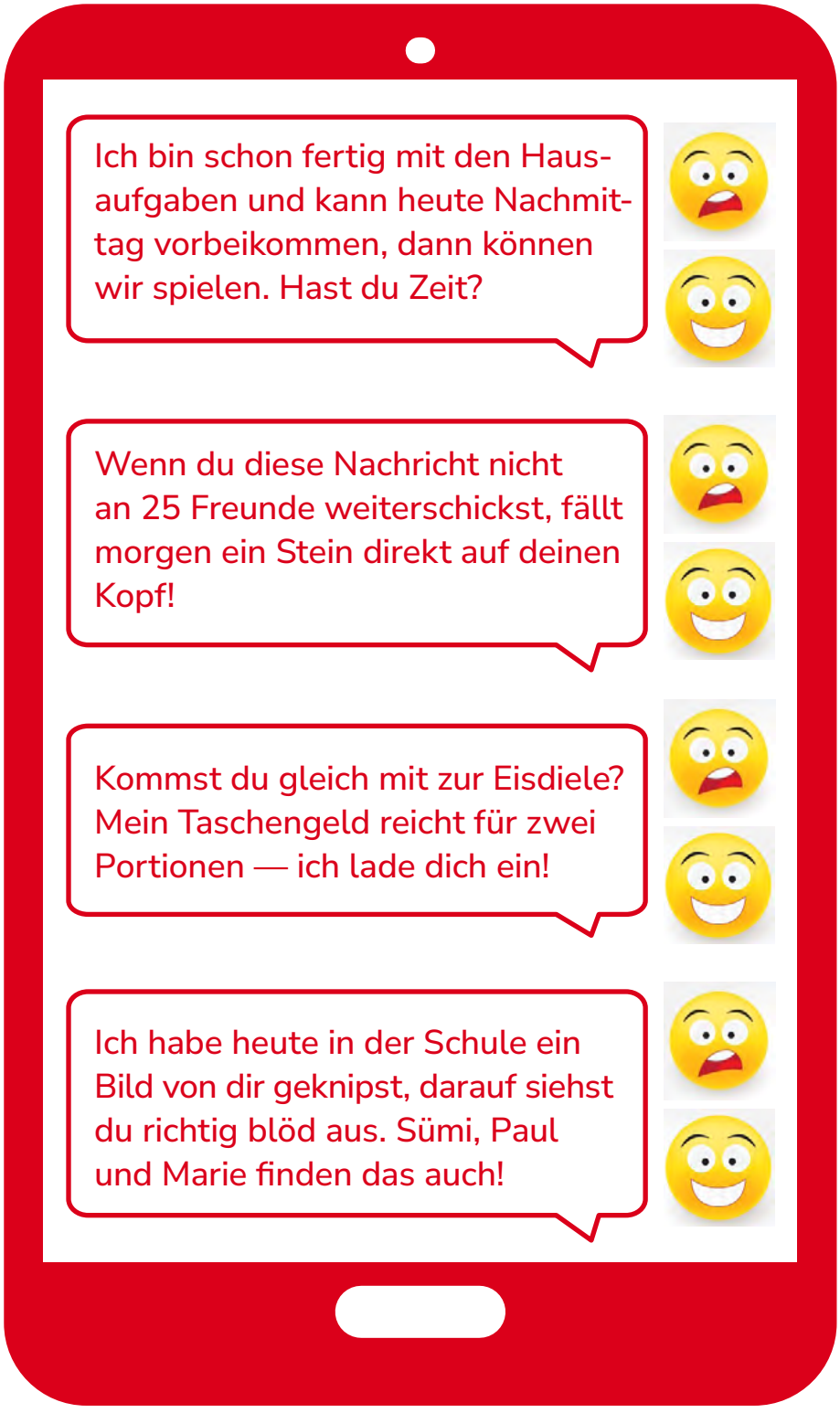
Dauer:	circa 10 Minuten
Ziel:	Ergebnissicherung
Schwierigkeit:	1 2 3
Material:	Arbeitsblatt „WhatsApp, Instagram und Co.: sicher in sozialen Netzwerken
Technik:	ohne
Sozialform:	Unterrichtsgespräch, Einzelarbeit
Umsetzung:	Zum Abschluss des Schwerpunkts „soziale Netzwerke“ werden in einem kurzen Unterrichtsgespräch 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.

4. Materialien



4.1 Arbeitsblatt „Handyampel“

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



Emoticons: designed by Milano83 – Freepik.com

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

4.2 Arbeitsblatt „Clevere Netzwerker:innen“ (Kurzversion)

Kennst du deinen Sitznachbarn/deine Sitznachbarin?

Wie lautet der Vorname deines Sitznachbarn/deiner Sitznachbarin?

Kreuze an:

In welche Schule geht er/sie?	☐ Grundschule	☐ weiterführende Schule	
Welche Hobbys hat er/sie?	☐ Sport	☐ Musik	☐ Freund:innen
	☐ Shoppen	☐ Lesen	☐ Computer
Was ist sein/ihr Lieblingsfach?	☐ Deutsch	☐ Kunst	☐ Mathe
	☐ Sport	☐ Musik	☐ Englisch

Kennst du deinen Sitznachbarn/deine Sitznachbarin?

Wie lautet der Vorname deines Sitznachbarn/deiner Sitznachbarin?

Kreuze an:

In welche Schule geht er/sie?	☐ Grundschule	☐ weiterführende Schule	
Welche Hobbys hat er/sie?	☐ Sport	☐ Musik	☐ Freunde
	☐ Shoppen	☐ Lesen	☐ Computer
Was ist sein/ihr Lieblingsfach?	☐ Deutsch	☐ Kunst	☐ Mathe
	☐ Sport	☐ Musik	☐ Englisch

4.3 Arbeitsblatt „Clevere Netzwerker:innen“ (Langversion)

Kennst du deinen Sitznachbarn/deine Sitznachbarin?

Wie lautet der Vorname deines Sitznachbarn/deiner Sitznachbarin?

Kreuze an:

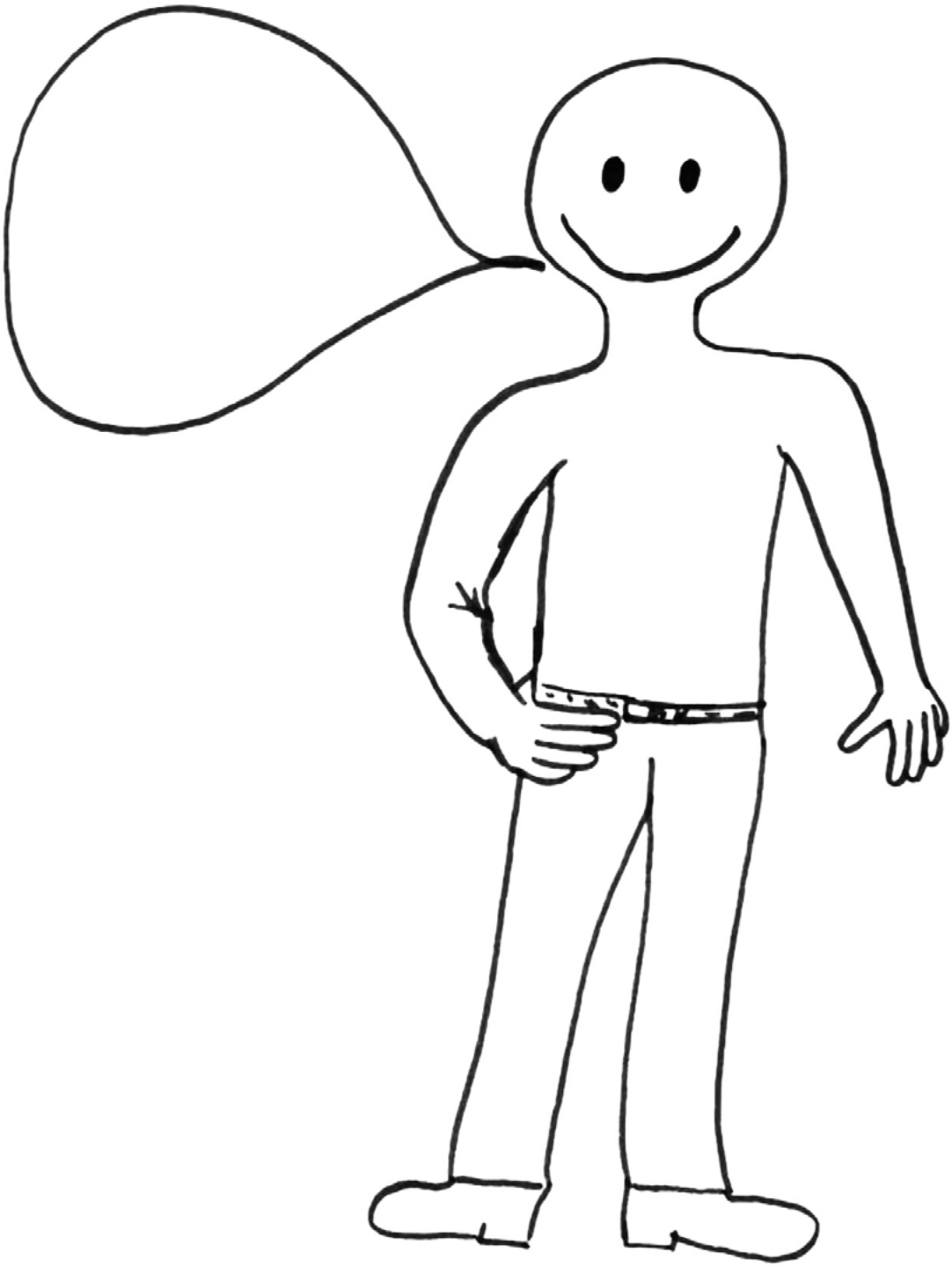
In welche Schule geht er/sie?	☐ Grundschule	☐ weiterführende Schule	
Wie kommt er/sie zur Schule?	☐ zu Fuß	☐ Die Eltern fahren.	☐ mit dem Fahrrad
	☐ mit dem Bus	☐ mit dem Roller	
Welche Hobbys hat er/sie?	☐ Sport	☐ Musik	☐ Freund:innen
	☐ Shoppen	☐ Lesen	☐ Computer
Was ist sein/ihr Lieblingsfach?	☐ Deutsch	☐ Kunst	☐ Mathe
	☐ Sport	☐ Musik	☐ Englisch
Was isst er/sie am liebsten?	☐ Pizza	☐ Döner	☐ Spaghetti
	☐ Hamburger	☐ Pfannkuchen	☐ Eis
Kennst du seine/ihre Telefonnummer?		☐ ja	☐ 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 ☐	nein ☐
Dem besten Freund/der besten Freundin?	ja ☐	nein ☐
Einer Nachbarin?	ja ☐	nein ☐
Einem Lehrer?	ja ☐	nein ☐
Der Schulleitung?	ja ☐	nein ☐
Einem Mädchen aus der 8. Klasse?	ja ☐	nein ☐
Dem Busfahrer?	ja ☐	nein ☐
An der Schuleingangstür aufhängen?	ja ☐	nein ☐
Bilde die Summe der „Jas“ und „Neins“.	ja	nein

4.4 Kopiervorlage „Was verrate ich von mir?“

Was verrate ich von mir?



4.5 Kopiervorlage „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

wovor ich Angst habe

mein Nachname

mein neuester Lieblingsfilm

Farbe meiner Unterwäsche

welchen Lehrer oder welche Lehrerin ich blöd finde

meine Telefonnummer

meine Handynummer

wo ich wohne

Namen meiner Eltern

ob ich Pickel habe

wer meine beste Freundin oder mein bester Freund ist

wie oft ich mir die Zähne putze

Öffentlich / für alle:

Auf jeden Fall privat:

Nicht eindeutig:

Für Freundinnen und Freunde:

4.6 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 Hacker:innen ganz schön leicht.

Ein sicheres Passwort sollte so aussehen:

- mindestens zwölf Stellen lang – je länger, desto besser!
- Mischung aus Groß- und Kleinbuchstaben, Zahlen und 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!

Lösung:
geheim, Passwort, 123456, hallo

So erstellt ihr ein sicheres Passwort in nur drei 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: „**I**ch **h**abe **1** **d**icken**,** **r**oten **K**ater**,** der **15** **J**ahre **a**lt **i**st **u**nd **v**iel **f**risst**.**"

3. **Schreibt die Anfangsbuchstaben und Satzzeichen ab:**

   Also so: **Ih1d,rK,d15Jaiuvf.**

   Fertig ist euer Passwort.

Schlüssel: Clker-Free-Vector-Images, Pixabay.com; Lizenz: CC0
Schloss: OpenClipart-Vectors, Pixabay.com; Lizenz: CC0

Ihr müsst euch nur noch den Satz merken!

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

Verbraucherzentrale Rheinland-Pfalz e.V., Stand: 2026

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"?

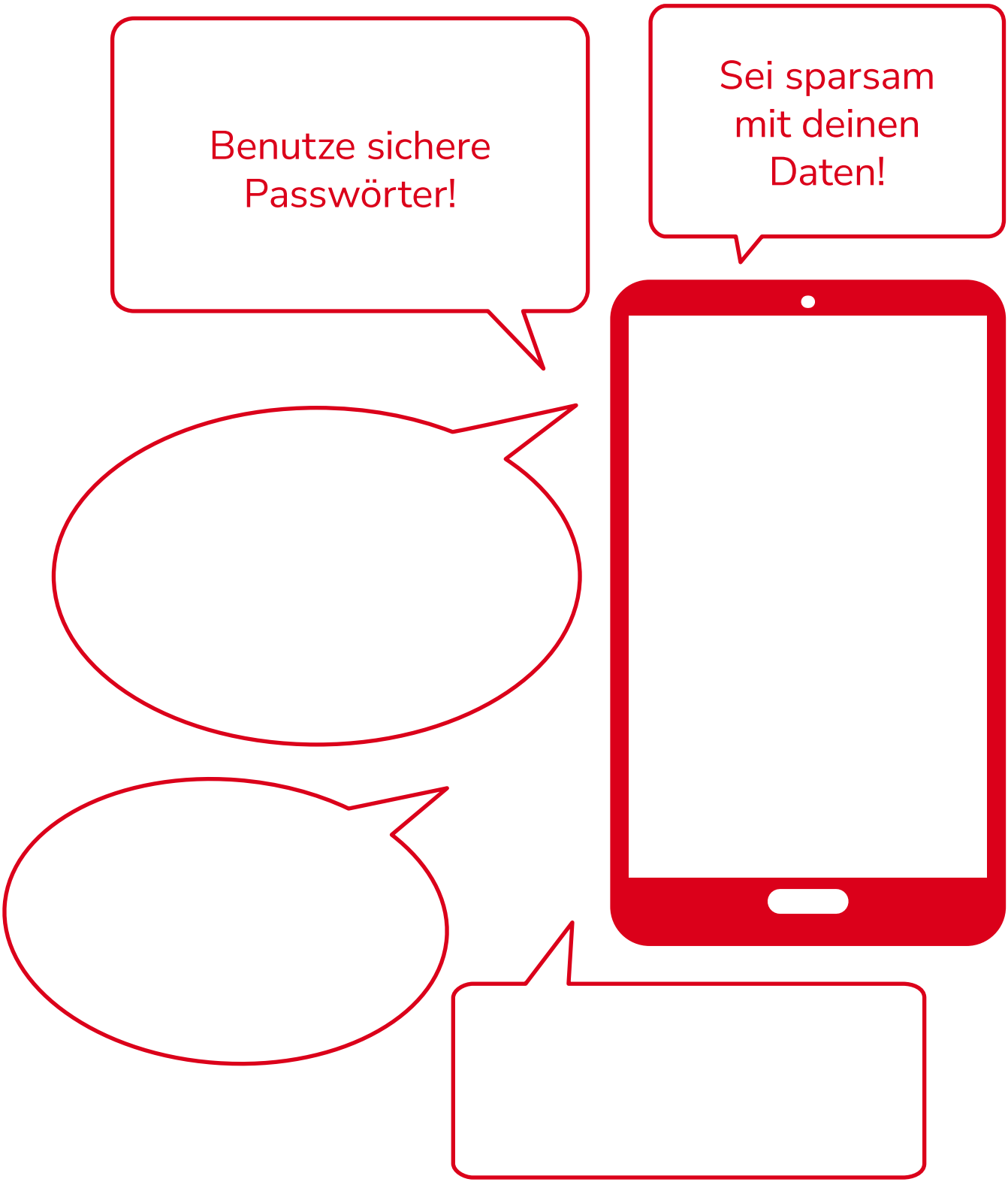
Und wie mit deinem eigenen, ausgedachten Passwort?

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

Lösung:
Sg#8Jeeenjnnj?ne

4.7 Arbeitsblatt „WhatsApp, Instagram und Co.: sicher in sozialen Netzwerken“

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



Verbraucherzentrale
Rheinland-Pfalz

Impressum

Herausgebeben von:
Verbraucherzentrale Rheinland-Pfalz e.V.
Seppel-Glückert-Passage 10, 55116 Mainz
T +49 6131 28480
F +49 6131 284866
info@vz-rlp.de
verbraucherzentrale-rlp.de

Für den Inhalt verantwortlich:
Heike Troue, Vorständin der Verbraucherzentrale Rheinland-Pfalz e.V.

Redaktion und Text:
Max Heitkämper, Ruth Preywisch, Jeanine Wein, Verbraucherzentrale Rheinland-Pfalz e. V.

Gestaltung:
alles mit Medien

Lektorat:
WORDS IN FLOW

Bildnachweise:
Titel – iStock.com/franckreporter

Stand:
01/2026

Gedruckt auf 100 % Recyclingpapier.

RheinlandPfalz
MINISTERIUM FÜR FAMILIE, FRAUEN, KULTUR UND INTEGRATION