GESELLSCHAFT FÜR FORSCHUNGS FÖRDERUNG NIEDERÖSTERREICH

DiabPeerS

TEIL 3 - SICHER UND KOMPETENT DURCHS INTERNET

Astrid Ebner-Zarl, Johanna Grüblbauer, Elisabeth Höld, Daniela Wewerka-Kreimel, Ursula Hemetek | FH_STP | FACHHOCHSCHULE ST. PÖLTEN GMBH CAMPUS-PATZ 1 A-3100 ST. PÖLTEN

GESELLSCHAFT FÜR FORSCHUNGS FÖRDERUNG NIEDERÖSTERREICH

DiabPeerS

Inhalt

1 Einleitung

Während Ihrer Tätigkeit als Moderatorin oder Moderator werden Sie sich öfter im Internet nach Artikeln und Materialien umschauen, um sie mit den Gruppenmitgliedern zu teilen oder sich auch selbst über bestimmte Themen kundig zu machen. Immer wieder werden Sie auch mit Beiträgen der Gruppenmitglieder umgehen müssen. Deswegen möchten wir Ihnen abschließend noch einige hilfreiche Tipps dazu geben.

Diese Fragen sollten Sie als Moderatorin oder Moderator im Hinterkopf behalten:

1) Welche Quellen zu Gesundheitsinformationen sind vertrauenswürdig? Wo gibt es medizinisch einwandfreie Informationen, etwa zur richtigen Ernährung bei Diabetes?
2) Was und wie viel gebe ich beim Aufruf von Websites oder bei der Nutzung von Apps über mich preis? Wie bekomme ich mehr Einblick und Kontrolle darüber?
3) Wo mischt sich Information mit Werbung bzw. wo ist Werbung als Information getarnt?
4) Welche problematischen Inhalte können bei meinen Internetrecherchen oder seitens der Gruppenmitglieder auftauchen und wie erkenne ich diese?

Die folgenden Kapitel sollen Ihnen Orientierung bezüglich dieser Fragen geben.

2 Vertrauenswürdige Quellen für Gesundheitsinformationen

Es gibt eine Reihe medizinischer Institutionen, die nur geprüfte Informationen online stellen. Diese wurden von medizinischen Fachleuten verfasst bzw. auf ihre inhaltliche Richtigkeit kontrolliert. In der Regel kann man sich auf deren Vertrauenswürdigkeit verlassen. Das Deutsche Institut für Qualität und Wirtschaftlichkeit im Gesundheitswesen (IQWiG) ist eine fachlich unabhängige wissenschaftliche Einrichtung der privaten und gemeinnützigen Stiftung für Qualität und Wirtschaftlichkeit im Gesundheitswesen. Die Stiftung verfolgt das Ziel, wissenschaftlich basierte Entscheidungen über Gesundheitsfragen zu unterstützen. Sie hat zu diesem Zweck einen Ratgeber mit Tipps für die Suche nach Gesundheitsinformationen herausgegeben. Die folgenden Such-Tipps basieren weitgehend auf diesem Ratgeber, abzurufen unter: https://www.gesundheitsinformation.de/pdf/informationsmaterialien/flyer-gute-gi.pdf?rev=122486

Wie finde ich gute Gesundheitsinformationen im Internet?

Gute von schlechten Gesundheitsinformationen zu unterscheiden, ist nicht einfach.
Merken Sie sich eine Auswahl von Seiten, die verlässliche Gesundheitsinformationen anbieten. Starten Sie mit Ihrer Suche beispielsweise auf diesen Seiten:

- Ärztliches Zentrum für Qualität in der Medizin**: www.patienten-information.de**
- Institut für Qualität und Wirtschaftlichkeit im Gesundheitswesen**: www.gesundheitsinformation.de**

Eine ausführliche Liste mit weiteren Seiten finden Sie in diesem Wegweiser für Patientinnen und Patienten: **www.sylvia-saenger.de/patientenwegweiser**

Diabetesspezifische Seiten:

- Österreichische Diabetes Gesellschaft: **https://www.oedg.at/**
- Initiative der ÖDG: **https://www.facediabetes.at/**
- DIÖ – Diabetes Initiative Österreich: **https://www.diabetesinitiative.at/impressum.html**
- Bundesministerium: **https://www.diabetesstrategie.at/**
- Das Diabetesinformationsportal diabinfo.de mit seinen Unterportalen Diabetes vorbeugen, Leben mit Diabetes und Informationen für Fachkreise ist ein gemeinsames Angebot des Helmholtz Zentrums München, des Deutschen Diabetes-Zentrums in Düsseldorf und des Deutschen Zentrums für Diabetesforschung. Initiiert wurde das Portal von der Bundeszentrale für gesundheitliche Aufklärung (BZgA). Die Förderung erfolgt durch die BZgA, das Bundesministerium für Gesundheit (BMG) sowie das Bundesministerium für Bildung und Forschung (BMBF): **https://www.diabinfo.de/**
- DGE – Diabetes und Ernährung: https://www.dge.de/ernaehrungspraxis/diaetetik/diabetes-mellitus/

Diabetes Selbsthilfe:

- Österreichische Diabetikervereinigung ÖDV: **https://www.diabetes.or.at/home/**

Angebote der Österreichischen Gebietskrankenkasse ÖGK

- Das Disease-Management-Programm Therapie Aktiv: **https://www.therapie-aktiv.at/**
- Tabakentwöhnungsangebote: **https://www.gesundheitskasse.at/cdscontent/?contentid=10007.826503&portal=oegknportal**

Diese Auflistung stellt eine Auswahl von Seiten dar, erhebt aber keinen Anspruch auf Vollständigkeit. Im Verlauf des DiabPeerS-Programms werden Sie auch eine Reihe anderer Seiten kennenlernen, die hier nicht angeführt sind.

Wie bewerte ich selbst eine Internetseite?

Wenn Sie eine Internetseite öffnen, die Sie nicht kennen, deren Inhalte Sie aber gerne mit der Gruppe teilen würden, sollten Sie sich vorab folgende Fragen stellen:

Wer betreibt und finanziert die Seite?	• Angaben meist am Ende der Seite unter „Impressum“, „Kontakt“ oder „Wir über uns“. • **Gute Seiten** nennen die Namen der betreibenden Personen, der Autorinnen und Autoren, deren Qualifikation sowie die Finanzierungsgrundlage der Website • **Problematisch** ist es, wenn Abhängigkeiten oder finanzielle Vorteile für die Betreibenden existieren (und diese sogar vertuscht werden). • Gegebenenfalls können Sie die Personen, die als Betreiber oder Betreiberinnen angegeben sind, auch googeln und ihre Hintergründe prüfen.
Sind die Motive und Ziele der Seitenbetreibenden genannt?	• Seien Sie vorsichtig, wenn Produkte oder Leistungen beworben oder direkt vermarktet werden und die Seite sich darüber finanziert. • Werden Sie misstrauisch, wenn Sie zu einer Entscheidung gedrängt werden, Ihnen Angst gemacht wird oder extreme Positionen dargestellt werden. • Gesundheitsinformationen aus dem Internet ersetzen nie den direkten Kontakt oder ein Gespräch mit einer Ärztin oder einem Arzt. Gute Seiten weisen darauf hin. • Eine seriöse Website sollte so klar und strukturiert aufgebaut sein, dass die genannten Informationen leicht auffindbar sind.

Gute Informationen können Gespräche mit Fachleuten ergänzen, aber nicht ersetzen. Stellen Sie keine Eigendiagnosen und besprechen Sie Behandlungsmöglichkeiten mit Ärztinnen und Ärzten.

Checkliste: Gute Seiten ...

Sprache	• vermitteln Wissen objektiv und neutral. • erklären Fachbegriffe. • vermeiden ideologische Begriffe wie „Schulmedizin“, „ganzheitliche Medizin“ oder „natürliche Medizin“.
Methoden der Erstellung	• stellen ihre Methoden und Prozesse der Erstellung deutlich dar. • lassen auch Patientinnen und Patienten sowie fachliche Expertinnen und Experten an der Texterstellung mitarbeiten.
Inhalt	• geben an, wie die Behandlungen wirken und welche Erfolge möglich sind. • erklären, was passiert, wenn die Erkrankung unbehandelt bleibt. • beschreiben alle wichtigen Behandlungsmöglichkeiten. • nennen Nebenwirkungen. • beschreiben, was in der Forschung noch unsicher ist. • machen Angaben über ergänzende Hilfen und weiterführende Angebote. • stellen dar, wenn für Behandlungen Kosten entstehen, die selbst zu tragen sind.

Quellen	• geben Quellen unter dem Text an: Woher kommen die Informationen, die hier weitergegeben werden? Sind keine Quellen vorhanden, wäre das ein erster Hinweis auf einen unseriösen Artikel. Ist ein Literaturverzeichnis angegeben, kann man dieses gegebenenfalls kontrollieren. Funktionieren die Links und man wird zu einer neuen Website weitergeleitet? Wurde in dem Artikel zitiert und wenn ja, wer wurde zitiert? • verwenden wissenschaftliche Artikel und geben den Inhalt korrekt wieder. • verwenden Erfahrungsberichte nicht als Beleg für die Wirksamkeit einer Therapie.
Aktualität	• geben das Veröffentlichungs- oder Aktualisierungsdatum an. • geben an, wann die nächste Aktualisierung geplant ist. • Es empfiehlt sich nicht nur das Aktualisierungsdatum zu prüfen, sondern auch zu prüfen, aus welcher Zeit die Quellen stammen. Auch ein aktueller Beitrag kann auf veralteten Informationen basieren.
Datenschutz	• beschreiben den Umgang mit Daten der Benutzerinnen und Benutzer (Datenschutzerklärung). Gerade, wenn Sie Ihre persönlichen Daten eingeben – zum Beispiel für einen Newsletter – ist dies wichtig.

Was ist bei Suchmaschinen wie Google zu beachten?

- Die Reihenfolge der Suchergebnisse sagt nichts über Qualität und Verlässlichkeit der Informationen aus.
- Schauen Sie sich mehr als die ersten 10 Treffer an: bei den ersten Treffern handelt es sich häufig um gekaufte Werbeanzeigen.
- Vergewissern Sie sich, wer hinter der Information steht und welche Ziele die Anbieter und Anbieterinnen verfolgen.

TIPP: Schauen Sie, wie andere Organisationen die Internetseite bewerten. Sie können zum Beispiel in das Suchfeld den **Namen der Seite** und den Zusatz „**Bewertung**“ oder „**Kritik**“ eingeben.

Vorsicht,

- wenn bei schweren Erkrankungen von Heilung die Rede ist.
- wenn „Schulmedizin“ als abwertender Begriff verwendet wird und einer „ganzheitlichen“ oder „natürlichen“ Medizin gegenübergestellt wird.
- wenn neben den Texten die Werbung zum passenden Produkt erscheint.
- wenn direkt oder über verlinkte Shop-Seiten Produkte verkauft werden.

Was ist bei Foren, in denen sich Betroffene zu bestimmten Erkrankungen austauschen, zu beachten?

- Internetforen bieten Raum zum Austausch, sind aber keine zuverlässigen Informationsquellen. Die Angaben sind subjektiv und werden nicht auf Richtigkeit und Qualität überprüft.
- Manche Personen können als Patientin oder Patient getarnt sein und versteckt für Produkte werben.

Die Links zu Artikeln und Videos, die Ihnen im Rahmen dieses Handbuchs bzw. der zugehörigen Einschulung zur Verfügung gestellt werden, sind von unseren Diätologinnen bzw. Ernährungswissenschaftlerinnen geprüft worden.

3 Kommerzielle Datensammlung – Preisgabe von Daten

Cookies und Tracking

Beim Besuch von Websites werden in der Regel „Cookies“ in Ihrem Browser abgelegt. Das sind kleine Dateien, die persönliche Informationen und Websiteeinstellungen beinhalten. Manche Arten von Cookies – die so genannten „essenziellen“ Cookies – sind notwendig, damit die betreffende Website überhaupt (sinnvoll) genutzt werden kann. Beispielsweise sorgen sie dafür, dass Produkte bis zum Ende des Bestellvorgangs im Warenkorb bleiben. Andere erleichtern die Nutzbarkeit, indem z. B. bei häufig besuchten Seiten nicht immer wieder die Anmeldedaten eingegeben werden müssen. Ein wesentlicher Bereich sind allerdings auch Marketing- und Trackingcookies. Das sind Cookies, die persönliche Daten wie Alter, Geschlecht und Wohnort sowie das Nutzungsverhalten aufzeichnen.

Diese Daten werden für personalisierte, also auf die jeweilige Person abgestimmte, Werbung verwendet (Schießl 2020a; 2020b; Aschermann 2020): Welche Produkte hat die Person bislang gekauft, nach welchen Informationen hat sie gesucht, welche persönlichen Umstände sind daraus abzuleiten (z. B. kleine Kinder im Haushalt, Garten, Haustiere, Erkrankungen, Hobbys, ...), welche Produkte haben andere Personen derselben Zielgruppe bereits erworben und was könnte somit für diese Person interessant sein?

Seit der Einführung der Datenschutzgrundverordnung (DSGVO) im Mai 2018 müssen die Betreiberinnen und Betreiber von Websites „Cookie-Hinweise“ platzieren. Mit diesen informieren sie die Nutzerinnen und Nutzer, dass Cookies gesetzt und/oder andere Tracking[1]-Verfahren verwendet werden. Häufig holen Websitebetreiberinnen und -betreiber auch explizit die Zustimmung der Nutzerinnen und Nutzer ein und lassen sie auswählen, welche Informationen erfasst werden dürfen. Diese Fenster sind aber oft so gestaltet, dass dabei versehentlich mehr preisgegeben wird als beabsichtigt. Die Auswahlmöglichkeiten, mit denen bestimmte Arten von Cookies ausgeschlossen werden können, werden oft hinter separaten Links oder Buttons versteckt, während die Option alle Cookies zu akzeptieren, farblich hervorgehoben ist (Utz u. a. 2019, 703). Da passiert es rasch, dass versehentlich allen Cookies zugestimmt wird. Auch wer sich die Mühe gemacht hat, Cookie-Präferenzen einzustellen, wird oft noch in letzter Sekunde durch farbliche Hervorhebung dazu gebracht, reflexartig nicht die getroffene Auswahl, sondern doch alle Cookies zuzulassen. Manchmal ist schon seitens der Website die datenschutzfreundlichste Variante (nur technisch notwendige Cookies) voreingestellt, und trotzdem verleitet ein farblich dominanter Button zur Akzeptanz aller Cookies – während die Nutzerin oder der Nutzer glaubt, nur der Auswahl zugestimmt zu haben (siehe Abbildung). Die Optionen sind oft zudem nicht nach dem gewohnten Muster JA / NEIN angeordnet, sondern die JA-Option, mit der alle Cookies akzeptiert werden, ist rechts platziert, was ebenfalls dazu verleitet auf sie zu klicken, obwohl nur die Auswahl bestätigt werden sollte. (Dasselbe Prinzip nutzen übrigens auch viele Websites, wenn sie um die Erlaubnis fragen, Push-Mitteilungen[2] senden zu

[1] Tracking bedeutet so viel wie „Nachverfolgung“ oder „Aufzeichnung“. Das Nutzungsverhalten einer Person wird damit erfasst.

[2] Push-Mitteilungen sind Benachrichtigungen einer App oder Website, die man auch dann erhält, wenn man die App bzw. die Website gerade nicht geöffnet hat. Beispielsweise könnte ein Blog oder ein Online-Magazin

dürfen. Links ist oft die Option platziert, Push-Mitteilungen abzulehnen, rechts die Option, sie zuzulassen.)

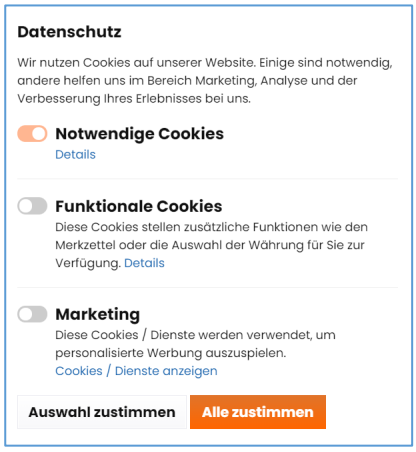

Abbildung 1: Voreingestellt sind in diesem Fall nur "notwendige Cookies", was die datenschutzfreundlichste Variante wäre. Dennoch zieht der orange hervorgehobene Button die Aufmerksamkeit auf sich und verleitet dazu, versehentlich alle Cookies zu akzeptieren. Quelle: Screenshot von https://www.deubaxxl.at/.

Auf manchen Websites gibt es auch keine Auswahlmöglichkeiten. Stattdessen werden die Nutzerinnen und Nutzer lediglich auf das Tracking aufmerksam gemacht. Sie sollen zustimmen oder erhalten nur den Hinweis, dass die weitere Nutzung der Website einer Zustimmung gleichkommt (Utz u. a. 2019, 703).

Die Betreibenden setzen zudem auf die so genannte „Entscheidungsmüdigkeit“ („decision fatigue“), die Nutzerinnen und Nutzer ereilt, wenn sie bei jeder Website, die sie besuchen, erneut ihre Präferenzen angeben müssen, und dies noch dazu auf kompliziertem Weg (Utz u. a. 2019, 704). Es lohnt sich also, beim Besuch einer neuen Website kurz innezuhalten und sich bewusst mit den Möglichkeiten auseinanderzusetzen – kurz: nicht automatisch allen Cookies zuzustimmen, sondern sich die Einstellungen anzeigen zu lassen, und sich nicht von Farbcodes leiten zu lassen, sondern auf die genaue Beschriftung und Anordnung der Buttons zu achten.

Lesetipp: Dieser Artikel hält einige Tricks bereit, wie unerwünschte Cookies vermieden werden können: https://praxistipps.chip.de/cookies-akzeptieren-oder-nicht-das-sollten-sie-tun_42136

Auch bei der Benutzung von Apps werden in der Regel über eingebaute Werbe- und Analysemodule, die für die Nutzerinnen und Nutzer nicht ersichtlich sind, Nutzungsdaten getrackt. Der Online-Ratgeber

Leserinnen oder Leser via Push-Mitteilung benachrichtigen, dass ein neuer Artikel online gegangen ist. Vielleicht kennen Sie Push-Nachrichten auch von Social Media wie Facebook: Sie werden benachrichtigt, wenn jemand auf einen Beitrag von Ihnen reagiert oder wenn eine Person, mit der Sie vernetzt sind, etwas Neues gepostet hat.

Mobilsicher.de empfiehlt für die Installation von Apps den „alternativen Appstore ‚F-Droid'" (Rehberg 2020). Dort werden solche Module vorab gelöscht oder sie werden zumindest für die Nutzerinnen und Nutzer erkennbar gemacht. Auf der Plattform „Exodus Privacy" können Apps zudem darauf überprüft werden, welche Tracker sie enthalten (Rehberg 2020). Im Projekt „DiabPeerS" läuft der verwendete Messenger aus Datenschutzgründen auf einem österreichischen Server. Es gilt die österreichische und europäische Gesetzgebung hinsichtlich des Datenschutzes. Es werden keine Daten an Dritte, etwa zu Marketingzwecken, weitergegeben – lediglich die an diesem Projekt beteiligten Forschenden erhalten zu Forschungszwecken die Kommunikationsdaten aus dem Messenger. Darüber hinaus wird kein Nutzungsverhalten aufgezeichnet.
Bei Fitness-Apps und Wearables[3] muss man ebenfalls damit rechnen, dass die Gesundheitsdaten an die Anbieterfirma und oft auch an Dritte übermittelt werden (Verbraucherzentrale.de 2020). Welche Apps über welche Berechtigungen verfügen, kann man in den Einstellungen des Smartphones herausfinden, dort können diese Berechtigungen auch umgestellt werden (Google Play Hilfe 2021). Bei der Entscheidung, welche Berechtigungen zugelassen werden sollen, hilft es, sich zu überlegen, welchen Zweck die App hat und auf welche Daten sie folglich logischerweise Zugriff braucht. So ist es logisch, dass eine Foto-Sharing-App auf die Kamera Ihres Smartphones zugreifen muss, um zu funktionieren; jedoch ist nicht nachvollziehbar, warum eine Taschenlampen-App Zugriff auf Ihren Standort brauchen sollte (Saferinternet.at 2021c).

Lesetipp:

Details zu „F-Droid" und „Exodus Privacy" sowie weitere Tipps, um Tracking über Apps unterbinden oder zumindest erkennen zu können, finden Sie hier: https://mobilsicher.de/ratgeber/schnueffel-module-in-apps-das-koennen-sie-tun

Lesetipp:

Details zur Studie der deutschen Verbraucherzentrale: https://www.verbraucherzentrale.de/marktbeobachtung/wearables-und-fitnessapps-40296

Selbst preisgegebene Daten

Daten werden aber nicht nur getrackt, auch selbst ist man immer wieder in der Situation, dass z. B. bei der Nutzung von Apps Informationen zur eigenen Person abgefragt werden. Auch hier ist empfehlenswert immer zu überlegen: Welche Informationen werden für die sinnvolle, zweckmäßige Nutzung tatsächlich benötigt? So benötigt eine Fitnessapp tatsächlich Größe, Gewicht und Alter der Person, damit die erhobenen Daten eingeordnet werden können. Das auf den Tag genaue

[3] Der Begriff „Wearables" bezeichnet am Körper getragene kleine Geräte, die Körperfunktionen (z. B. Herzfrequenz, Schlafrhythmus, gelaufene Schritte) aufzeichnen und auswerten und dadurch die kontinuierliche Selbstkontrolle dieser Werte ermöglichen, etwa Fitnessarmbänder oder Smartwatches (Hery-Moßmann 2017).

Geburtsdatum ist allerdings nicht wichtig, genauso wenig wie der echte Name der Person. Vermeiden sollte man außerdem, sich über einen Social Media Account bei anderen Diensten anzumelden, da dann die Daten aus beiden Anwendungen verknüpft werden können (Geiger 2020).

4 Verdeckte Werbung

Nicht nur die Datensammlung zu Werbezwecken, sondern auch Werbung selbst erfolgt neben den klassischen Erscheinungsformen (z. B. TV-Spots, Plakate) häufig mehr oder weniger stark verdeckt. Es gibt eine Vielfalt von subtilen Marketingstrategien, bei denen Werbung mit Information oder Unterhaltung vermischt oder überhaupt als solche getarnt wird. Durch das Wissen über diese Strategien und ihre Merkmale können sie leichter erkannt werden, was den bewussten Umgang damit erleichtert. Im Folgenden werden ausgewählte Phänomene vorgestellt, die Ihnen bei Ihrer Internetnutzung begegnen können, wenn Sie Inhalte und Materialien recherchieren.

Advertorials

Die Mischung von Werbung und Information spiegelt sich bei Advertorials schon direkt im Begriff wider. Dieser ist die Zusammensetzung zweier Wörter – „advertisement“, das im Englischen Werbeanzeige bedeutet, und „editorial“, womit redaktionelle Artikel bezeichnet werden. Advertorials sind also als redaktionelle Beiträge getarnte Werbeeinschaltungen in Printmedien (Köberer 2014, 99f.). Diese finden sich sowohl in gedruckten Ausgaben von Printmedien als auch in Online-Ausgaben. Sie wirken wie gewöhnliche Artikel und sind auch inmitten anderer, tatsächlich redaktioneller Artikel platziert. Ihr Werbecharakter eröffnet sich erst auf den zweiten Blick durch den beigegebenen Hinweis – etwa „Anzeige“, „gesponsert“ oder „Sponsored Post“. Die Trennung von redaktionellen und werblichen Inhalten in Form solcher Hinweise (Kennzeichnungspflicht) ist nach dem österreichischen und deutschen Medienrecht vorgeschrieben, auch wenn die gestalterische Aufmachung ähnlich sein darf. An diesen kurzen Hinweisen, die meist zu Beginn oder am Ende der Seite platziert sind (IONOS 2017; Rechtsinformationssystem des Bundes 2021), kann man sich orientieren, um Werbung und Redaktionelles auseinanderzuhalten. Die folgende Abbildung zeigt ein Beispiel eines Advertorials im Vergleich zu einem redaktionellen Artikel im Online-Auftritt des Magazins t3n. Das Advertorial (oben) sieht dem redaktionellen Artikel (unten) täuschend ähnlich – es unterscheidet sich nur durch die Hinweise „Anzeige“ bzw. „Sponsored Post“ und die rote Überschrift.

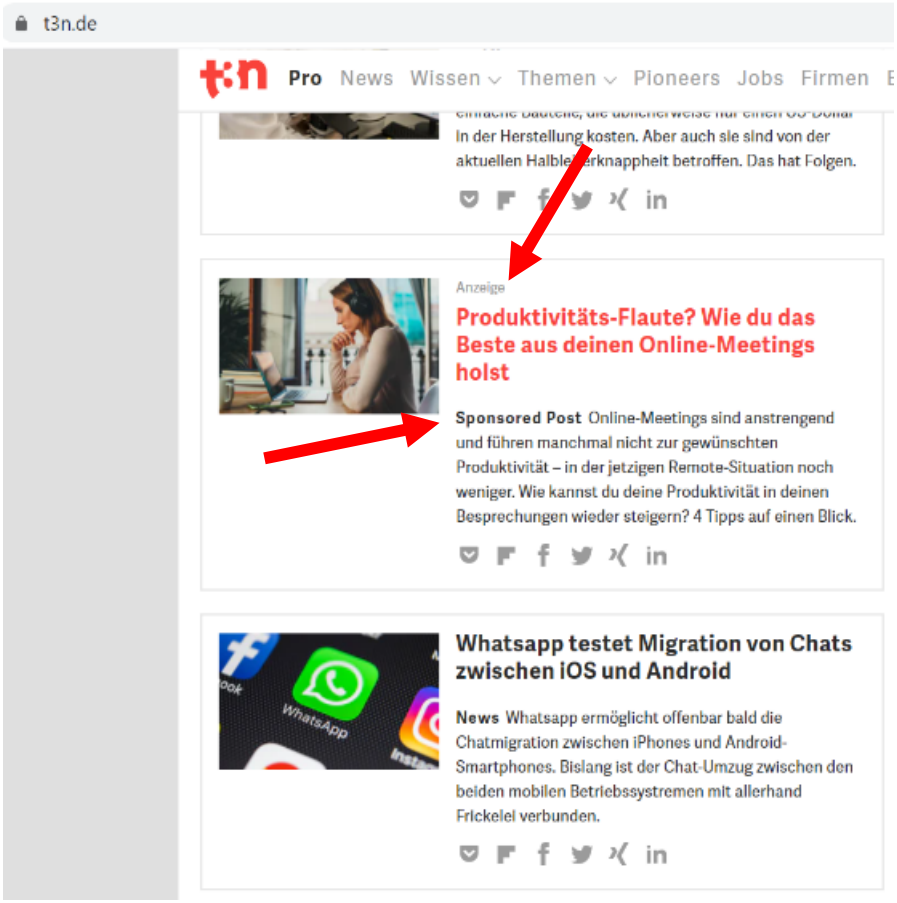

Abbildung 2: Advertorial und redaktioneller Artikel im Vergleich – Bildquelle: Screenshot von https://t3n.de/ (6.4.2021)

Bezahlte Suchergebnisse und gesponserte Posts auf Social Media

Übergänge zwischen Information und Werbung gibt es aber auch bei der Verwendung von Suchmaschinen. Nach Eingabe eines Suchbegriffs erscheint an der Spitze der Trefferliste vor den eigentlichen, inhaltlichen Treffern oft zuerst eine Reihe von Anzeigen. Auch diese können durch die Kennzeichnung als „Anzeige“ erkannt werden. Obwohl meist von Google die Rede ist, wenn solche Anzeigen in der Trefferliste thematisiert werden (dort heißen diese Anzeigen übrigens „AdWords“), gibt es solche bezahlten Suchergebnisse auch bei anderen Suchmaschinen, etwa Yahoo oder Ecosia, wie die folgende Abbildung zeigt. Erst nach den Anzeigen folgen jeweils die eigentlichen Suchergebnisse.

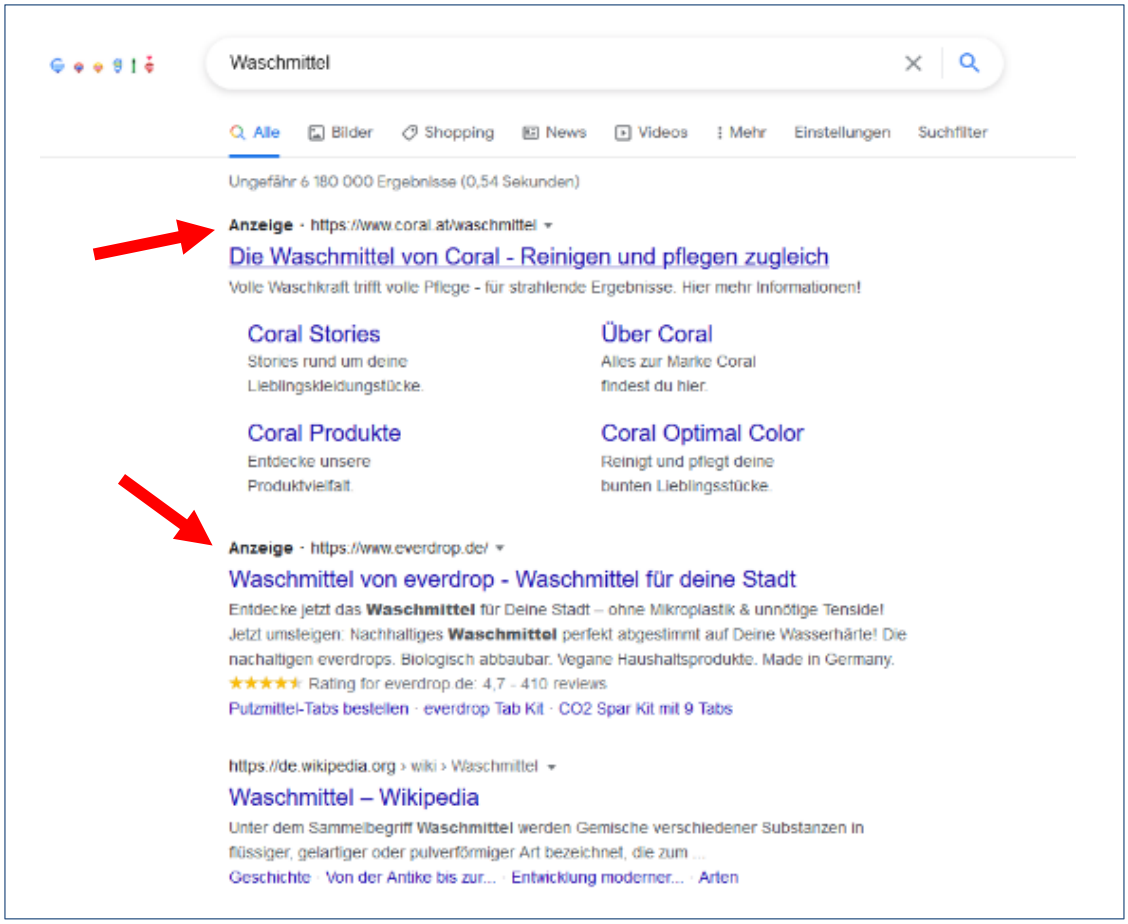

Abbildung 3: Bezahlte Anzeigen zum Suchwort „Waschmittel" in der Suchmaschine Google

Gesponserte Posts sind auch auf diversen Social Media gang und gäbe. Falls Sie z. B. ein Facebook- oder Twitter-Profil haben, werden Ihnen in Ihrer Timeline zwischen den Posts Ihrer Social Media Bekanntschaften und abonnierten Kanäle immer wieder werbliche Beiträge auffallen. Auch sie unterscheiden sich in ihrer Aufmachung nicht von den übrigen Posts, erneut gibt die Bezeichnung als „gesponsert“ oder „sponsored“ den Hinweis auf den werblichen Charakter.

Produktplatzierungen

Auch Produktplatzierungen (Product Placement) sind eine Möglichkeit „versteckt“ Werbung zu machen. Das jeweilige Produkt wird beispielsweise in einem Film, einer TV-Serie oder einem Video platziert. Es wird möglichst nahtlos in die Handlung integriert, damit der Werbecharakter nicht unmittelbar auffällt. Es gibt verschiedene Arten von Produktplatzierungen: Beim visuellen Product Placement ist das Produkt im Film zu sehen, wird also zum Beispiel von einem Filmcharakter verwendet. Auch Filmfiguren essen und trinken, fahren mit dem Auto, tragen Uhren oder Schmuck, benutzen Mobiltelefone usw. Insofern wirkt die Platzierung des Produkts wie ein natürlicher Bestandteil des Films und wird nur als Werbung erkannt, wenn der Film kritisch betrachtet wird. Verbales Product Placement bedeutet, dass der Name eines Produktes, eines Unternehmens oder einer Marke im Film erwähnt wird, etwa wenn Filmfiguren miteinander reden. Beim akustischen Product Placement wird mit Geräuschen und Tönen gearbeitet, die für eine Marke charakteristisch sind. So kann es zum Beispiel vorkommen, dass als Klingelton für das Smartphone einer Filmfigur das Soundlogo[4] eines Mobilfunkanbieters eingesetzt wird (Ebner-Zarl 2021, 278; Matthes und Naderer 2014, 59f.).

Werbespiele, In-Game-Werbung, In-App-Werbung

Es gibt Spiele, die gezielt deswegen hergestellt werden, um damit ein Produkt, ein Unternehmen oder eine Marke zu bewerben. Solche Spiele werden Werbespiele (Advergames) genannt. Diesen Spielen ist ihr werblicher Charakter nicht unbedingt von vorneherein anzusehen. Eines der ersten Werbespiele war beispielsweise das um die Jahrtausendwende (u. a. auch bei Jugendlichen) beliebte Moorhuhn-Spiel, hinter dem die Whisky-Marke Johnnie Walker steht. Verfügbar sind Werbespiele heute meist auf der jeweiligen Unternehmenswebsite, auf Social Media, in Form von Apps oder auf Spieleplattformen, üblicherweise gratis (Klein und Eppmann 2020, 488, 493; Nairn und Hang 2012, 5; Ebner-Zarl 2021, 280). Während der Werbecharakter bei der Einbettung in Unternehmenswebsites klar sein dürfte, vermischen sich auf Social Media, in App Stores und auf Spieleplattformen werbliche mit klassischen Spielen.

Bei In-Game Werbung (In-Game Advertising) handelt es sich um Werbung, die in Kaufspiele integriert wird. Es gibt eine Bandbreite von Erscheinungsformen: Virtuelle Bandenwerbung bei digitalen Fußballspielen kann genauso vorkommen wie Produktplatzierungen, ähnlich wie sie in Film und Fernsehen eingesetzt werden (Nairn und Hang 2012, 5f.; Ebner-Zarl 2021, 280). Aber auch Apps ohne Spielcharakter weisen integrierte Werbung auf (In-App Advertising). Wenn Sie sich für das

[4] Unter einem Soundlogo wird eine Tonfolge verstanden, die in Radio- oder TV-Spots eines bestimmten Unternehmens bzw. einer bestimmten Marke wiederkehrend verwendet wird. Diese Töne stehen für das Unternehmen bzw. die Marke und schaffen so einen hörbaren Wiedererkennungswert.

Projekt also beispielsweise eine Schrittzähler-App herunterladen, werden Sie vermutlich auch dort auf Werbung stoßen. Insbesondere kostenfreie Apps finanzieren sich über Werbeeinschaltungen von Dritten. Meist sind diese aber gut erkennbar, z. B. in Form von Bannern am unteren oder oberen Bildschirmrand.

In-App-Käufe

Mobile Spiele, aber auch Apps mit anderen Inhalten können oft gratis heruntergeladen und in einem bestimmten Umfang auch gratis genutzt werden. Im Laufe der Nutzung werden aber Käufe angeboten oder sind für eine optimale bzw. vollständige Nutzung der App sogar notwendig. Beispielsweise können so zusätzliche Funktionen aktiviert werden, die in der kostenlosen Version nicht verfügbar sind. Dies wird In-App Käufe genannt. Bei klassischen Games, die nicht in Form einer App angeboten werden, sondern z. B. als Computer- oder Konsolenspiel, wird von In-Game-Käufen gesprochen (Meschik 2018, 1–3; Ebner-Zarl 2021, 287; Eichfelder 2019).

Zum Teil werden durch In-App Käufe auch Abos eingegangen, sodass regelmäßig für bestimmte Funktionen bezahlt wird. Beispielsweise ist dies bei der App Office 365 der Fall (Eichfelder 2019), die u. a. die aus der klassischen Computernutzung bekannten Programme wie Word, Excel und Power Point enthält.

Wer das Risiko unbeabsichtigter In-App-Käufe nicht eingehen will, kann diese Möglichkeit im jeweiligen App Store deaktivieren. Bezahlt wird nämlich entweder (bei Android) mit der Zahlungsmethode, die Sie im Play Store eingestellt haben, oder (bei iOS) mit Ihrem Guthaben auf iTunes (Eichfelder 2019). Unter iOS können Sie In-App-Käufe unmittelbar deaktivieren, beim Betriebssystem Android ist eine eher indirekte Art der Deaktivierung möglich, indem Sie ein Passwort für In-App-Käufe vergeben, durch das Sie im Falle unbeabsichtigter Käufe aufmerksam gemacht werden, bevor Sie den Kauf tätigen. Nur durch Eingabe des Passworts kann der Kauf dann abgeschlossen werden. Wie die Deaktivierung von In-App Käufen in diesen beiden App Stores im Detail funktioniert, erfahren Sie im untenstehenden Lesetipp (Krug 2018).

Lesetipp:

Schritt für Schritt-Anleitung zum Deaktivieren von In-App-Käufen: https://praxistipps.chip.de/in-app-kaeufe-deaktivieren-anleitung-fuer-android-und-ios_92274

Eine andere Möglichkeit, um In-App-Käufe zu umgehen, ist beispielsweise auch die Nutzung des bereits in Abschnitt 3 erwähnten alternativen App-Stores F-Droid. Auf diesem werden ausschließlich frei verfügbare Programme (so genannte Open-Source Software) angeboten (Menge-Sonnentag 2020).

Influencer Marketing

Die meisten Menschen, die als Teil ihres Alltags Social Media Accounts betreiben oder bloggen, haben eine mehr oder weniger überschaubare Zahl von Abonnentinnen und Abonnenten. Einige können mit ihren Videos, Fotos und Posts jedoch ein großes, stabiles, oft sogar internationales Publikum begeistern. Zehn- oder hunderttausende oder sogar Millionen von Menschen folgen ihnen. Üblicherweise werden sie von ihren Fans sehr verehrt, d. h. sie haben Einfluss auf ihre Fans und werden deswegen auch als Influencerinnen bzw. Influencer bezeichnet (Einfluss heißt auf Englisch „influence“).

Influencer Marketing ist längst ein wesentlicher Bereich der Werbewirtschaft. Erfolgreiche Influencerinnen oder Influencer werden mitunter von Unternehmen um Kooperationen angefragt, um Werbung für bestimmte Produkte, Dienstleistungen und Marken auf ihren Kanälen zu machen. Es gibt sogar eigene Firmen (die so genannten Multi Channel Networks), die passende Influencerinnen und Influencer mit passenden Unternehmen zusammenbringen und beide Seiten bei ihren Aktivitäten unterstützen (Gebesmair 2017, 97f.; Ebner-Zarl 2021, 293f.). Die thematische Ausrichtung vieler Influencerinnen und Influencer macht sie per se äußerst geeignet für werbliche Aktivitäten. Gängige Themen von Influencerinnen und Influencern sind z. B. Reisen, Essen, Sport, Schminken oder Einrichtung, und gerade auf YouTube sind viele typische Videogenres auch um Produkte herum zentriert, etwa „Hauls“ (die Präsentation von getätigten Einkäufen), „Tutorials“ (Anleitungen, z. B. zum Schminken, Basteln, Kochen oder zur Softwarenutzung) und „Unboxing Videos“ (das Auspacken von Geschenken) (Ebner-Zarl 2021, 292f.; Gebesmair 2017, 14 f., 69–72).

Wie können werbliche Anteile in Inhalten von Influencerinnen und Influencern erkannt werden? Prinzipiell gibt es unterschiedliche Werbestrategien auch im Influencer Marketing – von Produktplatzierungen bis hin zu den so genannten „Affiliate Links“. Bei Letzteren handelt es sich um Verlinkungen zu Onlineshops oder Unternehmenswebsites. Auf den Websites, zu denen die Links führen, können Produkte, die im Beitrag gezeigt oder für die Gestaltung des Beitrags verwendet wurden, erworben werden. Eigentlich sind Influencerinnen und Influencer verpflichtet, werbliche Inhalte als solche zu kennzeichnen – nicht alle kommen jedoch ihrer Kennzeichnungspflicht nach (Gebesmair 2017, 37f.; Ebner-Zarl 2021, 293f.). Umgekehrt gibt es auf Instagram seit einer gerichtlichen Abmahnwelle die Tendenz, jegliche Beiträge, die eventuell als Werbung interpretiert werden könnten, sicherheitshalber zu kennzeichnen – auch wenn keine Bezahlung durch ein Unternehmen erfolgte. Auch dies behindert die Erkennbarkeit tatsächlicher Werbung (Ebner-Zarl 2021, 294; Zelenko 2018; Erxleben 2018; Gassner 2018).

Die Zahl der Abonnentinnen und Abonnenten, die jemand hat, ist übrigens nur ein ungenaues Indiz für werbliche Hintergründe. Zwar ist Reichweite für Werbetreibende attraktiv, aber nicht das einzige Kriterium, um jemanden unter Vertrag zu nehmen. Je nachdem, welches Potential in einer Person gesehen wird, arbeiten Werbetreibende oft auch mit Personen zusammen, die wenige tausend Abonnentinnen und Abonnenten haben. Für Rezipientinnen und Rezipienten ist also nicht leicht zu durchblicken, wo bzw. ab wann tatsächliche Werbung im Spiel ist.

Folgende Merkmale können jedoch als Anhaltspunkte dienen, um Accounts auf YouTube, Instagram, usw. hinsichtlich werblicher Aktivitäten besser einschätzen zu können:

- Gibt es in den Beschreibungen zu Videos und Fotos oder auch in den Posts selbst Links zu Unternehmenswebsites oder Onlineshops, die direkt zu im Video gezeigten oder verwendeten Produkten führen? (Affiliatelinks)

- Enthalten verwendete Hashtags[5] Markennamen?

- Wird sogar explizit auf den werblichen Charakter aufmerksam gemacht? (Kennzeichnungspflicht)

- Gibt es einen Hinweis auf ein Multi Channel Network, bei dem die Influencerin oder der Influencer unter Vertrag ist? Die wichtigsten Multi Channel Networks in Österreich sind Studio 71 und diego5 (Gebesmair 2017, 38). In Deutschland sind neben Studio 71 u. a. Mediacraft (auch: Mediakraft), Divimove, Endemol Beyond und TubeOne Networks besonders bekannt (Klicksafe.de o. J.).

- Gibt es einen Hinweis auf ein Management? Personen, die professionell gemanagt werden, üben ihre Social Media Tätigkeit eher nicht mehr privat aus, sondern bereits im Sinne eines Geschäfts.

Die meisten Influencerinnen und Influencer sind Jugendliche oder junge Erwachsene mit Inhalten, die ebenfalls auf eine junge Zielgruppe abgestimmt sind. Es gibt aber auch zunehmend Influencerinnen und Influencer im höheren und sogar hohen Alter mit mehreren zehntausend oder sogar mehreren Millionen von Abonnentinnen und Abonnenten[6] (vgl. z. B. Farinosi und Fortunati 2020). Auch so genannte „Diabetes Advocates“ sind auf Social Media aktiv. Das sind Personen, die meist selbst an Diabetes erkrankt sind, sich online für das Thema einsetzen, Tipps und Erfahrungswerte im Umgang mit der Krankheit teilen und sich bemühen Betroffene zur gegenseitigen Unterstützung miteinander zu vernetzen. Manche haben eine sehr hohe Reichweite und können als Influencerinnen bzw. Influencer bezeichnet werden. Betroffene finden hier oft eine Gemeinschaft vor, die sie bei der Bewältigung der Erkrankung stärkt und wichtige Informationen bereithält.

[5] Unter Hashtags versteht man Begriffe auf Social Media, denen eine Raute (#) vorangestellt ist. Personen, die sich auf Social Media über Diabetes austauschen, würden zur besseren Auffindbarkeit der Beiträge z. B. den Hashtag #Diabetes verwenden.
[6] Für Beispiele siehe u.a. die Liste auf: https://www.energy.de/national/lifestyle/die-coolsten-influencer-senioren-der-welt%20

5 Problematische Inhalte

Auf Social Media sind manchmal auch problematische Inhalte im Umlauf. Oft geschieht dies ohne böse Absicht derjenigen, die sie weitergeleitet haben. Es kann auch während des Projekts passieren, dass problematische Inhalte im Messenger auftauchen – etwa, wenn ein Gruppenmitglied die anderen vor einer vermeintlichen Gefahr warnen möchte, von der es gerade gelesen hat, oder eine besonders attraktiv scheinende Neuigkeit teilen will. Wichtig ist dann, diese Inhalte zu erkennen und adäquat zu reagieren, d. h. über den Problem- bzw. fehlenden Wahrheitsgehalt der Information aufzuklären und nicht weiter zu ihrer Verbreitung beizutragen. Einige Beispiele sollen hier angeführt werden, um Orientierung zu geben und den Blick zu schärfen.

Falschmeldungen (Hoaxes, Urban Legends) und Kettenbriefe

Unter Hoaxes sind Falschmeldungen zu verstehen, die von ihren Urheberinnen oder Urhebern bewusst veröffentlicht wurden. Oft verbreiten sie sich über Jahre und Jahrzehnte, indem sie von anderen Internetnutzerinnen und -nutzern an ihre Kontakte weitergeleitet werden (Saferinternet.at 2021a; Ziemann 2021a). Ein aktuelles Beispiel, das seit Jahren mit variierenden Namen über WhatsApp und Facebook verbreitet wird, ist die Warnung, die Freundschaftsanfrage einer bestimmten Person (z. B. Tobias Mathis, Anouk Theiler, Ute Lehr) nicht anzunehmen, da sich dahinter ein Virus verberge (Follmer 2020; Saferinternet.at 2021a).

Es gibt zahllose Beispiele für Internet-Hoaxes. Die TU Berlin führt seit den 1990er-Jahren eine Website, auf der viele Hoaxes, aber auch Kettenbriefe, Betrugsversuche usw. dokumentiert sind. Wer sich über eine erhaltene Nachricht unsicher ist, kann dort nachschlagen. Wenn der betreffende Fall noch nicht dokumentiert ist, kann man die Nachricht auch an den Websitebetreiber schicken, um sie zu melden bzw. prüfen zu lassen. Da die Seite schon über Jahrzehnte geführt wird, vermischen sich bei der Erklärung der behandelten Phänomene oft ältere Informationen mit neueren. Die Seite wird jedoch regelmäßig aktualisiert und um die aktuellsten Fälle ergänzt. Die letzten Updates stammen aus dem Frühjahr 2021[7]. In jüngster Zeit kursieren beispielsweise auf Social Media auch zahlreiche Falschmeldungen rund um die Coronapandemie. Links zur Website und zu einigen ausgewählten Passagen innerhalb der Website finden sich im unten stehenden Lesetipp.

Lesetipp: Die Hoax-Info Website der TU Berlin

- Hauptseite: https://hoax-info.tubit.tu-berlin.de/hoax/#4
- Aktuelle Falschmeldungen zur Coronapandemie (zur Erkrankung selbst, zu Impfungen, zu Masken, ...): https://hoax-info.tubit.tu-berlin.de/hoax/corona.shtml
- Hier können verdächtige Nachrichten gemeldet werden: https://hoax-info.tubit.tu-berlin.de/hoax/melden.shtml

[7] Stand: 9.4.2021

Eine einfache Lösung, um Nachrichten zu überprüfen, ist außerdem, Teile davon im Originalwortlaut in eine Suchmaschine einzugeben (Saferinternet.at 2021a). Handelt es sich um einen bekannten Hoax, Kettenbrief, etc. werden Sie sofort zahlreiche Treffer erzielen, speziell auch auf Seiten, die über solche problematischen Inhalte aufklären.

Auch folgende Merkmale einer Nachricht deuten darauf hin, dass es sich um einen Hoax oder andere fragwürdige Inhalte handelt (Follmer 2020):

- Es befinden sich zahlreiche Rechtschreib-, Tipp- und Grammatikfehler in der Nachricht.
- Es wird dringend dazu aufgerufen, diese Nachricht an alle Kontakte weiterzuleiten.
- Sehr drastische und unlogische Folgen werden angekündigt, z. B. dass schon allein durch die Annahme eines Anrufs von einer bestimmten Nummer ein Virus auf das Smartphone gelangen würde.

Der Hoax im klassischen Sinne ist oft harmlos und wird zu Zwecken des (fragwürdigen) Scherzes verbreitet. Oft verwischen aber die Grenzen zu Betrugsversuchen (z. B. Phishing) oder es wird bewusst darauf abgezielt, andere zu erschrecken (z. B. furchterregende Kettenbriefe) (Saferinternet.at 2021a). Nicht zuletzt können solche Falschnachrichten auch dazu beitragen, gefährliches Verhalten zu fördern oder wünschenswertes, sinnvolles Verhalten zu unterbinden. So gibt es beispielsweise Hoaxes darüber, dass die Grippeschutzimpfung das Risiko einer Coronainfektion erhöhen würde oder sich auf den Corona-Teststäbchen gefährliche Parasiten befinden würden (Ziemann 2021b).

Wenn Sie einen Hoax erhalten haben, leiten Sie ihn keinesfalls an Ihre Kontakte weiter. Klären Sie auch die Person, von der Sie die Nachricht bekommen haben, darüber auf, dass es sich um eine Falschinformation handelt (sofern es jemand ist, die oder den Sie persönlich kennen). Wenn Gruppenmitglieder solche Nachrichten in den Messenger einspeisen, klären Sie als Moderatorin bzw. Moderator bitte alle Beteiligten über die Falschinformation auf.

Eng verwandt mit Hoaxes sind übrigens so genannte Urban Legends (Großstadtlegenden). Das sind meist unwahre Geschichten, oft Schauergeschichten, die sich ähnlich einem Gerücht weiterverbreiten und sich sehr lange halten können. Der zentrale Unterschied zwischen Hoax und Großstadtlegende besteht darin, dass bei Ersteren die Falschinformation absichtlich ins Leben gerufen wird (Dunn und Allen 2005, 88). Ansonsten gibt es viele Überschneidungen. Erwähnt werden sollen sie an dieser Stelle, weil sie sich häufig auch auf Gesundheitsthemen beziehen, etwa vor krebserregenden Inhaltsstoffen in Nahrungsmitteln und Kosmetikprodukten warnen (Ziemann 2021a).

Ein ähnliches Phänomen sind auch Kettenbriefe, von denen es viele unterschiedliche Typen gibt: Häufig sind beispielsweise Nachrichten, die damit drohen, der Empfängerin oder dem Empfänger werde Schreckliches passieren, wenn sie oder er die Nachricht nicht in einem definierten Zeitraum an eine definierte Zahl von Menschen weiterleitet. Teils werden auch Fallbeispiele von Personen angeführt, die diese Nachricht ignoriert hätten und bei denen die dramatischen Konsequenzen dann eingetreten seien (Saferinternet.at 2016; Ziemann 2021a).

Es gibt aber u. a. auch Pyramiden-Systeme, bei denen die Empfängerinnen und Empfänger dazu gebracht werden sollen, einmalig einen Geldbetrag zu bezahlen oder ein Geschenk zu übermitteln, und dann das Spiel an eine bestimmte Zahl von anderen weiterzugeben, um so selbst Geld oder Geschenke zu erhalten. Auf diese Weise würde man ein Vielfaches mehr Geld verdienen oder Geschenke erhalten als man selbst gegeben hat. In Wahrheit gehen die meisten Teilnehmenden bei solchen Pyramidenspielen leer aus (Nowotny 2020b; Ziemann 2021a).
Ein weiteres Beispiel sind die bei Ziemann (2021a) so bezeichneten „Tränendrüsen-Briefe“: Dem Klassiker nach wünscht sich ein schwer krankes Kind, dass sein Brief „um die Welt gehen möge“ oder selbst Nachrichten aus aller Welt zu bekommen (Ziemann 2021a). Oft sind diese Kinder erfunden, es gibt aber auch Fälle, in denen das betreffende Kind tatsächlich existiert, aber die Kettenbriefe eine solche Eigendynamik entwickeln, dass die inzwischen genesenen Kinder selbst im Erwachsenenalter noch regelmäßig Nachrichten erhalten (Ziemann 2015). Nicht zuletzt versprechen u. a. auch erfundene Charity-Aktionen, eine großzügige Institution werde für jede weitergeleitete Nachricht einen bestimmten Betrag spenden (Ziemann 2021a).

In allen Fällen gilt: Solche Nachrichten sollten nicht weiterverbreitet werden. Wenn während des Projekts derartige Nachrichten ihren Weg in den Messenger finden sollten, machen Sie die Gruppenmitglieder bitte darauf aufmerksam, dass es sich um Falschinformationen und Unwahrheiten handelt und dass auch sie diese nicht weiterverbreiten sollen.

Bild- und Videomanipulation

Falschinformationen werden mitunter auch mit manipuliertem visuellem oder audiovisuellem Material untermauert. Lassen Sie sich daher auch dann nicht täuschen, wenn ein Bild oder ein Video die Falschinformation scheinbar überzeugend belegt.

Es gibt zahlreiche Möglichkeiten, Bildmaterial zu manipulieren (Niedersächsisches Kultusministerium u. a. 2017, 8):

- ➔ *„Montage: Personen oder Gegenstände werden auf einem Bild hinzugefügt oder entfernt.*
- ➔ *Bildausschnitte: Das Bild wird beschnitten, d. h. Teile werden weggelassen. Dadurch entsteht ein neues Bild, das eine ganz andere Aussage als das Originalbild transportiert.*
- ➔ *Lichtverhältnisse: Durch die Manipulation von Lichtverhältnissen kann beispielsweise eine andere Tageszeit simuliert werden.*
- ➔ *Fokus: In den Mittelpunkt des Bildes wird eine andere Person oder ein anderer Gegenstand als auf dem Originalbild gerückt. Dadurch kann die Aussage oder der Kontext des Bildes verändert werden.*
- ➔ *Kombination mehrerer Bilder: Teile von unterschiedlichen Bildern werden zusammengefügt. So entsteht ein neues Bild. Personen können so beispielsweise in eine andere Situation hineingebaut werden.*
- ➔ *Fehlender bzw. falscher Kontext: Häufig werden Bilder aus dem Kontext gerissen. Sie werden also einem anderen Inhalt oder Artikel zugeordnet und erhalten dadurch eine neue Bedeutung.“* (Niedersächsisches Kultusministerium u. a. 2017, 8)

Die so genannte „umgekehrte Bildersuche“ in Google kann dabei helfen, manche Eingriffe zu erkennen. Sie können dort entweder das fragliche Bild selbst hochladen oder seine Internetadresse (URL) eingeben und aufgrund der Ergebnisse nachvollziehen, auf welchen anderen Internetseiten das Foto noch verwendet wird. So kann man z. B. feststellen, dass ein mehrere Jahre altes Foto verwendet wurde, um einen erst kürzlich geschehenen Vorfall zu belegen, oder dass ein Bild bereits in unterschiedlichsten thematischen Zusammenhängen verwendet wurde. Auch Bearbeitungen können im Vergleich mit anderen Verwendungen des Bildes enttarnt werden. (Niedersächsisches Kultusministerium u. a. 2017, 8; Winter und Saferinternet.at o. J., 30).

So können Sie die umgekehrte Bildersuche von Google nutzen: Sie geben images.google.com in die Browserzeile ein. Danach klicken Sie auf das Kamerasymbol in der Suchzeile von Google. Sie haben nun die Möglichkeit entweder einen Link einzugeben, der zu einem Bild führt, oder ein Bild direkt hochzuladen (siehe Abbildung).

Abbildung 4: Umgekehrte Bildersuche auf Google

Ein jüngeres Phänomen der Manipulation von Videos und Audioaufnahmen sind die so genannten „Deep Fakes“. Dabei werden mithilfe von künstlicher Intelligenz Videos bzw. Tonaufnahmen hergestellt, die oft täuschend echt wirken, aber in Wahrheit gefälscht sind.
Vielleicht haben Sie schon einmal das 2018 veröffentlichte Video gesehen, in dem Ex-Präsident Barack Obama über den damals aktuellen Präsidenten der USA Donald Trump lästert und auch sonst teils vulgäre und abwertende Sprache verwendet. Bei diesem Video handelt es sich um ein solches Deep Fake, das von Schauspieler und Regisseur Jordan Peele gemeinsam mit seiner Produktionsfirma hergestellt wurde. Er wollte damit zeigen, wie einfach es ist, solche Videos zu produzieren. Echte Aufnahmen von Obama wurden dabei mit den Gesichtsbewegungen des Schauspielers verschmolzen. Besonders aufmerksamen Betrachterinnen und Betrachtern könnte auffallen, dass die Bewegungen von Obamas Mund manchmal ein wenig verzögert sind bzw. seine Stimme teilweise fremdartig klingt. Insgesamt wirkt das Video jedoch äußerst authentisch (Futurezone.at 2018).

Tipp:

Hier finden Sie das Deep Fake Video von Jordan Peele: https://futurezone.at/digital-life/deepfake-barack-obama-schimpft-in-video-ueber-donald-trump/400023301

Im Falle des Obama Deep Fakes wird die Fälschung noch im Video selbst aufgedeckt, um für die Problematik zu sensibilisieren. Üblicherweise ist dies aber nicht der Fall, da es ja gerade darum geht, andere zu täuschen oder zu diskreditieren. So wurden beispielsweise auch bereits die Gesichter von bekannten Persönlichkeiten in Pornovideos hineinmanipuliert (Futurezone.at 2018).
Für Aufsehen sorgte 2020 auch ein von Unbekannten nachträglich manipulierter Beitrag des Fernsehsenders NDR. In der Dokumentation zeigt eine Frau ein Bild an ihrer Wohnzimmerwand, das sie selbst gemalt hat. Während es sich im echten Fernsehbeitrag um ein nicht weiter ungewöhnliches Motiv handelt, hängt im gefälschten Video ein Hakenkreuzbild an der Wand. Die unbescholtene Frau wird damit als vermeintliche Nationalsozialistin diskreditiert – umso mehr, als das Deep Fake Video sich rasant auf Social Media verbreitet hat. Der NDR hat deswegen eine Anzeige gegen Unbekannt eingebracht. Es wird davon ausgegangen, dass das Video nicht mit Spezialsoftware hergestellt worden ist (Gensing 2020).

Tipp:

Hier finden Sie (ausschnittsweise) das echte Video des NDR und das gefälschte Video im Vergleich: https://meedia.de/2018/02/23/dokumentation-zeigt-hakenkreuz-als-wohnungsschmuck-ndr-erstattet-anzeige-gegen-unbekannt-wegen-manipulation/

Um Deep Fakes zu produzieren, muss man nicht unbedingt technisch versiert sein. Es gibt sogar freie Software im Internet, die auch für Laiinnen und Laien relativ einfach zu bedienen ist – etwa die Software FakeApp, die gemeinsam mit dem Bildbearbeitungsprogramm Adobe After Effects auch beim beschriebenen Deep Fake um Barack Obama zum Einsatz kam (Futurezone.at 2018).

Auch wenn sogar mit frei verfügbaren Programmen oft sehr echt wirkende Ergebnisse erzielt werden können, gibt es einige Hinweise, die dabei helfen können, Fälschungen zu erkennen. Beispielsweise:

- Gibt es kleine Verzögerungen (z. B. der Mimik, der Mundbewegungen), ruckelt das Bild manchmal?
- Wirkt nur das Gesicht einer Person unscharf, während der Rest des Videos scharf ist?
- Wirkt die Stimme der Person stellenweise leicht verzerrt?
- Blinzelt die Person nur sehr selten oder womöglich gar nicht?

- Wirkt die Mimik unnatürlich oder – bei einer bekannten Person – teilweise ungewöhnlich zu ihrer sonstigen Mimik?
- Wirkt der Blick der Person eher leer?
- Weicht der Hautton der Person von ihrem gewohnten Aussehen ab?
- Gibt es unstimmige Schattenwürfe und Spiegelungen?

(Christof 2019)

Wenn diese Fragen (oder manche davon) mit Ja zu beantworten sind, sollten Sie dem Video gegenüber skeptisch sein. Hilfreich, um Unstimmiges besser zu erkennen, ist auch die Videos im Vollbildmodus zu rezipieren, da dann Details besser sichtbar sind (Klicksafe.de o. J.).

Zudem ist auch bei Deep Fakes hilfreich sich die üblichen Fragen hinsichtlich der Seriosität einer Information zu stellen:

- Welche Quelle stellt dieses Video bereit? Handelt es sich dabei um eine seriöse Quelle – etwa den Online-Auftritt eines offiziellen und anerkannten Mediums – oder um eine Website, deren Hintergründe unklar sind?
- Wenn Sie das Video z.B. über Social Media erhalten haben: Wer ist die Originalquelle? Wo wurde das Video erstmals veröffentlicht?
- Passt das, was die abgebildete Person sagt oder tut, zu ihrem gewohnten Verhalten und Auftreten oder gibt es hier Widersprüche zu Gewohntem? Würde z. B. eine Politikerin oder ein Politiker so sprechen, wie sie oder er es in dem Video tut?
  (Klicksafe.de o.J.)

Sollten im Laufe des Projekts Videos in den Messenger getragen werden, die zu skurril, zu absurd, zu lustig, zu skandalös ... wirken, um wahr zu sein, bleiben Sie skeptisch. Fragen Sie nach der Originalquelle des Videos und weisen Sie gegebenenfalls auch auf den Manipulationscharakter hin.

Betrugsversuche

Das Internet ist wie die reale Welt mitunter auch Schauplatz von Betrugsversuchen.

„**Phishing**“ werden Versuche genannt, andere Personen zur Preisgabe von Daten (üblicherweise von Login-Daten wie Passwörtern, aber auch z. B. Kreditkartendaten) zu bewegen. Dies kann durch die eigene Dateneingabe auf gefälschten Websites oder durch Trojaner geschehen. Bei Letzteren handelt es sich um Schadprogramme, die auf das Gerät geschleust werden und diese Daten unbemerkt miterfassen.
Üblicherweise gehen die Betrügerinnen und Betrüger so vor, dass sie Nachrichten (via E-Mail, Chat, SMS ...) an beliebige Personen ausschicken. Teil der Nachricht sind auch Links oder Anhänge, die geöffnet werden sollen. Dahinter bzw. darin verbergen sich entweder Eingabemasken, Formulare, Login-Bereiche etc., in die Daten eingegeben werden sollen, oder es wird durch das Öffnen des Anhangs Schadsoftware auf das Gerät geladen (Saferinternet.at 2021b).
Dass keine Links und Anhänge, die von Unbekannten zugeschickt wurden, geöffnet werden sollten, liegt auf der Hand. Oft tarnen sich Menschen mit betrügerischen Absichten aber auch als Bank oder

Online-Versandhaus (wo Sie womöglich tatsächlich Kundin oder Kunde sind) und fordern wegen eines Systemwechsels die Bestätigung von Daten oder mahnen angeblich nicht bezahlte Rechnungen ein. Auch hier gilt es skeptisch zu sein: Vertrauliche Daten werden von Banken und anderen Unternehmen nie per E-Mail, Chat oder SMS abgefragt (Saferinternet.at 2021b). Haben Sie Zweifel, ob die Nachricht eventuell doch echt sein könnte, weil Sie z. B. vor kurzem tatsächlich bei dem Versandhaus etwas bestellt haben, vergewissern Sie sich lieber persönlich unter der offiziellen (nicht der womöglich in der E-Mail mitgeschickten!) E-Mailadresse oder Telefonnummer.
Eine besondere Herausforderung stellt es dar, wenn Phishing-Nachrichten von Personen kommen, die man kennt, mit denen man also auf Social Media (oder auch im echten Leben) befreundet bzw. bekannt ist. In diesen Fällen ist die Person selbst auf eine Phishing-Attacke hereingefallen und weiß womöglich noch gar nicht, dass in ihrem Namen Social Media Beiträge gepostet oder Nachrichten verschickt werden. Eine gängige Betrugsmasche ist beispielsweise der angebliche „Profil Viewer“ auf Facebook. Ein Beitrag oder eine private Nachricht einer befreundeten Person informiert dabei darüber, dass man angeblich sehen könne, wer das eigene Facebookprofil besucht hat. Dazu müsse man lediglich einen Link anklicken und sich bei der dann auftauchenden Facebook-Eingabemaske noch einmal anmelden oder eine App herunterladen. Im ersteren Fall handelt es sich um eine nachgebaute, also gefälschte Facebookseite, die lediglich dem Zweck dient, die Zugangsdaten zum Facebookkonto der Person abzugreifen. Fällt die Person auf den Trick herein, haben die Betrügerinnen und Betrüger volle Verfügung über ihr Facebookkonto. Folglich wird u. a. auch in ihrem Namen diese Betrugsnachricht an weitere Personen verschickt bzw. diese Nachricht auf ihrem Konto gepostet. Im zweiten Fall sorgt die heruntergeladene App dafür. Manchmal führt der Link auch zu einer Gewinnspielseite – wer seine Daten dort eingibt, wird in weiterer Folge meist mit Spam-Mails bombardiert (Nowotny 2020a; 2019). Schickt Ihnen eine Freundin oder ein Freund über einen Messenger eine sonderbare Nachricht oder befindet sich ein sonderbarer Post in ihrer oder seiner Timeline, reagieren Sie lieber nicht darauf. Fragen sie die Person lieber auf anderen Kanälen, ob die Nachricht wirklich von ihr stammt.
Sollte eine solche Nachricht den Weg in den Messenger unseres Projekts finden, machen Sie die Gruppenmitglieder darauf aufmerksam, dass es sich um einen Betrugsversuch handelt und drängen Sie auf das Löschen der Nachricht. Sind Sie sich bzgl. eines Posts nicht sicher, geben Sie einige Schlagworte davon in eine Suchmaschine ein. Im Falle eines Betrugsversuchs werden Sie meist einiges an Berichterstattung darüber finden. Auch die in Abschnitt 6 angeführten Websites können dabei helfen, verdächtige Nachrichten besser einzuschätzen.

Was können Sie (außer der oben erwähnten Hinweise) noch tun, um sich gegen Phishing-Attacken zu schützen?

- Sorgen Sie dafür, dass Ihre Geräte (auch das Smartphone!) immer mit einem aktuellen Virenschutz versehen sind. Laden Sie regelmäßig Updates für das Virenprogramm herunter.
- Installieren Sie auch regelmäßig die Sicherheitsupdates für Ihren Browser.
- Achten Sie in verdächtigen Nachrichten auf Rechtschreibung und Grammatik. Oft sind solche Nachrichten sehr fehlerhaft. Manchmal liegt der Fehler auch nur im Detail, sodass z. B. der Name einer Bank in der Browserzeile geringfügig abweichend geschrieben ist (etwa Bowag

statt Bawag). Achten Sie generell darauf, ob die angegebene Internetadresse derjenigen entspricht, die Sie offiziell von Ihrer Bank, Ihrem Versandhaus etc. kennen. Weicht die Adresse ab, handelt es sich mit hoher Wahrscheinlichkeit um eine gefälschte Seite.

- Rufen Sie Websites (z. B. für Onlinebanking, Onlineshopping, Social Media …) immer direkt mit den Ihnen bekannten, offiziellen Links auf – nicht mit Links, die Sie in einer E-Mail oder anderen Nachrichten erhalten haben.
- Sollten Sie einen solchen Link versehentlich doch geöffnet haben, geben Sie keinesfalls Daten ein. Schließen Sie das geöffnete Fenster sofort wieder und starten Sie einen Suchlauf Ihres Virenprogramms. Falls Sie unsicher sind, ob Sie womöglich Schadsoftware heruntergeladen haben, suchen Sie Ihren Mobile Shop auf – die Mitarbeiterinnen und Mitarbeiter dort können dies überprüfen und auch eventuelle Abos, die ungewollt abgeschlossen wurden, wieder beenden.
- Sind Sie sich bei einer Eingabemaske, einem Loginbereich etc. unsicher, geben Sie nicht gleich Ihre tatsächlichen Daten ein, sondern beliebige, frei erfundene Daten. Funktioniert das Einloggen auch mit den erfundenen Daten, wissen Sie, dass es sich um einen Betrug handelt. Schließen Sie dann sofort die Website.
- Bleiben Sie auch bei ungewöhnlichen Posts oder Nachrichten von Ihnen bekannten Personen wachsam. Fragen Sie sich: Würde sie oder er so etwas tatsächlich verschicken? Schreibt sie oder er tatsächlich so? (Stil, Rechtschreibung)

(Saferinternet.at 2021b; Nowotny 2019; Watchlist Internet 2020)

Beim „**Scam**“ melden sich Menschen mit Betrugsabsichten z. B. per Mail und locken mit der Möglichkeit schnell an viel Geld zu gelangen. Um an die vermeintliche Erbschaft oder den vermeintlichen Gewinn zu gelangen, müssen jedoch Zahlungen vorab geleistet werden. Die Betrügerinnen und Betrüger streichen die Zahlung ein, der Gewinn oder die Erbschaft folgen nie. Oft werden auch Notfälle vorgetäuscht – die Tochter oder der Enkel sitze im Ausland fest, sei dort erkrankt oder in Haft gelangt, und benötige dringend Geld (Watchlist Internet 2019b).

Vorsicht ist nicht zuletzt vor „**Fake Shops**“ angesagt. Menschen mit Betrugsabsichten betreiben dabei vorgeblich einen Online-Shop und haben eine entsprechende Website, auf der sie besonders günstige Produkte anbieten. Wer die Produkte erwerben möchte, muss im Voraus zahlen, die Produkte werden jedoch nie verschickt. Der Betrugscharakter dieser Websites ist meist nicht auf den ersten Blick offensichtlich (Watchlist Internet o. J.). Folgende Merkmale deuten auf einen Fake-Shop hin:

- Einzig Vorkasse wird als Zahlungsmöglichkeit angeboten. Oft werden zunächst auch andere Zahlungsmöglichkeiten eröffnet. Wer diese auswählt, erhält jedoch eine Fehlermeldung und kann die Bestellung nicht abschließen, ohne den Betrag im Voraus zu überweisen.
- Die Produkte sind sehr viel günstiger als auf anderen Kanälen. Seien Sie skeptisch, wenn ein Produkt um mehrere hundert Euro günstiger angeboten wird als in den meisten anderen Verkaufskanälen.
- Die Echtheit angeführter Gütezeichen ist nicht überprüfbar. Prüfen Sie auf den Websites der angeführten Zertifikate, ob sich der Onlineshop in der Liste der zertifizierten Betriebe befindet.

Stellen Sie sicher, dass Sie wirklich die Website der Zertifikatsstelle und nicht (z. B. über einen Link der Fake-Shop-Website) eine nachgebaute Seite geöffnet haben.

- Recherchen Sie die im Impressum angegebene UID-Nummer (Umsatzsteueridentifikationsnummer), den Firmennamen und die Firmenadresse. Wenn Sie die UID-Nummer auch auf Websites anderer Unternehmen finden oder die Firmenadresse nicht existiert oder mitten in einem Wohngebiet liegt, handelt es sich wahrscheinlich um einen Fake-Shop.
- Recherchieren Sie, ob online bereits schlechte Erfahrungen mit dem Shop geteilt wurden.

(Watchlist Internet 2019a)

Werbung für bestimmte Produkte (z. B. mit unmittelbarer Verlinkung zur Einkaufsmöglichkeit) sollte im Rahmen des Projekts generell vermieden werden – auch aus Sicherheitsgründen. Kommt es vor, dass Gruppenmitglieder Links zu Onlineshops posten, weisen Sie bitte darauf hin.

6 Empfehlenswerte Websites zu Medienkompetenz

Folgende Websites sind generell empfehlenswert, um sich über Internetsicherheit zu informieren. Sie sind auch gute Nachschlageseiten, wenn man sich z. B. über eine erhaltene Nachricht unsicher ist und prüfen möchte, ob dazu schon Informationen vorliegen.

Saferinternet.at, https://www.saferinternet.at/
Mimikama, https://www.mimikama.at/
Watchlist Internet, https://www.watchlist-internet.at/
Klicksafe, https://www.klicksafe.de/
Hoax-Info Service der TU Berlin, https://hoax-info.tubit.tu-berlin.de/hoax/
Hoaxsearch, https://www.hoaxsearch.com

7 Mögliche Aktivitäten: Quizze und Selbsttests

Vielleicht möchten Sie nach der Lektüre dieses Kapitels Ihr Wissen testen oder einige Anwendungsbeispiele ausprobieren. Oder Sie würden gerne einmal unter den Gruppenmitgliedern, die Sie im Projekt betreuen werden, den Austausch über Medien- und Informationskompetenz anregen. Hier finden Sie einige spielerische Aktivitäten dazu.

Der Newstest

Eine unterhaltsame und spielerische Möglichkeit die eigene Medienkompetenz zu testen und dabei eventuell auch Neues zu lernen, ist der „Newstest“ (https://der-newstest.de/). Dieser wurde von der Stiftung Neue Verantwortung mit Unterstützung der Bundeszentrale für politische Bildung, der Landesmedienanstalt für Medien NRW, der Medienanstalt Berlin-Brandenburg und der Beauftragten der deutschen Bundesregierung für Kultur und Medien entwickelt. Eine Österreichversion des „Newstest“ wurde von der FH St. Pölten ausgearbeitet (https://der-newstest.at).

Thematische Schwerpunkte sind die Orientierung auf Nachrichten-Websites und Social Media, die Beurteilung der Richtigkeit und Vertrauenswürdigkeit von Informationen und Quellen, die Einschätzung des eigenen Umgangs mit (potentiellen) Falschnachrichten und das Wissen über die wirtschaftlichen Strukturen hinter Medien (z. B. öffentlich-rechtlich/privat, Konzerne). Manche Fragen sind deutschlandspezifisch, aber viele behandeln allgemein Wissenswertes über die Einschätzung von Onlinequellen. Großteils wird mit ganz konkreten Beispielen, etwa Advertorials, Newsbeiträgen oder Falschmeldungen, gearbeitet, die dann beurteilt werden sollen. Der Test gibt nicht nur Auskunft darüber, wie „gut“ man auf den verschiedenen Dimensionen abschneidet, sondern die Auswertung zeigt auch im Einzelnen, welche Fragen warum (nicht) richtig beantwortet wurden und gibt konkrete Tipps für einen kritischeren Umgang im Online-Bereich.

Unter dem Link https://der-newstest.at bzw. https://der-newstest.de/ kann der Test gestartet werden. Wenn Sie möchten, können Sie den Test als Vorbereitung auf Ihre Tätigkeit als Moderatorin oder Moderator selbst machen. Sie können ihn zusätzlich aber auch an die Gruppenmitglieder weitergeben, um sich gegenseitig in puncto Medienkompetenz zu sensibilisieren und idealerweise auch den Dialog darüber in Gang zu bringen.

Fake News Quiz von Klicksafe

Bei diesem Quiz wird Wissen über Falschnachrichten und deren Merkmale abgefragt, zudem kann man in Anwendungsbeispielen erproben, wie gut man selbst Fake News einschätzen kann. Nach jeder einzelnen Frage erhält man Feedback in Form genauerer Erklärungen.

https://www.klicksafe.de/typo3conf/ext/quiz_maker/Resources/Public/game/?path=https%3A%2F%2Fwww.klicksafe.de%2F%3FeID%3DquizJson%26uid%3D6

Unterrichtsmaterial aus dem Digitalreport

Diese Unterrichtsmaterialien enthalten am rechten Rand Fragen zum Selbsttest, u.a. zu Falschnachrichten und Bildmanipulation.
https://www.digitalreport.at/wp-content/uploads/2018/07/Unterrichtsmaterial-Digitalreport.pdf

Deep Fake Quiz auf derStandard.at

In diesem Quiz werden Ihnen 10 Videos präsentiert. Einige von ihnen sind echt, einige sind Deep Fakes – hergestellt von einem Absolventen der FH St. Pölten. Können Sie die echten von den gefälschten Videos unterscheiden?
https://www.derstandard.at/story/2000124957110/erkennung-von-deepfakes-standard-user-nicht-viel-besser-als-der

Quellenverzeichnis

Aschermann, T. (2020). *Cookies akzeptieren oder nicht? Das sollten Sie tun*. https://praxistipps.chip.de/cookies-akzeptieren-oder-nicht-das-sollten-sie-tun_42136 [22.10.2021]

Christof, F. (2019, September 12). *Wie man DeepFake-Videos erkennt*. https://futurezone.at/digital-life/wie-man-deepfake-videos-erkennt/400600496 [22.10.2021]

Dunn, H. B., & Allen, C. A. (2005). Rumors, Urban Legends and Internet Hoaxes. In *Rumors, Urban Legends and Internet Hoaxes: Bd. Proceedings of the Annual Meeting of the Association of Collegiate Marketing Educators* (S. 85–91). https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.520.6959&rep=rep1&type=pdf [22.10.2021]

Ebner-Zarl, A. (2021). *Die Entgrenzung von Kindheit in der Mediengesellschaft Kinder zwischen Talentförderung, Leistungsdruck und wirtschaftlichen Interessen*. Springer VS.

Eichfelder, M. (2019, September 17). *Was sind In-App-Käufe? Einfach erklärt*. https://praxistipps.chip.de/was-sind-in-app-kaeufe-einfach-erklaert_42031 [19.10.2021]

Erxleben, C. (2018, Juni 18). Absurdes Instagram-Urteil: Wenn Juristen das Internet nicht verstehen. *BASIC thinking*. https://www.basicthinking.de/blog/2018/06/18/absurdes-urteil-instagram-vreni-frost/ [22.10.2021]

Farinosi, M., & Fortunati, L. (2020). Young and Elderly Fashion Influencers. In Q. Gao & J. Zhou (Hrsg.), *Human Aspects of IT for the Aged Population. Technology and Society* (S. 42–57). Springer International Publishing. https://doi.org/10.1007/978-3-030-50232-4_4 [11.10.2021]

Follmer, S. (2020, März 19). *WhatsApp Kettenbrief: Virus durch Tobias Mathis/Anouk Theiler - das sollten Sie tun*. https://praxistipps.chip.de/whatsapp-kettenbrief-virus-durch-tobias-mathisanouk-theiler-das-sollten-sie-tun_92992 [03.10.2021]

Futurezone.at. (2018, April 18). *Deepfake: Barack Obama schimpft in Video über Donald Trump*. https://futurezone.at/digital-life/deepfake-barack-obama-schimpft-in-video-ueber-donald-trump/400023301 [14.10.2021]

Gassner, H. (2018, Juni 29). Kennzeichnung als Werbung—Ist nun alles Werbung? *Austria Insiderinfo*. https://blog.austria-insiderinfo.com/treibgut/kennzeichnung-werbung/ [14.10.2021]

Gebesmair, A. (2017). *Die wirtschaftliche und gesellschaftliche Bedeutung von YouTube-Channels in Österreich. Eine Studie im Auftrag der RTR-GmbH.* Fachhochschule St. Pölten,. https://www.rtr.at/medien/aktuelles/publikationen/Publikationen/YouTube_Channels_2017.de.html [21.11.2021]

Geiger, J. (2020, März 1). *Fitnesstracker und Datenschutz: Das solltet ihr beachten*. Curved.de. https://curved.de/tipps/fitnesstracker-und-datenschutz-so-schuetzt-ihr-eure-gesundheitsdaten-671143 [22.10.2021]

Gensing, P. (2020, September 3). *Deepfakes: Auf dem Weg in eine alternative Realität?* tagesschau.de. https://www.tagesschau.de/faktenfinder/hintergrund/deep-fakes-101.html [30.9.2021]

Google Play Hilfe. (2021). *App-Berechtigungen bei Android 6.0 und höher verwalten—Google Play-Hilfe*, https://support.google.com/googleplay/answer/6270602?hl=de [22.11.2021]

Hery-Moßmann, N. (2017, August 21). *Wearables—Was ist das eigentlich?* CHIP. https://praxistipps.chip.de/wearables-was-ist-das-eigentlich_95328 [14.10.2021]

IONOS (2017, Januar 12). *Advertorials – die Königsklasse im Native Advertising*. IONOS Digitalguide. https://www.ionos.at/digitalguide/online-marketing/verkaufen-im-internet/was-sind-advertorials/ [14.10.2021]

Klein, K., & Eppmann, R. (2020). Spielbasiertes Marketing. In M. Bruhn, C. Burmann, & M. Kirchgeorg (Hrsg.), *Marketing Weiterdenken: Zukunftspfade für eine marktorientierte Unternehmensführung* (S. 487–507). Springer Fachmedien.

Klicksafe.de. (o. J.-a). *Deep Fakes: Eine neue Qualität der Desinformation?*, https://www.klicksafe.de/service/aktuelles/news/deep-fakes-eine-neue-qualitaet-der-desinformation/ [14.10.2021]

Klicksafe.de. (o. J.-b). *Was sind Multi-Channel-Netzwerke?* https://www.klicksafe.de/themen/kommunizieren/youtube/was-sind-multi-channel-netzwerke/ [14.10.2021]

Köberer, N. (2014). Advertorials als Schnittstelle von Werbung und Journalismus. In N. Köberer, *Advertorials in Jugendprintmedien* (S. 97–110). Springer Fachmedien Wiesbaden.

Krug, K. (2018, September 9). *In-App-Käufe deaktivieren: Anleitung für Android und iOS*. https://praxistipps.chip.de/in-app-kaeufe-deaktivieren-anleitung-fuer-android-und-ios_92274 [14.10.2021]

Matthes, J., & Naderer, B. (2014). Zum Einfluss von Nahrungsmittelplatzierungen in Unterhaltungsfilmen auf das Essverhalten und die Markeneinstellungen von Kindern. In H. Schramm & J. Knoll (Hrsg.), *Innovation der Persuasion. Die Qualität der Werbe- und Markenkommunikation in neuen Medienwelten* (S. 59–74). Herbert von Halem.

Menge-Sonnentag, R. (2020, Juni 17). *Android-Entwickler müssen sich entscheiden: F-Droid oder Google-Play-Verkäufe*. Developer. https://www.heise.de/news/Android-Entwickler-muessen-sich-entscheiden-F-Droid-oder-Google-Play-Verkaeufe-4786684.html [15.10.2021]

Meschik, M. (2018). „Loot Boxes" – Über die Verwandschaft von Videospiel und Glücksspiel. *Medienimpulse*, *56*(1), 1–20.

Nairn, A., & Hang, H. (2012). *Advergames: It's not child's play A Review of Research*. Family & Parenting Institute. http://www.agnesnairn.co.uk/policy_reports/advergames-its-not-childs-play.pdf [15.10.2021]

Niedersächsisches Kultusministerium, NLQ Hildesheim, JFF - Institut für Medienpädagogik, & FWU. (2017). *Fake News und Social Bots im digitalen Zeitalter. Unterrichtsmaterialien für den Einsatz im Sekundarbereich II der gymnasialen Oberstufe*. https://www.nibis.de/uploads/1chaplin/files/FakeNews_SekII.pdf [16.10.2021]

Nowotny, R. (2019, Oktober 9). Angebliche Facebook-Profilviewer und die Fallen dahinter. *Mimikama*. https://www.mimikama.at/aktuelles/angebliche-facebook-profilviewer-und-die-fallen-dahinter/ [14.10.2021]

Nowotny, R. (2020a, Februar 21). Sehen, wer dein Facebook-Profil besucht hat? Das geht immer noch nicht! *Mimikama*. https://www.mimikama.at/aktuelles/sehen-wer-dein-facebook-profil-besucht-hat-das-geht-immer-noch-nicht/ [14.10.2021]

Nowotny, R. (2020b, November 15). „Geheime Schwester"—Vorsicht vor dem Weihnachtswichteln-Schneeballsystem! *Mimikama*. https://www.mimikama.at/aktuelles/geheime-schwester-pyramidensystem/ [14.10.2021]

Rechtsinformationssystem des Bundes. (2021, April 19). *Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Mediengesetz, Fassung vom 19.04.2021*. RIS. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000719 [23.10.2021]

Rehberg, A. I. (2020, Oktober 1). *Tracking in Apps: Das können Sie tun (Android)*. mobilsicher.de. https://mobilsicher.de/ratgeber/schnueffel-module-in-apps-das-koennen-sie-tun [14.10.2021]

Saferinternet.at. (2016). *Kettenbriefe – Beispiele & Tipps für den kompetenten Umgang*. Saferinternet.at. https://www.saferinternet.at/fileadmin/categorized/Materialien/Kettenbriefe_BeispieleundTipps.pdf [14.10.2021]

Saferinternet.at. (2021a). *HOAX – was ist das?* Saferinternet.at. https://www.saferinternet.at/faq/viren-spam-und-co/hoax-was-ist-das/ [14.10.2021]

Saferinternet.at. (2021b). *Was ist „Phishing" und was kann ich dagegen tun?* Saferinternet.at. https://www.saferinternet.at/faq/internetbetrug/was-ist-phishing-und-was-kann-ich-dagegen-tun/ [14.10.2021]

Saferinternet.at. (2021c). *Wie behalte ich die Kontrolle über meine digitalen Daten?* Saferinternet.at. https://www.saferinternet.at/faq/selbstdarstellung/wie-behalte-ich-die-kontrolle-ueber-meine-digitalen-daten/ [14.10.2021]

Schießl, T. (2020a, Juli 23). *Cookie-Hinweise: Einfach akzeptieren - und dann?* BR24. https://www.br.de/nachrichten/netzwelt/cookie-hinweise-einfach-akzeptieren-und-dann,S5Mcj8r [1.10.2021]

Schießl, T. (2020b, Juli 23). *So werden Sie Herr über die Cookies*. BR24. https://www.br.de/nachrichten/netzwelt/so-werden-sie-herr-ueber-die-cookies,S5TLO3S [1.10.2021]

Utz, C., Koloßa, S., Holz, T., & Thielbörger, P. (2019). Die DSGVO als internationales Vorbild? *Datenschutz und Datensicherheit - DuD*, *43*(11), 700–705.

Verbraucherzentrale.de. (2020, November 12). *Wearables und Fitness-Apps*. Verbraucherzentrale.de. https://www.verbraucherzentrale.de/marktbeobachtung/wearables-und-fitnessapps-40296 [22.11.2021]

Watchlist Internet. (o. J.). *Fake-Shops*. Watchlist-Internet, https://www.watchlist-internet.at/fake-shops/ [22.11.2021]

Watchlist Internet. (2019a, April 23). *So erkennen Sie Fake-Shops bevor es zu spät ist!* Watchlist-Internet. https://www.watchlist-internet.at/news/detail/News/so-erkennen-sie-fake-shops-bevor-es-zu-spaet-ist/ [22.11.2021]

Watchlist Internet. (2019b, Juni 26). *Achtung vor Scamming im Internet*. Watchlist-Internet. https://www.watchlist-internet.at/news/detail/News/achtung-vor-scamming-im-internet/ [22.11.2021]

Watchlist Internet. (2020, Februar 10). *Betrügerische Raiffeisen SMS im Umlauf*. Watchlist-Internet. https://www.watchlist-internet.at/news/betruegerische-raiffeisen-sms-im-umlauf/ [22.11.2021]

Winter, J., & Saferinternet.at. (o. J.). *Checkst du's? Material für den Unterricht*, https://www.digitalreport.at/wp-content/uploads/2018/07/Unterrichtsmaterial-Digitalreport.pdf [22.11.2021]

Zelenko, M. (2018, Juli 9). Gerichtsurteil: Jetzt geht es Modebloggern an den Kragen. *Kurier Online*. https://kurier.at/style/gerichtsurteil-jetzt-geht-es-modebloggern-an-den-kragen/400062416 [21.11.2021]

Ziemann, F. (2015, Dezember 16). *TU Berlin—Hoax—Extra-Blatt: Die wahre Geschichte des Craig Shergold*. https://hoax-info.tubit.tu-berlin.de/hoax/craig.shtml [21.11.2021]

Ziemann, F. (2021a, März 12). *Hoax-Info Service. Über Computer-Viren, die keine sind (sog. „Hoaxes") und andere Falschmeldungen und Gerüchte*. https://hoax-info.tubit.tu-berlin.de/hoax/ [19.10.2021]

Ziemann, F. (2021b, April 8). *TU Berlin—Hoax-Info Extra-Blatt: Coronavirus—Allerlei Unfug kursiert*. https://hoax-info.tubit.tu-berlin.de/hoax/corona.shtml [21.11.2021]