DIGITAL CHECK NRW

Digital weiterwissen.

#digitalweiterwissen

Das Magazin Ausgabe 02 | 2024

Schwerpunkt Desinformation

Ratgeber Medienkompetenz | Phishing | Fakeshops

INHALT

#digitalweiterwissen
Das Magazin 02

VORWORT

DIGITAL CHECK NRW

Liebe Leser*innen!

Die vergangenen Jahre waren durch vielfältige politische und gesellschaftliche Herausforderungen geprägt, u. a. die COVID-19-Pandemie, Kriege innerhalb und außerhalb Europas und die Sorge um unsere Umwelt.

Die alltägliche Flut an Informationen macht es schwer, alle Perspektiven auf ein Thema gleichermaßen im Blick zu behalten und sich eine differenzierte Meinung zu bilden. Vor allem im Internet finden sich viele unwissenschaftliche Theorien, hasserfüllte Botschaften und auch gezielt verbreitete Falschnachrichten, die zusätzlich Verwirrung stiften. Solche manipulative Meinungsmache einzudämmen, ist nicht nur Aufgabe der Politik, sondern der gesamten Gesellschaft, angefangen bei jeder einzelnen Person. Aber wie stellen wir das am besten an?

Mit unserem Magazin #digitalweiterwissen möchten wir die Menschen in Nordrhein-Westfalen dabei unterstützen, ihre Medienkompetenz zu erweitern, damit sie sich selbstbestimmt und sicher in der digitalen Medienwelt bewegen können. Jede Ausgabe widmet sich einem inhaltlichen Schwerpunkt – in dieser Ausgabe geht es um das Thema Desinformation.

Zunächst erklärt Franco Rau, was Desinformation eigentlich ist und wie man sich den Manipulationsversuchen entgegenstellen kann. Vera Servaty und Reiner Gerrards ergänzen das Thema um einen spielerischen Zugang und die Frage, wie das Erkennen von Desinformation durch digitale Spiele unterstützt werden kann. Außerdem haben wir Marisa Wengeler vom Institute for Strategic Dialogue (ISD) interviewt, die sich dem Thema aus Sicht der Konfliktforschung nähert.

Im Ratgeberteil geht es diesmal darum, was mit dem Begriff Medienkompetenz überhaupt gemeint ist und welche Angebote zur Förderung es im Netz gibt. Außerdem beschäftigen wir uns mit dem Erkennen betrügerischer E-Mails („Phishing“) und dem Entlarven gefälschter Onlineshops („Fakeshops“).

Schaut auch gerne mal auf www.digitalcheck.nrw vorbei. Dort findet ihr viele weitere spannende Themen rund um digitale Medien sowie einen Onlinetest, mit denen ihr eure Medienkompetenz testen und erweitern könnt. Folgt einfach dem QR-Code.

Wir bedanken uns herzlich für euer Interesse und wünschen viel Vergnügen beim Lesen!

Euer #DigitalCheckNRW-Team

KRITISCH DENKEN – DESINFORMATION DURCHSCHAUEN

Franco Rau

SCHWERPUNKT

Wir alle kennen es: Ein Politiker äußert sich zu einem viel diskutierten Thema, und schon tauchen manipulierte Bilder oder irreführende Zitate im Netz auf. Artikel legen prominenten Menschen radikale Aussagen in den Mund, die nie gefallen sind. In sozialen Medien begegnen uns sowohl Werbeanzeigen, die gezielt unsere Gefühle ansprechen, als auch täuschend echte, aber künstlich erstellte oder veränderte Bild-, Video- und Sprachaufzeichnungen, sogenannte Deepfakes. Immer wieder stellen wir uns die Frage: „Stimmt das wirklich?" Diese Phänomene – von Pseudojournalismus über manipulative Werbung bis hin zu Propaganda – sind allesamt Formen von Desinformation, die weiter unten noch genauer erklärt werden.

WAS IST DESINFORMATION UND WO LIEGT DAS PROBLEM?

Desinformation bezeichnet absichtlich falsche oder irreführende Inhalte. Sie werden mit dem Ziel verbreitet, Menschen zu täuschen oder zu manipulieren. Meist verfolgen die Produzent*innen dieser falschen Nachrichten politische, ideologische oder wirtschaftliche Interessen, wollen Meinungen beeinflussen und öffentliche Debatten steuern.

Das Problem an Desinformation ist, dass sie Unsicherheit schafft, weil es zunehmend schwerer fällt, zwischen echten und gefälschten Inhalten zu unterscheiden. Dadurch leidet das Vertrauen in staatliche Institutionen, seriöse Medien und demokratische Prozesse. Auch die Entwicklung von KI-Technologien erschwert es weiter, Wahrheit von Fiktion zu unterscheiden. Sie ermöglichen es, Bild- und Videomaterial so zu bearbeiten, dass Personen darin Dinge sagen oder tun, die sie in Wirklichkeit nie gesagt oder getan haben. Die Verbreitung von Desinformation erfolgt häufig durch die strategische Nutzung digitaler Plattformen, über die bestimmte Personengruppen gezielt angesprochen werden.

IN WELCHEN FORMEN BEGEGNET UNS DESINFORMATION?

Desinformation kann uns in verschiedenen Formaten begegnen: manipulierte Bilder oder Screenshots in Kurznachrichten bei X (vormals Twitter), inszenierte Videos auf Plattformen wie YouTube, pseudo-journalistische Artikel in sogenannten alternativen Medien oder geteilte Textnachrichten und Memes (meist lustige Bilder oder kurze Videos mit Text) in den Gruppenchats von Messengern wie Telegram oder WhatsApp. Inhalte von Desinformationen können völlig frei erfunden sein, wie zum Beispiel Werbeanzeigen, die unrealistische Geldgewinne versprechen. Andere liegen nah an der Wahrheit, indem sie einen echten Vorfall in einen irreführenden Zusammenhang stellen. Zum Beispiel könnte ein Bild von einer Demonstration mit einer falschen Schlagzeile verbreitet und so ein politischer Bezug erzeugt werden, der so nicht existiert. Die Demonstrierenden können auf diese Weise z.B. in ein falsches Licht gerückt werden, damit die Leser*innen sich eine negative Meinung über sie bilden.

Um Desinformation besser einschätzen zu können, sind zwei zentrale Fragen hilfreich:

1. **Faktizität:** Wie sehr entsprechen die verbreiteten Inhalte der Wahrheit?
2. **Intention:** Liegt von Seiten der Produzent*innen eine bewusste Täuschungsabsicht?

Mit diesen Fragen lassen sich drei unterschiedliche Formen von Desinformation hervorheben.

Pseudojournalismus

Pseudojournalismus präsentiert Inhalte, die auf den ersten Blick wie seriöse Berichterstattung wirken, dabei aber die grundlegenden journalistischen Standards missachten. Die Artikel oder Videos scheinen vertrauenswürdig, basieren jedoch auf falschen oder irreführenden Informationen. Ziel ist es, das Publikum in eine bestimmte ideologische Richtung zu lenken.

Bekannte Beispiele hierfür sind Blogs von rechtspopulistischen Autor*innen. Häufig werden dort Falschinformationen oder aus dem Zusammenhang gerissene Aussagen veröffentlicht, um Sachverhalte politisch aufzuladen oder zu verdrehen. Dieses im Pseudojournalismus gängige Mittel wird Dekontextualisierung genannt: Aussagen oder Fakten werden aus ihrem ursprünglichen Zusammenhang gerissen, um eine verzerrte Botschaft zu vermitteln. So geschah es etwa zu Beginn der COVID-19-Pandemie mit einer Aussage des Virologen Christian Drosten zur Wirksamkeit von Schutzmasken: In einem Interview hatte Drosten ausführlich über die vorhandenen Erkenntnisse und bestehenden Wissenslücken zu Alltagsmasken gesprochen. Pseudojournalist*innen bezogen seine Aussage „reine Spekulationen" direkt auf die Alltagsmasken. Daraus wurden verallgemeinernde und dekontextualisierte Überschriften und Artikel formuliert, z. B.

KRITISCH DENKEN – DESINFORMATION DURCHSCHAUEN

Franco Rau

„Drosten zu Masken: ‚Reine Spekulation'". Es entstand der Eindruck, Drosten zweifle generell an ihrer Wirksamkeit. Diese verzerrte Darstellung wurde dann genutzt, um das Vertrauen in staatliche Institutionen zu Corona-Schutzmaßnahmen zu untergraben.

Manipulative (politische) Werbung

Manipulative politische Werbung setzt gezielt auf falsche oder irreführende Inhalte, um das Wahlverhalten oder politische Meinungen zu beeinflussen. Ein gutes Beispiel ist der Einsatz von KI-generierten Bildern im Wahlkampf. So nutzen populistische Parteien z. B. künstlich erstellte Bilder von erfundenen Personen, um für ihre Partei zu werben. Diese "Personen" werden mit ebenfalls erfundenen Zitaten präsentiert, die die Ansichten der Parteien unterstützen sollen.

Diese Art von Desinformation ist besonders wirksam, da sie echte Emotionen wie Ängste und Sorgen anspricht und die Menschen somit gezielt manipuliert. Solche Werbeinhalte werden häufig durch sogenanntes Microtargeting an bestimmte Bevölkerungsgruppen in sozialen Netzwerken ausgespielt. Das bedeutet: Mithilfe einer genauen Auswertung vorliegender Daten und Informationen durch Algorithmen und die gezielte Ansprache von Personen wird Werbung sehr passgenau unter die Leute gebracht. Die Manipulation wirkt so viel besser auf einzelne Menschen und ist für die breite Öffentlichkeit oft unsichtbar.

Propaganda

Eine besonders aggressive Form der Desinformation ist Propaganda. Sie verbreitet absichtlich falsche oder stark verzerrte Informationen, um politische oder gesellschaftliche Ziele zu verfolgen. Oft werden dabei bestehende Ängste geschürt und Misstrauen gesät. Ein Beispiel hierfür ist die von Russland verbreitete Erzählung, dass die Ukraine von Nazis regiert werde. Russlands Präsident Wladimir Putin rechtfertigte den Krieg gegen die Ukraine unter anderem mit dem Argument, das Land „entnazifizieren" zu müssen. Zwar gibt es rechtsradikale Mitglieder im ukrainischen Asow-Regiment, doch die Behauptung einer systematischen „Naziherrschaft" ist stark übertrieben und dient vor allem als Propaganda. Die Verbreitung erfolgt häufig in Verbindung mit sogenannten Bots, d. h. Programmen, die automatisiert große Mengen an Inhalten in sozialen Netzwerken verbreiten können. Diese Programme simulieren echte Menschen bzw. Benutzungskonten. Sie teilen und kommentieren gezielt Inhalte, um deren Reichweite zu erhöhen. Solche Desinformationskampagnen werden häufig von Regierungen oder ideologischen Bewegungen genutzt, um die Bevölkerung gegen vermeintliche Feinde aufzuwiegeln und politische Machtverhältnisse zu festigen.

MIT WELCHEN STRATEGIEN WERDEN DESINFORMATIONEN BEKÄMPFT?

Die Bekämpfung von Desinformation erfordert unterschiedliche Ansätze auf individueller und gesellschaftlicher Ebene:

- **Prebunking (frühzeitige Aufklärung):** Menschen werden im Vorfeld über mögliche Desinformationen aufgeklärt, bevor sie diesen begegnen. Durch frühzeitiges Entlarven von Manipulationsstrategien werden sie widerstandsfähiger gegenüber falschen Inhalten. Projekte wie Klicksafe bieten dazu hilfreiche Materialien an.
- **Debunking (Entlarvung und Korrektur):** Falschinformationen werden nachträglich widerlegt. Plattformen wie Correctiv oder der ARD-Faktenfinder bieten Faktenchecks an, um Desinformationen richtigzustellen und Vertrauen in verlässliche Quellen zu stärken.

KRITISCH DENKEN – DESINFORMATION DURCHSCHAUEN

Franco Rau

SCHWERPUNKT

- **Counter Speech und Counter Narratives (Gegenrede):** Aktive Gegenrede mit faktenbasierten, positiven Inhalten hilft, Desinformation zu konfrontieren. Kampagnen, die Demokratie und Solidarität fördern (z. B. das Programm Demokratie leben! oder das Kompetenznetzwerk gegen Hass im Netz), bieten gezielte Alternativen zu manipulativen Inhalten.
- **Medienkompetenz fördern:** Langfristig ist es entscheidend, die Medienkompetenz aller Menschen zu stärken. Sie sollen lernen, Informationen kritisch zu hinterfragen und Quellen zu bewerten. Projekte wie #DigitalCheckNRW unterstützen hier.
- **Plattformregulierung:** Soziale Netzwerke müssen stärker verantwortlich gemacht werden. Durch bessere Moderation und nachvollziehbare Algorithmen kann die Verbreitung von Desinformation verringert werden.

Diese unterschiedlichen Ansätze zeigen, dass ein umfassendes Vorgehen notwendig ist, um den Einfluss von Desinformation auf die Öffentlichkeit möglichst klein zu halten. Insbesondere bedarf es vielfältiger Bildungsmaßnahmen, damit alle Menschen Desinformation frühzeitig erkennen und Strategien zu ihrer Abwehr erlernen können.

WAS KANN ICH TUN?

Jede*r kann aktiv dazu beitragen, Desinformation zu bekämpfen. Hier sind einige einfache Schritte, um sich zu schützen:

- **Quellen prüfen und mehrere Quellen verwenden:** Hinterfrage immer die Quelle einer Information, besonders bei gefühlsmäßig aufgeladenen oder außergewöhnlichen Nachrichten. Sind die Informationen vertrauenswürdig? Gibt es unabhängige Bestätigungen an anderer Stelle?
- **Faktencheck-Dienste nutzen:** Plattformen wie Correctiv oder Mimikama bieten einfache Möglichkeiten, Informationen zu überprüfen. Nutze diese, bevor du Inhalte teilst.
- **Emotionale Inhalte hinterfragen:** Desinformation zielt oft auf starke Gefühle wie Wut oder Angst. Sei bei solchen Inhalten besonders kritisch.
- **Desinformation melden:** Melde Falschinformationen an Plattformbetreiber und kläre dein Umfeld darüber auf.
- **Aktiv an Diskussionen teilnehmen:** Bringe deine Perspektiven in Diskussionen ein und habe den Mut, Desinformation klar als solche zu benennen. So stärkst du eine offene und wahrheitsorientierte Debattenkultur.

Durch solches bewusstes Handeln können wir alle gemeinsam die Verbreitung von Desinformation eindämmen, ihre schädlichen Einflüsse auf die Menschen verringern und unser gesellschaftliches Zusammenleben verbessern.

Typen von Desinformation und Misinformation

Verschiedene Formen von Desinformation und ihre Verbreitung aus kommunikationswissenschaftlicher und rechtswissenschaftlicher Perspektive

Gutachten

Ziel dieses Gutachtens ist es, verschiedene zu beobachtende Phänomene von Desinformation aus kommunikationswissenschaftlicher Perspektive zu definieren und voneinander abzugrenzen, um sie anschließend einer anfänglichen rechtswissenschaftlichen Einordnung zuzuführen. Auf diese Weise soll der Begriff der Desinformation für den weiteren Diskurs zugänglich und handhabbar gemacht werden.

die medienanstalten – ALM GbR (Hrsg.)

DESINFORMATION SPIELERISCH ERKENNEN

Vera Servaty und Reiner Gerrards

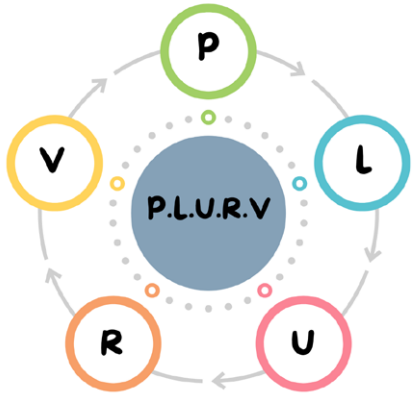
SCHWERPUNKT

Fast jeden Tag begegnen uns verschiedene Arten von Desinformationen, z. B. in Texten, Bildern und Videos, auf Social Media oder anderen Online-Plattformen. Dir ist das doch bestimmt auch schon mal passiert, oder? Manche Meldungen sind völlig absurd, andere allerdings täuschend echt. Umso wichtiger ist es, dass wir ein Bewusstsein für die Macht von Desinformation entwickeln und dass wir lernen, wie wir echte Informationen treffsicher von gefälschten unterscheiden können – auch um auf diese Weise ihre Weiterverbreitung zu stoppen.

WELCHE GAMES EIGNEN SICH ZUM ERKENNEN VON DESINFORMATION?

Aber wie kann dieses Lernen aussehen – und vielleicht sogar unterhaltsam sein? Könnten uns digitale Spiele dabei helfen, die eigenen Fähigkeiten für das Entlarven von Desinformation und damit die eigene Informations- und Nachrichtenkompetenz zu stärken? Geht das überhaupt? Schließlich will man doch vor allem Spaß beim Spielen haben, oder? Genau diesen Fragen sind wir nachgegangen. Wir wollten herausfinden, inwieweit Games geeignet sind, die eigene Kompetenz im Bereich Medienanalyse zu stärken. Konkret heißt das: Kann digitales Spielen dazu beitragen, dass Spielende danach Desinformation im Netz besser erkennen und entlarven können? Dazu ist es zunächst wichtig zu wissen, was wir eigentlich genau unter Desinformation verstehen, denn auf dieser Grundlage wurden die Kriterien für die Analyse der Spiele festgelegt und anschließend ausgewählte Games getestet.

Also, was genau ist Desinformation? Der Begriff bezeichnet mehr oder weniger alle Formen fehlerhafter Informationen, die bewusst so angelegt sind, dass sie dich täuschen oder manipulieren sollen. Desinformationen sollen vor allem dazu dienen, dich in deiner gesellschaftlichen oder politischen Meinung zu verunsichern oder deine Ansicht in Richtung der Haltung der Desinformant*innen zu lenken.



Desinformation nutzt dabei verschiedene Strategien zur Beeinflussung: Neben fehlenden Quellen und einer starken Gefühlsbetonung (= Emotionalisierung) in den Beiträgen kannst du Desinformation auch an den sogenannten P.L.U.R.V.-Strategien erkennen (Übersetzung des englischen F.L.I.C.C.-Konzepts, zum Thema Wissenschaftsleugnung).

P steht hier für Pseudoexpert*innen. Damit ist gemeint, dass der Begriff Experte oder Expertin nicht geschützt ist und erst einmal von allen gebraucht werden kann, anders als z. B. ein Doktortitel. Das Problem ist, dass es so schwieriger wird, wissenschaftliche Expert*innen von solchen zu unterscheiden, die sich selbst ohne nachgewiesene Fachkenntnisse Experte oder Expertin nennen. Das erzeugt große Unsicherheit. **L**ogikfehler beinhalten wiederum irreführende Vergleiche und setzen häufig auf den persönlichen Angriff statt auf eine sachliche Auseinandersetzung. **U**nerfüllbare Erwartungen und **R**osinenpickerei verzerren Diskussionen durch die Formulierung immer neuer Forderungen sowie durch die Auswahl von einzelnen Fakten aus einem größeren Zusammenhang. Die fünfte Strategie sind **V**erschwörungserzählungen. Sie unterstellen Ereignissen einen übergeordneten Plan, z. B. Vögel seien nicht echt, sondern fliegende Kameras, die uns überwachen. Die Erzählungen sollen in der Regel vor allem Gefühle wie Unsicherheit, Angst oder Wut hervorrufen.

Durch diese Strategien schafft es Desinformation, so viel Verwirrung zu erzeugen, dass du schnell nicht mehr weißt, was oder wem du glauben sollst. Die Desinformant*innen nutzen dann diese Verwirrtheit für ihre Zwecke und Ideen.

Ausgehend von diesem Grundlagenwissen haben wir uns die Frage gestellt, inwiefern das Erkennen von Desinformation auch spielerisch erlernt werden kann. Deshalb wurden von den Medienscouts der Gesamtschule Borbeck in Essen verschiedene digitale Spiele getestet, die sich mit dem Thema befassen. Das Medienscoutsprojekt ist ein Peer-to-Peer-Projekt, bei dem Schüler*innen im Alter von ca. 14 bis 18 Jahren zu Expert*innen in den Bereichen Internet, Social Media, digitale Spielkultur und zu vielen weiteren Themen rund um digitale Medien ausgebildet werden. Später sollen sie ihr Wissen auch an andere junge Menschen weitergeben.

Unter die Lupe genommen wurden vier kostenfreie Spiele, von denen die ersten beiden hier im Beitrag detailliert besprochen werden.

Kostenfreie Spiele zum Thema Desinformation:

- **True Fake:** (Spieleapp aus dem Jahr 2020; Entwicklung: ROTxBLAU; gefördert vom Bundesministerium für Familie, Senioren, Frauen und Jugend sowie der Amadeu Antonio Stiftung),
- **Im Bunker der Lügen:** (Actionbound-Spiel aus dem Jahr 2021; Entwicklung: Klicksafe),
- **Bad News:** (Browserspiel aus dem Jahr 2018; Entwicklung: DROG, University of Cambridge)
- **Wiebkes Wirre Welt:** (Browserspiel aus dem Jahr 2020; Entwicklung: Kubikfoto3, BAFF Filmproduktion, Bundeszentrale für politische Bildung).

DESINFORMATION SPIELERISCH ERKENNEN

Vera Servaty und Reiner Gerrards

SCHWERPUNKT

Hier einige Fragen, mit deren Hilfe die Spiele analysiert wurden:

Analysiert wurden die Spiele von den Medienscouts anhand verschiedener Fragen. Hier eine Auswahl:

- Sind Themenschwerpunkt und Lerninhalt deutlich erkennbar?
- Sind die Darstellungen fachlich richtig und führt das Spiel zu einer Erweiterung der Fähigkeiten?
- Ist das Spiel zielgruppen- und altersgerecht aufbereitet?
- Ist die Spieloberfläche einfach zu bedienen?
- Kann man gut in das Spiel eintauchen (= Immersion)?
- Macht das Spielen Spaß?

Im folgenden Abschnitt besprechen wir **True Fake** und **Im Bunker der Lügen** etwas detaillierter.

Zunächst ist uns beim Testen aufgefallen, dass beide Spiele ganz unterschiedliche Schwerpunkte besitzen. In **True Fake** geht es darum, möglichst viele Follower in sozialen Netzwerken für sich zu gewinnen, um auf diesem Weg die Stimmung innerhalb einer Demonstration positiv zu beeinflussen. Das Erkennen und Verbreiten von Real News (= echten Nachrichten) hebt dabei die Stimmung der Demonstrierenden, während Fake News (= Falschnachrichten) die Stimmung senken. Das Spiel dauert in etwa dreißig Minuten. Dir als Spieler*in stehen die Handlungsmöglichkeiten Surfen, Recherche, Reden und Posten zur Verfügung. Durch das Surfen gelangt man an Informationen aus dem Internet. Innerhalb der Recherche müssen aus den erhaltenen Infos die Real News von den Fake News getrennt werden. Anschließend postet man die Real News oder setzt sie beim Reden mit den Demonstrant*innen ein. Zusätzlich befinden sich Reporter*innen in der Spielwelt. Sie ermöglichen es, Auszeichnungen z. B. in den Bereichen Quellennutzung oder Schlagzeilen-Check zu erwerben, um die Stimmung der Demonstration schneller zu beeinflussen. Hat man Demonstrant*innen auf die eigene Seite gezogen, dann fangen sie an zu tanzen und lächeln dabei.

Positiv bewerteten die Medienscouts bei **True Fake** vor allem die Kriterien, die das Spieldesign und den Spielspaß betreffen. Besonders die Darstellung der gewonnenen Follower sorgte für Begeisterung. Kritik übten die Tester*innen vor allem auf der inhaltlichen Ebene. Hier wurde der Verzicht auf reale Nachrichtenbeispiele als problematisch eingestuft. Das Spiel nutzt lediglich schematische, verpixelte Platzhalter, in denen man nur bestimmte Bereiche wie das Wort „Impressum“ klar erkennen und zur Bewertung der News nutzen kann. Eine Einordnung der Nachrichten auf Grundlage ihrer Inhalte ist nicht möglich. Die Zielsetzung des Spiels ist für Spielende damit vielleicht nicht ganz klar. Um mit Hilfe des Spiels die eigenen Fähigkeiten beim Entlarven von Desinformationen zu schärfen, solltest du dich deshalb nach dem Spielerleben mit vertiefenden Fragen zum Thema beschäftigen. Ein weiteres Beispiel dafür, wo das Spiel Defizite aufweist: Für einen Spielerfolg ist das Vorhandensein einer seriösen Quelle für das Bewerten einer Nachricht wichtig, aber was macht diese überhaupt aus? Und wie kann sie außerhalb des Games von weniger seriösen Quellen unterschieden werden? Auf diese Fragen gibt das Spiel keine Antworten.

Während du also in das Spiel **True Fake** gut eintauchen kannst, es mit einer intuitiven Spieloberfläche überzeugt und dich – auch durch zusätzlich integrierte Minigames – mit viel Spielspaß locken kann, schneidet es vor allem in den zentralen Bereichen Lerninhalt, Themenschwerpunkt und fachliche Richtigkeit weniger gut ab. Grundsätzlich kann das Spiel aber ein motivierender Einstieg sein, sich näher mit dem Thema Desinformation zu beschäftigen.

Das zweite getestete Spiel **Im Bunker der Lügen** ist eine digitale Schnitzeljagd, die über die kostenfreie App Actionbound gespielt wird. Im Spielverlauf musst du dich mit Desinformation und Erzählungen eines Verschwörungsideologen auseinandersetzen, die dieser auf seinem Blog gepostet hat. In sechs Herausforderungen beantwortest du zumeist Quizfragen, z. B. zum Inhalt eines Impressums, schaust Videos oder liest Informationsblätter, z. B. zu Tricks und Strategien von „Fake News“. Für jede absolvierte Aufgabe gibt es sowohl einen Lösungsbuchstaben und, abhängig von der Qualität deiner Antwort, auch Punkte, die am Ende bestimmen, wieviel Zeit du hast, um das Lösungswort einzugeben. Eine Runde dauert etwa 25 Minuten.

Nach Einschätzung der Medienscouts zeigt das Spiel Schwächen im Bereich von Immersionspotenzial, Spielbarkeit und Spielspaß. Dafür ist es stärker auf das Thema,

DESINFORMATION SPIELERISCH ERKENNEN

Vera Servaty und Reiner Gerrards

einen klaren Lerninhalt und seine fachliche Richtigkeit ausgerichtet. So musst du z. B. innerhalb des Spiels Werkzeuge wie die „Google Reverse Search" (Rückwärtssuche in der Suchmaschine Google) zum Entlarven von Desinformation ausprobieren, um voranzukommen. Auf diese Weise werden eigene Fähigkeiten und Kompetenzen erweitert, die auch außerhalb des Spiels zum Erkennen realer Desinformation genutzt werden können. Ebenfalls greift die Spielhandlung Desinformationsstrategien wie Emotionalisierung und Verschwörungserzählungen gezielt auf.

Zusammenfassend kommen wir zu dem Schluss, dass die getesteten Games durchaus bei dir und anderen Spielenden Interesse am Thema Desinformation wecken können. Das reine Spielerleben allein reicht aus unserer Sicht jedoch nicht aus, um Desinformation im Anschluss schnell und zuverlässig entlarven zu können. Dazu sollten die in den Spielen angeschnittenen Inhalte im Nachhinein in Eigenarbeit noch weiter vertieft werden. Das kannst du u. a. mit dem Angebot des #DigitalCheckNRW tun, mit den Materialien von SogehtMedien oder auch mit Hilfe der Faktencheck-Seiten Mimikama.org oder Correctiv.org.

Für Spieleentwickler*innen ist es eine große Herausforderung, das richtige Verhältnis zwischen Lerninhalt, Thema, Fachlichkeit und Wissensvermittlung auf der einen Seite sowie Immersion, Spielbarkeit und Spielspaß auf der anderen Seite zu finden. Beim Testen haben wir das deutlich gemerkt, denn in beiden Spielen ist es unseres Erachtens nicht vollständig gelungen, beide Seiten zu bedienen.

Dennoch lohnt es sich, die Games einmal selbst auszuprobieren – ob nun allein, mit der Familie, mit Freund*innen oder in der Schule. Versuche dich dabei doch mal selbst als Spieletester*in und bilde dir deine eigene Meinung dazu, inwieweit die beiden besprochenen oder auch die beiden anderen Games (siehe Infokasten auf S. 11) geeignet sind, deine Fähigkeiten beim Entlarven von Desinformation zu verbessern. Wichtig ist, dass du dir vorab klar machst, was unter Desinformation zu verstehen ist und welche Strategien genutzt werden, um sie zu erstellen und zu verbreiten. Auf diese Weise erweiterst und festigst du deine eigene Informations-, Nachrichten- und Medienkompetenz!

Die Spiele können hier kostenfrei gespielt bzw. heruntergeladen werden:

- **True Fake:** rotxblau.de/truefake/
- **Im Bunker der Lügen:** klicksafe.de/materialien/actionbound-im-bunker-der-luegen
- **Bad News:** getbadnews.com/de/
- **Wiebkes Wirre Welt:** wiebkes-wirre-welt.de/

„Keine Person kann jede Desinformation fehlerfrei erkennen."

Marisa Wengeler

IM INTERVIEW

Frau Wengeler, Sie haben im Rahmen Ihrer Tätigkeit beim Institute for Strategic Dialogue (ISD) an der Entwicklung des Testbereichs „Desinformation" des #DigitalCheckNRW mitgearbeitet. Welche Aspekte waren Ihnen dabei wichtig?

Ein zentraler Aspekt bei der Sensibilisierung für das Erkennen von Desinformation ist, die Akteur*innen hinter der Verbreitung solcher Inhalte sowie deren Motive, Strategien und Ziele deutlich zu machen. Ohne ein Bewusstsein für diese Hintergründe fehlt oft die nötige Wachsamkeit, beim Überprüfen des Wahrheitsgehalts von Inhalten.

Ein weiterer Schritt besteht darin, die Methoden zu verstehen, mit denen Desinformationen „verpackt" werden. Sobald man sich dieser Techniken bewusst ist, lassen sich irreführende Inhalte wesentlich schneller identifizieren. Doch gerade hier liegt die Gefahr, denn die Methoden zur Verbreitung von Desinformation sind so raffiniert, dass sie sich schnell und unbemerkt verbreiten können. Bilder und Videos werden geschickt aus dem ursprünglichen Zusammenhang gerissen, wahre Informationen mit falschen Aussagen vermischt, oder es wird modernste Technologie genutzt, um Bilder und Videos täuschend echt zu manipulieren. All diese Techniken sind oft schwer zu durchschauen und führen dazu, dass Menschen immer stärker verunsichert werden, ob eine Information manipuliert wurde, oder nicht.

Um dieser Verwirrung entgegenzuwirken und Menschen wieder mehr Selbstbewusstsein und Sicherheit im Umgang mit Medien und Informationen zu geben, gibt es verschiedene Ansätze. Zum einen geht es darum, Verständnis für die Vorgehensweisen bei der Verbreitung von Desinformation zu schaffen. Wenn ich diese kenne, kann ich Inhalte bewusster hinterfragen und im nächsten Schritt prüfen, ob sie stimmen. Zum anderen müssen bestimmte Fertigkeiten erlernt bzw. vertieft werden, die es ermöglichen, Informationen verlässlich zu analysieren und einzuordnen. Dazu zählen unter anderem das Erkennen vertrauenswürdiger Expert*innen, eine sorgfältige Quellenüberprüfung oder Techniken wie die Bilderrückwärtssuche. Nur so kann Desinformation erfolgreich identifiziert und ihrer Verbreitung entgegentreten werden.

Desinformation meint, kurzgefasst, die bewusste Verbreitung von falschen Informationen, oftmals mit dem Ziel Verwirrung zu stiften, eine politische Agenda zu verfolgen oder einen finanziellen Vorteil zu erzielen. Können Sie ein paar konkrete Beispiele dazu benennen?

Die Ziele unterscheiden sich, je nachdem, wer die Desinformation verbreitet. Wenn es um politische Ziele geht, wird Desinformation oft genutzt, um politische Gegner*innen wie z. B. andere Parteien oder Staaten zu schwächen und gleichzeitig die eigene Machtposition zu festigen. Besonders populistische Parteien und Akteur*innen profitieren dabei von einer stark gespaltenen Gesellschaft und einer geschwächten Demokratie. Um dies zu erreichen, werden gezielt Desinformationen zu bestimmten Themen verbreitet, um die öffentliche Meinung zu manipulieren und starke Emotionen wie Hass oder Wut bei den Menschen zu erzeugen.

Ein anschauliches Beispiel für eine Desinformationskampagne, bei der langfristige Ziele und Strategien deutlich sichtbar werden, sind die Maßnahmen zur gezielten Beeinflussung der öffentlichen Meinung in Deutschland im Kontext des russischen Angriffskriegs auf die Ukraine. Seit Beginn des Krieges haben etwa russische und kremlfreundliche Akteur*innen Desinformationen verbreitet, die ukrainische Geflüchtete pauschal und unbegründet als Bedrohung darstellen. Zum Beispiel wurden in sozialen Medien und auf bestimmten Websites Desinformationen verbreitet, die behaupteten, dass ukrainische Geflüchtete in Deutschland überdurchschnittlich oft an gewalttätigen Vorfällen beteiligt seien. Einige dieser Berichte wurden zum Beispiel mit Fotos oder Videos in Verbindung gebracht, die in komplett anderen Zusammenhängen entstanden waren. Diese Desinformationen wurden dann zusätzlich mit der Behauptung verknüpft, dass nicht der Angriffskrieg Russlands, sondern westliche Waffenlieferungen für den Krieg und die Fluchtbewegungen verantwortlich seien. Auf diese Weise werden Vorurteile gegen Migrant*innen geschürt und gleichzeitig wird die Stimmung gegen deutsche Militärhilfen angeheizt. Diese negative Stimmung und das Fördern von Rassismus in der Gesellschaft schwächen die deutsche Regierung und ihre Politik. Das kommt letztlich der russischen Regierung zugute, die mit ihrer Ausdehnungspolitik gegen das Völkerrecht verstößt. Sich solcher Strategien bewusst zu sein, hilft enorm, um Desinformationen frühzeitig zu erkennen.

Außerdem beziehen sich Desinformationen häufig auf Themen, die starke emotionale Reaktionen hervorrufen, wie zum Beispiel Gesundheit oder politische Ereignisse wie Wahlen. Wenn wir emotional aufgewühlt sind, sei es durch Traurigkeit oder Wut, sind wir weniger geneigt, Informationen kritisch zu überprüfen. Dies schafft ideale Voraussetzungen dafür, dass Desinformation wirkt.

Während der Corona-Pandemie, einer Ausnahmesituation, die für viele Menschen eine enorme emotionale Belastung darstellte, wurden Desinformationen beispielsweise gezielt von betrügerischen Akteur*innen genutzt. Einige Unternehmen verkauften falsche Heilmittel gegen

„Keine Person kann jede Desinformation fehlerfrei erkennen."

Marisa Wengeler

COVID-19, wie etwa bestimmte Nahrungsergänzungsmittel oder „Wundermittel", die angeblich vor dem Virus schützen sollten. Diese falschen Informationen wurden über soziale Medien und betrügerische Websites verbreitet, um finanziellen Gewinn durch den Verkauf dieser Produkte zu erzielen.

Wenn ich mich für eine informierte und kritische Person halte, kann ich Desinformation dann leichter erkennen?

Ganz allgemein ist es natürlich gut, Informationen kritisch zu hinterfragen. Doch das bedeutet nicht zwangsläufig, dass auch die richtigen Schlüsse gezogen werden. Zunächst ist es wichtig, die eigenen Einstellungen, Vorurteile und sein persönliches Weltbild während des Medienkonsums im Hinterkopf zu haben. Diese beeinflussen nämlich maßgeblich, ob ich eine Information überhaupt erst hinterfrage. Ein Beispiel: Eine Person mit grundsätzlich negativer Einstellung gegenüber Migration und rassistischen Vorurteilen ist eher dazu geneigt, Desinformationen, die ihre Vorurteile bestätigen, unkritisch zu akzeptieren und nicht zu hinterfragen. Diesen Effekt nennt man Bestätigungsfehler, oder auf Englisch „Confirmation Bias". Daher empfiehlt das ISD in seinen Trainings zur Stärkung von Medienkompetenzen, ganz besonders jene Informationen zu hinterfragen, die das eigene Weltbild bestätigen. Wenn eine Information dann auch noch starke Emotionen in mir auslöst und auffällig oder vereinfachend präsentiert wird, ist besondere Vorsicht geboten. Quelle und Inhalt sollten dann sehr sorgfältig überprüft werden.

Neben dem Bestätigungsfehler gibt es weitere sogenannte kognitive Verzerrungen, die die eigene Mediennutzung beeinflussen. Dazu gehört der Dritte-Person-Effekt. Er besagt, dass wir glauben, weniger beeinflussbar zu sein als andere und negative oder manipulative Nachrichten – einschließlich Desinformation – uns nur wenig anhaben können. Diese Selbstüberschätzung führt dazu, dass wir uns selbst und unseren eigenen Medienkonsum weniger kritisch hinterfragen.

Als letztes ist noch der Fehlinformationseffekt zu nennen. Er beschreibt, wie falsche oder irreführende Informationen die Erinnerung an ein Ereignis verzerren können. Im Hinblick auf Desinformationen bedeutet dies, dass sich durch wiederholte oder gezielt gestreute Falschinformationen Erinnerungen oder Wahrnehmungen verändern können. Wenn etwa Desinformationen über politische Ereignisse, Migration oder Impfungen verbreitet werden, können diese falschen Informationen nachträglich das Gedächtnis beeinflussen. Selbst wenn Menschen die Wahrheit ursprünglich kannten, neigen sie durch wiederholte Konfrontation mit Fehlinformationen dazu, diese als wahr zu akzeptieren und ihre ursprünglichen Erinnerungen anzupassen. Dies verstärkt die Wirksamkeit von Desinformation, da Menschen letztlich die falschen Informationen als Teil ihres eigenen Wissens abspeichern.

Wichtig ist außerdem zu erkennen, dass die Verfestigung von Desinformationen stark vom sozialen Umfeld einer Person beeinflusst wird. Wenn Desinformationen innerhalb einer Gemeinschaft – etwa in Freundeskreisen, Familien oder Online-Gruppen – regelmäßig geteilt und bestätigt werden, steigt die Wahrscheinlichkeit, dass eine Person diese Falschinformationen unbewusst eher als wahr annimmt. Desinformationen stärken in gewissem Sinne auch den sozialen Zusammenhalt einer Gemeinschaft. Sie sind Ausdruck der eigenen Identität und fördern das Gefühl der Zugehörigkeit zu einer bestimmten Gruppe.

Grundsätzlich ist es von großer Bedeutung, sich gut zu informieren und einen kritischen Blick zu bewahren. Dieser sollte jedoch stets Strategien, Methoden und Motive der Akteur*innen, die Desinformationen verbreiten, miteinbeziehen und sich gleichzeitig auf die eigenen Anfälligkeiten und Verzerrungen bei der Mediennutzung richten. Der Fokus sollte außerdem darauf liegen, seriöse und verlässliche Quellen heranzuziehen. Im Internet findet man dazu zahlreiche Tipps, zum Beispiel bei der Bundeszentrale für politische Bildung. Aber auch im #DigitalCheckNRW gibt es zusätzlich zum Selbsttest viele hilfreiche Hinweise, die helfen, Quellen richtig einzuordnen.

Was möchten Sie den Leserinnen und Lesern unbedingt noch mitteilen?

Niemand ist vollständig vor den genannten Effekten geschützt, und keine Person kann jede Desinformation fehlerfrei erkennen. Wichtig ist letztlich, dass man bereit ist, dazuzulernen und dass gerechte und ausreichende Voraussetzungen für alle Mitglieder dieser Gesellschaft geschaffen werden, die nötige Medienkompetenz zu erwerben.

WAS IST DAS ISD?

*Seit 2006 zählt das Institute for Strategic Dialogue (ISD) zu den führenden Akteur*innen in der Analyse und Bekämpfung von Bedrohungen für die Demokratie. Die Organisation betrachtet das gesamte Spektrum digitaler und analoger Entwicklungen und erarbeitet innovative Ansätze zur Bekämpfung von Extremismus und gesellschaftlicher Polarisierung. Ihr Ziel ist es, die Demokratie im digitalen Zeitalter zu schützen. Beim ISD Germany liegt der Fokus auf gesellschaftlichen und politischen Trends in den deutschsprachigen Ländern und Europa, die aus einer globalen Perspektive analysiert und bearbeitet werden.*

MEDIENKOMPETENZ

RATGEBER

Medienkompetenz beschreibt einen selbstbestimmten, kritischen, kreativen und sozial verantwortlichen Umgang mit Medien. Doch was heißt das eigentlich genau? Was muss ich können, um als „medienkompetent" zu gelten? Sind manche Kompetenzen wichtiger als andere? Wie kann ich überprüfen, wie hoch meine Medienkompetenz ist? Und wie kann ich sie verbessern?

ALLE VERFÜGEN ÜBER MEDIENKOMPETENZ

Hast du schon einmal eine Nachricht über ein Smartphone verschickt? Ein Bild digital bearbeitet? Dich bei einem Nachrichtenbeitrag gefragt, ob die Inhalte der Wahrheit entsprechen? Hast du beim Öffnen einer E-Mail schon einmal gezögert, weil du nicht sicher warst, ob es sich um reine Werbung handelt? Oder die Benachrichtigungseinstellungen einer App verändert, damit du nicht über jede Neuigkeit informiert wirst? Wenn du eine oder mehrere dieser Fragen mit ja beantworten kannst, dann bringst du auf jeden Fall schon wichtige Kompetenzen der Mediennutzung mit.

Medienkompetenz meint mehr als nur Geräte bedienen zu können. Sie umfasst z. B. auch das kritische Mitdenken bei der Mediennutzung, die kreative Gestaltung von Medieninhalten sowie das Wissen darüber, wie verschiedene Inhalte für politische, wirtschaftliche oder andere Zwecke eingesetzt werden. Auch ein Grundverständnis davon, wofür neue Technologien verwendet werden können und wie sie funktionieren, gehört dazu. Eine Person, die ein Smartphone überhaupt nicht bedienen kann, dafür aber TV-Nachrichten regelmäßig hinterfragt, verfügt durchaus über Medienkompetenz, weist aber Defizite in Teilbereichen auf. Je mehr Wissen und Fähigkeiten du in den verschiedenen Bereichen mitbringst, desto selbstständiger und verantwortungsvoller kannst du deine Geräte nutzen, mit anderen kommunizieren, deinen Wissensschatz erweitern, mögliche Gefahrenstellen erkennen und praktische digitale Werkzeuge in deinen Alltag einbinden.

WELCHE KOMPETENZEN SIND DIE WICHTIGSTEN?

Jeder Kompetenzbereich ist für die gesamte Medienkompetenz wichtig. Daher sollte man sich grundlegende Kenntnisse quer durch verschiedene Bereiche aneignen, die später, je nach Interesse und Notwendigkeit, weiter vertieft werden können. Es gibt viele Weiterbildungsinstitutionen und medienpädagogische Organisationen, die Angebote zur Medienkompetenzförderung bereithalten und dabei helfen, sich in diesem weiten Feld zu orientieren, Übungsmaterialien zu bestellen und Lesetipps zu finden. Wir haben im Folgenden eine kleine Auswahl an Kompetenzen und passenden Angeboten zusammengestellt, die in NRW oder online verfügbar sind.

- Du solltest unterschiedliche digitale Geräte und Anwendungen bedienen können, z. B. Smartphones, Tablets und Laptops bzw. E-Mail-Dienstleister, Messenger und Browser. So kannst du mit der fortschreitenden Digitalisierung in verschiedenen Lebensbereichen mithalten und bist nicht nur auf ein Gerät oder Programm beschränkt.

Ein Konzept mit vielen Facetten

- **Digitalkompass:** Vielfältige Angebote, um die sichere und souveräne Nutzung digitaler Medien und Geräte zu fördern. Ein Projekt der Bundesarbeitsgemeinschaft der Seniorenorganisationen und Deutschland sicher im Netz.
- **Frag ZEBRA:** Hier erhältst du, laut der anbietenden Landesanstalt für Medien NRW, innerhalb von höchstens 24 Stunden konkrete und individuelle Unterstützung bei allen Medienfragen, die dir in deinem digitalen Alltag begegnen.

- Es ist praktisch zu wissen, welche digitalen Werkzeuge im Alltag zur Verfügung stehen, um von ihren Vorzügen profitieren zu können und eigene Vorlieben ausfindig zu machen. Dazu gehören z. B. verschiedene Apps zum Kommunizieren, gemeinsamen Arbeiten und für den alltäglichen Gebrauch z. B.:
  - digitale Kalender und Notizblöcke,
  - interessante Angebote passend zu deinen Hobbies,
  - Websites, auf denen du Bahntickets buchen oder Hotelzimmer reservieren kannst.
  - Es gibt viel Tolles zu entdecken! Du solltest die Sinnhaftigkeit dieser Angebote aber auch mit gesunder Skepsis beurteilen.
- **Switching.software:** Auf dieser Seite wird darüber informiert, welche Software von welchem Anbieter stammt und welche freien, datensparsamen Alternativen es jeweils gibt.

- Es ist wichtig zu verstehen, wie Medien und Programme produziert werden und wie Mensch und Maschine miteinander interagieren, um wechselseitige Einflüsse zu erkennen. Dazu gehören beispielsweise das Wissen über die Funktionsweise von Algorithmen und die Fähigkeit zu erkennen, wann Texte, Bilder und Videos möglicherweise durch Künstliche Intelligenz (z. B. Programme wie Midjourney oder ChatGPT) erstellt worden sind.
- **Medienbox NRW:** Ein Projekt zur Unterstützung beim Lernen von Audio- und Videoproduktion, das von der Landesanstalt für Medien NRW angeboten wird.
- **Medienpädagogik der Vielfalt:** Dateien von einem Gerät auf ein anderes übertragen, Fotos rechtssicher verschicken,

QR-Codes erstellen: Zu diesen und anderen Themen gibt die Gesellschaft für Medienpädagogik und Kommunikationskultur (GMK) viele Tipps und Tricks.

- Du solltest Nachrichten aus den Medien richtig einordnen und bewerten können, um passende, qualitativ hochwertige Informationen zu finden und effektiv recherchieren zu können. Dafür ist es wichtig zu wissen, wie du vertrauenswürdige Quellen in Suchmaschinen sowie gefälschte Bilder, Videos und Texte oder auch Werbung erkennen kannst. So kannst du Manipulation und künstlich erzeugter Meinungsmache entgehen.

➡ **Checked4you:** Ein Angebot der Verbraucherzentrale Nordrhein-Westfalen zum Prüfen von Nachrichten. Dort werden sowohl als falsch identifizierte Nachrichten veröffentlicht als auch Tipps zum Erkennen solcher gegeben.

➡ **Weitere Faktencheck-Seiten:** Mimikama.at, Correctiv.org

➡ **Newstest:** Ein Selbsttest, u. a. von der Bundeszentrale für politische Bildung, mit dem du deine Fähigkeiten im Umgang mit Nachrichten im Internet überprüfen kannst.

- Deine eigene Privatsphäre zu schützen und verantwortungsbewusst mit Daten anderer Personen umzugehen, ist in der digital geprägten Gesellschaft unerlässlich, um das Grundrecht auf informationelle Selbstbestimmung zu achten. Neben technischen Schutzmaßnahmen auf deinen Geräten hilft es dir auch zu wissen, welche Betrugsmaschen es gibt und wie Fremde potenziell an deine Daten gelangen können.

➡ **Landeszentrale für politische Bildung NRW:** Im Bereich „Digitale Medien" geht es u. a. um Themen wie digitale Demokratiekompetenz, digitale Zivilcourage und Künstliche Intelligenz. Zum Thema „Big Data" wird zudem ein sehr informatives Minispiel angeboten.

Ein Konzept mit vielen Facetten

➡ **Polizei für dich:** Eine Informationsseite zu vielen strafrechtlich relevanten Themen. Im Bereich „Sicherheit im Medienalltag" geht es beispielsweise um Cyberrisiken, Urheberrecht und das Recht am eigenen Bild. Ein Angebot der Polizeilichen Kriminalprävention der Länder und des Bundes.

- Es ist hilfreich zu wissen, wie du Medieninhalte wie Bilder, Videos und Texte selbst erstellen und aktiv mitgestalten kannst. Eigenständig neue Inhalte und Medien zu produzieren, hilft dir aktiv und kreativ zur Gesellschaft beizutragen, neue Interessen zu entwickeln und darüber mit anderen Menschen im Austausch zu bleiben.

➡ **iRights.info:** Ein Informationsangebot rund um das Thema Urheberrecht: Unterschiede von Lizenzen bei Texten, Bildern und Musik, Infos zu Filesharing und Streaming, AGB und Verträgen, Zitaten und Plagiaten, Datenschutz und IT-Sicherheit, sowie Tipps zur Vermeidung von und zum Umgang mit Abmahnungen.

- Auch wenn es nicht immer ganz einfach ist, solltest du die Zusammenhänge des sozialen Miteinanders und der digitalen Kommunikationskultur verstehen und über aktuelle Trends informiert bleiben, um mögliche Gefahrenquellen frühzeitig zu erkennen (z. B. persönliche, gesellschaftliche und wirtschaftliche Risiken).

➡ **Klicksafe.de:** Eine von der EU geförderte Initiative, die medienpädagogisches Material für verschiedene Zielgruppen zur Verfügung stellt, z. B. für Kinder, Eltern und Lehrkräfte. Auch die Formate reichen von Arbeitsblättern bis hin zu Erklärvideos oder Begleitmaterial für pädagogische Fachkräfte.

- Es ist wichtig, dass du deinen eigenen Medienkonsum reflektierst (z. B. die Dauer und die Inhalte) und diesen eigenständig regulierst, um dein digitales Wohlbefinden zu gewährleisten und eine Balance zwischen medialen und nicht-medialen Aktivitäten zu finden.

➡ **MobbingLine NRW:** Eine Telefonhotline für Beschäftige in NRW, um Betroffene von Mobbing am Arbeitsplatz schnell, anonym und kostenlos zu unterstützen.

➡ **Kompetenznetzwerk gegen Hass im Netz:** Aufklärungskampagnen, Beratung und Material für einen respektvollen Umgang im Netz. Ein Angebot von das NETTZ, HateAid, jugendschutz.net, den Neuen deutschen Medienmacher*innen und der Geselleschaft für Medienpädagogik und Kommunikationskultur.

Wenn du quer durch alle Kompetenzbereiche prüfen möchtest, wie es um deine Medienkompetenz steht und diese verbessern möchtest, dann kannst du den Online-Selbsttest des #DigitalCheckNRW auf www.digitalcheck.nrw machen.

MEDIENKOMPETENZ

DIGITAL CHECK NRW

6 FELDER DER Medienkompetenz*

1 Bedienen und Anwenden

- Geräte richtig anwenden
- Medien sinnvoll einsetzen und Grenzen von Medienkonsum verstehen
- Daten und Informationen organisieren
- verantwortungsvoll mit persönlichen und fremden Daten umgehen

2 Informieren und Recherchieren

- effizient recherchieren, Quellen gezielt auswählen
- Informationen auswerten und kritisch bewerten können
- unangemessene oder gefährdende Medieninhalte erkennen und mit ihnen umgehen

3 Kommunizieren und Kooperieren

- Regeln für eine sichere und zielgerichtete Kommunikation erlernen
- ethische Grundsätze beachten, kulturelle und gesellschaftliche Normen verinnerlichen
- Medien verantwortungsbewusst zur Zusammenarbeit nutzen

4 Produzieren und Präsentieren

- mediale Gestaltungsmöglichkeiten samt gesetzlicher Grundlagen der Medienproduktion kennen
- Kreativität bei der Planung und Umsetzung neuer Medienformate und Inhalte einsetzen

5 Analysieren und Reflektieren

- Vielfalt von Medien kennen
- kritisch mit Medienangeboten umgehen (z.B. Qualität von Inhalten unterscheiden)
- Medienangebote reflektiert, selbstbestimmt sowie selbstreguliert für die eigene Meinungs- und Identitätsbildung nutzen

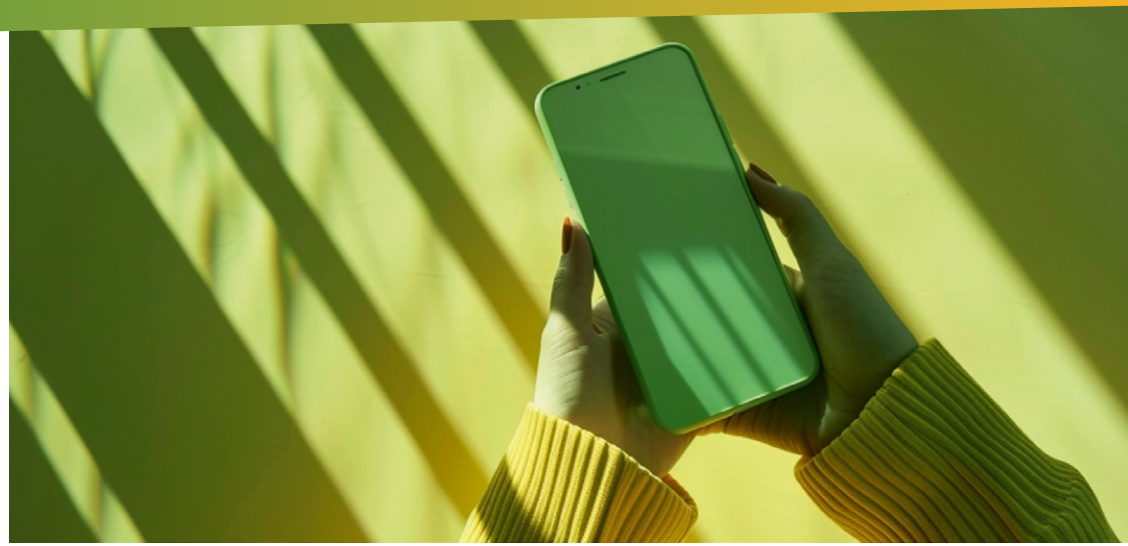
6 Problemlösen und Modellieren

- informatische Grundbildung erlangen, z. B. im Programmieren
- Einflüsse von Algorithmen und die Auswirkung der Automatisierung von Prozessen in der digitalen Welt reflektieren
- Lösungsstrategien entwickeln und anwenden

WWW.DIGITALCHECK.NRW

*des Medienkompetenzrahmens NRW

Ein Konzept mit vielen Facetten



WANN IST MAN AUSREICHEND KOMPETENT?

Neue Technologien, Geräte und Programme bringen immer neue Herausforderungen, Chancen, aber auch mögliche Gefahren mit sich. Sogar Einzelne Programme, z. B. Apps, über die man kommunizieren kann, können sogar Einfluss auf gesellschaftlicher oder politischer Ebene nehmen. So haben beispielsweise TikTok oder Instagram den Umgang mit Fotos und Videos beeinflusst, Videokonferenzen das berufliche Zusammenarbeiten verändert und über das Internet gesteuerte Haushaltsgeräte den Alltag vieler Menschen umstrukturiert.

Wenn du noch Verbesserungsbedarf bei deiner Medienkompetenz siehst, dann geht es dir wie vielen anderen auch. Da sich die Medienlandschaft schnell ändert und weiterentwickelt, sind alle Menschen dazu aufgefordert, ihre Kenntnisse und Fähigkeiten rund um den Konsum und die Nutzung von Medien aktuell zu halten. Ob eine Person noch sehr jung ist oder bereits im fortgeschrittenen Alter, macht dabei keinen Unterschied. Allerdings können sich die Ansatzpunkte, was noch gelernt oder verbessert werden sollte, stark voneinander unterscheiden. Auch die Nutzungsweise von Geräten (z. B. welche Geräte, wie lange, für welche Tätigkeiten genutzt werden) ist sehr individuell und bringt somit verschiedene Herausforderungen mit sich. Das Wichtigste ist, immer offen für neue Themen rund um Mediennutzung und Digitalisierung zu bleiben, dann kommen ganz automatisch nach und nach viele neue Kompetenzen dazu.

PHISHING

So erkennst du betrügerische E-Mails rechtzeitig

Phishing ist eine Form des Social Engineerings. Der Begriff setzt sich zusammen aus den englischen Wörtern für „Passwort" (password) und „angeln" (fishing). Gemeint sind verschiedene Betrugsmaschen, um Menschen schrittweise zu manipulieren, zu beeinflussen oder zu täuschen, sodass sie wichtige Informationen preisgeben, z. B. zu ihrer Person, zu ihren Finanzen oder auch persönliche Zugangsdaten. Für Kriminelle sind vor allem die Anmeldedaten für ein Computersystem, der Zugang zu einem Bankkonto oder die Passwörter für Accounts zu Onlineshops interessant.
*Da der Großteil aller geschäftsfähigen Menschen mindestens eine E-Mail-Adresse hat und diese Art der Kontaktaufnahme vergleichsweise wenig Aufwand bedeutet, wird Phishing besonders oft über E-Mails versucht. Häufig geben die Absender*innen dann vor, zu einer bekannten Organisation, einer Bank, einem Unternehmen o.Ä. zu gehören und eine offizielle E-Mail mit einem wichtigen Anliegen zu schreiben.*

GÄNGIGE BEISPIELE FÜR E-MAIL-PHISHING

- Die Deutsche Post, DHL oder ein anderer Versanddienstleister behauptet, dass dir ein Paket nicht zugestellt werden konnte und stellt dir einen Link zur Verfügung, um deine Sendung zu verfolgen.
- Amazon, Ebay oder ein anderer Onlineshop weist darauf hin, verdächtige Aktivitäten in deinem Konto festgestellt zu haben, die du mit einem Login in deinen Account überprüfen sollst.
- PayPal oder ein anderer Zahlungsdienstleister informiert dich darüber, dass du eine Zahlung erhalten hast, die du in deinem Konto bestätigen sollst.
- WeTransfer, Dropbox oder ein anderer Dienst zur Verwaltung von Dokumenten sendet dir eine Benachrichtigung, dass ein neues Dokument mit dir geteilt wurde und zum Herunterladen bereitsteht.
- Facebook oder eine andere Social-Media-Plattform schreibt dir, dass dein Konto wegen Inaktivität gesperrt wird, wenn du dich nicht in den nächsten 48 Stunden dort einloggst.
- Die Sparkasse, eine Bank oder ein Versicherungsdienstleister bittet dich um Aktualisierung deiner Daten, weil ein Datenschutzgesetz die regelmäßige Aktualisierung erfordert.

WAS WIRD MIT MEINEN DATEN GEMACHT?

Was mit den abgegriffenen Daten anschließend passiert, ist unterschiedlich. Einige nutzen die Anmeldedaten, um gezielt Geld abzuheben oder Waren einzukaufen. Andere probieren diese Daten an weiteren Stellen aus, in der Hoffnung, dass du dasselbe Passwort auch dort benutzt, wo es für die Betrüger*innen noch mehr „zu holen" gibt. Oft werden durch diese Tricks auch sehr große Mengen an Daten abgefangen und an weitere Betrüger*innen oder Werbetreibende verkauft.

TYPISCHE MERKMALE VON E-MAIL-PHISHING

- **Absendeadresse:** Der angezeigte Name der Absenderin / des Absenders kann irreführend sein. So kann dort beispielsweise der Name deiner Bank angegeben sein, obwohl die E-Mail von einer ganz anderen Adresse kommt. Die tatsächliche Absendeadresse kannst du dir mit einem Doppelklick auf den Absender anzeigen lassen. Wenn Absender*in und Adresse nicht zusammenpassen oder Zahlen, zusätzliche Satzzeichen oder Rechtschreibfehler enthalten sind, handelt es sich wahrscheinlich um Phishing.
- **Fehlende oder falsche persönliche Anrede:** Deine Bank würde dich nicht mit einem einfachen „Hallo", einem unpersönlichen „Guten Tag" oder einem verallgemeinerten „Sehr geehrte Damen und Herren" anschreiben. Die Anrede ist somit ein erster Punkt, auf den du achten kannst, wenn du sicher weißt, dass dem Unternehmen dein Name bekannt ist. Allerdings ist es Betrüger*innen oft auch möglich deinen Namen herauszufinden, vor allem wenn er Teil deiner E-Mail-Adresse ist oder auf der Website deines Arbeitgebers steht.
- **Fehler bei der Rechtschreibung und Grammatik:** Phishing-Mails werden in der Regel automatisiert erstellt. Sie können aus der ganzen Welt kommen, werden in unterschiedlichen Sprachen verfasst und müssen häufig übersetzt werden. Einen Betrugsversuch kannst du deshalb auch recht sicher daran erkennen, dass sich ein Fehler in die Schreibweise des absendenden Unternehmens eingeschlichen hat oder die Nachricht offenbar schlecht ins Deutsche übertragen wurde.
- **Aufforderung, persönliche Daten einzugeben:** Das Hauptziel der Absender*innen ist es meist, Namen, Adressen, E-Mailadressen, Kreditkartendaten und ganz besonders Login-Daten, also Benutzernamen in Kombination mit Passwörtern, zu bekommen. Ein häufig angewandter Trick ist die Bitte um Anmeldung bei deinem Konto über einen Link oder Button, den du anklicken sollst.
- **Fristsetzung und dringender Handlungsbedarf:** Es wird bewusst Druck aufgebaut, um dich in Panik zu versetzen und zu emotional geleitetem Handeln zu verleiten. Damit soll erreicht werden, dass du nicht lange nachdenkst, sondern die geforderten Anweisungen einfach durchführst. Formulierungen wie „Dringend: Ihr Konto wurde gesperrt" sollten dich hellhörig machen. Aber lass dich trotzdem auch nicht von ausgesprochen freundlichen Phishing-Mails täuschen.

So erkennst du betrügerische E-Mails rechtzeitig

RATGEBER

SO KANNST DU DICH VOR PHISHING SCHÜTZEN

- **Logisch mitdenken:** Kennst du das Unternehmen, das dich anschreibt nicht oder hast du mit der/dem Absender*in nichts zu tun? Wenn du nicht ganz sicher bist, weil es sich z. B. um eine Bank handelt, bei der du früher mal Kund*in warst, dann kontaktiere die/den Absender*in auf anderem Weg wie z. B. per E-Mail oder Telefon. Frag nach, welche Daten womöglich noch von dir gespeichert sind und bitte um die Löschung.
- **Bei der/dem vermeintlichen Absender*in nachfragen:** Du hast eine Mail deines Versicherungsanbieters bekommen und bist nicht sicher, ob sie echt ist? Dann nimm das Telefon in die Hand, ruf dort an und frag nach. Ob das Unternehmen dich tatsächlich kontaktiert hat, lässt sich meist schnell herausfinden. Faustregel: Frag lieber einmal zu viel als zu wenig.
- **Links prüfen:** Um die wahre Internetadresse zu verschleiern, werden entweder verkürzte Links eingesetzt oder die Links verstecken sich hinter Anzeigetexten wie „Hier klicken“. Wenn du eine E-Mail an deinem Computer öffnest und ohne zu klicken (!) mit der Maus über den verdächtigen Link fährst, dann erscheint am unteren linken Rand deines Bildschirms die Internetadresse, die sich hinter dem Linktext oder einem verkürzten Link verbirgt. Auf Mobilgeräten, bei denen du keine Maus zur Verfügung hast, funktioniert dieser Trick leider nicht. Warte mit dem Öffnen des Links daher bis du die Möglichkeit hattest, ihn an einem anderen Gerät zu überprüfen.
- **Nicht aus dem E-Mail-Postfach heraus handeln:** Auch wenn dir die E-Mail nicht verdächtig vorkommt, solltest du nicht den Link aus der E-Mail nutzen, um dich in einem Account anzumelden. Ruf die gewünschte Internetseite lieber, wie gewohnt, über deinen Browser oder deine App auf und verwende die Anmeldemaske, die du sonst auch immer verwendest.
- **Keine Anhänge öffnen oder herunterladen:** In den angehängten Dateien kann sich Schadsoftware verbergen, z. B. so genannte Trojaner, die dein Gerät ausspionieren. Dadurch können die Betrüger*innen an weitaus mehr Daten kommen als nur den Zugang zu dem einen Konto, durch den du angelockt wurdest. Zwar kann jede Datei Schadprogramme enthalten, auch Text- oder Bilddateien, die auf .pdf, .docx, .png oder .jpg enden, aber besonders vorsichtig solltest du bei den Dateiendungen .exe, .is, .lnk, .wsf, .scr, .jar und .bat sein. Diese zeigen bereits an, dass sich ein Programm dahinter verbirgt, keine einfache Text- oder Bilddatei.
- **Nie ein Passwort zweimal verwenden:** Möglicherweise fällst du auf einen Phishing-Betrug bei einem Dienst herein, bei dem gar nicht so sensible Daten von dir hinterlegt sind. Solltest du dieses Passwort aber auch noch woanders verwenden, kann der Schaden größer werden als zunächst angenommen. Nutze daher für jedes Konto ein anderes Passwort.
- **E-Mails in reinem Textformat anzeigen lassen:** Viele E-Mails werden heutzutage im HTML-Format verschickt, weil es dadurch möglich ist, verschiedene Schriftarten, fette oder kursive Schrift oder verschiedene Schriftgrößen einzubinden. In diese Formatierungen können aber auch schon Schadprogramme einprogrammiert sein, die du herunterlädst, auch ohne den Anhang der Mail geöffnet zu haben. Um ganz sicher zu gehen, kannst du in den Einstellungen deines E-Mail-Programms die Nachrichteninhalte von HTML auf Reintext/Plaintext stellen. Allerdings verzichtest du damit bei allen eingehenden und ausgehenden Mails auf die Möglichkeit, den Text zu formatieren.
- **Immer ausloggen:** Wenn du in einem Account nichts mehr zu tun hast, solltest du dich immer abmelden. Das Browser-Fenster zu schließen, ist keine richtige Abmeldung, da das Programm im Hintergrund weiterläuft. Durch das Ausloggen, bietest du weniger Angriffsfläche, falls du dir bereits Schadsoftware auf deinem Gerät eingefangen hast.

ERSTE-HILFE IN EINEM PHISHING-FALL

Phishing zu erkennen, ist nicht immer leicht – auch nicht für Profis. Manchmal wird man auch erst nach dem Klick auf einen Link oder nach der Eingabe persönlicher Daten von dem Gedanken geplagt, dass etwas nicht in Ordnung sein könnte. Wenn du also vermutest, dass du auf eine Betrugsmasche hereingefallen bist, solltest du Folgendes tun:

- Wechsle das Passwort für das Konto, um das es geht.
- Wechsle das Passwort in allen Accounts, für die du dieses Passwort verwendest.
- Wenn es sich um eine Bank handelt: Lass dein Konto sperren!
- Gib dem echten Unternehmen Bescheid: Viele Unternehmen schicken Warnungen vor betrügerischen Mails an ihre Kund*innen, wenn sie mitbekommen, dass vermehrt Betrugsversuche in ihrem Namen unternommen werden. So hilfst du mit dieser Panne sogar noch anderen.

Das Gute: Je häufiger du auf Aspekte des Phishings achtest, desto geübter wirst du darin, Betrug zu erkennen. An dieser Stelle schadet es auch nicht, ein wenig übervorsichtig zu sein. Wenn sich die E-Mail am Ende als echt herausstellt, dann weißt du wenigstens, dass du kompetent vorgegangen bist.

FAKESHOPS

RATGEBER

Hast du schon mal etwas online bestellt und die Ware nie erhalten? Oder hattest du plötzlich seltsame Abbuchungen auf deiner Kreditkarte? Dann bist du vielleicht auf einen Fakeshop reingefallen. Fakeshops sind betrügerische Onlineshops, die nur darauf abzielen, dir dein Geld oder deine Daten abzunehmen. Sie sind oft schwer zu erkennen, weil sie wie echte Shops aussehen. Wir zeigen dir, wie man einen Fakeshop erkennt und stellen den Fakeshop-Finder der Verbraucherzentralen vor, der dabei helfen kann.

WARUM IST ES WICHTIG, FAKESHOPS ZU ERKENNEN?

Fakeshops sind ein großes Problem. Sie locken mit supergünstigen Preisen, aber am Ende bekommst du entweder gar nichts oder minderwertige Ware. Oder schlimmer noch: Oft nutzen die Betrüger deine Kreditkartendaten oder andere persönliche Informationen missbräuchlich und verkaufen diese Daten weiter. Die Zahl der Beschwerden über Fakeshops bei den Verbraucherzentralen steigt ständig: 2023 waren es bundesweit über 6.900, fast sechsmal mehr als noch 2020! Die Erscheinungsformen sind sehr unterschiedlich: Mal werden die Websites bekannter Onlineshops kopiert, aber oft werden auch neue Websites für erfundene Shops angelegt.

WIE DU FAKESHOPS ERKENNEN KANNST

Es gibt einige Merkmale, die darauf hinweisen können, dass ein Onlineshop ein Fakeshop ist:

1. Zu gute Preise: Wenn die Angebote viel günstiger sind als anderswo, solltest du misstrauisch sein.

2. Merkwürdige Domainnamen: Stimmt die Domain (der namensgebende Teil der Internetadresse) mit dem Namen des Shops überein? Werden ungewöhnliche Endungen wie „.de.com“ verwendet, die auf eine deutsche Seite hindeuten, aber dann doch eine internationale Endung nutzen?

3. Kein Impressum: Seriöse Shops haben immer ein Impressum mit Kontaktinformationen der Verantwortlichen und ihrer Handelsregisternummer, denn diese Angaben sind für Anbieter verpflichtend.

4. Seltsame Bezahlmethoden: Wenn am Ende des Bestellprozesses nur unsichere Bezahlmethoden wie Vorkasse angeboten werden, oder andere als vorher angegeben, ist Vorsicht geboten.

5. Kein HTTPS: Achte darauf, dass die Adresse des Shops mit „https://“ beginnt. Das „s“ steht für „secure“ (sicher) und zeigt, dass die Verbindung verschlüsselt ist, was zumindest für erhöhte Sicherheit und Seriosität spricht.

Andere Merkmale sind nicht immer leicht zu erkennen. Genau hier kommt der Fakeshop-Finder ins Spiel: Mit ihm kannst du kostenlos und schnell eine Einschätzung zu einem Onlineshop einholen.

WIE FUNKTIONIERT DER FAKESHOP-FINDER?

Der Fakeshop-Finder, ein Angebot der Verbraucherzentrale NRW, ist ein kostenloses Online-Tool der Verbraucherzentrale NRW. Er prüft, ob ein Shop typische Merkmale eines unseriösen Anbieters aufweist. So funktioniert's:

1. Adresse eingeben: Du gibst die Internetadresse des Shops unter www.fakeshop-finder.de ein.

2. Analyse abwarten: Eine Künstliche Intelligenz (KI) überprüft die Website. Dabei wird sie nach bekannten Fakeshop-Merkmalen gescannt und es wird geschaut, ob die Seite auf seriösen Fakeshop-Listen steht. Das dauert nur wenige Sekunden.

3. Ergebnis erhalten: Du erhältst eine Einschätzung in Ampelfarben:

- **Rot:** Eindeutige Warnung, hier besser nicht bestellen.
- **Gelb:** Hier solltest du nochmal genau hinschauen.
- **Grün:** Alles in Ordnung, hier hat der Fakeshop-Finder keine Anzeichen für einen Fakeshop gefunden.

Die Datenbank des Fakeshop-Finders wächst ständig, jeden Monat kommen mehr als 1.000 neue Fakeshops hinzu. Bislang sind schon mehr als 60.000 erkannte Fakeshops darin gespeichert – allein aus dem deutschsprachigen Raum. Das Tool ist sehr benutzungsfreundlich und kann dir helfen zu entscheiden, ob ein Shop vertrauenswürdig ist. Die Verbraucherzentrale NRW und das Ministerium für Landwirtschaft und Verbraucherschutz des Landes Nordrhein-Westfalen unterstützen dieses Projekt.

RATGEBER

TIPPS FÜR SICHERES ONLINESHOPPING

Neben dem Fakeshop-Finder kannst du noch weitere Dinge beachten, um sicher online einzukaufen:

- **Lies Bewertungen:** Schau dir die Kundenbewertungen an, aber sei vorsichtig bei zu vielen, überschwänglich positiven Bewertungen, denn diese könnten möglicherweise gefälscht sein.
- **Achte auf Gütesiegel:** Zertifizierungen wie „Trusted Shop" können auf seriöse Shops hinweisen. Allerdings kann nicht ausgeschlossen werden, dass auch dieses Siegel kopiert oder gefälscht wurde. Wenn das Siegel nicht anklickbar ist, deutet es auf eine Fälschung hin.
- **Nutze sichere Zahlungsmethoden:** Bevorzugt Kreditkarte oder PayPal, da diese oft Käuferschutz bieten und keine direkte Angabe der Bankverbindung benötigen.
- **Prüfe die URL:** Vergewissere dich, dass du auf der richtigen Website bist, die URL auf den korrekten Shop hinweist und du nicht auf eine Drittseite umgeleitet worden bist.
- **Sei misstrauisch bei Druck:** Wenn dich ein Shop stark unter Druck setzt, sofort zu kaufen, solltest du skeptisch sein.

SO KANNST DU FAKESHOPS IM NACHHINEIN ERKENNEN

Manchmal muss es einfach schnell gehen. Die Bestellung wird zügig zusammengeklickt und nach dem Online-Einkauf kommen dann aber doch Zweifel an der Seriosität des Shops. Auch nach der Bestellung gibt es ein paar Kriterien, auf die du achten kannst:

- **Merkwürdige E-Mail-Adressen:** Seriöse Anbieter verwenden für die Unternehmenskommunikation seriöse Mailadressen. Eine Bestellbestätigung von einer zusammengewürfelten Mailadresse (z. B. susanne88a7667k@web.de) bietet somit einen Anhaltspunkt für einen unseriösen oder gefälschten Shop.

So schützt du dich beim Online-Shopping

- **Fehlende Bestellbestätigung:** Wenn du gar keine Bestellbestätigung per E-Mail erhalten hast, solltest du wachsam werden. Das kann zwar auch in seriösen Shops mal passieren, aber es schadet nicht nachzuhaken.
- **Unerwartete Abbuchung:** Stelle sicher, dass der korrekte Betrag für deine Bestellung abgebucht wird und keine versteckten Kosten auf dich zukommen.

Auch wenn die Kontrolle eines Shops ein paar Rechercheschritte benötigt, ist es wichtig, dass du auf Nummer sicher gehst. Solltest du tatsächlich in einem Fakeshop bestellt haben, kann es eventuell schwierig sein, dein Geld zurückzubekommen. So kann es beispielsweise sein, dass die Betreiber eines Fakeshops es schaffen, sich bei den kooperierenden Bezahldienstleistern (z. B. bei Klarna) als seriös zu verifizieren und die Rückerstattung des Geldes dadurch länger dauert. Eine Strafanzeige bei der Polizei solltest du in jedem Fall stellen, auch wenn diese vielleicht erfolglos bleibt. Wenn du mittels Kreditkarte gezahlt hast und das Gefühl hast, auf einen Fakeshop hereingefallen zu sein, solltest du auch deine Kreditkarte bei deiner Bank sperren lassen. So verhinderst du, dass Betrüger*innen deine Kreditkarte nutzen können oder dir noch mehr Geld abbuchen.

Wenn du mehr zum Thema wissen willst, schau auf www.fakeshop-finder.de vorbei. Dort gibt es auch viele nützliche Tipps und Informationen rund um das Thema Fakeshops.

Dieser Text ist in Kooperation mit Oliver Havlat entstanden. Oliver Havlat leitet das Projekt «Fakeshop-Finder» bei der Verbraucherzentrale NRW.

RATGEBER

FAKESHOPS:

FAKESHOPS? SO ERKENNST DU SIE

Es gibt einige Merkmale, die darauf hinweisen können, dass ein Onlineshop ein Fakeshop sein könnte.

DIGITAL CHECK NRW

1 Zu gute Preise
Wenn die Angebote viel günstiger sind als anderswo, solltest du misstrauisch sein.

2 Merkwürdige Domainnamen
Stimmt die Domain (der namensgebende Teil der Internetadresse) mit dem Namen des Shops überein? Werden ungewöhnliche Endungen wie „.de.com" verwendet, die auf eine deutsche Seite hindeuten, aber dann doch eine internationale Endung nutzen?

3 Kein Impressum
Seriöse Shops haben immer ein Impressum mit Kontaktinformationen der Verantwortlichen und ihrer Handelsregisternummer, denn diese Angaben sind für Anbieter verpflichtend.

4 Seltsame Bezahlmethoden
Wenn am Ende des Bestellprozesses nur unsichere Bezahlmethoden wie Vorkasse angeboten werden oder andere als vorher angegeben, ist Vorsicht geboten.

5 Kein HTTPS
Achte darauf, dass die Adresse des Shops mit "https://" beginnt. Das „s" steht für „secure" (sicher) und zeigt, dass die Verbindung verschlüsselt ist, was zumindest für erhöhte Sicherheit und Seriosität spricht.

MEHR INFORMATIONEN:
WWW.DIGITALCHECK.NRW

IMPRESSUM

UNSERE GASTAUTOR*INNEN IN DIESER AUSGABE:

Prof. Dr. Franco Rau ist Erziehungswissenschaftler und Professor für Mediendidaktik an der Universität Vechta. Zudem ist er Mitglied des Medienkompetenzzentrums Vechta und hat u. a. ein Projekt zur Dekonstruktion digitaler Desinformation geleitet.

Vera Servaty und Reiner Gerrards arbeiten an der Gesamtschule Borbeck in Essen. Sie wurden 2011 von der Landesanstalt für Medien NRW zu Beratungslehrkräften für Medien ausgebildet und leiten seitdem das Medienscoutsprojekt sowie die zugehörige AG an ihrer Schule. Die Medienscouts bilden als Peer-Expert*innen u. a. Mitschüler*innen und Lehrkräfte schulintern und -übergreifend z. B. im Bereich Gaming fort. Innerhalb ihrer Arbeit kooperierten sie bereits mit Electronic Arts, dem Spieleratgeber NRW, dem Spielemuseum in Berlin, dem Spielraum in Köln, dem Play Festival in Hamburg sowie dem Handysektor und Klicksafe.

Marisa Wengeler arbeitet beim Think and Do Tank Institute for Strategic Dialogue in Berlin im Bereich Civic Action. Dort beschäftigt sie sich vor allem mit Hintergründen, Strategien und Auswirkungen der Informationsmanipulation. Sie hält Vorträge und gibt Workshops zu den Themen Hass im Netz, Verschwörungserzählungen und Desinformation für das Projekt "Business Council for Democracy".

Oliver Havlat leitet das Projekt „Fakeshop-Finder" bei der Verbraucherzentrale Nordrhein-Westfalen. Der Beitrag zum Schutz vor Fakeshops ist in Kooperation mit dem #DigitalCheckNRW-Team entstanden.

Alle weiteren Beiträge wurden vom Team des #DigitalCheckNRW verfasst.

IMPRESSUM #digitalweiterwissen | Das Magazin - Ausgabe 2 / 2024

HERAUSGEBERIN

Gesellschaft für Medienpädagogik und Kommunikationskultur (GMK) e.V.
Obernstr. 24a | 33602 Bielefeld
www.gmk-net.de
Geschäftsführung: Dr. Friederike von Gross

GMK Gesellschaft für Medienpädagogik und Kommunikationskultur

GEFÖRDERT DURCH

Der Ministerpräsident des Landes Nordrhein-Westfalen

REDAKTION

#DigitalCheckNRW
Telefon: 0521/677 88
www.digitalcheck.nrw
E-Mail: digitalcheck@medienpaed.de

DIGITAL CHECK NRW
Digital weiterwissen.

GESTALTUNG

Katharina Künkel,
Büro für Gestaltung, Bielefeld
E-Mail: post@kkuenkel.de

Alle verwendeten Bilder wurden mit KI erstellt. Ausnahme: Abbildung auf S. 10: (c) Vera Servaty & Reiner Gerrards

„Falschmeldungen im Internet erkenne ich sofort. Du auch?“

Lerne digitale Medien besser kennen und verstehen: www.digitalcheck.nrw

ÜBER DEN #DIGITALCHECKNRW

Der #DigitalCheckNRW ist ein kostenfreier Selbsttest im Internet. Mit seiner Hilfe können Nutzer*innen herausfinden, wie kompetent sie im Umgang mit digitalen Medien sind und z. B. ihr Wissen zu Themen wie Künstliche Intelligenz, Cybersicherheit und Desinformation verorten. Neben dem Ergebnis liefert der Test passende Weiterbildungsangebote aus einer umfangreichen Datenbank – vor Ort oder auch online. Zudem finden sich auf der Website im Bereich #digitalweiterwissen weitere Informationsangebote rund um digitale Mediennutzung und die durch sie geprägten Lebenswelten. Der #DigitalCheckNRW ist ein Projekt der Gesellschaft für Medienpädagogik und Kommunikationskultur e.V. (GMK) und wird gefördert durch die Landesregierung Nordrhein-Westfalens. Der Test basiert auf dem bewährten Medienkompetenzrahmen NRW, der erst für Schulen entwickelt und nun für Erwachsene nutzbar gemacht wurde, um die Förderung von Medienkompetenz und Medienbildung in jeder Lebensphase zu ermöglichen.

FEEDBACK UND ANREGUNGEN? NACHBESTELLUNGEN?

Du hast Ideen und Wünsche für unsere nächsten Ausgaben oder möchtest weitere Exemplare bestellen? Dann schreib uns eine E-Mail an digitalcheck@medienpaed.de. Wir freuen uns auf deine Rückmeldung!

DIGITAL CHECK NRW