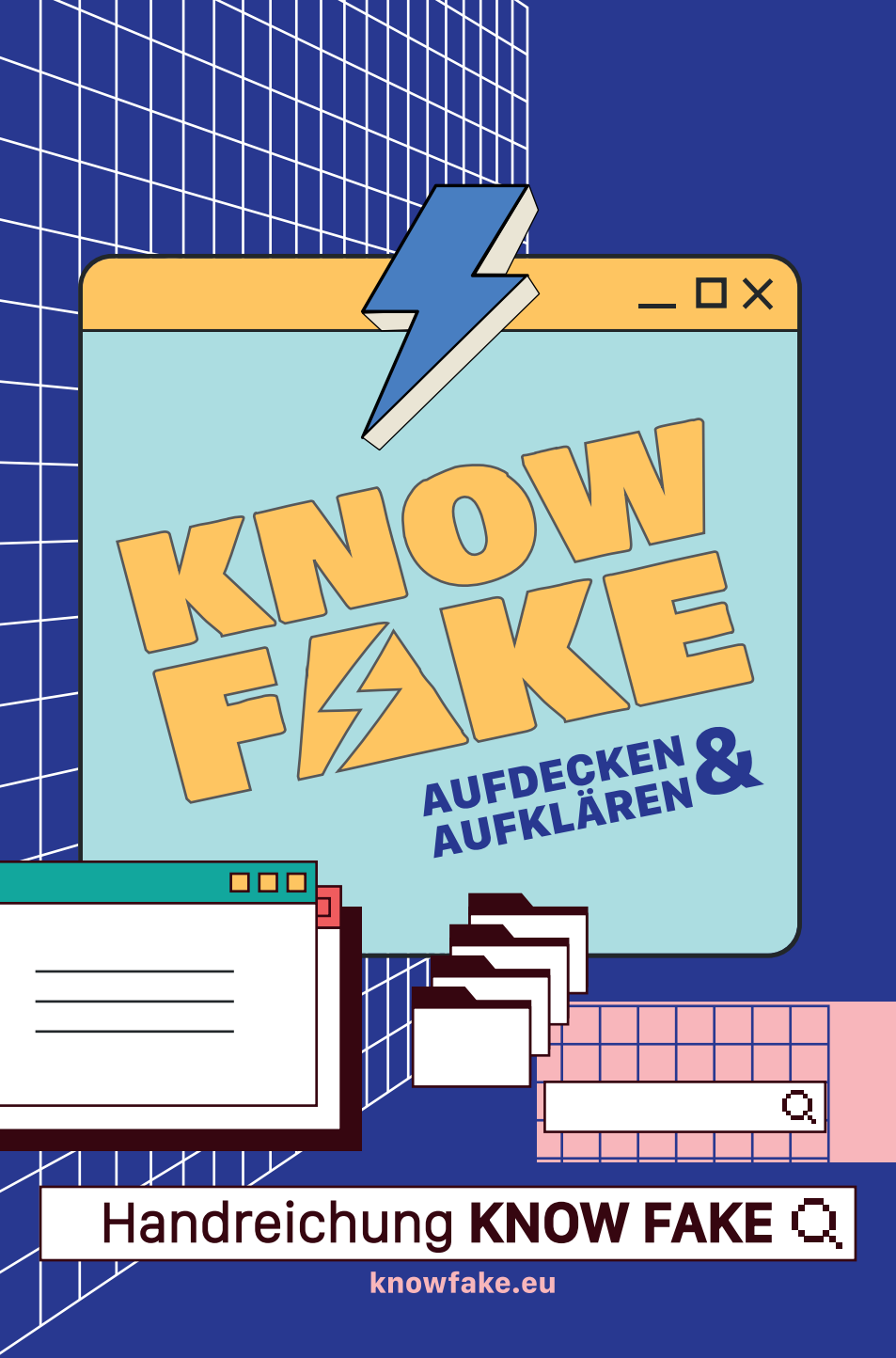


# Handreichung **KNOW FAKE**

knowfake.eu

## INHALTSVERZEICHNIS:



## KNOW FAKE REGELN & SPIELANLEITUNG

### SPIELANLEITUNG

Das Spiel KNOW FAKE fordert auf, Informationen genauer zu betrachten, Desinformationen zu erkennen und korrekt zuzuordnen. Deine Aufgabe ist es, die relevanten Informationen zu finden und sie richtig miteinander in Verbindung zu bringen.

***Viel Erfolg beim Aufdecken von Fakes!***

**Spielinhalt**
42 Spielkarten (21 Kartenpaare)
Spielanleitung

Das Spiel KNOW FAKE besteht aus insgesamt 21 Kartenpaaren, die auf der Vorderseite jeweils thematisch (Frage /Antwort) zusammenpassen, aber auf der Rückseite alle gleich aussehen.

**Der Spielablauf**
Zu Spielbeginn mischt ihr alle Karten verdeckt auf eurer Spielfläche, sodass die Rückseite nach oben zeigt. Anschließend ordnet ihr sie vereinzelt an. Die jüngste mitspielende Person beginnt, indem sie zwei Karten aufdeckt, danach geht es im Uhrzeigersinn weiter. Es werden zwei Karten aufgedeckt und die Texte darauf vorgelesen. Passen die beiden Karten zusammen, darf

die Person das Kartenpaar behalten und noch einen Versuch starten. Passen sie nicht zusammen, werden die Karten wieder verdeckt an den gleichen Ort gelegt, wo sie aufgedeckt wurden. Ein gutes Gedächtnis hilft dabei das Spiel zu gewinnen.

**Viel Spaß beim Spielen und viel Erfolg beim Finden der passenden Paare!**

## GEWINNEN ODER VERLIEREN BEI KNOW FAKE

Bei KNOW FAKE spielt ihr so lange, bis alle 21 zusammenpassenden Kartenpaare aufgedeckt sind. Nachdem eine Partie beendet ist, zählen alle Spielenden die Anzahl der Karten auf ihrem Stapel, um zu sehen, wer die meisten Kartenpaare gesammelt hat. Der/die Spielende mit den meisten Kartenpaaren gewinnt das Spiel.

## HINTERGRUNDINFORMATIONEN

Informationskompetenz bezieht sich auf die Fähigkeit, Informationen effektiv zu suchen, zu bewerten, zu nutzen und zu kommunizieren. Um Informationskompetenz zu verstehen und an Heranwachsende weitergeben zu können, ist es wichtig, über Hintergrundinformationen zu verfügen. In diesem Handbuch zum Spiel werden leicht verständliche und relevante Informationen bereitgestellt. Dies ermöglicht es, die Konzepte und Themen des Spiels besser zu verstehen und sie Kindern kompetent zu vermitteln.

Das Handbuch bietet nicht nur wichtige Informationen, sondern auch Anregungen und kleine Übungen für den Alltag, um die Informationskompetenz kontinuierlich zu fördern. Inhalte, die im Kartenspiel in komprimierter und spieladäquater Form präsentiert werden, werden im Handbuch vertiefend behandelt und ausführlich ergänzt. Dies erleichtert es, die vermittelten Themen umfassender zu begreifen und effektiv mit Kindern darüber zu sprechen.

## PROJEKTSEITE: KNOWFAKE.EU

Zusätzlich könnt ihr eine webbasierte App nutzen, die das analoge Kartenspiel präsentiert, ergänzt und erweitert. Diese App ist mehrsprachig (in 6 Sprachen), um eine breite Nutzung zu ermöglichen. Durch die Kombination von analogem Spiel und digitaler Unterstützung wird die Informationskompetenz auf vielfältige Weise gefördert und die Integra-

tion in verschiedene sprachliche und kulturelle Kontexte erleichtert. Durch die Nutzung dieser App wird der nachhaltige Gedanke gefördert, und es entsteht eine Möglichkeit für intergenerationelles Lernen innerhalb der Familie. Wir wünschen allen Nutzer:innen viel Freude beim Spielen und Lernen.

## *ÜBER DAS PHILOSOPHIEREN MIT KINDERN UND JUGENDLICHEN*

"Philosophie und Demokratie rufen uns dazu auf, dass wir uns unseres Urteilsvermögens bedienen, dass wir die für uns beste politische und gesellschaftliche Organisationsform wählen, dass wir selbst unsere Werte erkennen, kurz gesagt, dass wir in umfassender Weise das werden, was jeder von uns ist, nämlich ein freier Mensch." Federico Mayor, Generalsekretär der UNESCO
(Quelle: https://kinderphilosophie-gesellschaft.uni-graz.at/de/philosophieren-mit-kindern-und-jugendlichen/)
Philosophieren geht von grundlegenden und aktuell gesellschaftspolitischen Fragen aus und fördert die Denk- und Persönlichkeitsentwicklung von Kindern und Jugendlichen. Ausgehend von der eigenen Erfahrungswelt, dem Eingehen auf Fragen, dem Kennenlernen unterschiedlicher Perspektiven und der gemeinsamen Reflexion geht es dabei um die Beziehung zu sich selbst, zu anderen Menschen und zur Welt. Es ermutigt, Fragen zu stellen, über das eigene Denken nachzudenken und gemeinsam nach Antworten zu suchen. Es fördert das kritische, kreative und einfühlsame Denken („caringthinking"), Dialog-, Argumentations- und Urteilsfähigkeit. Durch das gemeinsame Nachdenken und den Dialog werden Kinder und Jugendliche auf neue Art einbezogen. Sie entdecken neue Handlungs- und Erfahrungsräume, die mit neuen Kommunikationsformen und veränderten Rollen einhergehen, was auch zur Verbesserung der Basiskompetenzen von Jugendliche beiträgt.
Philosophische Fragen helfen beim Verständnis verschiedener Themen und Ansichten. Zudem werden im Rahmen des Philosophierens eine Vielzahl von Fertigkeiten, Kompetenzen und intellektuellen Fähigkeiten entwickelt, die für eine interkulturelle, kosmopolitische, nachhaltige und digitale Bildung erforderlich sind.

Zusammengefasst ist das Philosophieren, eine Möglichkeit:
1. Kritisches Denken und Urteilsfähigkeit zu fördern
2. Entstehung und Wirkung von FAKE NEWS zu verstehen
3. Neue Handlungs- und Erfahrungsräume kennenzulernen
4. Basiskompetenzen zu verbessern

## WAS SIND FAKE NEWS

Das Wort „Fake" heißt „falsch" oder „gefälscht" und das Wort „News" heißt „Nachrichten" – somit sind Fake News gefälschte Nachrichten. Mit diesen Nachrichten werden mithilfe auffälliger Schlagzeilen falsche Bilder und Aussagen, falsche Informationen, Lügen und Propaganda verbreitet.
Sie erwecken den Eindruck, dass es sich um echte Nachrichten handelt - dies ist problematisch, weil die Meinung der Menschen manipuliert und beeinflusst werden kann und sich dies negativ auf die Gesellschaft auswirken kann. Das Ziel von Fake News ist es, die Menschen zu beeindrucken, damit sich die Nachrichten schnell verbreiten und dadurch Geld verdient werden kann. Kriminelle nutzen Fake News auch für verschiedene Betrugsversuche, wie das Einschleusen von Viren auf den Computer durch das Klicken auf einen Link (sogenanntes Phishing). Man muss also gut aufpassen, um zu erkennen, ob es sich um Fake News handelt oder nicht.

## ARTEN VON FAKE NEWS

Die technischen Möglichkeiten entwickeln sich immer weiter und es ist noch nicht absehbar, welche neuen Arten von Desinformationen und neue Missbrauchspotenziale entstehen werden. Hier nur ein paar Beispiele der Gegenwart:

*Falsche politische Behauptungen*

Beispielsweise verbreitete sich 2016 die falsche Behauptung, dass das FBI Hillary Clinton beschuldigte, private E-Mails gelöscht zu haben. Dies führte zu weitreichenden Spekulationen und politischer Kontroverse. (Quelle: The Washington Post - "The real story behind that fake FBI agent and the plot to frame Hillary Clinton," 2017).

*Clickbait und reißerische Überschriften*

Geschichten mit auffälligen Überschriften, die oft nicht den tatsächlichen Inhalt widerspiegeln, sind weit verbreitet. Ein Beispiel könnte eine übertriebene Gesundheitsbehauptung sein, die Aufmerksamkeit erregen soll, aber nicht auf wissenschaftlichen Fakten basiert. Dies ist besonders während der Corona-Pandemie und den Lockdowns aufgetreten (Quelle: BBC News - "Clickbait and impact: how academia has been hacked," 2017).

*Manipulierte Bilder und Videos*

Im Jahr 2018 gab es Fälle von gefälschten Bildern, die als Beweis für bestimmte Ereignisse präsentiert wurden. Ein Beispiel war ein manipuliertes Bild, das angeblich einen Flüchtlingsskandal darstellen sollte. Die Verbreitung manipulierter Bilder und Videos erschwert die Zuverlässigkeit dieser Medien als verifizierte Quelle (Quelle: The Guardian - "Manipulated images of child abuse scandal in Germany spread on social media," 2018).

*Verschwörungstheorien*
Ein bekanntes Beispiel ist die Verschwörungstheorie um die Mondlandung, bei der behauptet wurde, dass die Apollo-Mondlandung im Jahr 1969 inszeniert wurde. Diese Theorie wurde von verschiedenen Gruppen unterstützt, obwohl sie wissenschaftlich widerlegt ist. Auch dieser Bereich hat stark zugenommen. (Quelle: NASA - "Moon Landing," n.d.)
*Social-Media-Gerüchte*
Nach Naturkatastrophen werden oft Gerüchte verbreitet. Nach dem Hurrikan Katrina im Jahr 2005 verbreitete sich beispielsweise das falsche Gerücht, wilde Tiere aus dem örtlichen Zoo seien entkommen und sorgten für Chaos. Gerade in sozialen Medien geschieht dies oft in rasender Geschwindigkeit (Quelle: Snopes - "Katrina Zoo Animals," 2005).
*Deepfakes*
Mit fortschrittlicher Technologie können Deepfakes erstellt werden, bei denen künstliche Intelligenz verwendet wird, um realistische Videos oder Audiodateien zu erstellen, die Personen Dinge sagen oder tun lassen, die sie tatsächlich nie gesagt oder getan haben (Quelle: Beispiel einer künstlich hergestellten Rede des Bundeskanzlers Olaf Scholz zu einem AfD-Verbotsverfahren, https://afd-verbot.de/).

Diese Beispiele sind historischer Natur, und neue Fälle erfordern eine individuelle Überprüfung. Es ist ratsam, aktuelle Nachrichten von vertrauenswürdigen Nachrichtenquellen zu beziehen und stets die kritisch zu hinterfragen, die über soziale Medien oder andere Kanäle verbreitet werden.

## WARUM IST DESINFORMATION GEFÄHRLICH

Desinformation ist aus verschiedenen Gründen gefährlich:
*Verzerrtes Bild der Realität*
Desinformation führt zu einem verzerrten Bild der Realität. Wenn Menschen falsche oder irreführende Informationen erhalten, können sie Entscheidungen auf der Grundlage falscher Annahmen treffen.
*Beeinflussung der öffentlichen Meinung*
Desinformation kann die öffentliche Meinung beeinflussen und spalten. Indem falsche Informationen verbreitet werden, können Meinungsverschiedenheiten verstärkt und soziale Unruhen geschürt werden.
*Gefährdung der Demokratie*
Durch die Verstärkung von Meinungsverschiedenheiten kann das Vertrauen in öffentliche Institutionen untergraben werden.

*Wirtschaftliche Auswirkungen*
Falsche Informationen können wirtschaftliche Auswirkungen haben, indem sie Investitionsentscheidungen beeinflussen, den Marktzustand verzerren oder das Vertrauen von Verbraucher:innen und Investor:innen erschüttern.
*Gesundheitsrisiken*
Insbesondere im Bereich der Gesundheit kann Desinformation zu ernsthaften Risiken führen. Falsche medizinische Ratschläge oder irreführende Informationen über Gesundheitskrisen können Menschen gefährden und das Vertrauen in medizinische Fachkräfte untergraben.
*Soziale Auswirkungen*
Desinformation kann auch soziale Spannungen verstärken, Vorurteile fördern und das Zusammenleben in Gemeinschaften beeinträchtigen. Durch die Verbreitung von falschen Informationen können bereits bestehende Konflikte verschärft werden.
*Sicherheitsrisiken*
In bestimmten Fällen kann Desinformation auch direkte Sicherheitsrisiken darstellen. Zum Beispiel könnten falsche Informationen über militärische Angelegenheiten oder internationale Beziehungen zu Missverständnissen, Spannungen und Konflikten führen.

Wichtig ist außerdem, dass Desinformationen nicht nur durch Falschmeldungen, sondern vor allem durch die gezielte Verbreitung dieser Informationen, um bestimmte Ziele zu erreichen, problematisch sind. Die Auswirkungen von Desinformation können weitreichend und langfristig sein, weshalb die Bekämpfung und Aufklärung über Desinformation eine wichtige Rolle in der heutigen vernetzten Welt spielt.

## WIE ERKENNE ICH FAKE NEWS

Das Erkennen von Fake News erfordert Aufmerksamkeit, kritisches Denken und die Anwendung bestimmter Strategien. Hier sind einige Tipps, die dir helfen können, Fake News zu erkennen:
*Überprüfe die Quelle*
Schau dir die Quelle der Information an. Sind Nachrichten von dieser Quelle in der Vergangenheit zuverlässig gewesen? Unbekannte oder fragwürdige Quellen sollten mit Vorsicht behandelt werden. Seriöse Nachrichtenagenturen und anerkannte Medienhäuser prüfen ihre Quellen oft mehrfach.
*Prüfe andere Quellen*
Überprüfe die Information bei mehreren vertrauenswürdigen Nachrichtenquellen. Wenn nur eine Quelle die Nachricht verbreitet, könnte es sich um Fake News handeln.

*Achte auf den Schreibstil*
Ein sachlicher und ausgewogener Schreibstil ist oft ein Zeichen für Authentizität. Sensationslüsterne oder einseitige Berichterstattung sollte mit Vorsicht betrachtet werden.
*Überprüfe das Veröffentlichungsdatum*
Manchmal werden alte Nachrichten als aktuelle Ereignisse präsentiert. Überprüfe das Veröffentlichungsdatum, um sicherzustellen, dass die Information aktuell ist. Oft erscheinen ältere aus dem Kontext gerissene Fotos in Berichten. Hier kann z.B. die Google Bildersuche helfen.
*Kontrolliere die Fakten*
Nutze Faktencheck-Seiten, um herauszufinden, ob die Informationen bereits auf ihre Richtigkeit überprüft wurden. Websites wie FactCheck.org oder Correctiv.org bieten oft kostenlose Faktenprüfungen zu weit verbreiteten Behauptungen.
*Hinterfrage Bilder und Videos*
Falsche oder aus dem Zusammenhang gerissene Bilder und Videos können irreführend sein. Verwende Reverse Image Search-Tools (Rückwärtssuche), um die Herkunft von Bildern zu überprüfen.
*Bildung und Medienkompetenz*
Ein kontinuierliches Bewusstsein für neue Entwicklungen im Bereich Fake News ist wichtig. Bildung und Medienkompetenz ermöglichen es, sich auf dem Laufenden zu halten und effektiv gegen Fehlinformationen vorzugehen.

Es ist wichtig zu betonen, dass keine Methode absolute Sicherheit bietet. Die Anwendung mehrerer Überprüfungsansätze zusammen, kombiniert mit einem kritischen Bewusstsein und fortlaufender Informationsbildung, ist der beste Weg, um sich vor Fake News zu schützen.

## WAS TUN WENN ICH AUF EINE FAKE NEWS STOSSE

Wenn du auf Fake News stößt, gibt es mehrere Schritte, die du unternehmen kannst, um sicherzustellen, dass du korrekte Informationen erhältst und dazu beiträgst, die Verbreitung von Falschinformationen einzudämmen:

*Suche nach Faktenprüfungen*

Es gibt Faktentest-Websites, die sich darauf spezialisiert haben, Informationen auf ihre Richtigkeit zu überprüfen. Überprüfe, ob es Faktenprüfungen zu der speziellen Nachricht gibt, die du gefunden hast. Websites wie FactCheck.org oder Correctiv.org können dabei hilfreich sein.

*Nutze verschiedene Quellen*

Erhalte Informationen von verschiedenen Quellen, um eine ausgewogene Perspektive zu erhalten. Vermeide es, dich ausschließlich auf eine Quelle zu verlassen, insbesondere wenn sie als unzuverlässig bekannt ist.

*Kritisches Denken*

Hinterfrage kritisch die Plausibilität der Information. Wenn etwas zu gut klingt, um wahr zu sein, oder extreme Behauptungen aufstellt, kann es sich lohnen, genauer hinzusehen.

*Melde Fake News*

Plattformen und soziale Medien haben oft Mechanismen, um gefälschte Informationen zu melden. Melde die Fake News, damit die Plattformen Maßnahmen ergreifen können.

*Teile keine ungeprüften Informationen*

Vermeide es, ungeprüfte Informationen weiterzuverbreiten. Durch das Teilen von Fake News trägst du zur Verbreitung falscher Informationen bei. Teile stattdessen Fakten und informiere andere darüber, dass die Information möglicherweise nicht korrekt ist.

*Bildung und Sensibilisierung*

Informiere dich über Desinformation und Fake News, um besser in der Lage zu sein, sie zu erkennen. Sensibilisiere auch andere in deinem Umfeld für dieses Thema.

Indem du diese Schritte befolgst, trägst du dazu bei, die Verbreitung von Fake News einzudämmen und förderst eine informierte und auf Fakten basierende öffentliche Diskussion.

## FAKE FOTOS UND DEEP FAKES

Deep Fakes sind täuschend echte gefälschte Bilder oder Videos, die mithilfe von künstlicher Intelligenz erstellt werden und nur schwer von tatsächlichen Aufnahmen zu unterscheiden sind.

Diese Deep Fakes können zum Beispiel dazu genutzt werden, um Politik-

er:innen falsche Aussagen in den Mund zu legen. Wenn dir eine Aussage in einem Video komisch vorkommt, überprüfe diese, indem du zum Beispiel nach Medienberichten von seriösen Pressestellen suchst und ob diese Aussagen bestätigt wurden.

## WIE KANN ICH DEEP FAKES ERKENNEN

*Gibt es das Video nochmal?*
Wenn dir etwas in einem Video merkwürdig vorkommt, kannst du immer zuerst suchen, um zu sehen, ob du das Video ein zweites Mal finden kannst – vielleicht auf einer anderen Website. Wenn nicht, ist es verdächtig. Das gilt für alle Informationen im Internet!
*Details beachten*
Es kommt auf Kleinigkeiten an: achte z.B. darauf, ob die Ohren oder Haare seltsam geformt sind, ob bei der Person die Augenbrauen gleich sind oder mögliche Erkennungsmerkmale wie Sommersprossen, Muttermale etc.
*Übergänge beachten*
Achte auf die Übergänge am Körper – besonders die Übergänge zwischen Gesicht und Hals oder Haaren und Gesicht können bei Deepfakes unscharf sein. Ebenfalls unscharf ist manchmal das Innere vom Mund, wenn eine Person spricht.
*Bildschärfe beachten*
Passen die Qualität und Schärfe des Gesichts zum restlichen Video? Wenn der Körper oder der Hintergrund in einer schlechteren Qualität sind, kann das ein Hinweis dafür sein, dass es sich um einen Deepfake handelt. Ob ein Video eine niedrige Auflösung hat, kannst du daran erkennen, dass das Bild rauscht oder in dunklen Bereichen unscharf wirkt.
*Blinzelt die Person?*
Wenn die Person im Video nicht blinzelt, ist es eindeutig ein Deepfake. Denn wir Menschen haben einen automatischen Reflex, alle paar Sekunden zu blinzeln – das passiert ganz unbewusst.

## WAS BEDEUTET PHISHING

Phishing ist eine Form von Cyberangriff, bei der Betrüger:innen versuchen, sensible Informationen von Personen zu stehlen, indem sie sich als vertrauenswürdige Personen ausgeben. Dies geschieht in der Regel über gefälschte E-Mails, Websites, Nachrichten oder soziale Medien. Der Begriff "Phishing" leitet sich von "fishing" (Angeln) ab, da die Betrüger:innen "Köder" auswerfen, um Opfer zu fangen.

Typischerweise erfolgt ein Phishing-Angriff in folgenden Schritten

1. Der/die Betrüger:in erstellt eine gefälschte Kommunikation, die so aussieht, als käme sie von einer vertrauenswürdigen Quelle. Dies könnte eine gefälschte E-Mail einer Bank, einer Regierungsbehörde, einem sozialen Netzwerk oder einem anderen Online-Dienst sein.
2. Die gefälschte Kommunikation enthält oft einen Vorwand, der das Opfer dazu bringt, auf einen Link zu klicken oder persönliche Informationen preiszugeben. Dies kann beispielsweise eine gefälschte Warnung vor einem Konto- oder Sicherheitsproblem sein.
3. Wenn das Opfer auf den Köder hereinfällt, wird es auf eine gefälschte Website geleitet, die oft täuschend echt aussieht. Hier werden dann persönliche Informationen wie Benutzernamen, Passwörter, Kreditkartennummern oder Sozialversicherungsnummern abgefragt.
4. Die gestohlenen Informationen werden von den Betrüger:innen verwendet, um finanziellen Schaden zu verursachen, Identitätsdiebstahl zu betreiben oder auf andere Weise kriminelle Aktivitäten auszuführen.

Phishing stellt eine erhebliche Gefahr dar, da Betrüger:innen äußerst geschickt darin sind, ihre Opfer zu täuschen. Um sich vor Phishing zu schützen, ist es entscheidend, bei E-Mails oder Nachrichten von unbekannten Absendern besonders vorsichtig zu sein. Vermeide es, persönliche Informationen über nicht verifizierte Kommunikations-kanäle preiszugeben, und überprüfe stets die Authentizität von Websites und Links, bevor du draufklickst oder Informationen eingibst. Darüber hinaus ist es ratsam, Sicherheitssoftware und -tools einzusetzen, um Phishing-Versuche zuverlässig zu erkennen und zu blockieren.

*Anzeichen für Phishing-Versuche*

Phishing zu erkennen, erfordert Aufmerksamkeit und Skepsis gegenüber unerwarteten oder verdächtigen E-Mails, Nachrichten und Websites.
Hier sind einige häufige Anzeichen für Phishing-Versuche:

1. Unbekannter Absender: Sei vorsichtig bei E-Mails oder Nachrichten von unbekannten Absendern oder Adressen, die seltsam erscheinen.
2. Phishing-E-Mail-Anrede: Phishing-E-Mails verwenden oft allgemeine Anreden wie "Sehr geehrter Kunde" anstelle deines Namens oder deiner persönlichen Anrede.
3. Dringlichkeit und Bedrohungen: Phishing-E-Mails versuchen oft, Druck auf dich auszuüben, indem sie behaupten, dass sofortige Maßnahmen erforderlich sind, z.B. dass dein Konto gesperrt wird oder dass du eine Strafe zahlen musst.

4. Ungefragte Anhänge oder Links: Öffne niemals Anhänge oder klicke auf Links in E-Mails oder Nachrichten, es sei denn, du bist dir absolut sicher, dass sie legitim sind.
5. Überprüfe die URL: Bewege den Mauszeiger über Links, um die tatsächliche URL in der Statusleiste des Browsers anzuzeigen. Achte auf verdächtige oder abweichende URLs.
6. Rechtschreibung und Grammatik: Phishing-E-Mails enthalten oft Rechtschreibfehler, Grammatikfehler und seltsame Formulierungen.
7. Fordern nach sensiblen Informationen: Legitime Organisationen werden niemals per E-Mail oder Nachricht nach sensiblen Informationen wie Passwörtern, Kreditkartennummern oder Sozialversicherungsnummern fragen.
8. Überprüfe die Website-Sicherheit: Stelle sicher, dass Websites, auf die du gelangen möchtest, das "https://" in der URL haben und ein Schlosssymbol in der Adressleiste des Browsers anzeigen.
9. Prüfe die Absenderadresse: Überprüfe sorgfältig die E-Mail-Adresse des Absenders. Manchmal sind Phishing-E-Mails von Adressen, die zwar ähnlich aussehen, aber kleine Abweichungen aufweisen, z.B. "support@yourbank.com" vs. "support@yourbankk.com".
10. Sei skeptisch gegenüber zu guten Angeboten: Wenn dir ein Angebot zu gut erscheint, um wahr zu sein, ist es möglicherweise nicht echt.
11. Verwende Sicherheitssoftware: Installiere Antiviren- und Anti-Phishing-Software, die dir helfen kann, Phishing-Versuche zu erkennen und zu blockieren. Verwende Zwei-Faktor-Authentifizierung (2FA): Aktiviere 2FA für wichtige Online-Konten, um zusätzliche Sicherheit zu gewährleisten.
12. Melde verdächtige E-Mails oder Nachrichten: Wenn du eine Phishing-E-Mail erhältst, melde diese an deinen E-Mail-Anbieter oder an die Organisation, die angeblich die E-Mail gesendet hat.
13. Halte deine Software auf dem neuesten Stand: Aktualisiere dein Betriebssystem, deinen Browser und deine Sicherheitssoftware regelmäßig, um Sicherheitslücken zu schließen.

Durch die Einhaltung dieser Ratschläge und die sorgfältige Prüfung von E-Mails und Nachrichten kannst du das Risiko, Opfer von Phishing-Angriffen zu werden, minimieren. Es ist von großer Bedeutung, permanent auf der Hut zu sein, da Phishing-Betrüger:innen fortlaufend neue Taktiken und Kniffe entwickeln, um ihre Opfer zu täuschen.

## WAS SIND SOCIAL BOTS, FILTERBLASEN UND ALGORITHMEN UND WIE BEEINFLUSSEN SIE MEIN ONLINEVERHALTEN

*Social Bots* / Auch bekannt als „Social Media Bots".
Social Bots sind automatisierte Softwareprogramme oder Skripte, die in sozialen Medienplattformen wie X, Facebook und Instagram eingesetzt werden, um menschliches Verhalten zu imitieren und bestimmte Aufgaben zu erfüllen. Diese Bots können automatisch Beiträge erstellen, auf Beiträge reagieren, Follower gewinnen oder Inhalte teilen.
Während einige Social Bots für legitime Zwecke eingesetzt werden, wie das Verbreiten von Nachrichten oder das Beantworten von Kundenanfragen, gibt es auch solche, die für unehrliche Absichten genutzt werden. Diese können dazu dienen, Meinungen zu manipulieren oder Fehlinformationen zu verbreiten.

*Filterblase*
Die Filterblase beschreibt die Tendenz von Online-Plattformen und Algorithmen, Nutzer:innen personalisierte Inhalte und Informationen basierend auf ihren vorherigen Aktivitäten und Interessen zu präsentieren. Dies hat zur Folge, dass Nutzer:innen in einer „Blase" von Informationen gefangen sein können, die ihre bestehenden Ansichten und Meinungen verstärkt, da ihnen selten abweichende Standpunkte oder diverse Perspektiven angezeigt werden.
Diese Einschränkung kann die Vielfalt der Informationen begrenzen, denen Nutzer:innen ausgesetzt sind, und die Bildung von Echokammern begünstigen. In solchen Kammern interagieren Menschen hauptsächlich mit Gleichgesinnten und lehnen alternative Sichtweisen ab.

*Algorithmen*
Algorithmen sind komplexe mathematische Anweisungen und Regeln, die von Computerprogrammen verwendet werden, um Aufgaben oder Berechnungen auszuführen. Im Kontext sozialer Medien und des Internets im Allgemeinen kommen Algorithmen zum Einsatz, um Inhalte auszuwählen und anzuzeigen, die den individuellen Präferenzen und Verhaltensweisen der Nutzer:innen entsprechen.
Diese Algorithmen können Informationen priorisieren, basierend auf Faktoren wie Likes, Klicks, Interaktionen und anderen Datenpunkten, um personalisierte Feeds und Suchergebnisse zu erstellen.

Diese Konzepte können insgesamt das Online-Verhalten und die Verbreitung von Informationen beeinflussen. Sie haben sowohl positive als auch negative Auswirkungen, da sie die Möglichkeit bieten, personalisierte und relevante Inhalte zu erhalten, aber auch das Risiko bergen, die Vielfalt

der Meinungen und Informationen einzuschränken oder Fehlinformationen zu verbreiten. Es ist wichtig, sich der Rolle von Algorithmen und Social Bots bewusst zu sein und kritisch zu hinterfragen, welche Informationen und Meinungen man online ausgesetzt ist.

*Algorithmen, Filterblasen und Social Bots können dein Onlineverhalten auf verschiedene Weisen beeinflussen*

1. Personalisierte Inhalte: Algorithmen analysieren dein Online-Verhalten, einschließlich der von dir besuchten Websites, durchgeführten Suchen und Interaktionen in sozialen Medien. Anhand dieser Daten wählen sie Inhalte aus, die deinen Interessen entsprechen sollen. Dies kann dazu führen, dass du in deinem Online-Feed hauptsächlich Inhalte siehst, die deinen bestehenden Ansichten und Interessen entsprechen, da Algorithmen dazu neigen, ähnliche Inhalte zu priorisieren. Es ist wichtig, sich bewusst zu machen, dass die Personalisierung von Inhalten durch Algorithmen zu einer Filterblase führen kann, in der vielfältige Standpunkte möglicherweise weniger prominent dargestellt werden.
2. Filterblase: Filterblasen können dazu führen, dass du in einer Blase von Informationen gefangen bist, die deine bestehenden Meinungen und Ansichten verstärken. Möglicherweise siehst du weniger diverse oder abweichende Perspektiven. Dies kann dein (Online)-Verhalten beeinflussen, indem es deine Vorlieben und Überzeugungen verstärkt und dazu führt, dass du weniger bereit bist, alternative Sichtweisen zu akzeptieren oder mit Menschen, die unterschiedliche Meinungen vertreten, zu interagieren. Es ist wichtig, sich dieser dynamischen Beeinflussung bewusst zu sein und bewusst nach Möglichkeiten zu suchen, um eine vielfältigere Informationsbasis zu schaffen.
3. Einfluss von Social Bots: Social Bots können deine Interaktionen in sozialen Medien beeinflussen, indem sie Likes, Kommentare und Shares auf Beiträgen generieren oder gefälschte Informationen verbreiten. Wenn du mit gefälschten Konten oder Bots interagierst, könntest du dazu verleitet werden, Fehlinformationen zu verbreiten oder in Diskussionen involviert zu sein, die von Bots oder Trollen manipuliert werden. Es ist wichtig, sich bewusst zu sein, dass solche Bots die Dynamik und Authentizität von Online-Interaktionen beeinträchtigen können, und daher sollte man kritisch darauf achten, mit welchen Konten man interagiert.
4. Informationsüberflutung: Algorithmen können dazu führen, dass du von einer Flut von Informationen und Inhalten überwältigt wirst, da sie versuchen, personalisierte Feeds zu erstellen. Dies kann dein

Online-Verhalten beeinflussen, indem es deine Aufmerksamkeit auf bestimmte Inhalte lenkt und es schwieriger macht, relevante Informationen zu filtern und auszuwählen. Es ist wichtig, sich dieser Dynamik bewusst zu sein und gegebenenfalls Schritte zu unternehmen, um die Kontrolle über den Informationsfluss zu behalten und eine ausgewogene Informationsbasis zu gewährleisten.

Um dein Onlineverhalten positiv zu beeinflussen und sich vor den potenziell negativen Auswirkungen von Algorithmen, Filterblasen und Social Bots zu schützen, ist es wichtig, kritisch zu denken, Informationen zu überprüfen, verschiedene Quellen zu nutzen und sich aktiv darum zu bemühen, diverse Perspektiven zu suchen. Es ist auch hilfreich, sich bewusst zu sein, wie Algorithmen und personalisierte Inhalte funktionieren, und gegebenenfalls deine Einstellungen anzupassen, um eine breitere Palette von Informationen zu erhalten. Durch diese bewusste Herangehensweise kannst du die Kontrolle über dein Onlineerlebnis behalten und sicherstellen, dass du vielfältige und verlässliche Informationen erhältst.

## PROJEKTPARTNER:INNEN

Stiftung Medien-und Onlinesucht
Lüneburg, Deutschland
**www.stiftung-medienundonlinesucht.de**

Lernwerkstatt Europa e.V. Uchebna
RabotiInitsa Evropa Sdruzhenie, Bulgarien
**www.lernwerkstatt-bg.eu**

Educommart Treffpunkt für kreative
Bildung gemeinnützige Partnerschaft, Griechenland
**www.educommart.org**

Systeme in Bewegung e.V. Winsen, Deutschland
**www.systemeinbewegung.de**

Österreichische Gesellschaft für Kinderphilosophie,
Österreich
**https://kinderphilosophie-gesellschaft.uni-graz.at/en/philosophize-with-children-and-teenagers/**

PCO, Slowenien
**www.pco.si/sl/**

knowfake.eu

Kofinanziert von der Europäischen Union

Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen des Autors bzw. der Autoren und spiegeln nicht zwingend die der Europäischen Union oder der Europäischen Exekutivagentur für Bildung und Kultur (EACEA) wider. Weder die Europäische Union noch die EACEA können dafür verantwortlich gemacht werden.