

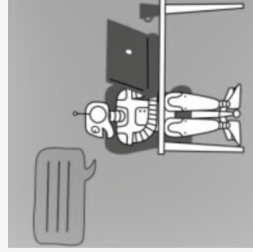
KI Campus-Die Lernplattform für Künstliche Intelligenz (o.D.) https://ki-cmpus.org/ (Abgerufen am 06.07.2023)	03
Seegerer, S. und Lindner, A. (o.D.) https://www.aiunplugged.org/ (Abgerufen am 06.07.2023)	07
Teachable Maschine (o.D.) https://teachablemachine.withgoogle.com/ (Abgerufen am 06.07.2023)	11
Maschine Learning for Kids (o.D.) https://machine-learningforkids.co.uk/#!/welcome (Abgerufen am 06.07.2023)	15
Feminist Tech Principles (o.D.) https://superrr.net/feministtech/ (Abgerufen am 06.07.2023)	19
ccc (o.D.) https://www.ccc.de/de/hackerethik (Abgerufen am 06.07.2023)	23
Data Detox Kit https://datadetoxkit.org/de/families/datadetox-x-youth/ (Abgerufen am 06.07.2023)	27

KI Campus - Die Lernplattform für Künstliche Intelligenz

<https://ki-campus.org/>

Lernangebote entdecken

Schwerpunktthemen



Chatbots und
Sprachassistenten



Data Literacy



KI in der Medizin



KI in der Schule

Alle Themenseiten

Über den KI-Campus

Unsere Vision: Eine KI-kompetente Gesellschaft.

Unsere Mission: Wir stärken KI-Kompetenzen durch kostenlose, digitale Lernangebote für alle.

Der KI-Campus ist die Lernplattform für Künstliche Intelligenz mit kostenlosen Online-Kursen, Videos und Podcasts zur Stärkung von KI- und Datenkompetenzen. Als F&E-Projekt wird der KI-Campus vom Bundesministerium für Bildung und Forschung (BMBF) gefördert. Der Stifterverband, die Charité, das Deutsche Forschungszentrum für Künstliche Intelligenz (DFKI), die Duale Hochschule Baden-Württemberg (DHBW), die FernUniversität in Hagen, das Hasso-Plattner-Institut (HPI), die Humboldt-Universität zu Berlin, das mmb Institut und NEOCOSMO entwickeln den KI-Campus gemeinsam mit zahlreichen Partnern.

Unsere Lernangebote

Die Lernenden stehen für uns im Mittelpunkt. Wir möchten ihnen eine vielfältige Auswahl hochwertiger KI-Lernangebote gebündelt auf unserer Lernplattform zur Verfügung stellen. Dabei gilt: Auch andere haben gute Ideen! Der KI-Campus entwickelt daher einerseits eigene Lernangebote (KI-Campus-Originale) und macht andererseits auch spannende externe Lernangebote sichtbar.

Alle Lernangebote sind kostenlos verfügbar, unsere eigenen Lernangebote auch mit offener Lizenz (CC BY-SA 4.0). Der KI-Campus umfasst sowohl Grundlagen als auch interdisziplinäre Fragestellungen und Vertiefungen einzelner Bereiche der KI (wie z. B. Machine Learning). Darüber hinaus gibt es spezifische Angebote, die gezielt die Bedürfnisse einzelner Berufsfelder bzw. Fachbereiche (wie z. B. KI in der Medizin) abdecken.

Unsere Leitprinzipien

1 Technische Interoperabilität und die Kooperation mit anderen Plattformen und (Landes-)Initiativen gelten als handlungsleitend.

2 Lernende und Lernprozesse stehen im Mittelpunkt der Angebote (Shift from Teaching to Learning).

3 Die didaktischen Konzepte für den KI-Campus sind zukunftsfähig, innovativ und beinhalten soziale Lernformate.

4 Die Plattform basiert auf einer agilen, partizipativen und nutzerorientierten Produktentwicklung.

5 Die Angebote nutzen selbst KI-Verfahren (z. B. Learning Analytics und Empfehlungssysteme) und bieten eine hohe Übersichtlichkeit, Personalisierbarkeit und Adaptivität.

6 Alle erstellten Lernangebote und genutzten Technologien folgen dem Prinzip der Offenheit von Ressourcen und Quellcodes.

AI Unplugged

<https://www.aiunplugged.org/>
Stefan Seegerer and Annabel Lindner

AI UNPLUGGED

Activities and teaching material on artificial intelligence. Download the brochure in German, English, Korean, Spanish, or Portuguese (BR).

- German
- English
- Korean
- Portuguese
- Spanish



Wir ziehen künstlicher Intelligenz den Stecker

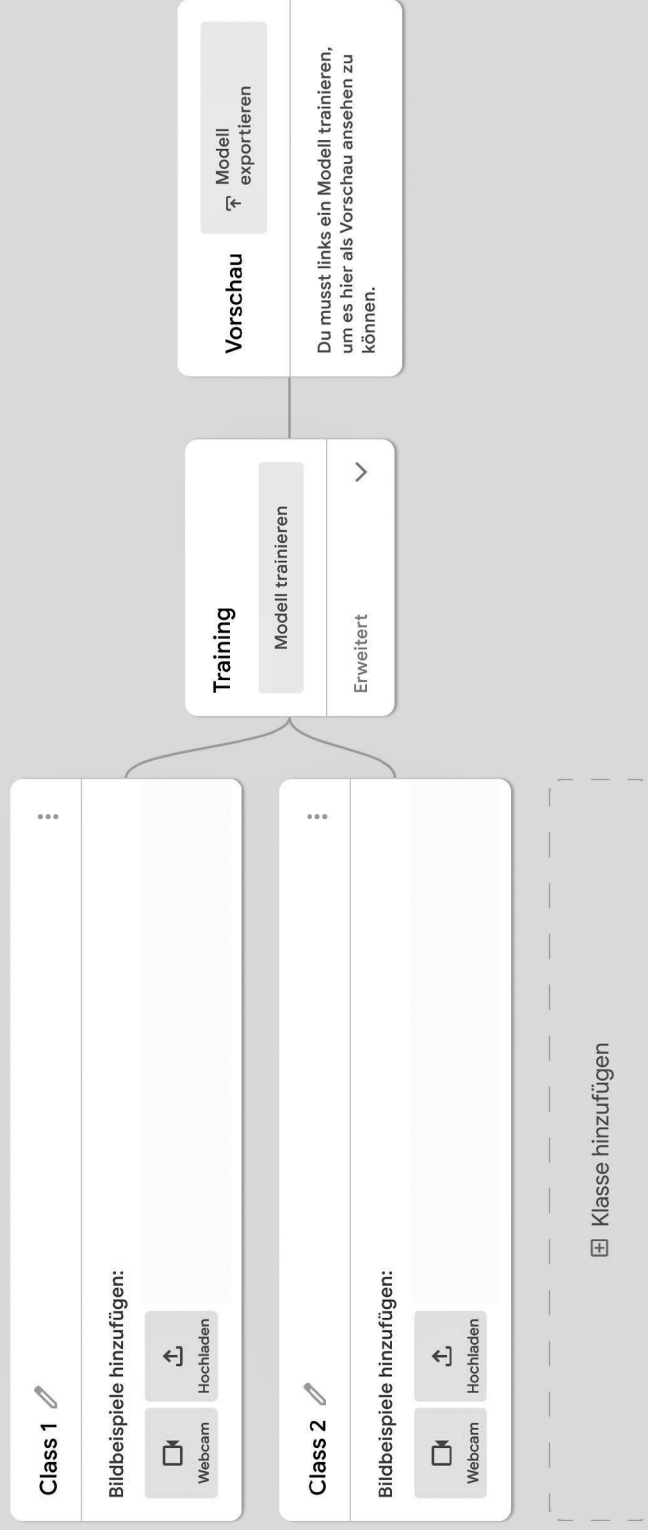
Aktivitäten und Unterrichtsmaterial zu künstlicher Intelligenz ohne Strom

Nicht erst seit der Veröffentlichung der KI- Strategie der Bundesregierung Ende 2018 gewinnt das Thema künstliche Intelligenz (KI, engl. AI für Artificial Intelligence) zunehmend an gesellschaftlicher Bedeutung. Schon heute interagieren wir wie selbstverständlich mit KI- Systemen, etwa wenn wir Sprachassistenten wie Siri oder Alexa nutzen. Dennoch wissen laut Umfragen über 50% der Deutschen bisher nicht, was künstliche Intelligenz ist. Damit das nicht so bleibt, finden Sie hier eine Sammlung verschiedener Unplugged Aktivitäten, die rund um das Thema KI angesiedelt sind. Unplugged Aktivitäten stellen Ansätze bereit, mit denen Lernende jeden Alters Ideen und Konzepte der Informatik enaktiv erfahren können und die explizit auf den Einsatz des Computers verzichten. Die vorliegende Broschüre umfasst fünf Aktivitäten, mit denen Sie Ideen und Konzepte, die dem Thema künstliche Intelligenz zugrunde liegen, zielgruppengerecht vermitteln können. Im Allgemeinen wird KI heute vor allem über maschinelles Lernen realisiert, aber künstliche Intelligenz ist weit mehr als das. Das Thema KI umfasst nicht nur technische Aspekte, sondern wirft auch Fragen mit gesellschaftlicher Relevanz auf. Diese Broschüre zeigt Möglichkeiten, wie die genannten Themen mit Kindern, Jugendlichen und auch Erwachsenen diskutiert werden können. Bei Fragen, Kommentaren oder Anmerkungen zum vorliegenden Material zögern Sie nicht, uns unter hi@aiunplugged.org zu kontaktieren.

Teachable Maschine

<https://teachablemachine.withgoogle.com/>

Teachable Machine



Teachable Machine

Bring einem Computer bei, deine eigenen Bilder, Töne und Posen zu erkennen.

Du kannst schnell und einfach Modelle für maschinelles Lernen für deine Websites und Apps erstellen – ganz ohne Fachwissen oder Programmierkenntnisse. Erste Schritte
Was ist Teachable Machine? Person, die sich die Teachable Machine-Website ansieht und winkt

Teachable Machine ist ein webbasiertes Tool, mit dem sich Modelle für maschinelles Lernen schnell und einfach erstellen lassen und das für alle zugänglich ist. (Hinweis: Die erste Version von Teachable Machine aus dem Jahr 2017 findest du hier.) So funktioniert's Beispielabbildungen von Katzen 1 Zusammentragen

Du kannst Beispiele zusammentragen und sie in Klassen oder Kategorien gruppieren, die der Computer lernen soll. Video: Beispiele zusammentragen Darstellung einer Schaltfläche, die geklickt wird, mit der Aufschrift „Modell trainieren“ 2 Trainieren

Trainiere dein Modell und teste es danach sofort, um herauszufinden, ob es neue Beispiele korrekt klassifiziert. Video: Trainiere dein Modell Darstellung eines Webbrowsers auf einem Computer und einem Mobilgerät mit einem Teachable Machine-Beispielprojekt 3 Exportieren

Exportieren Sie Ihr Modell für Ihre Projekte, Websites, Apps und mehr. Sie können Ihr Modell herunterladen oder online hosten. Video: Exportiere dein Modell Was kann ich zum Trainieren des Modells verwenden?

Teachable Machine ist flexibel – du kannst Dateien verwenden oder Beispiele live erfassen. Das Tool respektiert deine Arbeitsweise. Und du kannst es sogar komplett auf dem Gerät verwenden, ohne dass Webcam- oder Mikrofondaten deinen Computerverlassen.

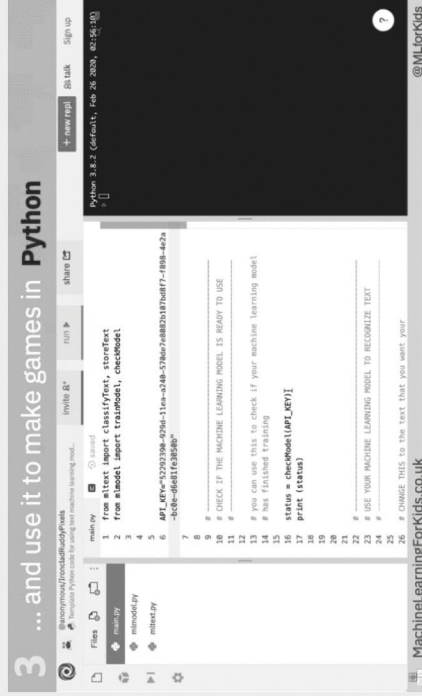
Maschine Learning for Kids

<https://machinelearningforkids.co.uk/#!/welcome>



Machine Learning for Kids

In 6 Sekunden...



In 20 Minuten...



Dieses Tool führt dich zum Thema Künstliche Intelligenz und das Maschinelle Lernen heran.

Es bietet eine einfache Möglichkeit zum Trainieren von Modellen mit Texten, Zahlen und Bildern.

Zur einfachen Herangehensweise bietet das Thema Programmieren die blockbasierte Programmiersprache Scratch (eine weit verbreitete Plattform) verwendet. Learning Modelle können in der Programmierumgebung zum Beispiel ein Spiel programmieren.

Hier erfährst du mehr über das Tool.

Stories

Warum?

Maschinelles Lernen umgibt uns überall. Wir können es in vielen Bereichen nutzen.

Technologie

Das Tool ist vollständig webbasiert und benötigt keine Installation.

Pre-trained models

Machine Learning for Kids bietet eine Vielzahl von vortrainierten Modellen, die für verschiedene Aufgaben wie Textklassifizierung, Sentimentanalyse und Bilderkennung geeignet sind.

Weitere Informationen

Machine Learning for Kids ist ein kostenloses Online-Tool, das es Kindern ermöglicht, Machine Learning zu lernen. Es bietet eine einfache Möglichkeit, Modelle zu trainieren und zu testen, und ist für Kinder ab 10 Jahren geeignet.

Machine Learning for Kids

Was?

Dieses Tool führt über praktische Übungen an das Thema Künstliche Intelligenz, insbesondere das Maschinelle Lernen (Machine Learning) heran.

Es bietet eine einfach zu bedienende Umgebung zum Trainieren von maschinellen Lernmodellen, um Texte, Zahlen sowie Bilder zu klassifizieren.

Zur einfachen Heranführung und Vermittlung an das Thema Programmieren wird unter anderem die blockbasierte Programmiersprache Scratch (eine weit verbreitete Programmier-Lern-Plattform) verwendet. Die trainierten Machine Learning Modelle können in der Programmierumgebung verwendet werden, um zum Beispiel ein Spiel zu programmieren.

Warum?

Maschinelles Lernen umgibt uns überall. Wir alle benutzen täglich maschinelle Lernsysteme - wie Spam-Filter, Empfehlungssysteme, Sprachübersetzungsdienste, Chatbots und digitale Assistenten, Suchmaschinen sowie Systeme zur Betrugserkennung.

In nicht allzu ferner Zukunft werden selbstfahrende Autos ebenso normal sein wie Systeme, die Ärzte dabei unterstützen, Krankheiten zu erkennen und zu behandeln.

Es ist wichtig, dass jeder, und vor allem Kinder und junge Erwachsene, wissen, wie unsere Welt funktioniert. Der beste Weg, um die Möglichkeiten und Auswirkungen von Künstlicher Intelligenz zu verstehen, ist, die Technologie selbst anzuwenden und eigene Applikationen zu bauen.

Technologie

Das Tool ist vollständig webbasiert und erfordert keine Installation und kein kompliziertes Setup.

Es wurde für den Einsatz im Unterricht an Schulen, für AG's oder Projektage entwickelt. Der Lehrkraft wird eine Administrator-Seite bereitgestellt, um Accounts für die SchülerInnen anzulegen und den Zugang der SchülerInnen verwalten zu können.

Das Tool wurde von Dale Lane erstellt und nutzt APIs von der IBM Watson Developer Cloud .

Feminist Tech Principles

<https://superrr.net/feministtech/>

Feminist Tech principles

The Feminist Tech principles are a set of guidelines for tech policy-making and technology creation.

They are intended as responsive work-in-progress that reflect the evolving nature of our digital world. The principles were drafted in a collaborative process between the team at SUPERRR Lab and a group of activists, policy-makers, writers, designers, technologists, researchers, and educators, that advocate for digital rights and the rights of marginalized groups. Use the QR code to read more about the principles and the contributors, and to download the card deck.



feminist.tech

1. Climate action and social equity are interlinked.

Tech solutions are not neutral: what they optimise must be interrogated. The current system follows a political and economic model that privatises gains in the hands of a few and socialises harms on populations and the planet. To optimise for a feminist future centered around equality and sustainability, it is crucial to see and understand the links between climate action, historical and contemporary colonial structures and social equity.

2. Equity and visibility along the supply chain.

Today's digital technologies rely upon the extraction of non-renewable resources and labour which numerous processes render invisible and often amounts to modern slavery. This exacerbates social inequalities and global North-South injustice. Supply chains as well as the inequality footprint of our technology must be made visible. Exploitative working conditions must end and profits must be shared equitably along the chain of production.

3. Sustain, maintain and share.

Innovation should not come at any cost. We should move away from short-term innovation cycles, towards longevity and openness. This is paramount to creating tech that functions within planetary boundaries. The appreciation of, and value accorded to, maintenance and interoperability must increase.

4. Healing and empowerment over profit maximisation and tech-solutionism.

Algorithmic decision-making systems and facial recognition tools used by governments and industries currently obscure and reinforce existing injustices. Instead of creating safer spaces for discourse and exchange, social media networks capitalise on trauma and hate speech. More broadly, digital technologies surveil, control and radicalise their users. To ensure collective and individual well-being and flourishing, technologies must center around the needs of communities rather than prioritising profit maximisation above all.

5. Accessibility, equitable participation and representation.

Accessibility is not a «nice to have». It is a human right. Marginalised groups must be active stakeholders at all stages of design and policy processes. Building with marginalized people, not for them.

6. No to progress at any cost.

Some technologies are simply too harmful to be deployed in the first place. Red lines on harmful technological practices must be set and more research must be conducted on the potential harm of emerging technologies on communities at the margins. Processes for feedback, evaluation and veto must be established.

7. Name, acknowledge and share.

The work, concepts and ideas that new digital technology is being built upon must be credited. We must demystify technology's founding narratives. «The first unavoidable step into a feminist internet is the act of naming all creators, inventors that nurture the infrastructure and the code.»
— Valentina Pelizzer Hvale

8. Publicly-financed software should be open source.

In this way, anyone can build upon public investment and create something new. Public funders have to value maintenance and care for critical systems at least as much as innovation.

9. Creating safer spaces online is an ongoing relational negotiation process.

In order to create safer spaces online, technology must be designed to counter hate speech, dis- and misinformation. Effective, trauma-informed mechanisms to report and analyse abuse or harmful flaws in tech must become mandatory. Creating online spaces for collaboration and exchange where people have support, and feel empowered to speak freely is an ongoing and relational negotiation process.

10. Design for informed consent.

Asking for and obtaining consent respects a person's right to autonomy and agency. For consent to be valid, it must be voluntary, informed and reversible. However, individuals should not be burdened with every decision. We also need strong policies that protect the privacy of individuals and groups.

11. Your (digital) identity is yours to define.

Our identities are not static and this must be reflected in the digital realm. We need mechanisms that allow for digital identities to be fluid, to change over time, embrace non-binary concepts and defy established categorisations. Self-determination must be at the core of digital identity.

12. Privacy by default, not surveillance.

Self-governance of data is fundamental to the equitable functioning of the internet. We must all have the agency to determine how, for what purposes, when and for how long our data is used, shared and saved.



Created by SUPERRR Lab in cooperation with Cami Rincón, Carolina Reis, Chenai Chair, Chinmayi SK, Felix Reda, Francesca Schmidt, Helene v. Schwichow, Kat Waters, Katrin Fritsch, Laurence Meyer, Maya Ober, Michelle Thorne, Nakeema Stefflbauer, Naomi Alexander Naidoo, Neema Githere, Nighat Dad, Raziye Buse Çetin, Safa Ghnaim, Sarah Devi Chander, Vanessa A. Opoku, and Victoria Kure-Wu. This project is supported by the Robert Bosch Foundation under their Support Program «Reducing Inequalities Through Intersectional Practice». Thank you to Anna-Dorothea Grass, Rana Zin-cir Celal and Pramada Menon for guidance and support.

This project is a set of work-in-progress guidelines for feminist tech policy-making and technology creation. The guidelines consist of 12 principles for feminist technology, which range from the intrapersonal to the global, and which are accompanied by a card deck and six essays envisioning more just technological futures.

This project is created by Superrr Lab and contributors of the Superrr Community. Superrr Lab develops visions and projects with the goal of creating more equitable futures. We research technologies, build networks and shape new narratives. Superrr is playful, visionary and feminist.

»We are committed to interrogating the capitalist logic that drives technology towards further privatization, profit, and corporate control. We work to create alternative forms of economic power that are grounded in principles of cooperation, solidarity, commons, environmental sustainability and openness.« — Feminist Internet

Contemporary digitisation narratives are economic in nature and serve the interests of corporations over the needs of societies and minorities. By contrast, feminist tech policy takes a holistic view of digitisation, to look at it in terms of intersectional patterns of discrimination. By taking a feminist approach we are able to think and see beyond existing stories and structures. We question current innovation narratives and examine the value of maintenance, accessibility, openness and care for the digital societies of the future.

By building up this kind of open digital knowledge archive on feministtech.org as well as the Feminist Tech Principles card deck, we aim to facilitate a long-term exchange on the topics of intersectionality and digitisation. The principles, observations, good practice examples and future visions are intended to guide government institutions, organisations, companies and individuals to envision, plan, and make decisions related to technology. We intend for this project to broaden current discourse and highlight the changes that are needed to ensure that all groups in society benefit equitably from digitisation.

Who are the principles for? In what contexts can they be used?

The principles are made for governments, civil society organisations and companies, as well as activists, designers, policymakers, technology creators and other individuals who aim to create more just and equitable technologies, designs and/or tech policies – or who want to discuss and critically assess their practice through these principles.

We hope they help make the world of the digital commons look a little more like this:

»A flourishing digital public space should be welcoming and safe for diverse publics, help us understand and make sense of the world, connect people near and far across

Hackerethik

<https://www.ccc.de/de/hackerethik>

Die ethischen Grundsätze des Hackens – Motivation und Grenzen:

Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein. Alle Informationen müssen frei sein. Mißtraue Autoritäten – fördere Dezentralisierung. Beurteile einen Hacker nach dem, was er tut, und nicht nach üblichen Kriterien wie Aussehen, Alter, Herkunft, Spezies, Geschlecht oder gesellschaftliche Stellung. Man kann mit einem Computer Kunst und Schönheit schaffen. Computer können dein Leben zum Besseren verändern. Mülle nicht in den Daten anderer Leute. Öffentliche Daten nützen, private Daten schützen.

Die Hackerethik ist nur bedingt einheitlich definiert. Es gibt eine ursprüngliche Version aus dem Buch „Hackers“ von Steven Levy (ISBN 0-440-13405-6). Unstrittig ist insofern, daß die ursprüngliche Version aus dem MIT-Eisenbahnerclub (Tech Model Railroad Club) kommt und demnach aus einer Zeit stammt, in der sich verhältnismäßig viele Leute wenige Computer teilen mußten und entsprechende Überlegungen zum Umgang miteinander und der Materie sinnvoll waren.

Die letzten beiden Punkte sind Ergänzungen des CCC aus den 1980er Jahren. Nachdem einige mehr oder weniger Durchgeknallte aus der Hackerszene bzw. aus dem Umfeld auf die Idee kamen, ihr „Hack-Knowhow“ dem KGB anzubieten, gab es heftige Diskussionen, weil Geheimdienste konträr zur Förderung freier Information stehen. Aber auch Eingriffe in die Systeme fremder Betreiber wurden zunehmend als kontraproduktiv erkannt.

Um den Schutz der Privatsphäre des Einzelnen mit der Förderung von Informationsfreiheit für Informationen, welche die Öffentlichkeit betreffen, zu verbinden, wurde schließlich der bislang letzte Punkt angefügt.

Die Hackerethik befindet sich – genauso wie die übrige Welt – in ständiger Weiterentwicklung und Diskussion. Dabei dürfen natürlich alle mitdenken, die sich grundsätzlich mit dieser Hackerethik anfreunden können. Bis dahin stehen die o. g. Regeln als Diskussionsgrundlage und Orientierung.

Verbesserungsvorschläge und Eingaben dazu gerne jederzeit an den Chaos Computer Club.

Data Detox Kit von Tactical Tech

<https://datadetoxkit.org/de/families/datadetox-x-youth/>

Das Data Detox Kit ist Dein Reiseführer für die Welt Deiner persönlichen Daten. Wie sieht diese Welt aus? Warum wird darüber so viel gesprochen? Und wie bekommst Du Deine Daten in den Griff?

DIGITALE
PRIVATSPHÄRE



BEKOMME DEINE DATEN IN DEN GRIFF

...weil sie Dir davonlaufen

Es scheint doch keine große Sache zu sein, wenn Firmen gewisse Dinge über Dich wissen. Wen kümmert es schon, ob Du ein Fan von Baby Yoda bist, oder ob Du mehr Katzenvideos als andere Leute anschaust?

Das Problem ist, was mit Deinen Daten passiert. Im Laufe der Zeit nimmt Dein Online-Verhalten eine eigene Identität an mit Deinen Gewohnheiten, Vorlieben, Dingen, die Du magst oder nicht magst und Deinen Geheimnissen. Es kann sich selbstständig und in die Hände von Datenhändlern gelangen – Firmen, die mit diesen Informationen Geld verdienen.

Lass uns loslegen!

Ein Produkt von

**TACTICAL
1980**

datadetoxkit.org
#datadetox

1

BRING DEINE APPS AUF ZACK

Apps nutzen wertvolle Akkulaufzeit und Gigabytes an Speicher, aber sie können auch Daten sammeln – selbst dann, wenn Du die Apps gar nicht nutzt. Ein paar davon loszuwerden, ist ein schneller Weg, um Deine Datenspuren zu reduzieren und dazu noch noch Akkulaufzeit und Speicherplatz zu sparen! Bonus!

Probiere diese Schritte und finde heraus, ob Du ein App-Hamsterer bist:

Hey!
Wenn Du kein eigenes Smartphone hast, mach es mit jemandem zusammen.

Rate zuerst einmal, wie viele Apps Du auf dem Handy hast (nicht gucken!)

Und jetzt zähle, wie viele Du tatsächlich hast:

Frage Dich, wie viele dieser Apps Du wirklich brauchst. Gehe dann alle Apps einmal durch und lösche die, die diesen Test nicht bestehen. So geht's:

Hey!
Wenn Du Dir unsicher bist, ob Du eine App löschen möchtest, frage Dich: Kann ich das auch im Browser machen?

Android: Einstellungen → Apps → Wähle die App aus, die Du deinstallieren möchtest → Deinstallieren

iPhone: Drück lange auf die App, die Du deinstallieren möchtest, und wähle dann „App Löschen“.

2

WEIß DEIN HANDY, WO DU WARST?

Einige der wertvollsten Deiner privaten Daten sind Deine Standortdaten. Wo Du Dich rumtreibst, kann viel über Dich aussagen – von etwas sehr Offensichtlichem wie Deinem Alter bis zu viel Privaterem, zum Beispiel wer Dein bester Freund / Deine beste Freundin ist. Deine Apps verfolgen möglicherweise laufend und ohne Dein Wissen Deine Aktivitäten. Und das kann mehr über Dich verraten, als Du möchtest.

Überlege für jede App, ob sie Zugang zu Deinen Standortdaten braucht. Nutze die folgende Skala:

Diese App muss wissen, wo ich mich befinde:

Nie
Manchmal
Immer

Hey!
Manche Apps müssen manchmal wissen, wo Du bist, wie eine Karten- oder Wetter-App.

Schreibe auf, welche Deine drei beliebtesten Apps sind:

APP 1:
APP 2:
APP 3:

Sehen wir uns doch mal Deine Lieblings-Apps an.

Prüfe jetzt die Einstellungen dieser Apps, um ihre Standortberechtigungen einzurichten und diejenigen abzuschalten, die nicht wissen müssen, wo Du Dich aufhältst, um zu funktionieren:

Android:
Einstellungen → Apps → Verwalte den Standortzugriff der einzelnen Apps

iPhone:
Einstellungen → Datenschutz → Ortungsdienste → Verwalte den Standortzugriff der einzelnen Apps

Bonus :

Jetzt, wo Du die „freie Fahrt für alle“ mal etwas eingeschränkt hast, durchsuche auch die Zugangsberechtigungen der Apps für weitere Funktionen wie Kontakte, Kamera und Mikrofon.

Umdrehen für mehr!

WER BIST DU WENN MAN GOOGLE FRAGT?

Wenn Du Gratisanbieter wie Google nutzt, gibst Du ihnen laufend Deine Daten. Google kann diese Daten nutzen, um ein Profil über Dich zu erstellen, das Werbefirmen helfen kann zu verstehen, was Du magst. Aber diese Profile sind oft anders, als man denkt.



Sehen wir doch mal, was sie denken. Markiere zuerst alle Google-Produkte, die Du nutzt:

Suchmaschine	Gmail	YouTube	Maps	Classroom	Drive	Hangout	Family link
--------------	-------	---------	------	-----------	-------	---------	-------------

Gehe zu myactivity.google.com → Logge Dich ein → Andere Google-Aktivitäten → Einstellungen für Werbung →

Jetzt schau nach, wie Google Dich sieht:

Bonus :)

Deaktiviere unter myaccount.google.com/activitycontrols auch das Speichern Deiner Web-Aktivitäten, des Standort- und YouTube Verlaufs.

Haben Dich einige dieser Ergebnisse überrascht? Vielleicht haben sie sich mit Deinem Alter vertan, oder sie behaupten, Du liebst es zu backen, obwohl Du noch nie im Leben auch nur einen Kuchen gebacken hast? Wenn Du lieber nicht möchtest, dass sie ein Profil von Dir für Anzeigen erstellen, **kannst Du diese Funktion oben auf dieser Seite abstellen.**

WENN TEILEN ZUM AUSPLAUDERN WIRD

Wir wissen alle, wie cool es ist, sich auf Social-Media-Plattformen mit Freunden zu connecten. Aber es ist auch der Ort, wo wir besonders viele Informationen von uns preisgeben – auch an Unbekannte, oder die Firmen, die diese Plattformen betreiben.

Möchtest Du sicher sein, dass Du Dich nur Deinen Freunden und Followern mitteilst, aber nicht Deinen Apps? Nimm eine der folgenden Apps und versuch mal, wie weit Du kommst:

Instagram
Profil → Einstellungen:
Konto → Kontaktsynchronisierung → Kontaktsynchronisierung deaktivieren
Konto → Verknüpfte Konten → Verknüpfung entfernen

Snapchat
Profil → Einstellungen:
Mehr Möglichkeiten → Verwalten → Werbepräferenzen → Alle deaktivieren
Mehr Möglichkeiten → Interessen und Lifestyle → Deaktiviere alle Interessen
Mehr Möglichkeiten → Karten → Kartennutzung abschalten

Hey!

Wenn Du Dich bei neuen Apps registrierst, mach es nicht mit Deinen anderen Social Media Accounts. Weil das den Firmen erlaubt, Deine Infos untereinander zu teilen. Nutze stattdessen Deine E-Mail-Adresse dafür.

Bonus :)

Nutzt Du Gaming-Plattformen wie Fortnite oder Minecraft? Verstärke auch gleich dort Deine Einstellungen zur Privatsphäre.

Mein Online-Privatleben

Gratuliere! Du hast es zum Ende des Detox zur **Online-Privatsphäre** geschafft. Lehn Dich zurück, entspann Dich und hake alles ab, was Du erreicht hast:

- ☐ Ich habe meine Apps auf Zack gebracht und meine Datenmengen reduziert.
- ☐ Ich habe meine Standort-Daten Spuren verringert.
- ☐ Ich habe erfahren, wie Google mich sieht.
- ☐ Ich habe aufgehört, zu viel von mir in den sozialen Medien zu teilen.

Auch wenn Du nur eines dieser Dinge getan hast, hast Du bereits Fortschritte mit Deiner Online-Privatsphäre gemacht. Wir leben in einer von Daten geprägten Welt, was bedeutet, wir müssen diese Fertigkeiten üben, bis wir sie ohne groß nachzudenken können.

Erzähle es weiter! Ermuntere Deine Freunde und Familie, auch ein Daten-Detox zu machen.

ALS
NÄCHSTES:
DIGITALE
SICHERHEIT

DATA
DETOX
KIT

DIGITALE
SICHERHEIT
I

SCHNAPP DIR DIE SICHERHEIT

...mit soliden
Passwörtern

Wenn das Internet nur dazu da wäre, Bilder von Hunderten in Dinosaurierkostümen zu teilen, dann bräuchtest du keine großen Sicherheitsvorkehrungen. Aber das Internet ist ein Ort, an dem du viel Zeit verbringst, darum solltest du deine Accounts sicher machen.

So kannst du das überprüfen: Nutzt du den Namen Deines Haustiers als Passwort? Heutzutage gibt es keine Ausrede mehr, ein schwaches Passwort zu verwenden. Da Hacker besser geworden sind im Knacken von Accounts, musst du besser werden, um sie draußen zu halten.

In diesem Daten-Detox wirst du den besten Weg kennenlernen, um ein starkes und sicheres Passwort zu erstellen und Fremde von Deinem Account fernzuhalten.

Lass uns loslegen!

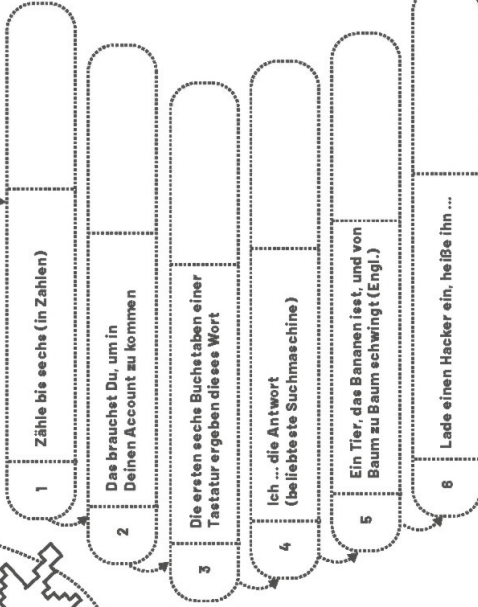
Ein Produkt von

TACTICAL
1966
datadetoxkit.org
 #datadetox

1

SO FREUNDST DU DICH MIT EINEM HACKER AN

Es gibt einen ganz leichten Weg, sich mit Hackern anzufreunden: Erstelle ein ganz einfaches Passwort, damit sie sich willkommen fühlen.



Bonus :)

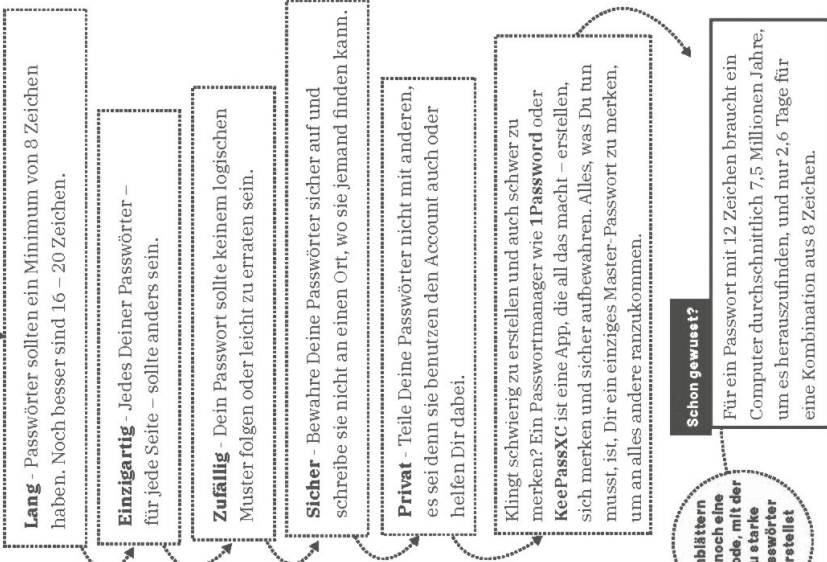
Prüfe, ob dein Passwort schon „pwned“ ist. Auf haveibeenpwned.com kannst du sehen, ob dein E-Mail-Konto schon mal von einem Datenklau betroffen war. Wenn dem so ist, wäre das doch ein guter Zeitpunkt, um deine Passwörter sicherer zu machen!

2

TSCHÜSS „123456“

Es ist einfach, spitzenmäßige Passwörter zu kreieren. Du musst nur ein paar einfache Regeln

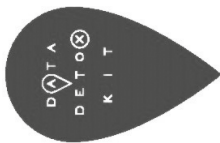
So sollten Deine Passwörter sein:



Schon gewusst?

Für ein Passwort mit 12 Zeichen braucht ein Computer durchschnittlich 7,5 Millionen Jahre, um es herauszufinden, und nur 2,6 Tage für eine Kombination aus 8 Zeichen.

Umblättern für noch eine Methode, mit der Du starke Passwörter erstellst



DIGITALE
SICHERHEIT
II

F@ULTIER HUEPFT WILDL*Y*! IMsuperMARKT

Warum reden wir plötzlich über
Faultiere? Dieser Abschnitt handelt
von Passwortsätzen oder Passphrasen
– einer zufälligen Reihenfolge von
eigenartigen Wörtern, die so seltsam
ist, dass man sie sich leichter merken
kann als ein herkömmliches Passwort,
die aber um einiges schwieriger für
einen Eindringling zu erraten ist.

Versuch es selber mal. Schreibe fünf zufällige Wörter auf, die einen
eigenartigen Satz ergeben, so wie im Titel dieses Abschnitts:

1	2	3	4	5

Und jetzt mache ein paar der Buchstaben zu GROSSBUCHSTABEN und füge ein
paar Satzzeichen (!?)-,-) und Zahlen hinzu und schreibe sie noch mal auf:

1	2	3	4	5

Gratuliere, Du hast gerade einen
Passwortsatz kreiert!

Die meisten von uns tun sich schwer
damit, sich willkürliche Kombinationen
von Zahlen, Zeichen und Buchstaben
(Passwörter) zu merken, aber wir finden
es viel einfacher, uns Sätze und Wörter
(Passphrasen) für ein Login zu merken.

Hey!

Denk dran, dass Du Deine
Passwörter nirgends aufschrei-
ben solltest, wo sie jemand sehen
kann. Das bedeutet, Du kannst
den Passwortsatz von oben nicht
benutzen. Aber jetzt, wo Du weißt,
wie es geht, kannst Du selber
einen an einem Ort erfinden, wo
niemand es mitbekommt und
Du die Spuren davon gut
vernichten kannst.

DIGITALES SCHLOSS MIT DOPPELVERRIEGELUNG

Wenn Du den Schritten oben gefolgt
bist, solltest Du es jetzt für
jemanden, der in Deinen Account
einbrechen möchte, ziemlich
schwierig gemacht haben. Aber
selbst superschwierige Passwörter
sind nicht unknackbar.

Zwei-Faktor-Authentifizierung (2FA) oder
Multi-Faktor-Authentifizierung (MFA) ist eine
zusätzliche Sicherheitsebene, um zu verhindern,
dass jemand in Deinen Account eindringt, selbst
wenn er Dein Passwort weiß – stell es Dir wie ein
zweites Schloss an der Tür vor.

Die meisten Apps haben diese
Funktion. Versuche auf einem Deiner
Accounts eine einzurichten:

Instagram:
Einstellungen → Sicherheit →
Zweistufige Authentifizierung →
Leg los

Snapchat:
Einstellungen →
2-Faktoren-Bestätigung

Google:
Melde Dich an auf
<https://myaccount.google.com>
Sicherheit → Bestätigung in
zwei Schritten

Hey!

Wenn du auswählen
musst, nimm Deine
E-Mail-Adresse oder ein
Einmal-Passwort („OTP“) statt
Deiner Telefonnummer. Auf
diese Weise kommst Du immer
noch in Deinen Account, wenn
Dir Dein Telefon ins Klo
gefallen ist.

Meine Digitale Sicherheit

Gratuliere! Du hast es zum Ende des Detox
zur digitalen Sicherheit geschafft. Lehn
Dich zurück, entspann Dich und hake alles
ab, was Du erreicht hast:

- ☐ Ich weiß, welche Passwörter ich nicht
benutzen sollte.
- ☐ Ich kenne die fünf grundlegenden
Prinzipien eines starken und sicheren
Passworts.
- ☐ Ich habe meinen eigenen,
einzigartigen Passwortsatz (oder
Passphrase) erstellt.
- ☐ Ich habe für mindestens einen
Account eine Zwei-Faktor-
Authentifizierung eingerichtet.

Jetzt, wo Du Dich gegen Hacker geschützt
hast, **teile dieses Wissen mit Familie und
Freunden**. Jeder, der mit Dir verbunden ist,
wird durch Deine Bemühungen ein
bisschen sicherer.

ALS NÄCHSTES:
DIGITALE
ZUFRIEDENHEIT

DIGITALE ZUFRIEDENHEIT 1

SO ÜBERLEBST DU EINE TRENNUNG

...von Deinem Handy

Passiert es Dir manchmal, dass Du einfach auf den Bildschirm Deines Handys schaust und gar nicht weißt, wieso? Oder Du wolltest nur mal kurz etwas nachschauen und BAMM! – du hast eine Stunde auf Instagram herumgescrollt?

Unsere Beziehung zur Technologie nimmt uns sehr in Anspruch, besonders mit all dem Summen, Pingen, den Lichtern und Alarmen, die wir bekommen.

Manchmal weiß man nicht mehr, wieso wir es überhaupt mögen, ein Smartphone zu haben.

Wenn Du diesem Daten-Detox folgst, **wirst Du lernen, eine bessere Beziehung zu Deinem Gerät zu haben.**

Lass uns loslegen!

Ein Produkt von

TACTICAL

datadetoxkit.org
#datadetox

1

DENK AN DIE GUTEN ZEITEN!

Uns kann eine Hass-Liebe mit unserer Technologie verbinden. Das, was wir daran lieben, wie zum Beispiel Freundschaften finden und pflegen, kann auch das sein, was wir daran hassen, wie Gefühle der Einsamkeit und FOMO.

Was machst Du am meisten im Internet (Spielen, mit Freunden chatten, Filme schauen)? Schreibe es unten in das mittlere Rechteck. Schreibe dann rings herum, was Du daran magst und was nicht.

DAS MAG ICH:
DIE MEISTE ZEIT IM INTERNET VERBRINGE ICH MIT:
DAS MAG ICH NICHT:

Bonus :)

Denkst Du, Du kannst einige der Dinge auf der Liste „Das mag ich nicht“ am Ende dieses Daten-Detox streichen? Denke darüber nach, wie Du diese Dinge ins Lot bringen kannst, um mehr von Deinem Gerät zu haben.

2

VERGISS NICHT, ES IST NICHT DEINE SCHULD!

Es kommt Dir vielleicht so vor, als wollten alle Dir und all Deinen Freunden immer nur sagen, ihr sollt das Handy weglegen. Aber hast Du Dir schon mal überlegt, dass es vielleicht gar nicht Deine Schuld ist, dass Du so vernarrt in Dein Handy bist? Es ist für uns schon ganz natürlich zu wünschen, liken, scrollen und zu teilen. Aber gewisse Designtricks sind häufig schuld daran, dass wir so viel Zeit online verbringen.

Die **Tipplase** – die kleinen Pünktchen, die zeigen, dass jemand gerade tippt. Oh, weich Spannung!

Der **neue Trend** – ein neuer Tanz, ein Meme oder Stil, der Deinen Feed überrollt

Das **Autoplay** – Du brauchst nichts zu klicken, das nächste Video kommt in 3, 2, 1 ...

Das **unendliche Wischen** – neue Inhalte, die einfach kommen

Die **Beutekiste** – Gaming-Preise oder Währung, die Du für mehr Items eintauschen kannst

Der **Like-Button** – einen Daumen hoch oder ein Herz für tollen Content

Die **Erfolgsserie** – die Belohnung für Deine Treue. Verlier sie und Du mußt noch mal von vorne anfangen.

Ziehen zum Aktualisieren – die Spannung bis der neue Inhalt lädt

Schon gewusst?

Durchschnittlich tippt, klickt und wischt jeder über 2.600-mal am Tag. Wie häufig machst Du es?

Mehr auf der nächsten Seite!

1. YouTube
2. TikTok
3. Snapchat
4. Fortnite
5. Instagram
6. Netflix
7. Spotify
8. WhatsApp

Hey!

Es kann sein, dass manche Designtricks bei mehreren Apps vorkommen.

Versuche die Designtricks (links) mit den korrekten Apps (rechts) zu verbinden:

DIGITALE
ZUFRIEDENHEIT
II

3

HALTE ABSTAND

Wenn also das Design dafür entwickelt ist, Dich in seinen Bann zu ziehen, was kannst Du dagegen tun? Das Gute ist, dass die meisten Plattformen es einfacher machen, diese Designtricks zu überwinden. Entweder mit eingebauten Erinnerungen – wie bei „Du bist auf dem neuesten Stand“ bei Instagram – oder mit einer einfachen Änderung der Einstellungen.

Hier sind einige, die Du vornehmen kannst:

WhatsApp

Einstellungen → Account → Datenschutz → Lesebestätigung → Deaktivieren

YouTube

Autoplay → Deaktivieren

Instagram

Einstellungen → Deine Aktivität → Benachrichtigungseinstellungen → Alle anhalten

TikTok

Privatsphäre und Einstellungen → Digital Wellbeing → Bildschirmzeit-Management → Aktivieren und Zeit festlegen

Vergiss nicht, dass diese Einstellungen ja nicht für immer sein müssen. Der Trick ist es, die erste Hürde zu überwinden, wenn Du den Drang hast, dauernd auf Dein Handy zu schauen. Wenn Du sie dann mal wieder aktivierst, wirst Du merken, wie nervig sie eigentlich sind.

Bonus :)

Fällt Dir noch ein anderer Life-Hack ein, um nicht mehr so oft auf Dein Handy zu schauen?

LIFEHACK

VERSUCH'S NOCH MAL

4

Wenn Du willst, dass Deine Beziehung mit Deinem Handy funktioniert, muss es nach Deinen Regeln laufen. Geh zurück zur ersten Übung, wo Du aufgeschrieben hast, was Dir an der Technologie gefällt. Es kann richtig gut sein, oder? Der Trick dabei ist, sicherzustellen, dass Du online wirklich Spaß hast.

Suche Dir noch ein paar Reserve-Strategien aus, damit es für Dich klappt. Hier ein paar Vorschläge, die Du versuchen könntest:

Lege das Telefon mit dem Bildschirm nach unten, oder noch besser: außer Sicht.

Stelle es zeitweise auf Stumm oder stelle die Benachrichtigungen ab.

Wenn Leute von Dir genervt sind, weil Du am Handy bist, erkläre ihnen, was Du machst. (Denke dran: Für andere starst Du einfach auf den Bildschirm!)

Du merkst, dass Du nach dem Handy greifen willst? Frage Dich, warum.

Prüfe Deine Nutzungsstatistiken – und beginne eine Challenge zwischen Dir und Deinen Freunden, die Werte zu reduzieren.

Meine Digitale Zufriedenheit

Gratuliere! Du hast es zum Ende des Detox zur digitalen Zufriedenheit geschafft. Lehn Dich zurück, entspann Dich und hake alles ab, was Du erreicht hast:

☐ Ich habe erkannt, was ich an Technologie mag und was nicht.

☐ Ich kenne ein paar der häufigsten Designtricks meiner Apps.

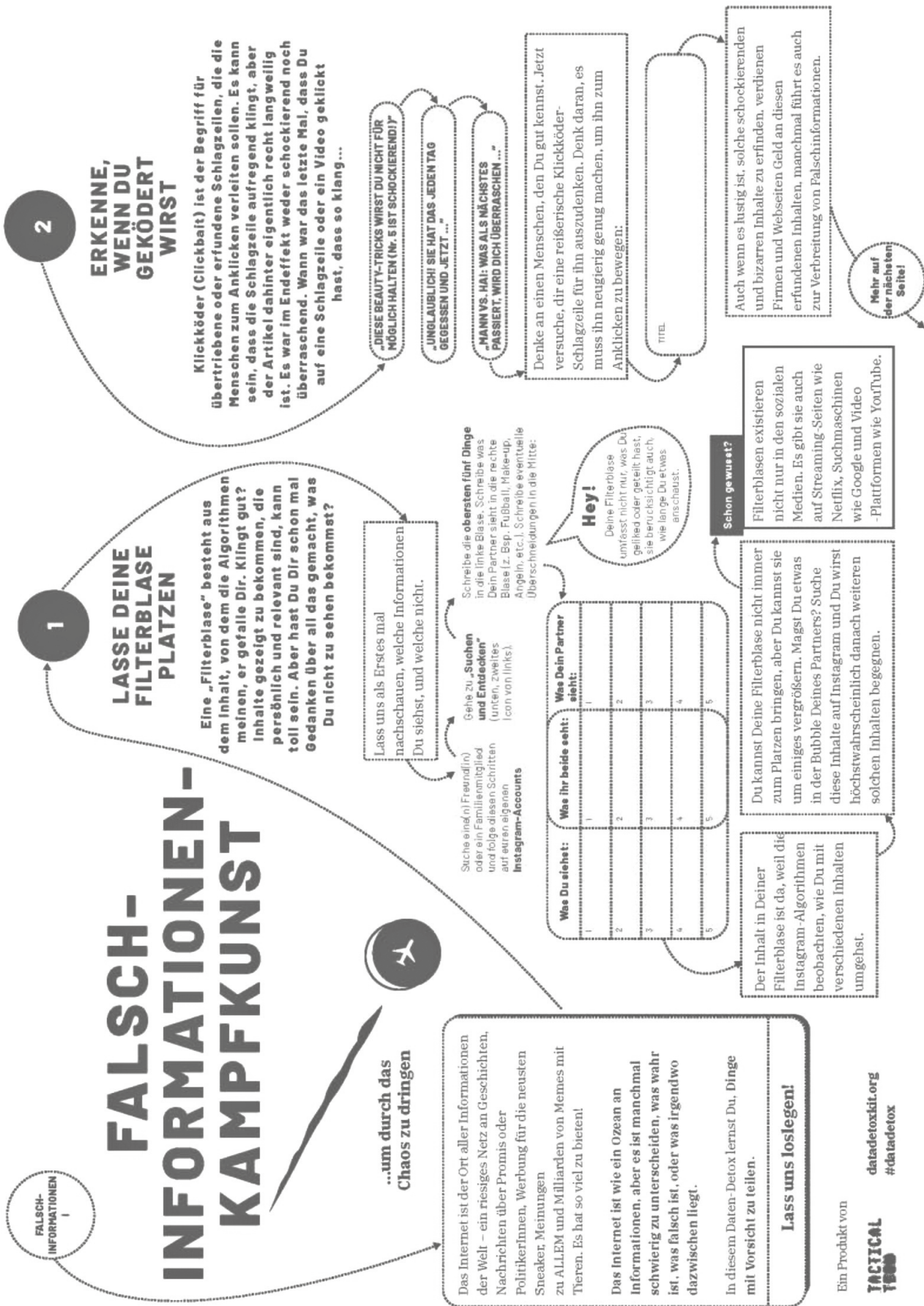
☐ Ich habe gelernt, wie ich diese Designtricks abschalten kann.

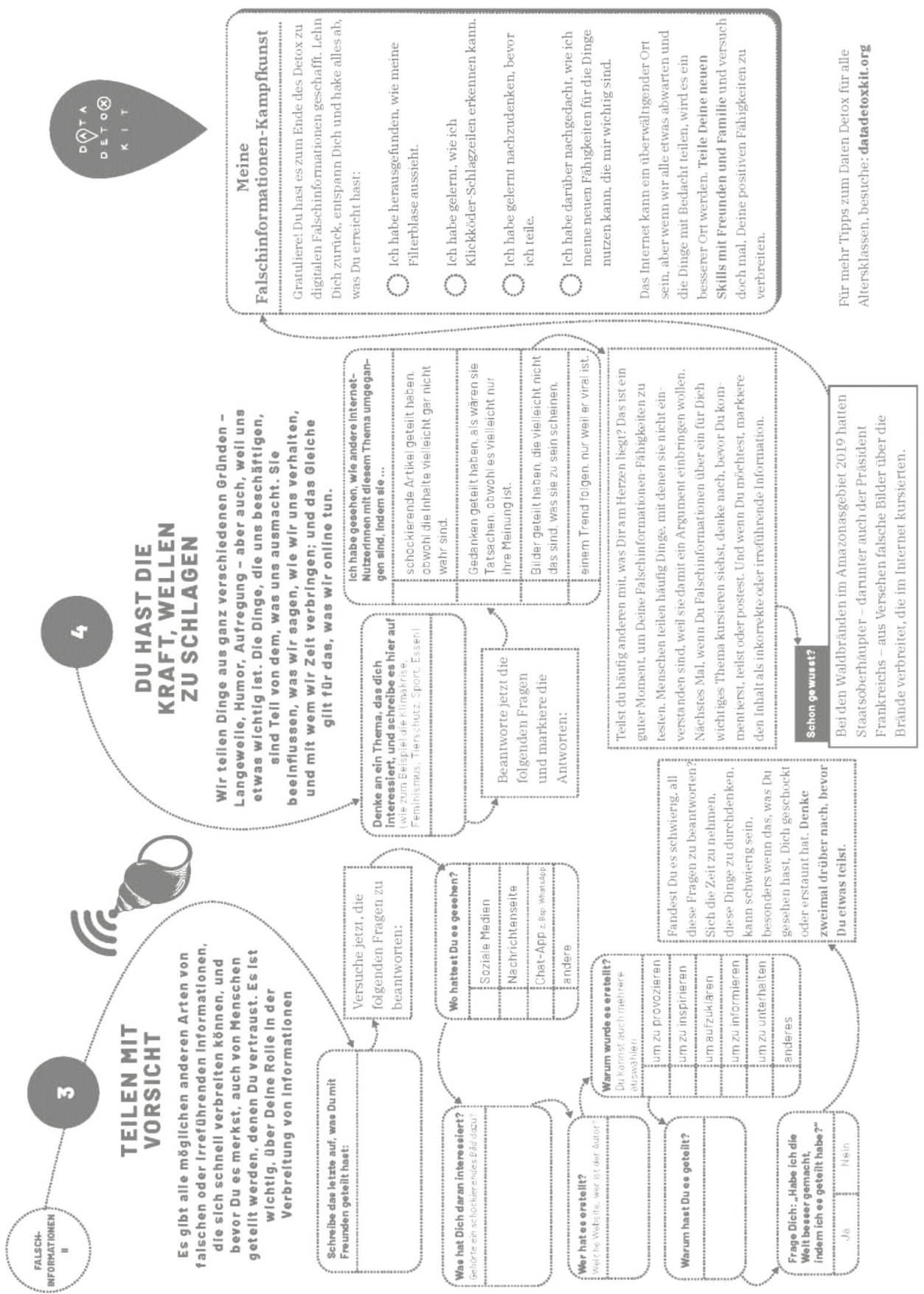
☐ Ich habe meinen eigenen Weg gefunden, wie meine Beziehung zur Technologie etwas mehr im Gleichgewicht ist.

Smart zu sein mit dem Smartphone heißt nicht, das Ding gleich in den Fluss zu werfen; es bedeutet, **einen Weg zu finden, damit Spaß zu haben, ohne dass es im Leben überhandnimmt**. Versuche doch, einige diese Techniken für Zufriedenheit auch mit Freunden und Familie zu teilen.

D T A
D E T O X
K I T

ALS NÄCHSTES:
FALSCH-
INFORMATIONEN





The AI Learning Kit

Björn Naumann und Wayra Aguilar

From Tech To Purpose

betreut von Prof. Christian Zöllner

Tom Witschel & Robin Goodwill

Sommersemester 2023

Burg Giebichenstein Kunsthochschule Halle

