Modul 4
Privatsphäre & Mündigkeit



digitale jugend arbeit

YOUTH POLICY LABS

#povwe
Professional Open Youth Work in Europe

genesis
Institut für Generationen- und Bildungsforschung

Kofinanziert durch das Erasmus+ Programm der Europäischen Union

Europäischer Digitalkompetenzrahmen für Bürger:innen DigComp 2.1

OPEN KNOWLEDGE FOUNDATION DEUTSCHLAND

Impressum

digitale jugend arbeit

Projekt Digitale Jugendarbeit

Das Projekt *Digitale Jugendarbeit* (DJA) ist ein Kooperationsprojekt von und mit *Demokratie & Dialog* (D&D), *Genesis Institut* (GEN), *Open Knowledge Foundation* (OKF), *Professional Open Youth Work in Europe* (POYWE) & *Youth Policy Labs* (YPL). Ihr findet uns auf digitalejugendarbeit.de.

Youth Policy Labs gGmbH

c/o *Youth Policy Labs* – gemeinnützige Gesellschaft für Jugendforschung mbH
Eingetragen im Handelsregister Berlin mit der Registernummer HRB 194069.
Unsere Umsatzsteueridentifikationsnummer ist DE316934284.
Vertreten durch Andreas Karsten, Geschäftsführung.

Youth Policy Labs gGmbH
Knesebeckstr. 77
10623 Berlin, Deutschland
T: +49 30 2300 1050
F: +49 30 2300 1051
M: ahoy@youthpolicy.org

Layout & Gestaltung → Gustav Berneburg & Tom Pincus
Projektlogo & Gestaltungskonzept → Jakob Fuchs & Simon Störk
Illustrationen → Daria Rüttimann
Druck → *Solid Earth, Berlin*

Redaktion → Alexandra Beweis, Andreas Karsten, Anneliese Mehlmann, David Gevers, Erik Dubs, Friedemann Schwenzer, Gustav Berneburg, Jakob Fuchs, Marika Welz, Marc Boes, Mathias Reymann, Maximilian Voigt, Ole Sievers, Theresa Walter & Tom Pincus

Testpilot:innen → Alisa Ofner, Andrea Portmann, Claudia Schwegler, Clemens Ritter, Darya Maksimenko, Frank Jannack, Johanna Zimmermann, Karin Peham-Strauß, Katharina Altmayer, Lisa Klette, Lisa Lohrmann, Maria Sonnleithner, Marlen Berg, Martina Krattenmacher, Nele Schmidt, Olaf Roschke, Otmar Brandweiner, Patricia Fekete, Rebecca Brunner, Sarah Wilke & Sonja Rappold

Moderationsteam → Janne Ratschinski & Marvin Müller

Begleitforschung → Andreas Karsten & Johanna Böhler

Beratung & Unterstützung → Marlene Mayer & Sabine Jansen von *Jugend für Europa*, der Nationalen Agentur für die EU-Programme *Erasmus+ Jugend in Aktion* und *Europäisches Solidaritätskorps*.

Kofinanziert durch das Erasmus+ Programm der Europäischen Union

Unser Projekt wurde durch *Erasmus+ Jugend in Aktion* unter der Leitaktion 2 als Strategische Partnerschaft mit der Projektnummer 2018-2-DE04-KA205-016683 gefördert.

Verantwortlich für den Inhalt nach § 55 Abs. 2 RStV:
Andreas Karsten, Geschäftsführung, *Youth Policy Labs gGmbH*.

Schriftfamilien: ***GT Sectra*** by Dominik Huber, Marc Kappeler and Noël Leu: https://www.grillitype.com/blog/typeface-stories/gt-sectra-development and ***Stratos*** by Yoann Minet and Emmanuel Labard: https://www.productiontype.com/family/stratos.

Diese Bildungsmaterialien sind, soweit nicht anders markiert, mit einer **Creative Commons-Lizenz** vom Typ **Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 International** lizenziert.
Eine Kopie dieser Lizenz könnt ihr unter https://creativecommons.org/licenses/by-sa/4.0/deed.de einsehen.

Gedruckt auf 100 % Recyclingpapier, Blauer Engel.

Modul 4:

Privatsphäre und Mündigkeit



Einleitung & Vorwort Modul 4: Privatsphäre und Mündigkeit

Liebe Freund:innen der digitalen Jugendarbeit,

als sich in 2018 fünf Organisationen an der Schnittstelle von Jugendarbeit, Jugendengagement, Jugendforschung und Jugendbildung zusammenrauften, um mit großzügiger Unterstützung von *Erasmus+ Jugend in Aktion* ein modulares Curriculum für digitale Jugendarbeit auf die Beine zu stellen, war Corona weit weg, und Digitalität für viele im Jugendbereich noch recht komisch. *Fast forward* drei Jahre, und unser siebenteiliges Curriculum trifft auf eine Welt, die ganz anders auf Digitales schaut. Wie verrückt!

Unsere Idee in 3 Sätzen

Wir wollten und wollen digitale und nonformale Bildung zusammenzudenken. Dafür haben wir uns den Digitalkompetenzrahmen der Europäischen Union *DigComp 2.1* geschnappt und darauf aufbauend ein modulares Trainingsangebot entwickelt. Wir möchten damit zu einem emanzipatorischen, mündigen und konstruktiven Blick auf Digitalisierung im Jugendbereich beitragen.

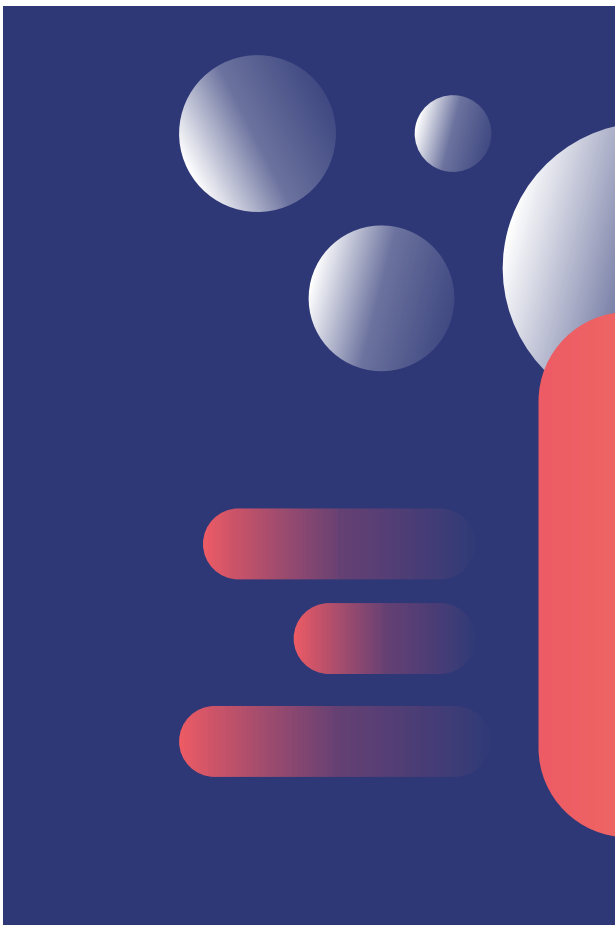
An wen richtet sich dieses Handbuch?

Das Handbuch richtet sich zunächst an Trainer:innen, für die digitale Bildung mehr ist als die reine Vermittlung von Tools. Mit unserem Curriculum zielen wir genauso auf die Vermittlung von praktischen Fähigkeiten ab wie auf eine gesellschaftspolitische Auseinandersetzung mit dem Prozess der Digitalisierung. Zielgruppe für das Curriculum sind vornehmlich Jugendarbeiter:innen, die sich niedrigschwellig mit Digitalisierung auseinandersetzen wollen.

Und was heißt das konkret?

DigComp 2.1 besteht aus acht Kompetenzstufen, von Level 1 bis Level 8, und fünf Kompetenzbereichen – 1) Daten und Information 2) Kommunikation und Zusammenarbeit 3) Inhalts- und Medienentwicklung 4) Privatsphäre und Mündigkeit, und 5) Problemfindung und Lösungsentwicklung. Für unser Projekt haben wir zusätzlich zwei weitere Kompetenzbereiche entwickelt: 6) Digitalität und Gesellschaft sowie 7) Digitalität und Jugendarbeit.

Diese Kompetenzbereiche untergliedern sich in insgesamt 29 Kompetenzen. Für diese haben wir jeweils zwei Übungen entwickelt: eine zum Einstieg in die Kompetenz (führt zu *DigComp* Level 3) und eine zur Vertiefung der Kompetenz (führt zu *DigComp* Level 5). Insgesamt gibt es damit also 58 Übungen, 29 davon zum Einstieg und 29 weitere zur Vertiefung.



Was finde ich im Handbuch?

Das Buch, welches du gerade in den Händen hältst (oder durch das du gerade scrollst) enthält den Kompetenzbereich 4, welcher 4 Kompetenzen beinhaltet.

Für jede Kompetenz findest du in diesem Buch eine Illustration, eine thematische Einführung, zwei Übungen und Arbeitsmaterialien. Die Arbeitsmaterialien sind jeweils mit @Trainer:innen oder @Teilnehmer:innen gekennzeichnet, je nachdem an wen sie sich richten.

Für jede Aufgabe führen wir die Dauer ebenso an wie die nötigen Materialien. Den Grundstock für außerschulische non-formale Bildung rund um digitale Jugendarbeit führen wir dabei als „Bildungsmaterialien“ auf. Dazu gehören Pinnwände, Flipcharts und Marker ebenso wie internetfähige Geräte für alle Teilnehmer:innen, stabiles Internet und eine Druckmöglichkeit.



digitale jugend arbeit

Kompetenzbereich
Privatsphäre und Mündigkeit

Enthält Kompetenzen
4.1, 4.2, 4.3, 4.4

Stufen
Einstieg und Vertiefung

Methoden
Stationenlernen, Elevator Pitch, Raumaufstellung, Kreatives Schreiben, Bewegtes Feedback, Recherche, Gruppenarbeiten, stille Diskussion, Kleingruppenarbeit

Dauer gesamt
8 · 90+ min. = 720+ min.

Wie können die Materialien für Bildungsarbeit eingesetzt werden?

Unser Anliegen ist, dass die Materialien so flexibel eingesetzt werden können wie möglich. Die Übungen sind deshalb keine in sich geschlossenen Workshops, sondern fokussieren sich auf den Hauptteil im klassischen Seminarphasenmodell, die Erarbeitungsphase. Um das in der Praxis rund zu machen, braucht es auf jeden Fall eine Rahmung durch Einstieg/Kontext und Abschluss /Reflexion.

Habt keine Scheu davor, Dinge neu zu kombinieren, wegzulassen, dazuzuerfinden! Bildungsarbeit gelingt am besten, wenn sie sowohl den Bedürfnissen der Trainer:innen als auch denen der Teilnehmer:innen entspricht! Damit das Remixen einfach ist, stehen die Materialien unter einer **CC-BY SA 4.0** Lizenz. Ihr könnt sie also nach Belieben anpassen, verändern und verwenden, sofern ihr irgendwo Credits an uns, das *Projekt Digitale Jugendarbeit*, gebt und sie unter gleichen Lizenzbedingungen teilt. Na dann mal los!

Viele erfüllende Bildungserlebnisse wünschen euch

aleX, Andreas, Anneliese, Daria, David, Erik, Friedemann, Gustav, Jakob, Marika, Marc, Mathias, Max, Ole, Simon, Theresa und Tom –

und unsere Teams und Organisationen: *Digitale Jugendarbeit (DJA), Genesis Institut (GEN), Open Knowledge Foundation (OKF), Professional Open Youth Work in Europe (POYWE)* und *Youth Policy Labs (YPL)*.

Hier geht es zur zentralen Downloadseite der Materialien: »bit.ly/dja-material«

Inhaltsverzeichnis Privatsphäre & Mündigkeit

KOMPETENZBEREICH 4 von 7

KOMPETENZ 4.1 **Schützen der digitalen Arbeitsumgebung** 7

Thematische Einführung 8
Privatsphären-Arcaden 9
Pitch mir meine Sicherheit 20

KOMPETENZ 4.2 **Schützen von personenbezogenen Daten und der Privatsphäre** 23

Thematische Einführung 24
Seepferdchen: Digitale Selbstverteidigung 25
Hurra, diese Welt geht unter!? 40

KOMPETENZ 4.3 **Schützen von Gesundheit und Wohlbefinden** 45

Thematische Einführung 46
Das Internet und ich – eine Beziehungskrise? 47
Ein Unglück designt sich nicht von allein 51

KOMPETENZ 4.4 **Umweltschutz & Digitalisierung** 57

Thematische Einführung 58
Familie Freiraum und die digitale Nachhaltigkeit 59
Wahlkampf: Digital und Nachhaltig – aber wie? 61

4.1

Schützen der digitalen Arbeitsumgebung

Digitale Geräte und Umgebungen schützen sowie Risiken und Bedrohungen verstehen. Über Maßnahmen, die die eigene Privatsphäre und Sicherheit schützen, Bescheid wissen.



Illustration: Daria Rüttimann

Kompetenzbereich

Privatsphäre und Mündigkeit

Kompetenz

Schützen der digitalen Arbeitsumgebung

Version 1.2
Lizenz: Namensnennung – Weitergabe unter gleichen Bedingungen 4.0 International (CC BY-SA 4.0)

Hier geht es zur zentralen Downloadseite der Materialien:
bit.ly/dja-material

Thematische Einführung

digitale jugend arbeit

Facebook, *Microsoft*, *Mastercard*, *Uber*, *Nintendo*, *Google*, *Reddit*, *Sony* und *Gmail*. Alle diese Unternehmen litten in den letzten Jahren unter sogenannten Data Breaches. Das heißt, dass riesige Mengen vertraulicher Daten durch die Handlung von Hacker:innen und durch Schwachstellen im Sicherheitsnetzwerk der Firmen nach Außen gelangen konnten. Diese Datensätze wurden dann meistens gegen Geld im Internet verkauft oder anderweitig missbraucht. Diese Größenverhältnisse sind zwar für uns nicht alltäglich, aber auch in kleineren Arbeitskontexten oder auf dem Privatlaptop können sensible Daten durch Hackingangriffe, Betrug-Emails oder Data Breaches bei größeren Firmen, denen wir (bewusst oder unbewusst) freiwillig unsere Daten anvertrauen, in die falschen Hände geraten.

Deshalb ist – egal ob im privaten oder professionellen Bereich – der Schutz von Daten ein hohes Gut. Hierbei werden besonders in Arbeitskontexten vertrauliche Daten verarbeitet, denen besondere Vorsicht bemessen werden sollte. Dies macht den Schutz der digitalen Arbeitsumgebung – unabhängig von der Größe einer Organisation – besonders beachtenswert.

Hierbei tun sich Fragen auf wie beispielsweise: Wo und wie speichere ich vertrauliche Daten im Arbeitskontext? Von welchen Daten sollte ich welches Backup erstellen? Wie kommuniziere ich sicher in Arbeitsbeziehungen? Wem gebe ich potentiell wichtige Daten in die Hände, wenn ich digital mit meinen Kolleg:innen zusammenarbeite? Welche Programme und welchen Service nutzt mein Arbeitgeber und wie sicher sind diese in puncto Datenschutz? Wie gehe ich mit meinen Passwörtern im Arbeits- aber auch privaten Kontext um?

Die Beantwortung der meisten dieser Fragen sollte zwar in der Verantwortung der Arbeitgeber:innen liegen, für die korrekte Umsetzung sind allerdings die Mitarbeiter:innen verantwortlich. Deshalb ist es besonders wichtig, allgemein ein Bewusstsein für diese Themen zu schaffen. Außerdem sollten alle Mitglieder einer Organisation mit einbezogen werden. Hiermit wird sichergestellt, dass nicht nur Arbeitnehmer:innen das jeweilige Datenschutzkonzept verstehen und umsetzen können, sondern auch dass mögliche Veränderungen im Arbeitsablauf mit Verständnis angenommen werden.

Dieses Modul nähert sich dem Schutz der digitalen Arbeitsumgebung, indem es über verschiedene Themenkomplexe in diesem Bereich aufklärt. Hierbei eignen sich die Teilnehmer:innen sowohl spielerisch als auch durch Eigenrecherche praktisches Wissen über Vorgehensweisen, Programme und mögliche Sicherheitslücken rund um dieses Thema an. Ein besonderer Fokus liegt dabei auf dem Abschätzen zwischen Funktionalität und Sicherheit.

Inhalt **Seite**

Aufgabe ❶	s.09
Arbeitsmaterial 1	s.11
Arbeitsmaterial 2	s.12
Arbeitsmaterial 3	s.15
Arbeitsmaterial 4	s.16
Arbeitsmaterial 5	s.17
Aufgabe ❷	s.20
Trainingsmaterial 1	s.21

Privatsphäre-Arcaden

@Trainer:innen · Moderationsbriefing · 4.1

digitale jugend arbeit

Kompetenzbereich
Privatsphäre und Mündigkeit

Kompetenz
Schützen der digitalen Arbeitsumgebung

Stufe
Einstieg

Methode
Stationenlernen

Ausstattung
Bildungsmaterialien + Ausgedruckte Arbeitsmaterialien

Dauer
90 Minuten

Ziel dieser Aufgabe ist es, dass die Teilnehmer:innen sich spielerisch mit den potenziellen Sicherheitsrisiken einer digitalen Arbeitsumgebung auseinandersetzen. Darüber hinaus entdecken sie Wege, wie sie sich davor schützen können.

Ablauf

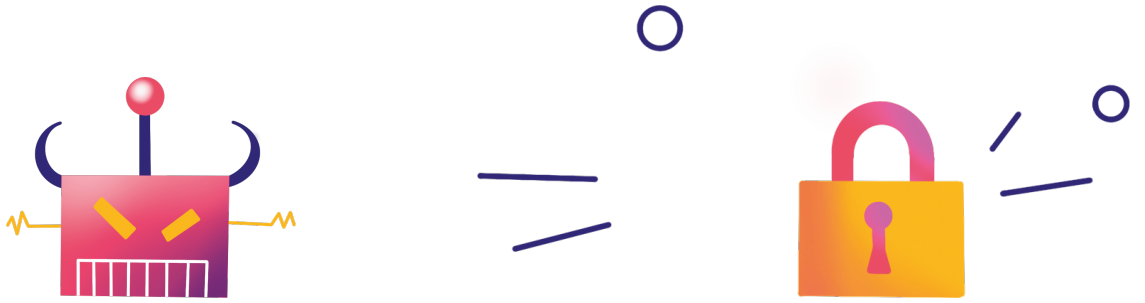
Diese Aufgabe ist als Stationenlernen gedacht. Die Teilnehmer:innen absolvieren die einzelnen Stationen zu zweit oder zu dritt und erfüllen dort die verschiedenen Aufträge oder Spiele. Nach dem Absolvieren des Spiels sollen sie auf einem ausliegenden Flipchart zur Station passende Ideen sammeln – ein konkreter Auftrag dazu ist an den Stationen jeweils beschrieben. Abschließend werden die Ergebnisse der einzelnen Stationen (auf dem Flipchart) im Plenum gemeinsam ausgewertet und offene Fragen geklärt.

Bis auf Station 1 ist es sinnvoll, die einzelnen Stationen mit (mind.) einem stationären Endgerät (Laptop bspw.) auszustatten, da die Aufgabe jeweils durch eine Webseite begleitet wird. Die Teilnehmer:innen können aber auch mit ihren eigenen Geräten die Tour durch die Stationen absolvieren.

Hinweise zur Moderation

- Da die Stationen nicht aufeinander aufbauen, können problemlos einzelne Stationen ausgelassen oder andere in ihrem Umfang erweitert werden.
- Bei den einzelnen Stationen ist jeweils eine Teilnehmer:innenzahl angegeben. Dies ist lediglich eine Empfehlung. Jede Station ist darauf ausgelegt, in Teams mit 2–3 Leuten absolviert zu werden, einige Stationen können aber auch in Einzelarbeit bearbeitet werden.
- Für die abschließende Besprechung im Plenum kann es sinnvoll sein, die Teilnehmer:innen im vorhinein darauf hinzuweisen, dass sie sich offene Fragen, die währenddessen aufkommen, notieren sollen.
- Im Arbeitsmaterial für Station 1 müssen Kärtchen ausgeschnitten und als Stapel auf der Station ausgelegt werden.
- Das Security Risks Game in Station 6 ist auf Englisch. Daher ist es sinnvoll, darauf zu achten, dass mindestens eine Person in den Teams über grundlegende Englischkenntnisse verfügt. Das Spiel funktioniert auf Touchscreens nicht ganz vollumfänglich – wenn ihr ein Gerät mit Tastatur zur Verfügung habt, setzt es an der Station alternativ ein.

Hier geht es zur zentralen Downloadseite der Materialien: »bit.ly/dja-material«



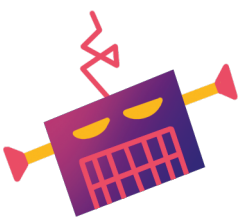
Stationsübersicht mit Lernzielen & *Hinweisen zur Vorbereitung*

digitale jugend arbeit

Safety-Buzzwords
Hier denken die Teilnehmer:innen gemeinsam über Begrifflichkeiten aus dem Bereich Schutz ihrer digitalen Umgebung nach. Im Anschluss notieren sie diejenigen Begriffe, die sie nicht kannten, auf dem ausliegendem Flipchart.
Hier sollten entweder die Karten aus Arbeitsmaterial 1 ausgedruckt und ausgeschnitten werden oder alternativ die Begriffe auf kleine Papierschnipsel geschrieben werden.

Passwort-Merk-Spiel
Die Teilnehmer:innen treten gegeneinander an und versuchen dabei, sich möglichst starke Passwörter auszudenken und sich diese auch einzuprägen. Danach reflektieren sie ihre Passwort-Strategien auf dem ausliegenden Flipchart.
Hier sollten Stifte und kleine Zettel für die Teilnehmer:innen bereitliegen. Außerdem wird eine Liste für die erreichten Zeiten der Teilnehmer:innen benötigt.

Phishing erkennen
Woran erkenne ich gefälschte E-Mails, die in meinem Postfach auftauchen und an meine Daten heranwollen? Nachdem die Teilnehmer:innen solche in einem Online-Spiel identifiziert haben, sammeln sie auf dem Flipchart Strategien zum Erkennen von Phishing-Mails.
Hier kann (mind.) ein Endgerät mit der geöffneten Webseite von Google eingerichtet werden. Außerdem wird eine Liste für die erreichten Zeiten der Teilnehmer:innen benötigt.



Reflexion Datenpreisgabe
Diese Station umfasst einen Test zur persönlichen Datenpreisgabe im Internet, welcher den Teilnehmer:innen am Ende einen Score ausgibt. Auf dem Flipchart sollen sie dann Tipps zum Schutz persönlicher Daten angeben.
Hier kann (mind.) ein Endgerät mit der geöffneten Webseite von netzpolitik.org eingerichtet werden. Außerdem wird eine Liste für die erreichten Zeiten der Teilnehmer:innen benötigt.

Twitter-Wettrennen
Hier versuchen die Teilnehmer:innen innerhalb eines *Twitter*-Accounts schnellstmöglich eine spezifische Einstellung zur Privatsphäre oder der Account-Sicherheit zu finden. Auf dem Flipchart ergänzen sie dann ihre Tipps und Tricks zu den Account-Einstellung sozialer Netzwerke.
Hier ist es sinnvoll, mind. 2 Endgeräte mit neu erstellten Twitter-Accounts auszulegen. Die Suchaufträge sollten in mehrfacher Ausführung ausgedruckt, ausgeschnitten und verdeckt auf den Tisch platziert werden. Außerdem wird eine Liste für die erreichten Zeiten der Teilnehmer:innen benötigt.

Security Risks Game
In diesem englischsprachigen Klick-Such-Spiel identifizieren die Teilnehmer:innen mögliche Sicherheitsrisiken in einem Büro. Danach sammeln sie weitere mögliche Sicherheitsrisiken und ergänzen jene auf dem ausliegenden Flipchart.
Hier kann (mind.) ein Endgerät mit der geöffneten Webseite von Living Security eingerichtet werden. Außerdem wird eine Liste für die erreichten Zeiten der Teilnehmer:innen benötigt.



Kompetenzbereich
Privatsphäre und Mündigkeit

Kompetenz
Schützen der digitalen Arbeitsumgebung

Stufe
Einstieg

Methode
Stationenlernen

Ausstattung
Bildungsmaterialien + Ausgedruckte Arbeitsmaterialien

Dauer
90 Minuten

Hier geht es zur zentralen Downloadseite der Materialien: »bit.ly/dja-material«

Safety-Buzzwords

Im Bereich Datenschutz findet man sich schnell mit vielen – in Teilen sehr kryptisch klingenden – Fachwörtern, die nicht selten aus dem Englischen entstammen, konfrontiert. Um Strategien zum Schützen der digitalen Arbeitsumgebung besser verstehen oder auch identifizieren zu können, ist es sinnvoll, sich einmal mit diesen Fachbegriffen auseinandergesetzt zu haben.

Im vor euch liegenden Stapel findet ihr Begriffskarten mit diversen Fachwörtern. Zieht nacheinander zufällig einen von den Begriffen und überlegt gemeinsam, was das Wort bedeuten könnte. Dann notiert ihr auf dem ausliegenden Flipchart, ob ihr den Begriff kanntet oder ob ihr zum Verständnis erst ein wenig recherchieren musstet. Wiederholt das beliebig oft. Vielleicht fallen euch ja auch noch weitere Begriffe ein, die ihr auf dem Flipchart ergänzen könnt.

Scammer	Passwort-Manager	Privacy	Phishing	Backup
PGP Key	Firewall	Antiviren-programm	Catfishing	Chatbot
Zwei-Faktor-Authentifi-zierung	Encryption	Cookies	Metadaten	Geoblocking
Profiling	VPN	DSGVO	BCC	Bot
Scam	Zählpixel	Ransom-ware	Zero-Click Attacke	

Passwort-Merk-Spiel

An dieser Station tretet ihr gegeneinander an: Wer von euch kann sich das sicherste Passwort ausdenken und merken? Dazu braucht ihr **Zettel**, **Stift** und eine **Stoppuhr**.

Lest euch **zuerst die Arbeitsanleitung** komplett durch. Zückt danach einen Zettel und Stift pro Person. Startet die Stoppuhr, sobald ihr bereit seid.

Wenn ihr fertig seid, könnt ihr euch überlegen, welche Strategie für ein sicheres Passwort die beste war. Haltet diese auf dem ausliegenden Flipchart fest. Gerne könnt ihr auch eine Hitliste der eurer Meinung nach unsichersten Passwörter aufschreiben.



Anleitung



1) Jede:r von euch hat **30 Sekunden Zeit**, um sich ein möglichst starkes Passwort auszudenken, auf den Zettel aufzuschreiben und auch einzuprägen.

2) Sind die **30 Sekunden vorbei**, dreht ihr eure Zettel um und legt sie vor euch hin.

3) Jetzt habt ihr **2 Minuten Zeit**, um nicht an euer Passwort zu denken. Unterhaltet euch zum Beispiel über die lustigste Spammail, die ihr je erhalten habt.

4) Danach habt ihr 15 Sekunden, um das von euch **gemerkte Passwort auswendig auf einen Zettel aufzuschreiben** (ohne unter den umgedrehten Zettel zu gucken, selbstverständlich).

5) Jetzt könnt ihr die **Zeit anhalten** und überprüfen, ob ihr euch euer Passwort richtig gemerkt habt.

6) Gebt gemeinsam die Passwörter auf der Webseite wiesicheristmeinpasswort.de ein, die ihr im 4. Schritt aufgeschrieben habt.

7) Die Webseite verrät euch, wie lange ein Computer bräuchte, um euer Passwort zu knacken. Außerdem könnt ihr einsehen, aus welchen „Bausteinen“ sich euer Passwort zusammensetzt, nach denen ein Programm zum Passwortknacken Ausschau hält.

8) Das Passwort, für das ein Computer am längsten bräuchte, ist das sicherste und gewinnt, vorausgesetzt, ihr habt es euch richtig gemerkt.

wie sicher ist mein Passwort .de

Passwort-Sicherheits-Check

Phishing erkennen



Unter *Phishing* versteht man betrügerische Versuche, auf digitalem Weg an Daten oder Geld heranzukommen. Das passiert beispielsweise mittels gefälschter E-Mails, Kurznachrichten, oder Webseiten. Viele Phishing-Versuche bekommt ihr zum Glück nur in dem Spam-Ordner eures E-Mail-Accounts zu sehen, da sie automatisch als unecht erkannt werden. Viele dieser Nachrichten sind oft sogar sehr amüsant.

In diesem kleinen Quiz von *Google* könnt ihr testen, wie gut ihr Phishing-Mails von ungefährlichen Mails unterscheiden könnt. Wenn ihr wollt, könnt ihr auch gegeneinander antreten und schauen, wer von euch der:die Phishing-Expert:in wird.

phishingquiz.withgoogle.com/?hl=de

Wenn ihr fertig seid, könnt ihr überlegen, welche Strategie(n) ihr verwendet, um Phishing-Mails von echten Mails zu unterscheiden. Ergänzt diese auf der ausliegenden Mindmap. Wenn ihr möchtet, schreibt eure persönliche Hitliste der absurdesten Phishing-Mail-Maschen auf.



Wie sicher ist dein digitales Ich?

Wie sicher ist dein digitales Ich? Diese Frage stellt dir das Online-Magazin für digitale Freiheitsrechte *netzpolitik.org*. Durch 10 Fragen wird dein persönlicher Privacy-Score berechnet. Es geht bei diesem Quiz weniger darum, euch anschließend zu vergleichen, wer die meisten Punkte erreicht hat. Vielmehr soll ein wenig das eigene Verhalten reflektiert und ein Verständnis entwickelt werden, welche Faktoren einen Einfluss auf den erreichten Score haben.

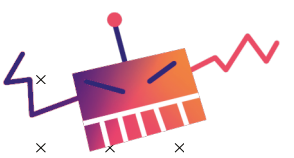
Wenn ihr fertig seid, könnt ihr euch überlegen, welche Auswirkung die Nutzung bestimmter Medien im Arbeitsalltag auf euren Datenfußabdruck hat. Danach könnt ihr Tipps zum Schützen der persönlichen Daten im Netz auf der ausliegenden Mindmap ergänzen.

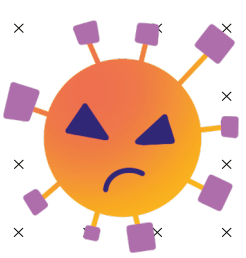
Twitter-Wettrennen: Privatsphäre Einstellungen

In den Einstellungen deines Social-Media-Accounts kann man weitaus mehr ändern als nur die Sprache oder das eigene Passwort. An dieser Station sollt ihr ein wenig in die Einstellungen eines *Twitter*-Accounts eintauchen – verpackt in einem kleinen Suchspiel.
Jede:r von euch benötigt ein eigenes Endgerät. Wenn ihr ein kleines Wettrennen daraus machen wollt, solltet ihr zunächst sicherstellen, dass ihr mit den gleichen Startvoraussetzungen antretet. Dazu gehören bspw. die gleiche *Twitter*-Anwendung (App oder Browser, iOS oder Android bspw.) auf eurem Endgerät, den gleichen Internetzugang und am besten ein möglichst unkonfigurierten *Twitter*-Account.

Anleitung
Vor euch findet ihr kleine Zettel (noch sind sie allerdings umgedreht). Darauf befinden sich 5 kleine Suchaufträge, die ihr in den „Einstellungen" eures *Twitter*-Accounts finden könnt.
Wenn ihr bereit seid, könnt ihr gemeinsam die Zettel umdrehen und so schnell wie möglich versuchen, euch an die Orte in den entsprechenden Einstellungen zu navigieren. Gefunden? Das ist gut, jetzt schreibt ihr euch entweder den entsprechenden Pfad auf einen Zettel oder ihr macht einen Screenshot als „Beweis", dass ihr die Aufgabe erfüllt habt.
Wer zuerst alle 5 Einstellungen gefunden hat, gewinnt das *Twitter*-Wettrennen. Wenn ihr möchtet, könnt ihr eure Zeit stoppen und euer Ergebnis auf dem Flipchart festhalten. Dann solltet ihr für die nächste Gruppe noch die Aufgabenzettel wieder umdrehen.

Wenn ihr damit fertig seid, könnt ihr auf dem ausliegenden Flipchart eure persönlichen Empfehlungen für „Das solltet ihr unbedingt in den Einstellung eures Sozialen-Netzwerks festlegen" ergänzen.





Teilnehmer:in Twitter-Wettrennen

Ändern der Schriftgröße
Entfernen des angegebenen Geburtsdatums
Art der Zwei-Faktor-Authentifizierung einstellen
Einsehen, welche weiteren Apps auf meinen Account zugreifen können
Anzeigen lassen von personalisierten Trends, basierend auf dem eigenen Standort

Teilnehmer:in Twitter-Wettrennen

Ändern der Schriftgröße
Entfernen des angegebenen Geburtsdatums
Art der Zwei-Faktor-Authentifizierung einstellen
Einsehen, welche weiteren Apps auf meinen Account zugreifen können
Anzeigen lassen von personalisierten Trends, basierend auf dem eigenen Standort

Teilnehmer:in Twitter-Wettrennen

Ändern der Schriftgröße
Entfernen des angegebenen Geburtsdatums
Art der Zwei-Faktor-Authentifizierung einstellen
Einsehen, welche weiteren Apps auf meinen Account zugreifen können
Anzeigen lassen von personalisierten Trends, basierend auf dem eigenen Standort



Security Risks Game

Herumliegende Festplatten oder unverschlüsselte Tablets, die mit wichtigen Daten gefüllt sind, werden meistens erst dann zum Problem, wenn sie in die falschen Hände geraten. Der Teufel steckt wie so oft im Detail. Dieses kleine Wimmelbild-Spiel sensibilisiert für jene Details, die im eigenen Arbeitsalltag potenzielle Sicherheitslücken darstellen.

Besucht die folgende – leider nicht für Touchscreen-Bildschirme optimierte – Webseite und schult eure Wahrnehmung für solche Sicherheitslücken. Ihr könnt gegeneinander antreten und schauen, wer von euch schneller ist oder gemeinsam versuchen, einen Überblick zu bekommen: hotspot.livingsecurity.com

Da die Webseite auf Englisch ist, solltet ihr schauen, dass keine:r allein den Sprachbarrieren ausgesetzt ist und dass ihr am Ende die Ergebnisse besprecht.
Wenn ihr fertig seid, dürft ihr euren (Gruppen-)Highscore, die Zeit, die ihr gebraucht habt, und die gefundenen Dinge auf dem ausliegenden Flipchart in eine Liste ergänzen. Danach könnt ihr gemeinsam überlegen, welche potentiellen Sicherheitslücken euch noch einfallen oder welchen davon ihr vielleicht im Alltag begegnet. Ergänzt diese ebenfalls auf dem Flipchart und fügt auch ein paar Strategien zum Verhindern dieser Sicherheitslücken hinzu, sofern euch welche einfallen.

Pitch mir meine Sicherheit

@Trainer:innen · Moderationsbriefing · 4.1

digitale jugend arbeit

In dieser Aufgabe lernen die Teilnehmer:innen diverse Methoden zum Schutz der digitalen Arbeitsumgebung im Hinblick auf ihre Vor- und Nachteile einzuschätzen. Außerdem erwerben sie die Kompetenz, ihr erlerntes Wissen an andere weiterzugeben.

Kompetenzbereich
Privatsphäre und Mündigkeit

Kompetenz
Schützen der digitalen Arbeitsumgebung

Stufe
Vertiefung

Methode
Elevator Pitch

Ausstattung
Bildungsmaterialien

Dauer
90 Minuten

Ablauf

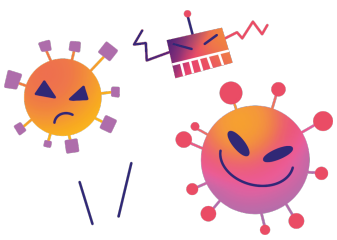
Die Teilnehmer:innen teilen sich in Gruppen von je 2–3 Personen auf. Jede Gruppe zieht eine der Recherchefragen (Trainingsmaterial 1), sammelt dazu selbstständig Informationen im Internet und bereitet einen kurze Präsentation vor (maximal 5 Minuten). Danach stellen sich die einzelnen Gruppen die Antworten auf ihre jeweiligen Recherchefragen gegenseitig im Plenum vor.

Hinweise zur Moderation

- Das Trainingsmaterial 1 muss vorher ausgedruckt und die einzelnen Recherchefragen ausgeschnitten werden, sodass sie zufällig bspw. aus einer Schüssel gezogen werden können.
- Die Gruppengröße und Recherchezeit kann je nach Bedarf und Anzahl der Teilnehmer:innen variiert werden.
- Abhängig von der Zeit können im Anschluss, nach Bedarf, einzelne Aspekte der Vorträge im Plenum diskutiert werden.

Hier geht es zur zentralen Downloadseite der Materialien: »bit.ly/dja-material«





Recherchefragen

Lokaler Server vs. Cloud:

Welche Vor- und Nachteile bringt es, die Daten der Organisation auf einem eigenen, lokalen Server bzw. bei einem externen Cloud-Dienstleister zu speichern?
Welche verschiedenen Optionen bieten diese Dienste jeweils an?

Kommunikation im Arbeitskontext:

Welche Kommunikationstools nutzt ihr im Arbeitskontext?
Wie sicher sind diese jeweils?

Backup von Daten:

Für welche Daten und Dokumente sollten definitiv Backups erstellt werden? Wie oft sollte gebackuped werden? Sollten alte Backupversionen aufbewahrt werden? Wenn ja, wie weit sollte das zurückreichen? Wo werden die Backups gespeichert? Sollte diese Aufgabe auf externe Unternehmen ausgelagert werden?

Passwort-Manager:

Lohnt es sich einen Passwort-Manager zu verwenden? Welche Arten von Passwort-Managern gibt es und wie sicher und praktisch sind diese jeweils?

Daten und Dienste:

Was passiert, wenn ich mich bei verschiedenen Diensten z. B. mit meinem oder dem Arbeits-Google-Konto anmelde? Wie wird hier mit meinen Daten umgegangen?

Digitale Teamarbeit:

Welche Programme und Dienste zur Online-Teamarbeit (bspw.: Programme zum kollaborativen Schreiben, geteilte Teamterminkalender, etc.) nutze ich? Wie wird hier jeweils mit meinen vertraulichen Daten umgegangen? Gibt es hierzu Alternativen, die besonderen Wert auf Datensicherheit legen?

.2

Schutz von personenbezogenen Daten und Privatsphäre

Persönliche Daten und Privatsphäre in digitalen Umgebungen schützen. Verstehen, wie man persönliche Informationen benutzt und teilt, ohne sich oder andere Menschen damit zu schaden. Privatsphäre-Einstellungen und -Politiken digitaler Dienste verstehen.



Illustration: Daria Rüttimann

Kompetenzbereich

Privatsphäre und Mündigkeit

Kompetenz

Schützen von personenbezogenen Daten und der Privatsphäre

Version 1.2
Lizenz: Namensnennung – Weitergabe unter gleichen Bedingungen 4.0 International (CC BY-SA 4.0)

Hier geht es zur zentralen Downloadseite der Materialien:
bit.ly/dja-material

Thematische Einführung

digitale jugend arbeit

Daten sind, so heißt es, das Gold des 21. Jahrhunderts. Je mehr Bereiche unseres Lebens digitalisiert werden, desto mehr Daten werden gesammelt. In unserem digitalen Alltagsleben generieren wir fast immer und überall auswertbare Informationen – die Frage nach Privatsphäre und Datenschutz stellt sich daher mit einer neuen Dringlichkeit. Auf einer individuellen Ebene geht es dabei vor allem darum, sich selbst möglichst gut zu schützen und mündig im Netz zu bewegen. Da diese Daten zumeist in den Händen von einzelnen Institutionen liegen und diese dadurch eine gewisse Macht bekommen, müssen wir auch auf einer gesellschaftlichen Ebene eine Diskussion über unsere Zukunftsvisionen in Sachen Privatsphäre und Datensouveränität führen.

Aber der Reihe nach. In unserem Alltag hinterlassen wir ständig Spuren im Netz. Häufig machen wir das bewusst, weil wir etwa personenbezogene Daten angeben, um uns für eine digitale Dienstleistung anzumelden. Doch nicht immer machen wir uns klar, dass wir etwa schon mit dem Öffnen einer App, der Suche nach einem vegetarischen Bologneserezept oder dem Knipsen eines Fotos Datenspuren hinterlassen. Diese können sehr viel über eine Person verraten, beispielsweise Informationen über den Tagesablauf, Vorlieben, Freizeitverhalten usw. Da *Facebook, Google* & Co. einen großen Teil ihrer Einnahmen durch Werbung generieren, nutzen sie die gesammelten Daten, um diese Dienstleistung besonders effektiv anzubieten. Unsere Daten werden aber auch algorithmisch verarbeitet. So kennt *Spotify* deinen Musikgeschmack nach einer gewissen Nutzungsdauer ziemlich gut und kann dich gezielt auf neue Künstler:innen aufmerksam machen. Problematischer wird es, wenn Algorithmen darüber entscheiden, welche Inhalte angezeigt werden und welche nicht. Ein bedeutender Teil unserer gesellschaftlichen Debatte und Meinungsbildung wird auf diese Art maßgeblich von privatwirtschaftlichen Unternehmen mitgestaltet. Die demokratische Öffentlichkeit hat nur begrenzten Einfluss darauf, diese Räume des Austauschs und deren Regeln zu formen oder zu kontrollieren.

Die Asymmetrie zwischen den Konsument:innen und den datensammelnden Unternehmen wird immer größer. Während erstere immer mehr von sich preisgeben und somit durchleuchtbarer werden, bleiben zweitere weitestgehend im Verborgenen. Dass und von welchen Tech-Konzernen Daten gesammelt werden, ist weitestgehend bekannt, oder in Teilen einsehbar. Doch zu welchem Zweck und in welcher Form diese Daten weiterverarbeitet werden, entzieht sich oft demokratischer Kontrolle und Mitbestimmung. Das führt dazu, dass rund um Datenschutz – meist nicht unbegründet – oft sehr dystopische Zukunftsszenarien entworfen werden. Die Diskussion um die Gestaltbarkeit und Regulierbarkeit von positiven Datenschutz-Konzepten kommt dabei häufig zu kurz.

In diesem Modul wird das Schützen von personenbezogen Daten und der Privatsphäre sowohl auf einer individuellen als auch auf einer gesellschaftlichen Ebene angegangen. Zunächst setzen sich Teilnehmer:innen damit auseinander, wie sie im Alltag ihre Privatsphäre und ihre Daten schützen können. Im zweiten Abschnitt diskutieren sie dystopische und utopische Datenschutz-Zukünfte.

Inhalt	Seite
Aufgabe ❶	s.25
Arbeitsmaterial 1	s.28
Arbeitsmaterial 2	s.29
Arbeitsmaterial 3	s.30
Arbeitsmaterial 4	s.31
Arbeitsmaterial 5	s.32
Arbeitsmaterial 6	s.33
Arbeitsmaterial 7	s.34
Arbeitsmaterial 8	s.35
Arbeitsmaterial 9	s.36
Arbeitsmaterial 10	s.37
Arbeitsmaterial 11	s.38
Arbeitsmaterial 12	s.39
Aufgabe ❷	s.40
Arbeitsmaterial 1	s.42



Seepferdchen: Digitale Selbstverteidigung

@Trainer:innen · Moderationsbriefing · 4.2

digitale jugend arbeit

Kompetenzbereich
Privatsphäre und Mündigkeit

Kompetenz
Schützen von personenbezogenen Daten und der Privatsphäre

Stufe
Einstieg

Methode
Stationenlernen

Ausstattung
Bildungsmaterialien + Kopfhörer empfohlen, Stempel und Stempelkissen

Dauer
90+ Minuten

In dieser Aufgabe setzen sich die Teilnehmer:innen mit wesentlichen Aspekten des Datenschutzes, der Privatsphäre und ihres eigenen Umgangs mit personenbezogenen Daten auseinander. Ziel dieser Übung ist die Sensibilisierung für Datenschutzthemen, das Kennenlernen praktischer Strategien bis hin zur Planung von konkreten Maßnahmen hin zu einer aktiven digitalen Selbstverteidigung.

Ablauf

Diese Übung ist als Stationenlernen angelegt und besteht aus bis zu **11+1 Stationen.** Diese können je nach zur Verfügung stehender Zeit sowie den Bedürfnissen und Vorkenntnissen der Teilnehmer:innen frei miteinander kombiniert werden. Die Teilnehmer:innen können sich allein oder in Kleingruppen, in selbst gewählter Reihenfolge (mit Ausnahme der letzten Station) und in ihrem eigenem Tempo mit den einzelnen Stationen beschäftigen. Dabei sammeln sie pro Station auf ihrem Seepferdchen-Ausweis (Trainingsmaterial 1) Stempel. Erst ab einer von der Trainer:in festgelegten Stempelzahl können sie sich die Station „Ich gelobe Besserung!“ (Arbeitsmaterial 12) freispielen. Diese finale Station dient zur Planung konkreter Maßnahmen der digitalen Selbstverteidigung und bildet den Abschluss des Stationenlernens.

Hinweis zur Moderation

- Auf dem Seepferdchen-Pass sind **12 Stempelfelder.** Pro Station soll ein Feld abgestempelt werden. Da die Station „Ich gelobe Besserung“ als letzte absolviert werden soll, bietet es sich an, als Trainer:in vorzugeben, nach wie vielen Stempeln diese „freigespielt“ wird.



Hier geht es zur zentralen Downloadseite der Materialien: »bit.ly/dja-material«

Stationenübersicht mit Lernzielen & Hinweisen zur Vorbereitung

digitale jugend arbeit

Kompetenzbereich
Privatsphäre und Mündigkeit

Kompetenz
Schützen von personenbezogenen Daten und der Privatsphäre

Stufe
Einstieg

Methode
Stationenlernen

Ausstattung
Bildungsmaterialien + Kopfhörer empfohlen, Stempel und Stempelkissen

Dauer
90+ Minuten

Hier geht es zur zentralen Downloadseite der Materialien: »bit.ly/dja-material«

Data Dance
Die Teilnehmer:innen nähern sich auf niedrigschwellige Art und Weise dem Thema des Datenschutzes. *Systemabsturz* ist nach eigenen Angaben die beste und gleichzeitig schlechteste Datenschutz-Elektropunk-Band der Welt. Die Teilnehmer:innen tanzen zur Hit-Single *Daten, Daten, Daten*.

Datenscham
Die Teilnehmer:innen berechnen mithilfe des Datenscham-Rechners von *netzpolitik.org* ihren persönlichen Privacy-Score. Dadurch lernen sie, welche ihrer Verhaltensweisen den Datenschutz wie beeinflussen und können ihren eigenen Umgang mit Daten und Privatsphäre besser einschätzen.

Von Ende zu Ende ohne lose Enden
Die E-Mail ist immer noch eines der wichtigsten Kommunikationsmittel. An dieser Station lernen die Teilnehmer:innen datenschutzfreundliche Anbieter:innen kennen und setzen sich mit sicherer E-Mail-Kommunikation auseinander.

Der heilige Gral
In der eigenen E-Mail-Adresse laufen meist alle Stränge zusammen. Schließlich erfolgt die Anmeldung bei fast allen Onlinediensten über einen E-Mail-Account. Deshalb ist beim Schutze dieses „heiligen Grals" besondere Vorsicht geboten.

Anonyme Datenschutzsünder:innen
Einsicht ist oft der erste Schritt zur Besserung. Bei dieser anynomen Datenschutz-Beichtstelle können Teilnehmer:innen ihre Sünden beichten und von anderen Sünder:innen lernen.

qwertz
An dieser Station setzen sich die Teilnehmer:innen mit sicheren Passwörtern, deren Verwaltung und mit Zwei-Faktor-Authentifizierung auseinander. So viel vorab: „qwertz" ist kein sicheres Passwort!

Alternativlos?
Häufig sind die datenschutzfreundlichen Alternativen zu beliebten digitalen Anwendungen einfach nicht bekannt. Ziel dieser Station ist es, die Teilnehmer:innen dafür zu sensibilisieren und sie mit einigen Alternativen bekannt zu machen.

Von Füchsen und Zwiebeln
An dieser Station lernen Teilnehmer:innen datenschutzfreundliche Alternativen zu gängigen Browsern kennen.

Auch ein gutes Pferd muss trainiert werden!
Ein Browser bietet oft viele Möglichkeiten, ihn datenschutzfreundlicher einzustellen. Dafür bekommen die Teilnehmer:innen grundlegende Hinweise.

In aller Munde
Das Cookie-An-und-Ablehnen ist eine lästige Tätigkeit, die durch das manipulative Design vieler Cookie-Auswahl-Banner bewusst erschwert wird. An dieser Station lernen die Teilnehmer:innen, wie sie pragmatisch und datenschutzfreundlich mit Cookies umgehen können.

Datenschutz-Tuning
Browser-Plugins sind nützliche kleine Tools, auch wenn es um Datenschutz und Privatsphäre geht. Die Teilnehmer:innen lernen grundlegende Datenschutz-Plugins kennen.

Ich gelobe Besserung!
Der 28. Januar jeden Jahres ist Europäischer Datenschutztag. Die Teilnehmer:innen schreiben eine E-Mail an sich selbst, die auf den nächsten Datenschutztag datiert ist. Darin halten sie konkrete Schritte fest, die sie bis dahin umgesetzt haben möchten.

Seepferdchen-Ausweis:
Digitale Selbstverteidigung

digitale jugend arbeit

1 2 3 4 5 6

7 8 9 10 11 Bonus-Station * 12

zum Abstempeln oder Abhaken

*„Ich gelobe Besserung“

Seepferdchen-Ausweis:
Digitale Selbstverteidigung

digitale jugend arbeit

1 2 3 4 5 6

7 8 9 10 11 Bonus-Station * 12

zum Abstempeln oder Abhaken

*„Ich gelobe Besserung“

Data-Dance

Datenschutz-Elektropunk? Klingt merkwürdig, gibt es aber wirklich. *Systemabsturz* heißt das Berliner Duo, welches sich diesem ungewöhnlichen Genre verschrieben hat. Nach eigenen Angaben sind sie gleichzeitig die beste und schlechteste Band ihres Fachs – allerdings ist nur wenig darüber bekannt, wie viel Konkurrenz sie in ihrer Sparte tatsächlich haben. Immerhin aber liefern sie den Beweis dafür, dass Datenschutz tanzbar ist!

Schnapp dir ein paar Kopfhörer, klick auf den Link, oder gib den Titel *Daten, daten, Daten* auf *YouTube* ein und pack die besten Dance-Moves aus, zu denen du heute in der Lage bist:

youtube.com/watch?v=Zc8MF_SWKG0

Wenn Du ausgiebig und ausgelassen deinen ersten Data Dance gedanced hast, vergiss nicht, dich mit einem Seepferdchen-Punkt in deinem Ausweis zu belohnen!



Datenscham

Hast du Grund zu Datenscham? Oder bist du bereits ein echter Privacy-Ninja? *netzpolitik.org* hat – zum Zwecke eines hauseigenen Spendenaufrufes – einen Datenschamrechner entwickelt, mit dem du anhand von 10 kurzen Fragen deinen persönlichen Privacy-Score ermitteln kannst. Damit wirst du, ob nun mit oder ohne Spende, für Datenschutz und IT-Sicherheit sensibilisiert. Begib dich auf datenscham.org, um deinen eigenen Privacy-Score zu errechnen. Anschließend solltest du dir noch die Auswertung der einzelnen Fragen anschauen – keine Sorge, wirklich schämen brauchst du dich für deine Ergebnisse natürlich nicht.

Mit deinem persönlichen Privacy-Score im Gepäck, hast du dir den Seepferdchen-Punkt dieser Station mehr als verdient!

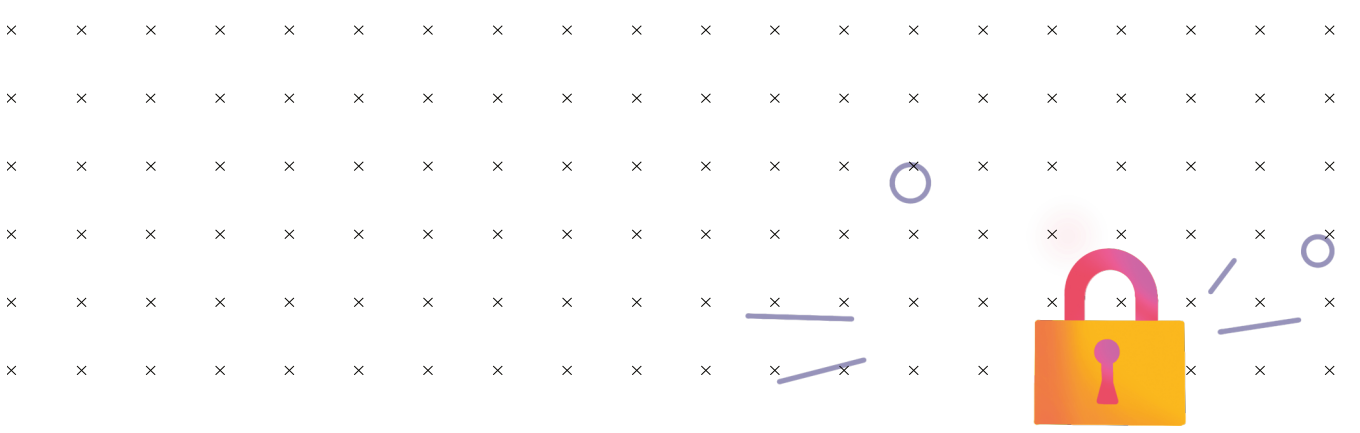


Kryptische Fernmeldung: von Ende zu Ende ohne lose Enden

Sichere, datensparsame E-Mail-Kommunikation fängt bei der Wahl des Anbieters an. Kostenlose Anbieter wie beispielsweise *Googlemail* sind zwar unentgeldlich nutzbar, ihre Dienste bezahlst du aber im Grunde mit dem Verlust deiner Privatsphäre und deinen Daten. Anbieter wie *mailbox.org* und *posteo.de* kosten dahingegend zwar etwas Geld, sind aber im Hinblick auf Datenschutz, Werbefreiheit und sogar auch Nachhaltigkeit die bessere Wahl.
Viele dieser E-Mail Anbieter bieten bezüglich der Datensicherheit sehr komfortable Lösungen. Bei *Posteo* zum Beispiel kann man per Klick alle Mails und Adressen so verschlüsseln, dass sie selbst vom Anbieter nicht mehr eingesehen werden können. Auch gibt es die Möglichkeit, eine sogenannte *TSL*-Garantie (*TSL* steht für *Transport Layer Security*) zu aktivieren, die sicherstellt, dass die Mail nur mit Hilfe dieser Verschlüsselung verschickt wird. Das bietet deiner E-Mail schon einen recht guten Schutz auf dem Transportweg.
TSL ist aber leider auch nicht der Weisheit letzter Schluss. Eine *Ende-zu-Ende-Verschlüsselung*, wie man es von manchen Messengern kennt, bietet *TSL* nicht. *Ende-zu-Ende-Verschlüsselung* bedeutet, dass wirklich nur der Absender und Empfänger die Nachricht entschlüsseln können. Auch für die Kommunikation per E-Mail kann so etwas eingerichtet werden – doch dafür musst du über die Möglichkeiten eines gutes E-Mail Anbieters hinaus selbst aktiv werden. In diesem – schon etwas in die Tage gekommenen, aber immer noch informativen – Video erfährst du die Grundprinzipien dafür:

https://vimeo.com/17610424

Um das alles in die Tat umzusetzen, braucht es ein bisschen Ruhe, Recherche und Zeit, dem man sich auch nach dem Seepferdchenabzeichen widmen kann. Aber wenn du bis hierhin gelesen und wahrscheinlich auch das Video angesehen hast, kannst du dir schon einen Punkt in deinem Seepferdchen-Pass gönnen!



Der heilige Gral

Die Sicherheit deiner E-Mail-Adresse hat im Hinblick auf den Schutz deiner persönlichen Daten oberste Priorität – denn meist laufen dort alle Stränge zusammen. Häufig lassen sich Passwörter, die in den sozialen Medien oder für andere digitale Dienstleistungen verwendet werden, über einen E-Mail-Account zurücksetzen. Der Zugang dazu ist deswegen so etwas wie ein heiliger Gral. Es empfiehlt sich daher, ein separates E-Mail Postfach zu haben, welches du nur zur Registrierung und zum Anlegen für Accounts, aber nicht zur Kommunikation benutzt. So ist diese Adresse im Idealfall niemandem außer dir bekannt. Außerdem solltest du natürlich ein einzigartiges Passwort benutzen und deinen Account mit einer Zwei-Faktor-Authentifizierung absichern. Was das ist und wieso das wichtig ist, erklärt dir die Station mit dem merkwürdigen Namen *qwertz*. Tatsächlich kommt es immer wieder vor, dass es Angreifer:innen gelingt, Datensätze von E-Mail Anbieter:innen zu erbeuten. Vielen Menschen ist oft gar nicht mehr bewusst, wo die eigene E-Mail-Adresse überall hinterlegt ist. Eine Spiele-App, eine Ahnenforschungswebsite, ein Carsharing-Anbieter, eine Datingplattform – die E-Mail-Adresse ist schnell ins Anmeldeformular eingegeben. Das Problem ist, dass bei jedem dieser Anbieter Daten auch verloren gehen können. Das kann durch Fahrlässigkeit der Plattform-Betreiber:innen, aber auch durch ausgeklügelte Hacking-Angriff geschehen. Um herauszufinden, ob persönliche Daten von dir erbeutet worden sind, kannst du dieses Tool des *Hasso-Plattner-Instituts* benutzen:

https://sec.hpi.de/ilc/search?

Wenn Du den Text oben gelesen und eventuell die Sicherheit deiner Mail-Adresse überprüft hast, vergiss nicht, dich mit einem Seepferdchen-Punkt in deinem Ausweis zu belohnen!



Anonyme Datenschutzsünder:innen

Datenschutz ist zumeist ein Problem des inneren Schweinehunds. Oft wissen wir, dass die Art und Weise, wie wir mit unseren Daten im digitalen Raum umgehen, eigentlich nicht optimal ist, ändern aber trotzdem nichts. Und weil Einsicht oft der erste Schritt zur Besserung ist, haben wir diese Beichtstelle für anynome Datenschutzsünder:innen eingerichtet. Vergeben werden müssen deine Sünden zwar nicht, aber vielleicht steigt deine Motivation, dich zu Besserung zu geloben, wenn du dich hier verewigt hast.

Nachdem du dich eingetragen hast, vergiss nicht, dich mit einem Seepferdchen-Punkt in deinem Ausweis zu belohnen

„Ich klicke bei Cookies oft einfach auf ›Akzeptieren‹.“

„Ich bin auf *Facebook*, obwohl ich weiß, dass es datenschutzrechtlich schwierig ist!“

qwertz

„qwertz“, also die ersten 6 Zeichen der obersten Buchstabenreihe deiner Tastatur, ist kein sicheres Passwort. Oft scheitert die Passwortsicherheit an der eigenen Faulheit oder Kreativität. Dabei sind gute Passwörter die einfachste und zugleich wichtigste Maßnahme, die du für die Sicherheit deiner Daten ergreifen kannst. In diesem Video erfährst du, worauf du beim Erstellen eines Passwortes unbedingt achten solltest:

https://www.youtube.com/watch?v=cqE1djdxipc

Eine gute Möglichkeit, deine Passwörter zu verwalten, sind digitale Passwortmanager. Diese Programme erlauben es dir, alle Passwörter in einem Dienst abzuspeichern und abzurufen. So musst du dir im Grunde nur ein Passwort merken, nämlich das für den Passwort-Manager.

Eine weitere wichtige Maßnahme ist es, wichtige Zugänge mit der sogenannten *Zwei-Faktor-Authentifizierung* abzusichern. Das kann zum Beispiel eine SMS auf dein Handy sein, durch die dir ein Code zugeschickt wird, den du zusätzlich zu deinem Passwort eingeben musst. Diese Maßnahme sichert meist durch Wissen (dein Passwort) und Besitz (in diesem Fall dein Handy) deinen Zugang ab, bezieht also zwei Faktoren ein und ist entsprechend sicherer.

Wenn du verstanden hast, warum du nie mehr „qwertz“ oder ähnliche Passwörter festlegen solltest, kannst du dir passwortfrei ein Seepferdchen in deinen Ausweis stempeln!

Von Füchsen und Zwiebeln

Dein Browser ist dein Tor zum World Wide Web. Mit jedem Schritt, den du innerhalb von diesem machst, hinterlässt du in jenem einen digitalen Fußabdruck. Sobald du das Internet betrittst, versammeln sich in deinem Browser daher die Unternehmen, die deine Aktivitäten im Internet tracken (wollen) und eröffnen einen kleinen Marktplatz. Der Schutz des Browsers ist deswegen eine der wichtigsten Maßnahmen, um dem Tracking deiner Daten entgegenzuwirken.

Wie sich manch eine:r vielleicht schon denkt, sind die gängigen Browser wie *Google Chrome*, *Microsoft Edge* oder *Safari* keine besonders datenschutzfreundlichen Fortbewegungsmittel. Da *Googles Chrome* von den Werbeeinnahmen lebt, welche der Browser mit den Daten seiner Nutzer:innen macht, verwendet er entsprechend viele Tracking Cookies. Auch *Edge*, der Browser von *Microsoft* behält sich in seinen Datenschutzeinstellungen das Recht vor, Daten an Dritte weiterzugeben. Sowohl *Microsoft* als auch *Apple* sind laut Edward Snowden außerdem Teil des *PRISM*-Überwachungsprogramms, welches Daten direkt an die *NSA* weitergibt.

Eine datenschutzfreundliche und funktionale Alternative ist *Mozilla Firefox*: Keiner der anderen großen Browser achtet so sehr auf Datenschutz wie *Firefox*. Außerdem wurde *Firefox* von der gemeinnützigen *Mozilla Foundation* entwickelt, ist also nicht darauf ausgelegt, möglichst viele Daten von dir zu ergattern, um sie an Werbetreibende zu verkaufen. Zudem ist *Firefox* ein *Open-Source*-Projekt – d. h. dass der Quelltext der Software für jeden zugänglich veröffentlicht ist und unabhängig kontrolliert werden kann. Auch in puncto Plugins (mehr dazu erfährst du bei der Station „Browser-Tuning“) kann *Firefox* punkten.

Wer die maximale Datenschutzerfahrung will, kann auch noch einen Schritt weitergehen und auf einen sogenannten Privacy-Browser zurückgreifen. Der wohl bekannteste und von Edward Snowden 2017 auf *Twitter* empfohlene Browser ist *Tor*, kurz für *The Onion Router*. Wenn du dich damit mit dem Internet verbindest, geschieht das durch das sogenannte *Tor*-Netzwerk – ein Netzwerk an Servern. Wenn du in *Tor* eine Website ansteuern willst, geschieht das über eine zufällige Route, die dich über mehrere Server des *Tor*-Netzwerks zum Ziel führt. Am Ende ist nicht mehr zurückzuverfolgen, wo der Startpunkt war, die IP-Adressse des Computers, mit dem du dich eingewählt hast, bleibt also anonym. Wer sich für einen solchen Privacy- Browser entscheidet, muss allerdings damit rechnen, beim Surf-Komfort einige Abstriche zu machen. Hier gilt es gut zwischen Sicherheit und Funktionalität abzuwägen.

Wenn du bis hierhin gelesen hast und dich in Zukunft vorzugsweise mit Hilfe von Füchsen und Zwiebeln ins Internet begeben willst, kannst du dich mit einem Stempel in deinem Seepferdchen-Pass belohnen!

Auch ein gutes Pferd muss trainiert werden

Schon mit einigen wenigen Einstellungen, kann ein Browser um einiges datenschutzfreundlicher werden. Bei einem Browser wie *Chrome* ist es unbedingt notwendig, diese Möglichkeit zu nutzen, da die Standardeinstellungen seinem Geschäftsmodell entsprechend maximal datenhungrig sind. *Firefox* hingegen bietet seinen Nutzer:innen bereits in den Standardeinstellungen einen guten Schutz der Privatsphäre. Da die Möglichkeiten der Datenschutzeinstellungen mit den Browsern zusammen variieren, lässt sich keine Pauschalempfehlung für datenschutzfreundliche Einstellungen abgeben. Trotzdem gibt es einige Punkte, die man bei den Datenschutzeinstellungen aller Browser beachten sollte. Dazu gehören:

- Datenschutzfreundliche Standardsuchmaschine festlegen (z. B. *DuckDuckGo*)
- Passwortspeicherung und andere Auto-Fill-Speicherfunktionen deaktivieren
- Browserdaten regelmäßig löschen
- Führen einer Chronik deaktivieren (wenn möglich, z. B. bei *Firefox*)
- Unnötige Cookies blockieren, insbesondere Drittanbieter-Cookies
- Pop-ups blockieren
- „Do-Not-Track“ Funktion aktivieren

Insgesamt ist es zu empfehlen, bei der Einrichtung des Standardbrowsers einmal alle Sicherheitseinstellungen Stück für Stück durchzugehen. Denn je nach Browser können potentiell auch noch weitere individuelle Schutzmaßnahmen für die Privatsphäre ergriffen werden.

Wenn du bis hierher gelesen und dir vorgenommen hast, deinen Browser mithilfe der richtigen Einstellung gegen den Krieg der Kekse zu rüsten, vergiss nicht, dich mit einem Seepferdchen-Punkt in deinem Ausweis zu belohnen.

In aller Munde

Cookies sind spätestens seit der Datenschutz-Grundverordnung (DSVGO) 2018 durch die Europäische Union in aller Munde. Oder nicht? Das Cookie-An-und-Ablehnen ist eine lästige Tätigkeit, die durch das manipulative Design vieler Cookie-Auswahl-Banner nicht gerade erleichtert wird. Wer in Eile ist, lässt sich daher gerne mal ein ganzes Dutzend Cookies andrehen, die sich mit dem persönlichen Datenschutz nicht besonders gut vertragen. Aber wie kann man Cookies so akzeptieren, dass man seine Daten schützt und die entsprechende Webseite trotzdem problemfrei besuchen kann? Und was sind Cookies überhaupt? Schau dir das folgende Video an, um herauszufinden, wie du Cookies pragmatisch und datenschutzfreundlich akzeptieren kannst:

youtube.com/watch?v=p4Y7l_RyZoM&t=1s

Wenn dir die Wortspiele nicht auf den Keks gegangen sind, vergiss nicht, dich mit einem Seepferdchen-Punkt in deinem Ausweis zu belohnen!



Datenschutz-Tuning

Deinen Browser kannst du mithilfe von kleinen Programmen tunen, sogenannte Plugins. Diese kleinen Helfer kannst du in deinem Browser installieren. Sie unterstützen dich bei allen möglichen Sachen, aber auch bei der digitalen Selbstverteidigung. Hier eine kleine Auswahl an Programmen, die für dich diesbezüglich nützlich sein könnten:

Privacy Badger
Der *Privacy Badger* ist ein Browser-Plugin, welches (auch unsichtbare) Tracker anhand von ihrem Verhalten automatisch erkennt und blockiert, wenn sie ohne deine Zustimmung deine Aktivitäten verfolgen. Das Plugin muss nur im Browser installiert werden und läuft sofort, ohne das weitere individuelle Einstellungen vorgenommen werden müssen. Der *Privacy Badger* bietet somit eine solide Datenschutzgrundlage fürs Surfen, auch für Menschen, die sich mit den technischen Details nicht auseinandersetzen wollen oder können. Gut zu wissen: Der *Privacy Badge*r ist von der *Electronic Frontier Foundation (EFF)* entwickelt worden, einer gemeinnützigen Organisation, die sich für zivilgesellschaftliche digitale Freiheiten einsetzt und keine ökonomischen Interessen verfolgt.

HTTPS Everywhere
Die Abkürzung HTTPS steht für „Hypertext Transfer Protocol Secure", das heißt: „Sicheres Hypertext-Übertragungsprotokoll". Durch diese Übertragungsprotokoll kommunizieren Webbrowser und Webserver miteinander. Im Gegensatz zum HTTP (das gleiche wie HTTPS nur ohne ‚Secure') verschlüsselt HTTPS diese Kommunikation. Wer durch HTTPS kommuniziert, ist also deutlich besser geschützt. Welches Übertragungsprotokoll benutzt wird, legt der:die Betreiber:in der jeweiligen Webseite fest. Das Browser Plugin *HTTPS Everywhere* ermöglicht es Nutzer:innen jedoch, die Kommunikation mit allen dafür geeigneten Webseiten durch HTTPS zu verschlüsseln, auch wenn diese das nicht von sich aus anbieten.

Click & Clean
Auch die besten Datenschutzeinstellungen halten einen Browser im Regelfall nicht davon ab, Informationen über seine Nutzer:innen zu sammeln. Mit dem Browser-Plugin *Click & Clean* können die Browser *Google Chrome* und *Firefox* einer Art Grundreinigung unterzogen werden. Nutzer:innen können dabei individuell einstellen, was genau zu welchem Zeitpunkt und unter welchen Bedingungen gelöscht werden soll. So können durch *Click & Clean* z. B. alle Browserdaten automatisch gelöscht werden, sobald der Browser geschlossen wird.

Wenn Du bis hierher gelesen hast und eventuell schon deine Daten getunet hast, vergiss nicht, dich mit einem Seepferdchen-Punkt in deinem Ausweis zu belohnen.

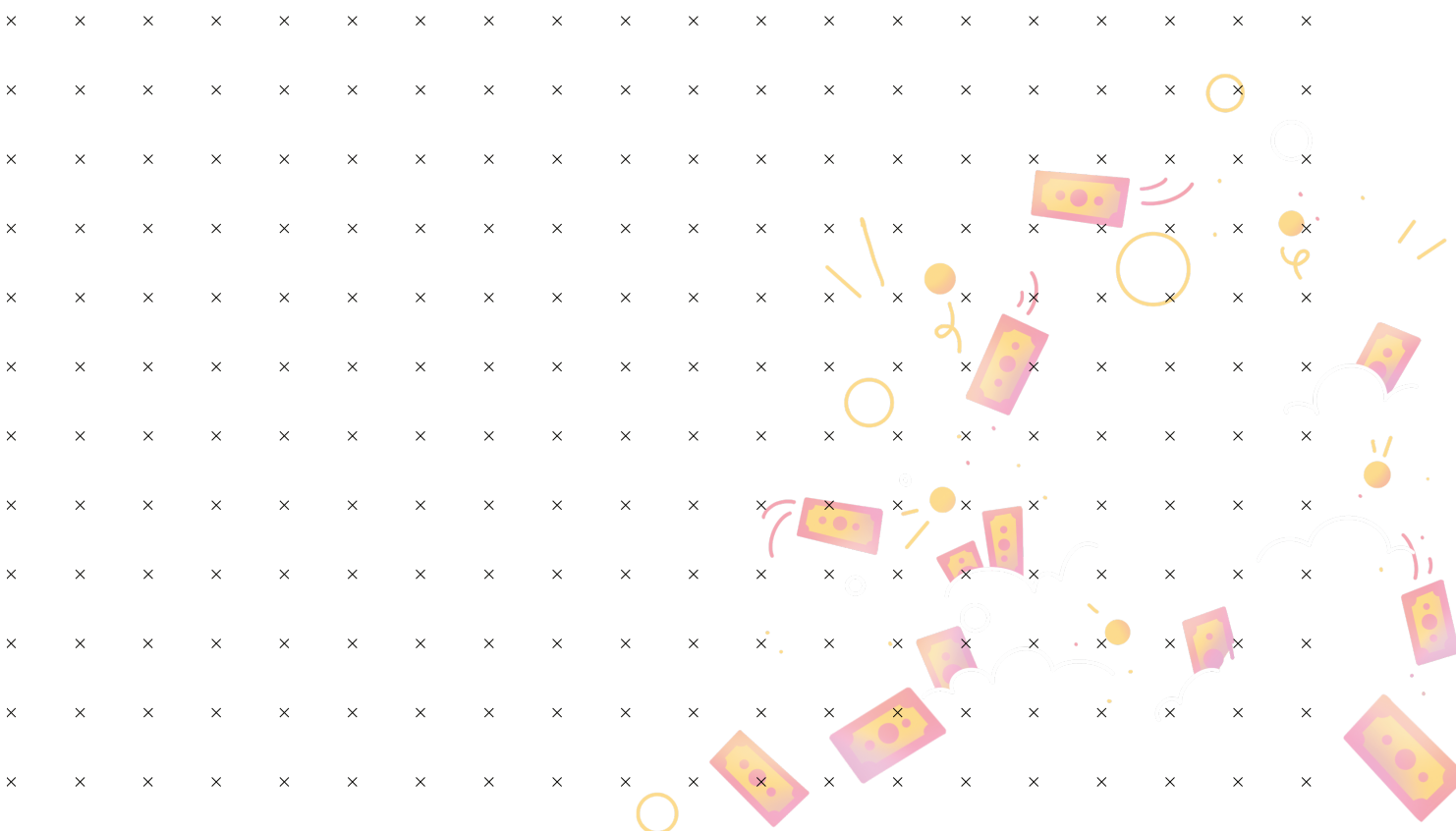
Alternativlos?

Häufig sind datenschutzfreundliche Alternativen zu bekannten digitalen Tools vorhanden, aber schlicht nicht bekannt. Es lohnt sich deshalb, einfach kurz zu recherchieren, welche datenschutzfreundlichen Alternativen es gibt, bevor man unbedacht wieder auf die datenhungrigeren Tools zurückgreift. Hier ist eine kleine unvollständige Liste solcher alternativen Optionen, die du in den meisten Fällen sogar kostenlos nutzen kannst:

Aus Sicht des Datenschutzes ist...

... *DuckDuckGo* besser als *Google*
... *nuudel* besser als *Doodle*
... *Vimeo* besser als *YouTube*
... *Signal* besser als *WhatsApp*
... *Posteo* besser als *GMX*-Mail
... *OpenStreetMap* besser als *Google Maps*
... *Jitsi* besser als *Zoom*
... *Mozilla Firefox* besser als *Google Chrome*
... *CryptPad* besser als *Google Docs*

Wenn du dir vorgenommen hast, deinen nächsten Termin zu nuudeln anstatt zu doodeln, kannst du dich mit einem Seepferdchen-Punkt belohnen!



Ich gelobe Besserung!

Am 28. Januar jedes Jahres ist der Europäische Datenschutztag. Der Tag wurde in Erinnerung an den 28. Januar 1981 gewählt, an dem die Europäische Datenschutzkonvention unterzeichnet wurde, und soll die Bürger:innen Europas für den Datenschutz sensibilisieren.

Nimm dir kurz Zeit, um zu überlegen, welche drei Datenschutzkniffe aus der Stationenarbeit du bis zu diesem Datum in deinem Alltag integrieren möchtest. Schreibe anschließend mithilfe von mailnudge.de eine Email an dich selbst, welche du auf den 28. Januar im nächsten Jahr datierst: Wünsche dir in dieser Email einen frohen Datenschutztag und erinnere dich selbst daran, was du bist dahin für den Schutz deiner personenbezogener Daten und deiner Privatsphäre getan haben möchtest.



Hurra, diese Welt geht unter!?



digitale jugend arbeit

@Trainer:innen · Moderationsbriefing · 4.2

Kompetenzbereich
Privatsphäre und Mündigkeit

Kompetenz
Schützen von personenbezogenen Daten und der Privatsphäre

Stufe
Vertiefung

Methode
Raumaufstellung + kreatives Schreiben

Ausstattung
Bildungsmaterialien

Dauer
90 Minuten

Ziel dieser Aufgabe ist, dass sich die Teilnehmer:innen mit wesentlichen Fragestellungen rund um das Thema Datenschutz auf einer gesellschaftlichen Ebene beschäftigen. Sie entwickeln ein Bewusstsein für Privatsphäre als politisches Thema und nähern sich kreativ an utopische und dystopische Daten-Zukünfte an.

Ablauf

Diese Übung besteht aus zwei Teilen. Im ersten Teil wird eine Raumaufstellung vorgenommen, bei welcher sich die Teilnehmer:innen zu wesentlichen Fragestellungen (Trainingsmaterial 1) der Privatsphäre und des Datenschutzes positionieren. Durch kurze Interviews im Anschluss an die einzelnen Fragen können erste Diskussionen entstehen. Der Fokus liegt an dieser Stelle darauf, die Teilnehmer:innen auf zentrale Fragestellungen aufmerksam zu machen.

Im zweiten Teil dieser Übung entwerfen die Teilnehmer:innen utopische und dystopische Zukunftsvisionen. Um den Teilnehmer:innen Anhaltspunkte zu geben, sind grundlegende Elemente der Geschichten jeweils vorgegeben (Trainingsmaterial 2). Zum Ende hin werden die Zukunftsszenarien im Plenum oder in Kleingruppen vorgestellt und diskutiert.

Hinweis zur Moderation

- Die Positionierungsfragen sind bewusst kontrovers formuliert, sodass sie Diskussionen auslösen. Bei der Raumaufstellung geht es vor allem darum, die Teilnehmer:innen auf grundlegende Ideen, Konzepte und Positionen aufmerksam zu machen und diese zu diskutieren. Durch geschicktes Nachfragen kann so ein fruchtbarer Austausch entstehen.



Hier geht es zur zentralen Downloadseite der Materialien: »bit.ly/dja-material«

Positionisierungsfragen

Big Data

- „Menschen sind die Daten-Sklaven einiger wenigen Tech-Konzerne!“
- „*Google*, *Facebook* und Co. müssen zerschlagen werden!“

Open data

- „Daten, die im Interesse der Allgemeinheit sind, sollten für alle Menschen ohne Einschränkung nutzbar sein!“
- „Daten müssen frei handelbares Privateigentum bleiben!“

Algorithmen

- „Algorithmen entscheiden in Zukunft über unser aller Leben!“
- „Algorithmen gehören verboten!“

Überwachung

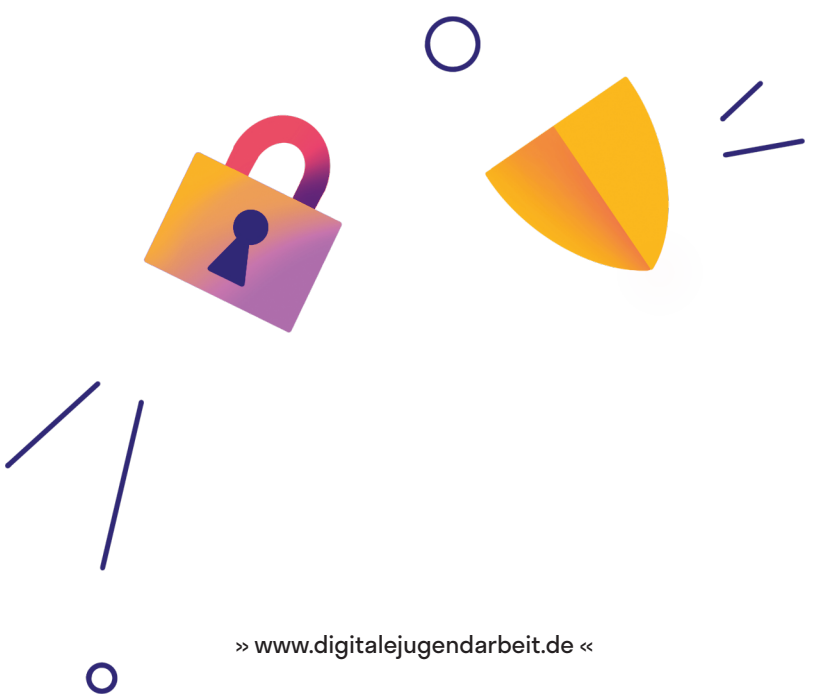
- „Wer nichts zu verbergen hat, muss sich auch nicht verstecken!“
- „Wer von Überwachung redet, darf vom Kapitalismus nicht schweigen.“

Post-Privacy

- „In einer vollständig digitalisierten Welt lässt sich Datenschutz nicht mehr umsetzen. Deshalb muss sich der Mensch der Technik anpassen und das althergebrachte Konzept von Privatsphäre aufgeben.“
- „Transparenz ist die Zukunft – ob nun für den Staat, für Unternehmen oder für das Individuum!“

Privacy by design

- „Mündige Bürger:innen sind selbst verantwortlich für den Schutz ihrer Daten.“
- „Datenhungrige Produkte oder Dienstleistungen sollten verboten werden.“



Szenarien

Szenario 1:
Du bist ein:e Politiker:in im Jahr 2030 und kandidierst für den Vorsitz der radikalen Datenschutzpartei. Schreib die Parteitagsrede!

Szenario 2:
Du bist ein:e Whistleblower:in im Jahr 2040 und veröffentlichst einen Insider-Bericht aus dem größten Tech-Konzern der Welt. Schreib den Insider-Bericht!

Szenario 3:
Du bist ein Mensch im Jahr 2050 und schreibst einen Brief an die Menschheit heute, um sie zu warnen. Schreib den Brief!

Briefpapier



.3

Schützen von Gesundheit und Wohlbefinden

Vermeiden von physischen und psychischen Gesundheitsrisiken beim Benutzen von digitalen Technologien. Sich vor möglichen Gefahren schützen, die in digitalen Umgebungen auftreten können. Möglichkeiten kennen, digitale Technologien zum eigenen Wohlbefinden einzusetzen und zur sozialen Inklusion beizutragen.



Illustration: Daria Rüttimann

Kompetenzbereich

Privatsphäre und Mündigkeit

Kompetenz

Schützen von Gesundheit und Wohlbefinden

Version 1.2
Lizenz: Namensnennung – Weitergabe unter gleichen Bedingungen 4.0 International (CC BY-SA 4.0)

Hier geht es zur zentralen Downloadseite der Materialien:
bit.ly/dja-material

Thematische Einführung

digitale jugend arbeit

Inhalt	Seite
Aufgabe ❶	s.47
Arbeitsmaterial 1	s.49
Arbeitsmaterial 2	s.50
Aufgabe ❷	s.51
Arbeitsmaterial 1	s.52
Arbeitsmaterial 2	s.53
Arbeitsmaterial 3	s.54

Du möchtest nur schnell etwas auf deinem Smartphone nachgucken und bemerkst plötzlich, dass du eine halbe Stunde rumgesurft hast. Du willst dir nur ein *YouTube* Video anschauen, kannst dich aber erst nach dem zehnten Video wieder vom Bildschirm lösen. Du öffnest eine Social Media App, weil du eine Popup Nachricht bekommen hast, und liest dann deinen gesamten Feed durch. Du arbeitest stundenlang im Homeoffice und dir fällt danach auf, dass du währenddessen krumm gesessen hast, deine Augen angestrengt sind und du kaum etwas getrunken hast. Die meisten von uns kennen diese Szenarien aus dem eigenen Alltag.

Uns allen ist längst bewusst, dass für den Großteil der Gesellschaft ein Alltag ohne Smartphones oder Internet mittlerweile undenkbar ist. Die gefühlten Anforderungen möglichst viel auf Social Media aktiv zu sein, aktuelle Geschehnisse weltweit im Auge zu behalten und immer erreichbar zu sein, können dabei schwer wiegen. Die grundsätzliche Möglichkeit, mit Freunden und Familie über Distanz in Kontakt zu bleiben, Nachrichten in Echtzeit zu verfolgen und bei Notfällen erreichbar zu sein, ist aber nichts schlechtes und hat viele Leben bereichert. Und genauso wie manche Apps und Tools uns unter Stress setzen und uns das Gefühl geben können, vielleicht etwas zu verpassen, wenn wir nicht aufmerksam bleiben, gibt es dagegen auch viele Apps und Tools, die uns helfen können, mal abzuschalten und uns wieder auf uns selbst zu besinnen.

Entscheidend ist im Endeffekt, wie wir unser Verhältnis zu diesen Anforderungen und Möglichkeiten gestalten. Darüber hinaus müssen wir uns ab und an bewusst die Zeit nehmen, um immer wieder neu zu evaluieren, was uns gerade gut und was uns weniger gut tut und daraufhin unseren Alltag und unser Verhalten anzupassen. Hier ein paar Fragen, die uns bei dieser Überprüfung helfen könnten:

Wie viel Zeit verbringe ich an einem Tag durchschnittlich an Bildschirmen? Wie leicht fällt es mir, mich vom Internet zu lösen, wenn ich mit dem fertig bin, was ich tun wollte? Fühle ich mich ohne mein Smartphone „nackt“? Kann ich mir ohne Probleme vorstellen einen Tag oder sogar ein Wochenende ohne Internet zu verbringen? Habe ich Probleme abends runterzukommen und einzuschlafen? Wie schnell gucke ich auf mein Smartphone, nachdem ich wach geworden bin? Vergesse ich im ganzen Digitalen, wie es meinem Körper dabei ergeht? Habe ich oft Nacken- und/oder Rückenschmerzen?

Wenn wir uns bei solchen Fragen doch – eventuell sogar etwas beschämt – eingestehen, dass wir uns eher ungesund am Internet und unseren Smartphones festklammern, ist es wahrscheinlich ein guter Zeitpunkt, um zu überlegen, was wir daran ändern könnten.

In diesem Modul bekommen die Teilnehmer:innen einen Raum, über ihre Gesundheit und Wohlbefinden in Bezug auf Digitales zu reflektieren. Gleichzeitig werden gemeinsam Lösungsansätze entwickelt. Im zweiten Abschnitt wird die gesellschaftliche Dimension von Gesundheit, Wohlbefinden und Digitalisierung in den Blick genommen.



Das Internet und Ich – eine Beziehungskrise?

digitale jugend arbeit

@Trainer:innen · Moderationsbriefing · 4.3

Kompetenzbereich
Privatsphäre und Mündigkeit

Kompetenz
Schützen von Gesundheit und Wohlbefinden

Stufe
Einstieg

Methode
Bewegtes Feedback, Recherche

Ausstattung
Bildungsmaterialien + Kopfhörer, Matten

Dauer
90 Minuten

Ziel dieser Aufgabe ist es, dass die Teilnehmer:innen sich über ihr eigenes Verhältnis zu Smartphones und dem Internet bewusst werden und Konzepte kennenlernen, die dabei unterstützen können, dieses Verhältnis aktiv und gut zu gestalten.

Ablauf

Diese Aufgabe besteht aus drei Teilen – eine Reflexionsübung zum Einstieg, eine Rechercheaufgabe zum tieferen Eintauchen und eine Entspannungsübung zum Ausklang.

Die Reflexionsübung ist angelehnt an die Methode des bewegten Feedbacks. Die Teilnehmer:innen reagieren damit auf ausgewählte Reflexionsfragen aus Trainingsmaterial 1. Ihre Reaktionen können aus Körperbewegungen, -haltungen und/oder Geräuschen bestehen.

Anschließend ziehen die Teilnehmer:innen einzeln oder in Kleingruppen ein Thema aus Arbeitsmaterial 1, recherchieren zu dem jeweiligen Thema und überlegen sich, ob und wie dies ihnen im Alltag dabei helfen könnte, ihre Gesundheit und ihr Wohlbefinden zu schützen. Daraufhin besprechen die Teilnehmer:innen im Plenum, was sie herausgefunden haben und wie es ihnen helfen könnte.

Abschließend ziehen sie eine Entspannungsinspiration aus dem Arbeitsmaterial 2 und folgen den jeweiligen Anweisungen.

Hinweise zur Moderation

- Die Arbeitsmaterialien 1 und 2 müssen vor Beginn der Aufgabe ausgeschnitten werden. Je nach Gruppengröße muss das Arbeitsmaterial 2 eventuell mehrmals ausgedruckt und ausgeschnitten werden.
- Für die Entspannungsübungen aus dem Arbeitsmaterial 2 lohnt es sich, wenn die Teilnehmer:innen kleine Matten oder ähnliches zur Verfügung haben, um sich währenddessen entspannt hinlegen oder setzen zu können.
- Die Reflexionsfragen aus Trainingsmaterial 1 sind eine Liste an Vorschlägen, die nicht in ihrer Gänze abgefragt werden müssen. Bei jeder Durchführung können eine Handvoll aus den drei thematischen Blöcken ausgesucht oder durch eigene Fragen ergänzt werden.

Hier geht es zur zentralen Downloadseite der Materialien:
»bit.ly/dja-material«



Reflexionsfragen: Fragensammlung zum Vorlesen
Wie fühlst du dich, wenn...

In Gedanken beim Handy:

... du an all die E-Mails, Nachrichten oder SMS denkst, die du noch nicht beantwortet hast?
... du nach deinem Handy greifen willst, es aber nicht da ist?
... du mit einer Person unterwegs bist, die alle paar Minuten auf ihr Handy schaut?
... du merkst, dass du stundenlang nicht auf dein Handy geschaut hast?
... du dein Handy Zuhause vergessen hast?

Digitales Soziales:

... du eine Benachrichtigung auf dein Handy bekommst?
... du denkst, dass dein Handy vibriert, nachschaust, dann aber doch keine Nachricht bekommen hast?
... du an die Benachrichtigungssymbole und -töne von sozialen Netzwerken und Messengern auf deinem Handy denkst?
... du den Neewsfeed in einem sozialen Netzwerk refreshst und dir neue Inhalte angezeigt werden?
... du etwas postest und sehr viel Bestätigung in Form von Likes und Kommentaren bekommst?
... du etwas postest und kaum jemand darauf reagiert?
... du Hass, Gewalt oder Mobbing im Internet erlebst?
... du dich für mehrere Stunden online im Leben von anderen Menschen vertieft hast und plötzlich merkst, dass du eigentlich alleine in deinem Zimmer sitzt?
... du im Newsfeed eines sozialen Netzwerkes mit den Erfolgen von anderen Menschen bombardiert wirst?
... du ein lustiges Katzenvideo gesehen hast?

Die Zeit verfliegt:

... du nur kurz gucken wolltest, wie viel Uhr es ist, und auf einmal merkst, dass du zwei Stunden an deinem Handy gehangen hast?
... du acht Stunden oder länger vor einem Bildschirm gesessen hast?
... du eine Serie bis tief in die Nacht gebingewatched hast?
... du im Internet prokrastinierst, ganz genau weißt, dass du eigentlich etwas anderes tun solltest, es aber einfach nicht schaffst, dich vom Bildschirm zu lösen?
... du statt ein Problem zu lösen, zwei Stunden lang mögliche Lösungen googelst, nur um dann nichts davon zu tun?
... du für mehrere Monate im Homeoffice gesessen hast?



Inputthemen zum Ausschneiden (4x)

Flug-/Konzentrationsmodus	Flug-/Konzentrationsmodus
Focus -To-Do (App)	Focus -To-Do (App)
Digital Detox	Digital Detox
Dopamin Fasten	Dopamin Fasten
Dynamisches Sitzen	Dynamisches Sitzen
Blaulichtfilter	Blaulichtfilter
Bildschirmzeit/Anzahl der Entsperrungen kontrollieren	Bildschirmzeit/Anzahl der Entsperrungen kontrollieren

Flug-/Konzentrationsmodus	Flug-/Konzentrationsmodus
Focus -To-Do (App)	Focus -To-Do (App)
Digital Detox	Digital Detox
Dopamin Fasten	Dopamin Fasten
Dynamisches Sitzen	Dynamisches Sitzen
Blaulichtfilter	Blaulichtfilter
Bildschirmzeit/Anzahl der Entsperrungen kontrollieren	Bildschirmzeit/Anzahl der Entsperrungen kontrollieren

Entspannungsinspirationen zum Ausschneiden

Weightless – Macaroni Union
„Weightless" von *Macaroni Union* ist von Neurowissenschaftler:innen zum entspannendsten Lied der Welt erklärt worden. Schnapp dir ein paar Kopfhörer, lehn dich zurück und tauche für acht Minuten in die Musik ein. marconiunion.bandcamp.com/album/weightless-ambient-transmissions-vol-2

---

7 Mind
Schnapp dir ein paar Kopfhörer, installiere die hier verlinkte App und schau dich um, was diese so zu bieten hat. Hör dafür mindestens in eine Audiodatei hinein. 7mind.de/download

---

Headspace
Schnapp dir ein paar Kopfhörer, installiere die hier verlinkte App und schau dich um, was diese so zu bieten hat. Hör dafür mindestens in eine Audiodatei hinein.

iOS: apps.apple.com/de/app/headspace-meditation-schlaf/id493145008
Android: play.google.com/store/apps/details?id=com.getsomeheadspace.android&hl=de&gl=US

Calm
Schnapp dir ein paar Kopfhörer, installiere die hier verlinkte App und schau dich um, was diese so zu bieten hat. Hör dafür mindestens in eine Audiodatei hinein.

iOS: apps.apple.com/de/app/calm/id571800810
Android: play.google.com/store/apps/details?id=com.calm.android&hl=de&gl=US

Smiling Mind
Schnapp dir ein paar Kopfhörer, installiere die hier verlinkte App und schau dich um, was diese so zu bieten hat. Hör dafür mindestens in eine Audiodatei hinein.

iOS: apps.apple.com/us/app/smiling-mind/id560442518
Android: play.google.com/store/apps/details?id=com.smilingmind.app&hl=de&gl=US

Progressive Muskelentspannung
Schnapp dir ein paar Kopfhörer, schaue das verlinkte Video an und lass deine Muskeln entspannen: youtube.com/watch?v=Qz-3YHaeGb4

Atemübung
Schnapp dir ein paar Kopfhörer, schaue das verlinkte Video an und mache ein paar Atemübungen zur Entspannung. youtube.com/watch?v=NJn5FOI4Mng

Ein Unglück designt sich nicht von allein

digitale jugend arbeit

@Trainer:innen · Moderationsbriefing · 4.3

Kompetenzbereich
Privatsphäre und Mündigkeit

Kompetenz
Schützen von Gesundheit und Wohlbefinden

Stufe
Vertiefung

Methode
Gruppenarbeit

Ausstattung
Bildungsmaterialien

Dauer
90 Minuten

Ziel der Aufgabe ist es, die Teilnehmer:innen dafür zu sensibilisieren, dass digitale Angebote häufig durch Design darauf ausgelegt sind, ihre Aufmerksamkeit zu binden. Die Teilnehmer:innen lernen, sich in die Logiken der Aufmerksamkeitsökonomie hineinzudenken und entwickeln gemeinsam individuelle und gesellschaftliche Widerstandsmöglichkeiten.

Ablauf

Die Teilnehmer:innen finden sich zunächst in Kleingruppen zusammen. In diesen überlegen sie sich den Szenarien in den Arbeitsmaterialien 1, 2 und 3 entsprechend Strategien, mit welchen psychologischen Tricks sie ihre Zielgruppen zugunsten des maximalen Konsums ihrer jeweiligen Produkte manipulieren können. Ihre Ergebnisse halten sie auf Plakaten fest, welche anschließend im Plenum präsentiert werden. Nach jeder Präsentation besprechen die Teilnehmer:innen im Plenum, auf welche Weisen individueller und gesellschaftlicher Widerstand gegen die präsentierten psychologischen Tricks geleistet werden kann.

Folgende Fragen können dabei behandelt werden:

1) Sind die präsentierten Strategien mir in meinem Alltag bereits begegnet? Wenn ja: Welche Erfahrungen habe ich mit ihnen gemacht?
2) Wie kann ich meine Gesundheit und mein Wohlbefinden vor digitalen Angeboten schützen, die per Design darauf angelegt sind, meine Aufmerksamkeit zu binden und süchtig zu machen?
3) Wie kann ich andere Menschen dabei unterstützen, ihre Gesundheit und ihr Wohlbefinden bei der Nutzung solcher digitalen Angebote zu schützen?
4) Welche Möglichkeiten gibt es, sich politisch gegen digitale Angebote zu engagieren, deren Geschäftsmodell auf gesundheitsschädlichen psychologischen Tricks basiert?

Hinweise zur Moderation

- Ein Fokus dieser Aufgabe liegt auf den Designtechniken, welche digitale Angebote nutzen, um die Aufmerksamkeit ihrer Konsument:innen zu binden. Es macht daher Sinn, den Teilnehmer:innen bunte und vielfältige Materialien zur kreativen Gestaltung ihrer Plakate zur Verfügung zu stellen und sie dazu aufzufordern, bei der Entwicklung und Visualisierung ihrer Strategien einen besonderen Schwerpunkt auf Designfragen zu legen.

- Unter cdn.ttc.io/s/datadetoxkit.org/youth/Data-Detox-x-Youth_DE.pdf befindet sich ein Daten-Detox-Kit, welches 2017 für den *Glass Room London* erarbeitet, von *Tactical Tech* kuratiert und von *Mozilla* präsentiert wurde. Das Arbeitsmaterial mit dem Titel „So überlebst du eine Trennung...von deinem Handy“ ist eine gute Ergänzung zu dieser Aufgabe und kann je nach Zeit und Schwerpunktsetzung ausgedruckt und z. B. als individuelle Abschlussreflektion verwendet werden. Die Website dazu ist datadetoxkit.org/de.

Hier geht es zur zentralen Downloadseite der Materialien: »bit.ly/dja-material«



Arbeitsauftrag Soziales Netzwerk

Ihr arbeitet für ein großes soziales Netzwerk. Euer Job ist es, euch diverse Strategien zu überlegen, wie ihr die Nutzer:innen dazu bringen könnt, so viel Lebenszeit wie möglich in eurem sozialen Netzwerk zu verbringen. Ihr müsst das Rad dabei nicht unbedingt neu erfinden – es reicht, wenn ihr auf die Strategien zurückgreift, die euch diesbezüglich im Alltag begegnen und euch diese bewusst macht.

Dabei könnt ihr folgende Fragen mit einbeziehen:

- Überlegt euch, welche Bedürfnisse, Wünsche und Träume eure Nutzer:innen haben könnten. Wie könnt ihr dieses Wissen nutzen, um sie dazu zu bringen, so viel Zeit wie möglich in eurem Netzwerk zu verbringen?
- Überlegt euch, welche Schwächen, Ängste und Unsicherheiten eurer Nutzer:innen haben könnten. Wie könnt ihr dieses Wissen nutzen, um sie dazu zu bringen, so viel Zeit wie möglich in eurem Netzwerk zu verbringen?
- Was wisst ihr über Psychologie? Wie könnt ihr psychologische Tricks nutzen, um eure Nutzer:innen dazu zu bringen, so viel Zeit wie möglich in eurem Netzwerk zu verbringen?
- Was wisst ihr über Sucht? Wie muss euer Netzwerk gestaltet sein, um so süchtig wie möglich zu machen?
- Wie muss der Newsfeed designt sein, um Nutzer:innen dazu zu bringen, ihn immer wieder neu zu aktualisieren?
- Wie müssen Benachrichtigungen designt sein, um die Aufmerksamkeit der Nutzer:innen zurückzugewinnen, wenn sie gerade nicht im Netzwerk aktiv sein?
- Ihr wollt, dass eure Nutzerinnen, wenn sie ein Problem haben oder es ihnen schlecht geht, als Bewältigungsstrategie auf die Nutzung eures Netzwerkes zurückgreifen. Überlegt euch eine Strategie, mit welcher ihr eure Nutzer:innen auf diese Art und Weise an euer Netzwerk binden könnt.

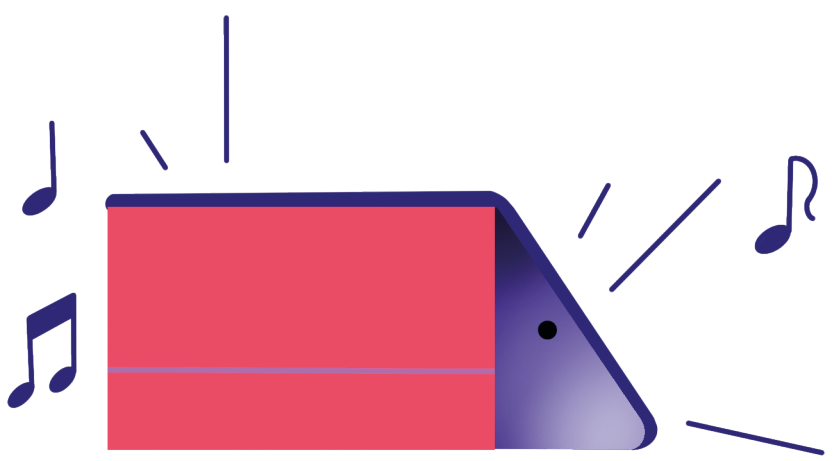


Arbeitsauftrag App

Ihr entwickelt eine App. Euer Job ist es, euch diverse Strategien zu überlegen, wie ihr die Nutzer:innen dazu bringen könnt, so viel Lebenszeit wie möglich in eurer App zu verbringen. Ihr müsst das Rad dabei nicht unbedingt neu erfinden – es reicht, wenn ihr auf die Strategien zurückgreift, die euch diesbezüglich im Alltag begegnen und euch diese bewusst macht.

Dabei könnt ihr folgende Fragen mit einbeziehen:

- Überlegt euch, welche Bedürfnisse, Wünsche und Träume eure Nutzer:innen haben könnten. Wie könnt ihr dieses Wissen nutzen, um sie dazu zu bringen, so viel Zeit wie möglich in eurer App zu verbringen?
- Überlegt euch, welche Schwächen, Ängste und Unsicherheiten eurer Nutzer:innen haben könnten. Wie könnt ihr dieses Wissen nutzen, um sie dazu zu bringen, so viel Zeit wie möglich in eurer App zu verbringen?
- Was wisst ihr über Psychologie? Wie könnt ihr psychologische Tricks nutzen, um eure Nutzer:innen dazu zu bringen, so viel Zeit wie möglich in eurer App zu verbringen?
- Was wisst ihr über Sucht? Wie muss eure App designt sein, um so süchtig wie möglich zu machen?
- Wie müssen Benachrichtigungen designt sein, um die Aufmerksamkeit der Nutzer:innen zurückzugewinnen, wenn sie gerade nicht in der App aktiv sein?
- Ihr wollt, dass eure Nutzer:innen, wenn sie ein Problem haben oder es ihnen schlecht geht, als Bewältigungsstrategie auf die Nutzung eurer App zurückgreifen. Überlegt euch eine Strategie, mit welcher ihr eure Nutzer:innen auf diese Art und Weise an eure App binden könnt.



Arbeitsauftrag Videostreamingdienst

Ihr arbeitet für einen großen Videostreamingdienst. Euer Job ist es, euch diverse Strategien zu überlegen, wie ihr die Nutzer:innen dazu bringen könnt, so lange wie möglich Videos am Stück auf eurer Plattform zu schauen. Ihr müsst das Rad dabei nicht unbedingt neu erfinden – es reicht, wenn ihr auf die Strategien zurückgreift, die euch diesbezüglich im Alltag begegnen und euch diese bewusst macht.

Dabei könnt ihr folgende Fragen mit einbeziehen:

- Wie muss die Startseite designt sein, damit Nutzer:innen möglichst schnell ein Video finden, was sie anspricht?
- Was wird auf eurer Plattform angezeigt, wenn ein Video endet?
- Was wisst ihr über Psychologie? Wie könnt ihr psychologische Tricks nutzen, um eure Nutzer:innen dazu zu bringen, so viel Zeit wie möglich auf eurer Plattform zu verbringen?
- Was wisst ihr über Sucht? Wie muss eure Plattform gestaltet sein, um so süchtig wie möglich zu machen?
- Wie müssen Benachrichtigungen designt sein, um die Aufmerksamkeit der Nutzer:innen zurückzugewinnen, wenn sie gerade nicht auf der Plattform aktiv sind?
- Ihr wollt, dass eure Nutzer:innen, wenn sie ein Problem haben oder es ihnen schlecht geht, als Bewältigungsstrategie auf die Nutzung eurer Plattform zurückgreifen. Überlegt euch eine Strategie, mit welcher ihr eure Nutzer:innen auf diese Art und Weise an eure Plattform binden könnt.




15:04
3405
NIMM AB!
KLICK!
DRINGEND:

.4

Umweltschutz und Digitalisierung

Sich über den Einfluss digitaler Technologien auf die Umwelt bewusst sein.



Illustration: Daria Rüttimann

Kompetenzbereich

Privatsphäre und Mündigkeit

Kompetenz

Umweltschutz und Digitalisierung

Version 1.2
Lizenz: Namensnennung – Weitergabe unter gleichen Bedingungen 4.0 International (CC BY-SA 4.0)

Hier geht es zur zentralen Downloadseite der Materialien:
bit.ly/dja-material

Thematische Einführung

digitale jugend arbeit

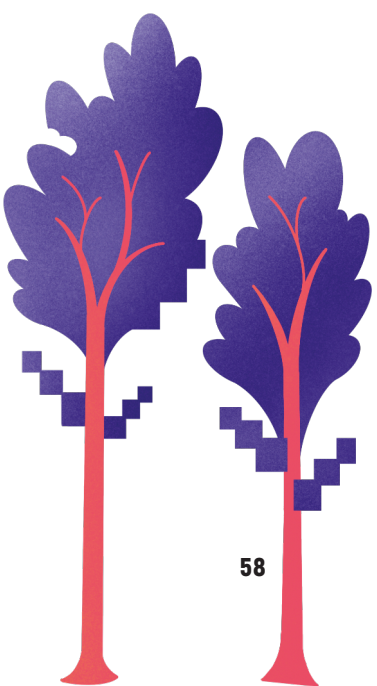
Inhalt	Seite
Aufgabe ❶	s.59
Trainingsmaterial 1	s.60
Aufgabe ❷	s.61
Arbeitsmaterial 1	s.62

Die Digitalisierung unter dem Gesichtspunkt des Klimaschutzes nachhaltig zu gestalten, wird eine der großen gesellschaftliche Aufgaben des nächsten Jahrzehnts sein. Zwar werden durch Digitalisierung einerseits Ressourcen geschont: Denken wir etwa an die Berge Papier, die früher ein einfaches Büro verbraucht hat. Auch kann durch Videokonferenzen der eine oder andere Flug eingespart werden und durch technischen Fortschritt entstehen immer wieder klimaschützende Innovationen. Trotzdem greift es zu kurz, Digitalisierung nur als Fortschritt und Lösung zu begreifen und nicht als Teil des Problems.

Je mehr Lebensbereiche digitalisiert werden, desto größer wird auch der digitale CO^6-Fußabdruck. Das zeigt sich anschaulich am Beispiel von *Netflix, Amazon Prime* und Co. Die Streaminganbieter haben alte Medien wie DVDs so gut wie obsolet werden lassen und auch Videotheken fast vollständig aus dem Stadtbild verdrängt. Das Binge-Watching an einem regnerischen Sonntag hat jedoch auch Schattenseiten. Um den CO^6-Fußabdruck dieses Vergnügens zu berechnen, müsste man mit der Filmproduktion anfangen, die Speicherung der Serien und Filme genauso mit einbeziehen wie deren Übertragung vom Server bis zum Endgerät, um schlussendlich noch den Stromverbrauch des Endgerätes zu beziffern. Da kommt so einiges zusammen. Ganz genau benennen kann man das nicht – 30 Minuten netflixen, so heißt es jedoch immer wieder, stößt so viel CO^6 aus wie 6 Kilometer Autofahren. Dieses anschauliche Beispiel kann man auch auf andere digitale Anwendungen und Dienste übertragen. Überall wo Daten gespeichert, abgerufen und übertragen werden fällt potentiell ein hoher Energiebedarf an.

Die gute Nachricht ist jedoch, dass viele Technologien immer umweltfreundlicher werden. Mobile Daten werden beispielsweise beim Umstieg von 3G auf 4G deutlich klimaschonender. Wenn wir der Umwelt etwas Gutes tun wollen, sollten wir dennoch nicht so viel mobile Daten konsumieren, denn der Internetzugang über WLAN ist immer noch am nachhaltigsten. Überhaupt: Wenn man sich informiert, wird man schnell feststellen, dass man als Privatperson so einiges dafür tun kann, seinen eigenen digitalen CO^6-Fußabdruck zu minimieren: Geräte gebraucht kaufen und richtig entsorgen, Reparaturwerkstätten besuchen, statt alte Geräte wegzuschmeißen, genau überlegen, ob man Videotelefonie braucht oder ob der einfache Anruf ausreicht usw.

Die Verantwortung allein den Konsument:innen zu übertragen greift allerdings zu kurz. Die nachhaltige Gestaltung der Digitalisierung ist eine gesamtgesellschaftliche Aufgabe. Den Weg dahin muss deshalb politisch und demokratisch ausgehandelt werden. Ganz in diesem Sinne nähert sich dieses Modul dem Thema Digitalisierung und Nachhaltigkeit sowohl auf einer individuellen wie auch auf einer gesellschaftlichen Ebene an.



Familie Freiraum und die digitale Nachhaltigkeit

digitale jugend arbeit

@Trainer:innen · Moderationsbriefing · 4.4

Kompetenzbereich
Privatsphäre und Mündigkeit

Kompetenz
Umweltschutz und Digitalisierung

Stufe
Einstieg

Methode
Stille Diskussion

Ausstattung
Bildungsmaterialien

Dauer
90 Minuten

Ziel dieser Übung ist es, die Teilnehmer:innen dafür zu sensibilisieren, welche Auswirkungen ihr digitaler Alltag auf Umwelt und Klima hat. Gemeinsam erarbeiten sie zudem praktische Möglichkeiten, den eigenen digitalen CO^6-Fußabdruck zu reduzieren.

Ablauf

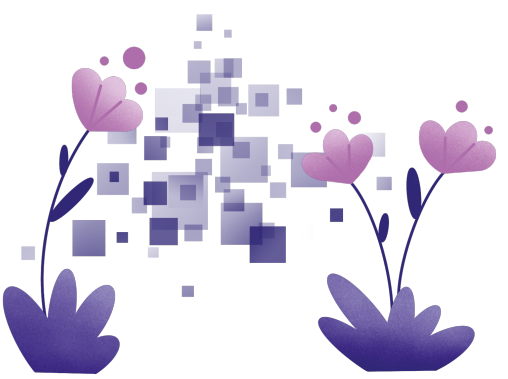
Diese Aufgabe ist in ein narratives Szenario eingebettet. Anhand der fiktiven Familie Freiraum (Mutter Miriam, Vater Volker, Teenager Toni, Kind Kai) werden alltagsnahe Szenarien erzählt (siehe Trainingsmaterial 1). Diese sind so im Raum verteilt, dass die Teilnehmer:innen sie schriftlich kommentieren können.
Die Teilnehmer:innen bearbeiten die Szenarien in frei gewählter Reihenfolge und in ihrem eigenen Tempo in einer stillen Diskussion. Dazu recherchieren sie eigenständig im Internet und halten ihre Rechercheergebnisse neben den Szenarien fest. Wenn alle Szenarien bearbeitet worden sind, bietet sich ein Gallery-Walk zum Abschluss an.

Hinweis zur Moderation

- Es ist vorteilhaft, das narrative Szenario um Familie Freiraum zu Beginn der Übung mit einer kurzen Erklärung einzuführen.

Hier geht es zur zentralen Downloadseite der Materialien: »bit.ly/dja-material«





Szenarien Familie Freiraum

Diese Szenarien können beispielsweise auf A4-Papier übertragen werden und zur Bearbeitung durch die Teilnehmer:innen auf Metaplan-Stellwänden angebracht werden:

- Teenager Toni regt sich auf, dass Kind Kai *YouTube*-Videos immer über mobile Daten anschaut. Das sei schlecht für's Klima. Hat Toni Recht? Was könnte Kind Kai tun, um guten Gewissens auch unterwegs Videos anzuschaun?

- Der Laptop von Vater Volker ist kaputt. Er möchte lieber seinen Laptop reparieren, als einen neuen zu kaufen, weiß aber nicht wie. Was kann Vater Volker tun?

- Mutter Miriam freut sich, weil durch die Digitalisierung nicht mehr so viel Ressourcen für Blue-rays, DVDs und Videokassetten verschwendet werden. Teenager Toni sieht Streaming aber aus ökologischer Sicht kritisch. Warum?

- Teenager Toni möchte ein neues Smartphone. Vater Volker wendet ein, sie soll ihr altes Handy weiter benutzen, um Ressourcen zu schonen. Welche knappen Ressourcen stecken in Smartphones? Wie lang sollte die Nutzungsdauer eines Handys sein? Welche Kompromissvorschläge könnte Vater Volker Teenager Toni machen?

- Vater Volker freut sich: Seitdem er eine Cloud hat, muss er für die Urlaubsfotos keine externen Festplatten mehr befüllen. Aber sind Clouds auch nachhaltig? Und gibt es Unterschiede zwischen den Anbietern?

- Mutter Miriam weist Vater Volker auf sein volles E-Mail-Postfach hin. Wenn er es regelmäßig leeren würde, wäre das gut fürs Klima. Vater Volker wundert sich – was hat denn sein E-Mail-Account damit zu tun?

- Kind Kai will beim Müll rausbringen auch die defekten Elektrogeräte entsorgen. Mutter Miriam sagt, dass diese Geräte nicht in den normalen Müll gehören. Hat Mutter Miriam Recht? Und wo gehören die Geräte sonst hin?

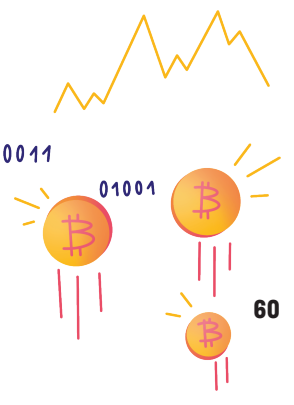
- Teenager Toni will sein Taschengeld in Bitcoins investieren. Er findet digitale Währung aus Perspektive der Nachhaltigkeit besser. Hat Teenager Toni Recht?

- Mutter Miriam kritisiert, dass Teenager Toni immer Videotelefonate macht, obwohl eigentlich meistens ein Telefongespräch ausreicht. Ist die Kritik von Mutter Miriam aus Sicht des Klimaschutzes berechtigt?

- Teenager Toni erzählt Mutter Miriam von Suchmaschinen, die sich für Nachhaltigkeit einsetzen. Welche gibt es? Und wie setzen sie sich für Nachhaltigkeit ein?

- Familie Freiraum beschließt, eine Liste der besten digitalen Klimaschutzmaßnahmen für den Alltag anzulegen. Ergänze die Liste:

    - Songs als Audio abspielen, statt als Video über *YouTube* zu streamen oder das Video in geringerer Auflösung anschauen



Wahlkampf: Digital und Nachhaltig – aber wie?

digitale jugend arbeit

@Trainer:innen · Moderationsbriefing · 4.4

Kompetenzbereich
Privatsphäre und Mündigkeit

Kompetenz
Umweltschutz und Digitalisierung

Stufe
Vertiefung

Methode
Kleingruppenarbeit

Ausstattung
Bildungsmaterialien

Dauer
90 Minuten

Ziel dieser Übung ist es, dass sich Teilnehmer:innen mit gesellschaftlichen Fragestellungen betreffs Digitalisierung und Nachhaltigkeit auseinandersetzen. Dabei entwickeln sie eigene Zukunftsvision für eine nachhaltige digitale Zukunft.

Ablauf

In dieser Übung gründen die Teilnehmer:innen in Kleingruppen ihre eigene fiktive Klimaschutzpartei. Als thematischer Einstieg dienen dabei Postkarten (Arbeitsmaterial 1), die jede Kleingruppe als Gesprächsimpuls nutzen kann. Diejenige Postkarte, die in der Gruppe am meisten Resonanz ausgelöst hat, soll dabei als Ausgangspunkt für eine Recherche, das Wahlprogramm und schließlich die Parteigründung genutzt werden. Am Ende dieses Prozesses gestaltet jede Gruppe ein eigenes Plakat, auf dem folgende Punkte ersichtlich sind:

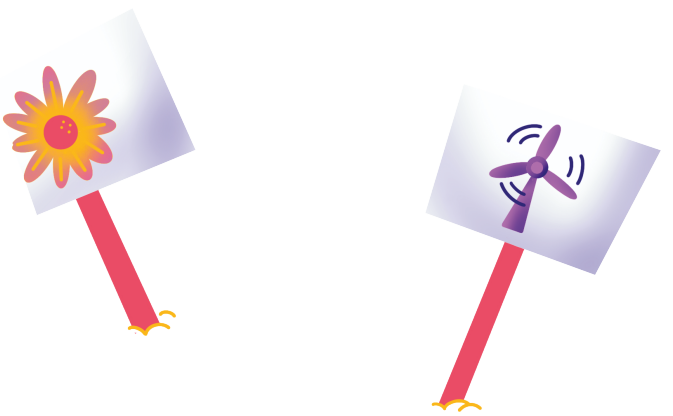
1) Name der Partei
2) Eventuell ein Logo
3) Ein Slogan, der die Vision der Partei von Digitalisierung und Nachhaltigkeit kompakt zusammenfasst.
4) Die wichtigsten konkreten Maßnahmen, welche die Partei umsetzen möchte.

Abschließend werden die Parteien in der Wahlkampfarena des Plenums vorgestellt und Rückfragen geklärt. Die Plakate verbleiben anschließend im Seminarraum, sodass die Teilnehmer:innen in Pausen ihre Stimme abgeben können. Dafür können beispielsweise Klebepunkte verwendet werden. Zum Tagesabschluss kann dann ein:e Wahlsieger:in gekürt werden.

Hinweis zur Moderation

- Es lohnt sich, die Postkarten beidseitig ausgedruckt zur Verfügung zu stellen. Auf der Rückseite finden sich nützliche Informationen.

Hier geht es zur zentralen Downloadseite der Materialien: »bit.ly/dja-material«



Postkarten zum Ausschneiden

Die Postkarten wurden von der Forschungsgruppe „Digitalisierung und sozial-ökonomische Transformation“ in Zusammenarbeit mit der Grafikerin Lone Thomasky entwickelt. Die Grafiken sind unter CC-BY-NC-SA Lizenz verwendbar und als Druckversion hier abrufbar:

nachhaltige-digitalisierung.de/veroeffentlichungen/postkarten

Mehr Informationen zur Forschungsgruppe, ihren Mitgliedern und Forschungsschwerpunkten, finden sich unter nachhaltige-digitalisierung.de.

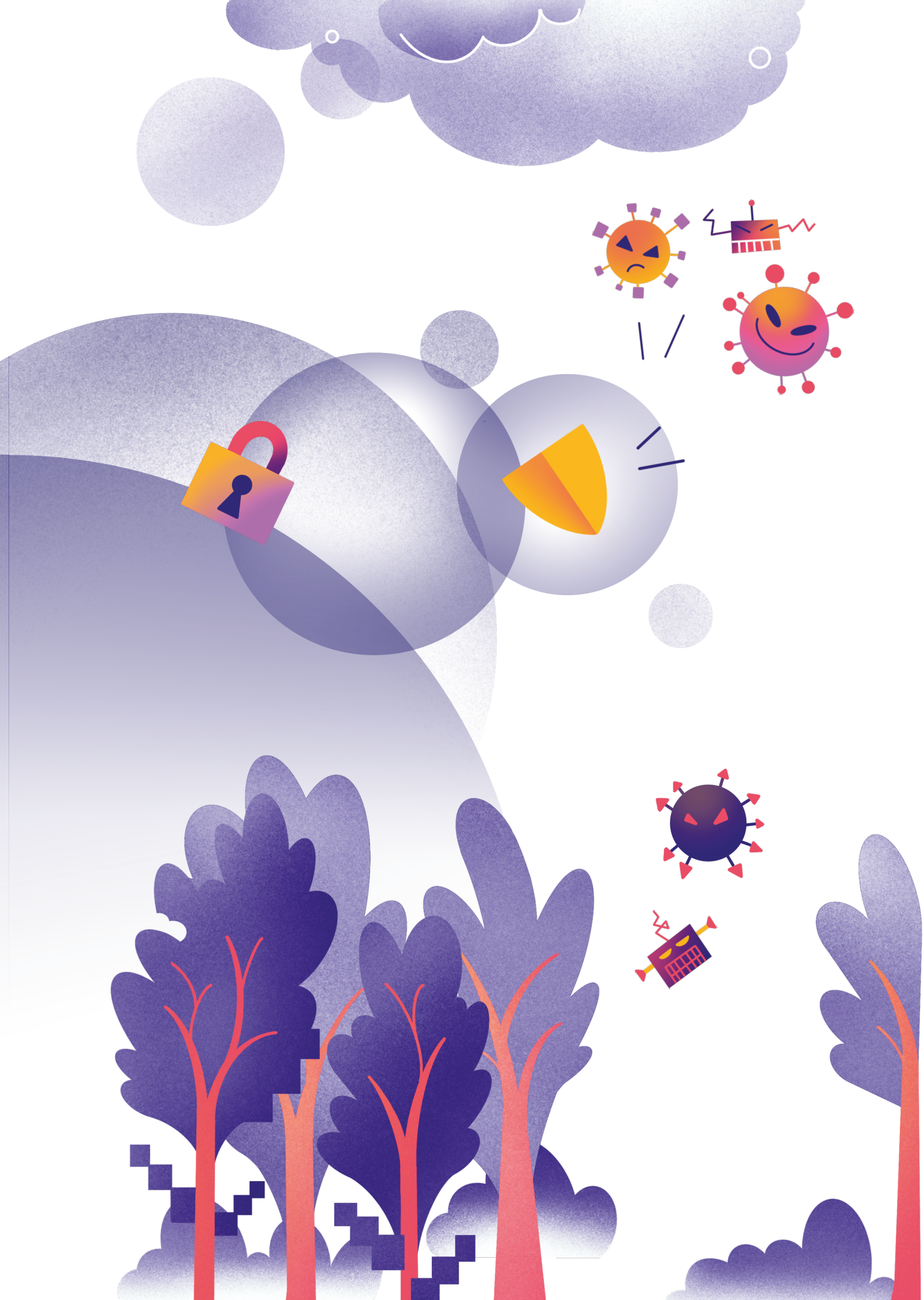









15:04
3405
0011
01001



digitale jugend arbeit



» www.digitalejugendarbeit.de «