DE

# DATA DETOX KIT

Alltägliche Schritte, mit denen du deine digitale Privatsphäre, Sicherheit und Wohlbefinden kontrollieren kannst, und die zu dir passen.

**datadetoxkit.org**

Ein Produkt von:

TACTICAL TECH

Firefox

## RATGEBER

Adaptiert von:

BEE SECURE

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse
Service national de la jeunesse

Kofinanziert von der Fazilität „Connecting Europe" der Europäischen Union

**Editeur :**
**Service National de la Jeunesse (SNJ)**
B.P. 707 · L-2017 Luxembourg
**www.snj.lu**
**www.bee-secure.lu**

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse
Service national de la jeunesse

kanner jugend telefon

Co-financed by the Connecting Europe Facility of the European Union

BEE SECURE est une initiative gouvernementale du Grand-Duché de Luxembourg, opérée par le Service National de la Jeunesse (SNJ) et le Kanner-Jugendtelefon.



ISBN: 978-2-919796-05-2

Version digitale
Data Detox DE - 08.2020

DATA DETOX KIT

## KONTROLLIERE DEINE SMARTPHONE-DATEN

um deine Online-Privatsphäre zu erhöhen

## ÄNDERE DEINE EINSTELLUNGEN

um deine Daten zu schützen

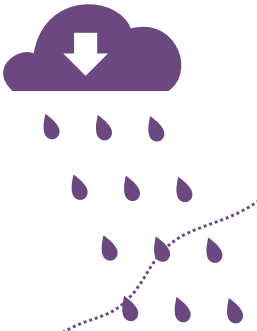
## BEFREIE DICH VON DEN STANDARDEINSTELLUNGEN

und verbessere dein digitales Wohlbefinden

## 6 TIPPS, UM ONLINE FALSCHINFORMATIONEN ZU UMGEHEN

Aktualisiert: März 2020

DATA DETOX KIT



# KONTROLLIERE DEINE SMARTPHONE-DATEN

um deine Online-Privatsphäre zu erhöhen

Wenn du darüber nachdenkst, was deine Daten anderen über dich verraten, dann scheint es vielleicht keine große Sache zu sein: Wen interessiert es schon, ob du gern Country-Musik hörst; dass du mehr Schuhe kaufst, als du tragen kannst; oder deinen nächsten Urlaub schon ein Jahr im Voraus planst?

Das Problem ist, was mit deinen Daten passiert. Über einen Zeitraum gesammelt kommen intime digitale Muster zum Vorschein: deine Gewohnheiten, Bewegungen, Beziehungen, Vorlieben, Ansichten und Geheimnisse eröffnen sich denjenigen, die sie analysieren und von ihnen profitieren, wie Unternehmen und Datenbroker.

Im Verlauf dieses Daten-Detox erhältst du einen Einblick, wie und warum all das passiert, und ergreifst praktische Maßnahmen, um deine Datenspuren im Internet zu kontrollieren.

Legen wir los!

1.

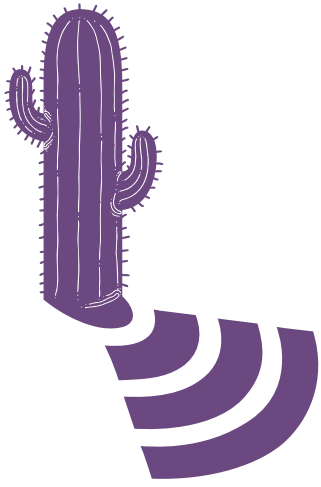
# ÄNDERE DEINEN GERÄTENAMEN

Irgendwann einmal hast du deinem Handy vielleicht für WLAN oder Bluetooth einen „Namen gegeben“ – oder ein Name wurde automatisch während der Einrichtung festgelegt.

Das heißt, dass „Alex Jungs Telefon“ für den Besitzer des WLAN-Netzwerks sichtbar ist, und falls du Bluetooth aktiviert hast, sieht dies auch jeder in der Gegend, der sein Bluetooth ebenfalls aktiviert hat.

Du würdest deinen Namen auch nicht verkünden, wenn du ein Café, Restaurant oder den Flughafen betrittst – und dein Handy sollte das auch nicht.

Du kannst **den Namen Deines Handys ändern**, in etwas, **das dich nicht persönlich identifiziert**, aber immer noch eindeutig du bist. So gehst du dabei vor:



iPhone:
**Einstellungen → Allgemein → Info → Ändere den Namen**

Android:
**Gerätenamen für WLAN ändern:**
**Einstellungen → WLAN → Menü → Erweitert / Weitere Optionen → Wi-Fi Direct → Gerät umbenennen**
**Gerätenamen für Bluetooth ändern:**
**Einstellungen → Bluetooth → Aktiviere Bluetooth, wenn es deaktiviert ist → Menü → Telefon umbenennen → Deaktiviere Bluetooth**

2.

## LÖSCHE DEINE STANDORT-FUSSABDRÜCKE

Es mag dir so vorkommen, als wären deine Standortdaten nur zusammenhanglose Brocken an Informationen. Betrachtet man sie aber im Ganzen, können sie **wichtige Details über dich** und deine Gewohnheiten enthüllen – beispielsweise wo du wohnst, wo du arbeitest und wo du dich gern mit Freunden triffst. Aus diesem Grund sind sie bei vielen Unternehmen und Datenbrokern heiß begehrt.

Du kannst **die Berechtigungen jeder einzelnen App** durchgehen und **die Standortdienste deaktivieren**. Halte Ausschau nach den Apps, für deren Dienste diese Angabe nicht nötig ist (Muss dieses Spiel wirklich wissen, wo du gerade bist?), und bei denen du nicht willst, dass sie sie bekommen.

Android:
**Einstellungen → Apps → Verwalte den Standortzugriff auf App-Basis**

iPhone:
**Einstellungen → Datenschutz → Ortungsdienste → Verwalte den Standortzugriff auf App-Basis**

3.

## RÄUME DEINE APPS AUF

Deine Social-Media-Apps, Spiele und Wetter-Apps sind an deinen Daten interessiert … Und sie sammeln ziemlich viele davon.

**Diese beliebigen Apps die du nicht benutzt auf deinem Handy loszuwerden, kann ein großer Schritt zum Detox deines digitalen Selbst sein.**

Dazu kommt, dass das Aufräumen auch neuen Speicherplatz auf deinem Telefon freigibt, die Datennutzung verringert und die Akkulaufzeit erhöht. Je nach App kann sich dadurch sogar die Leistung allgemein verbessern.

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

iPhone:
**Drücke auf eine App, bis alle beginnen zu wackeln und kleine Kreuze in der linken oberen Ecke jeder App auftauchen.**
**Tippe auf das kleine Kreuz einer App, um sie zu löschen.**
**Drücke auf den Home-Button, um zurückzukehren.**

4.

## HINTERLASSE WENIGER SPUREN

Der Browser auf deinem Handy speichert eine Menge Informationen über dich – deinen Standort, wonach du suchst, Webseiten die du besuchst – und verrät diese möglicherweise anderen. Auf Handys, Tablets und Computer sind üblicherweise Browser vorinstalliert, denen deine Privatsphäre nicht sehr wichtig ist. An ihrer Stelle kannst du **einen Browser herunterladen und benutzen**, der deine Aktivitäten im Netz **standardmäßig privat** hält und dich vor Trackern schützt.

Und für eine zusätzliche Erhöhung deiner Privatsphäre kannst du Extras installieren, die „Add-ons und Erweiterungen" heißen. (Dabei handelt es sich um Mini-Programme für deinen Browser, die **Deine Online-Aktivitäten besser schützen können**).

**Um neugierige Werbung und unsichtbare Tracker zu blockieren,** kannst du uBlock Origin (für Chrome, Safari und Firefox) oder Privacy Badger (für Chrome, Firefox und Opera) installieren.

**Um sicherzustellen, dass deine Verbindungen zu Webseiten wo möglich sicher sind,** kannst du HTTPS Everywhere installieren: Das ist eine Erweiterung für den Browser, die dafür sorgt, dass deine Kommunikation mit vielen großen Webseiten verschlüsselt und bei der Übertragung geschützt wird. Wenn du Safari benutzt und dir diese Option gefällt, dann kannst du deine Standard-Suchmaschine von Google zu einer anderen wie DuckDuckGo ändern, die dich automatisch zu verschlüsselten Verbindungen umleitet.

5.

## ENTMARKIERE DICH SELBST UND ANDERE

Hast du zur Datenmenge über deine Freunde beigetragen, indem du sie in der Vergangenheit in Fotos oder Beiträgen markiert hast? Mindere Ihre Datenlast (und erleichtere gleichzeitig auch dein Gewissen), indem du **sie entmarkierst** – in so vielen Fotos und Beiträgen wie möglich.

**Sag es weiter!** Sporne deine Freunde, Verwandten und Kollegen dazu an, sich dir bei der Kontrolle von diesen flüchtigen Daten anzuschließen. Wenn wir alle zusammenarbeiten, um die Kontrolle über unsere Datenspuren zu gewinnen, dann können wir uns gegenseitig beim Detox helfen.

Ein Produkt von
TACTICAL TECH

Unterstützt durch
Firefox

**datadetoxkit.org**
**#datadetox**

Aktualisiert: März 2020

DATA DETOX KIT

# ÄNDERE DEINE EINSTELLUNGEN

um deine Daten zu schützen

Wäre das Internet nur ein Ort, an dem Bilder von Hunden in Dinosaurierkostümen geteilt werden, dann wären Passwörter nicht so wichtig. Aber im Internet zahlst du auch Rechnungen, orderst Nachschub an deinen verschriebenen Medikamenten und meldest dich für Wahlen an. Wenn du an all deine „virtuellen Wertsachen" denkst, die im ganzen Internet geteilt werden – und auf deinen Geräten gespeichert – warum solltest du sie dann nicht so sicher verwahren wie deine Brieftasche oder Schlüssel?

Es gibt eine einfache Methode, es anderen zu erschweren an deine virtuellen Wertsachen heranzukommen: Mach es ihnen nicht leicht, deine Passwörter zu erraten. Die meisten benötigen keine speziellen technischen Fertigkeiten, um in deine Konten zu gelangen; sie schaffen das, indem sie nur versuchen, deine Passwörter zu erraten, oder ein automatisiertes Programm laufen lassen.

Und sobald sie es in einen Account geschafft haben, können sie dieses geknackte Passwort auch bei anderen versuchen, Informationen über dich und deine Gewohnheiten sammeln, andere deiner Konten oder sogar deine digitale Identität übernehmen.

Im Verlauf dieses Daten-Detox wirst du praktische Maßnahmen kennenlernen, die deine Online-Sicherheit erhöhen.

Legen wir los!

1.

## VERSPERRE DEINE DIGITALE TÜR

Bildschirmsperren: Passwort, Muster, Fingerabdruck oder Face ID, die du benutzt, um dein Gerät zu entsperren, sind einige **deiner besten Verteidigungen** gegen jemanden, der sich Zugriff auf dein Gerät verschaffen will. Aber es gibt viele verschiedene Methoden, und es kann schwierig sein herauszufinden welche die richtige für dich ist. Jede Sperre für dein Handy, Tablet oder Computer schützt dich besser, als überhaupt keine zu haben. Und genauso wie bei den verschiedenen Arten von Türschlössern sind **einige Bildschirmsperren sicherer als andere.**

Unter all den verfügbaren Sperren sind lange, einzigartige Passwörter die stärksten. Das bedeutet, wenn du ein Passwort zum Entsperren deines Geräts benutzt, sollte es Buchstaben, Zahlen und Sonderzeichen beinhalten.

Nehmen wir einmal an, dass du ein einfaches Wischen zum Entsperren deines Handys benutzt. Dann kannst du deine Sicherheit steigern, indem du ein langes Passwort einrichtest. Oder benutzt du zurzeit eine Mustersperre? Wie wäre es, wenn du dein Muster verlängerst? Lautet deine PIN 1234? Dann versuche doch, siebenmal zu würfeln und Dir stattdessen diese PIN zu merken. **Eine kleine Änderung kann dich der Kontrolle über deine Geräte schon ein gutes Stück näher bringen.**

2.

## LASSE NICHT DEN FALSCHEN HEREIN

Es ist nicht schwer gute Passwörter zu erstellen. Du musst dabei nur einige Grundsätze beachten. So sollten deine Passwörter sein:

Lang: **Passwörter sollten mindestens 12 Zeichen lang sein. Noch besser sind 16 – 20 Zeichen.**

Einzigartig: **Jedes deiner Passwörter – für jede Seite – sollte anders sein.**

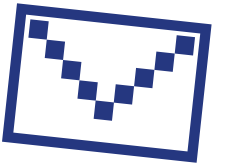
Zufällig: **Dein Passwort sollte keinem logischen Muster folgen oder leicht zu erraten sein. An dieser Stelle können Passwortmanager sehr hilfreich sein.**

Die sichersten Passwörter verwenden eine Kombination aus Buchstaben, Zahlen und Sonderzeichen. Dieser althergebrachte Rat gilt noch immer für ein starkes und schwer zu erratendes Passwort. Einige Passwortsysteme lassen leider keine Sonderzeichen (wie @#$%-=+) zu, aber eine längere Kombination aus Buchstaben und Zahlen ist immer noch besser als eine kurze.

Im Idealfall solltest du einen **speziellen Passwortmanager** benutzen, um all deine Passwörter zu generieren und zu speichern. Ein Passwortmanager – wie 1Password und KeePassXC, die oft von Sicherheitsexperten empfohlen werden – ist im Grunde genommen eine App, deren einziger Zweck darin besteht deine Anmeldedaten und andere sensible Informationen zu schützen.

3.

# FÜGE EINEN ZWEITEN SCHLÜSSEL HINZU



Richtest du eine Zwei-Faktor-Authentisierung (2FA) oder Multi-Faktor-Authentisierung (MFA) ein, bedeutet das, dass selbst wenn jemand dein Passwort knackt, **er wahrscheinlich nicht den anderen benötigten anderen Faktor zum Einloggen hat.**

Sieh dir einmal die Sicherheitseinstellungen der von dir am häufigsten genutzten Seiten an und überprüfe, ob du diesen zusätzlichen Schlüssel einrichten kannst. Beginne mit den wichtigsten – Apps für Finanzielles oder Dienste wie E-Mail, welche du benötigst, um andere Konten wiederherzustellen.


Google:
**Melde dich bei myaccount.google.com an → Sicherheit → Bestätigung in zwei Schritten → Jetzt starten**

Facebook:
**Menü → Einstellungen → Sicherheit und Login → Verwende die zweistufige Authentifizierung**

**Tipp:** Wenn du eine neue Ebene der Verifizierung einrichtest, musst du eine zweite Methode angeben, mit der du bestätigst, dass du es bist. Versuche, SMS (Textnachrichten, die an deine Handynummer geschickt werden) zu vermeiden, nur für den Fall, dass du dein Handy einmal verlieren solltest. E-Mail ist für gewöhnlich die verlässlichere Methode.

4.

## SCHÜTZE DEINE VIRTUELLEN WERTSACHEN

**So wie du auf wertvolle Dinge bei dir zu Hause achtest, solltest du dich auch um die Informationen kümmern, die du virtuell lagerst.** Ob es sich nun um Finanzunterlagen, Scans deines Reisepasses oder sogar um deine Adresse und Telefonnummer handelt – es lohnt sich, einmal darüber nachzudenken, wo du deine wertvollsten persönlichen Daten speicherst, und wie du sie schützen kannst.

Eine **punktuelle Reinigung** eignet sich hervorragend, wenn du ein paar schnelle Verbesserungen bei einer Tasse Kaffee erreichen willst. Suche dafür nach bestimmten Information in Deinen E-Mails oder anderen Konten und lösche sie: Scans von deinem Ausweis, Bankverbindung oder Informationen zu deiner Krankenversicherung, um nur einige zu nennen. Wenn du etwas findest, was du später brauchst, kannst du es jederzeit herunterladen oder ausdrucken, bevor du es aus deinem E-Mail-Konto löschst.

Eine **Tiefenreinigung** ist gründlicher und empfiehlt sich einmal im Jahr. Archiviere alles in deinem E-Mail- oder Social-Media-Konto, lade es auf deinen Computer herunter und lösche die entsprechenden Inhalte im Konto, um neu zu beginnen.

**Tipp:** Lösche nicht einfach nur – leere auch den Papierkorb und die temporären Dateien!

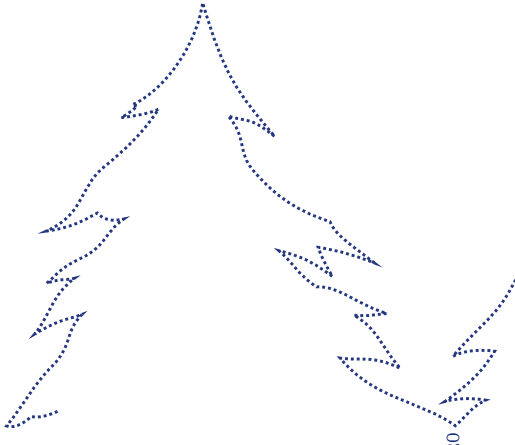
5.

## SAG ES WEITER

Auch wenn man es schnell vergisst, trägt „das Netz“ nicht grundlos seinen Namen. **Wir sind alle online miteinander verbunden** über verschiedene Netzwerke – nicht nur als „Freunde“ in den sozialen Medien, sondern auch durch die Kontakte in unseren E-Mail-Konten und durch die Fotos, die wir online teilen.

Wenn du deine Konten sicherer machst, deine Passwörter verstärkst und deine daten aufräumst, dann profitierst nicht nur du selbst davon – **jeder, der mit dir verbunden ist, wird durch deine Bemühungen ein bisschen sicherer.**

**Sag es weiter!** Mit ein paar einfachen Schritten lässt sich deine digitale Sicherheit erhöhen. Teile dieses Daten-Detox mit deiner Familie, deinen Freunden und Kollegen, um ihnen dabei zu helfen, ihre Gewohnheiten auf für sie sinnvolle Weise zu ändern.



Ein Produkt von
TACTICAL TECH

Unterstützt durch
Firefox

datadetoxkit.org
#datadetox

Aktualisiert: März 2020

DATA DETOX KIT

# BEFREIE DICH VON DEN STANDARDEINSTELLUNGEN

und verbessere dein digitales Wohlbefinden

Wann hast du das letzte Mal „den Stecker gezogen“ und für einen Tag – oder auch nur eine Stunde – die Finger von jeglicher Technik gelassen? Wenn du etwas so oft tust, möchtest du das Gefühl haben, dass es sich auch lohnt. Wie kannst du dafür sorgen, dass die Zeit mit deinem Gerät auch gut investiert ist?

Es beginnt damit, dass du dir bewusst werden musst, dass dein Hang zur Technik nicht deine Schuld ist! Vielleicht wirst du es nicht glauben, aber deine Lieblings-Apps und -Webseiten sind so designt, dass jede Funktion, jede Farbe und jeder Ton dazu „optimiert“ wurde, dich zu fesseln, zu überzeugen und immer wieder nach dem Handy greifen zu lassen.

Möchtest du ein gesundes Gleichgewicht zwischen deinem Leben online und dem offline finden? Genau darum geht es in diesem Teil des Daten-Detox.

Legen wir los!

1.

## ERLEBE DEN MOMENT

Dieser Tipp ist schwieriger, als er klingt. Im Hier und Jetzt zu bleiben, erfordert tägliche Übung. Es ist wie ein Muskel in deinem Gehirn, den du regelmäßig trainieren musst, damit er an Stärke gewinnt. Du kannst damit beginnen, dir deiner Beziehung zur Technik bewusst zu werden.

**Wie viel Zeit verbringst du mit deinem Handy?**

Wenn dir deine Antwort nicht gefällt, gibt es Einstellungen und Strategien, denen du folgen kannst, um deine Techniknutzung wieder unter Kontrolle zu bekommen.

Wenn du dir zum Ziel machst, weniger Zeit auf Facebook, Instagram oder mit Snapchat zu verbringen, dann ändere die Einstellungen dieser Apps, damit sie für dich besser funktionieren. Einige Apps wie Instagram haben sogar eine Funktion, die dich dezent darauf hinweist, wenn du dein tägliches Limit erreicht hast.

Instagram:
**Profil→ Menü → Einstellungen → Konto → Deine Aktivität → Richte eine tägliche Erinnerung ein**

Wenn du findest, dass dein Handy deine Unterhaltungen im echten Leben mit Klingeln, Summen oder Blinken stört, kannst du es vorübergehend auf Lautlos stellen, es mit dem Display nach unten ablegen oder es auch wegstecken, damit es sich nicht mehr in deinem Blickfeld befindet.

2.

## ERKENNE DIE DESIGNTRICKS

Übliche Designanstöße umfassen die Verwendung von bestimmten Farben, die Platzierung von Buttons, unklaren Text oder unvollständige Informationen. Manchmal sind diese Tricks offensichtlich, oft sind sie aber schwerer zu entdecken. Einige davon sind dir vielleicht schon aufgefallen, wenn du ein Abo abgeschlossen hast, oder beim Online-Shopping. Der Grund, warum man diese Designtricks überall findet, ist einfach: Sie funktionieren. Sie bringen uns zum Anklicken und Abonnieren, lassen uns öfter kaufen und immer wieder zurückkehren. Je mehr du dir der subtilen Aufforderungen und Manipulationen auf den Webseiten die du besuchst, bewusst wirst, umso versierter und informierter wirst du werden.

**Es gibt eine Reihe von Dingen, die du tun kannst, um deine Apps zu überlisten.**

**Bemerke, dass du gedrängt wirst:** Das Erste, was du tun kannst, ist, dir einfach der Verwendung dieser Methoden bewusst zu werden.

**Mache Screenshots und teile sie:** Nimm einen Screenshot auf, wann immer du online auf beeinflussende Designs triffst, und teile ihn mit deinen Freunden. (Vermeide dabei alle Details zu deiner Person – Sicherheit geht vor!) Du kannst Unternehmen auch darauf hinweisen ihre Praktiken zu ändern.

**Bewahre die Ruhe:** Wenn es auf einer Verkaufsseite einen Countdown-Zähler gibt, dann stelle dir selbst die folgende Frage: „Ist es wirklich dringend?“ Wenn du dich dabei erwischst, dass du auf einen Button klickst, obwohl du es gar nicht wirklich wolltest, denke über den Wortlaut auf den Buttons oder die verwendeten Farben des Dienstes nach. Wenn du verwirrt wirst, nimm nicht sofort an, es sei deine Schuld – betrachte die von der Website oder App benutzten Wörter, denn sie könnten unklar sein.

3.

# BLEIB MEDIEN INTELLIGENT

So wie du lernen kannst, die Funktionen und Designs zu überlisten, die dich immer weiter scrollen und klicken lassen, kannst du auch lernen wie du Nachrichtenartikel oder Beiträge erkennst, die dich in die Irre führen sollen.

Inzwischen hast du bestimmt schon einmal von den Problemen der „Falschinformationen“ und „Fake News“ gehört. du kannst Falschinformationen auf die Schliche kommen, wenn du dir angewöhnst, kritische Fragen zu allen Nachrichten, die du liest und hörst, zu stellen,– vor allem wenn sie überraschend, ungeheuerlich oder zu gut um wahr zu sein, klingen.

Schließlich wirst du vielleicht herausfinden wollen, welche Meldungen echt und welche falsch sind – besonders dann, wenn du sie mit deiner Familie und Freunden teilen willst.

**Von welcher Webseite stammt sie?**
**Wer hat das geschrieben (und wann)?**
**Was sagt der komplette Artikel, über die Überschrift hinaus?**
**Auf welche Quellen wird sich bezogen?**

Bist du der Meinung, es handelt sich um eine Falschinformation und möchtest ihre Verbreitung verhindern, bieten dir die meisten Plattformen eine Möglichkeit den Beitrag zu melden. Du kannst auch überlegen, ob du dem Account der sie veröffentlicht hat, weiterhin folgen möchtest oder nicht.

DATA DETOX KIT

4.

## VERSCHAFFE DIR GEHÖR

Wenn dich die fesselnden oder überzeugenden Designs sowie Falschinformationen, auf den von dir oft besuchten Webseiten oder deinen Apps stören, kannst du E-Mails schicken oder twittern und so Unternehmen wissen lassen, dass du mit ihren Praktiken nicht einverstanden bist. Werden Unternehmen von ihren wertvollsten Anlagen – ihren Nutzern – gedrängt etwas zu unternehmen, besteht die Chance dass sie sich ändern.

Wenn du glaubst, dein Feedback stößt auf taube Ohren, dann gibt es etwas sehr Mächtiges, was du tun kannst: Benutze eine andere Website oder App. Wenn du sie hast wissen lassen, dass du mit etwas, das ihre Webseite oder App tut nicht einverstanden bist und sie dann tatsächlich nicht mehr benutzt oder deinstallierst – und genügend andere das ebenfalls tun – **dann werden sie es bemerken.**

5.

## LASS ES ALLE WISSEN

Sag es weiter! Dieser Tipp ist leicht zu vergessen, aber er kann einen großen Effekt haben. Erzähle deinen Freunden, deiner Familie und Kollegen von dem was dir auffällt, oder frage sie sogar, ob sie sich dir nicht bei diesem Detox anschließen möchten! Jeder hat Probleme dabei seine Angewohnheiten mit dem Handy im Griff zu behalten. Wichtig ist, dass du eine Art und Weise findest, die sich für dich richtig anfühlt und zu deinem Lebensstil passt. Experimentiere bis du das Passende für dich findest und passe deine Gewohnheiten an, wenn sich deine Bedürfnisse mit der Zeit ändern. Es gibt hierbei keine Universallösung.

Und schließlich lasse die Menschen um dich herum auch deine Entscheidungen bezüglich der Techniknutzung wissen. Angenommen du bist jeden Tag nach 20 Uhr nicht mehr über deine Messenger-App zu erreichen, weil dann deine bildschirmfreie Zeit beginnt, dann sag deiner Familie und deinen Freunden Bescheid, damit sie dich stattdessen anrufen.

Bleibe offen für den Dialog und stelle Fragen, dann kannst du ein ausgeglichenes Online-Leben führen, das zu dir passt.

Ein Produkt von
TACTICAL TECH

Unterstützt durch
Firefox

**datadetoxkit.org**
**#datadetox**

Aktualisiert: März 2020

DATA DETOX KIT

# 6 TIPPS, UM ONLINE FALSCHINFORMATIONEN ZU UMGEHEN

Apps, Webseiten und Online-Medien können toll sein um Neuigkeiten, Life-Hacks und Unterhaltung zu finden. Aber bei all diesen Inhalten kann es schwierig sein, Ablenkungen zu ignorieren und das zu finden, was du wirklich suchst.

Dazu kommt, dass sich zwischen Fakt und Fiktion nicht immer leicht unterscheiden lässt, wenn du online auf ein Video, Bild oder einen Artikel stößt.

Von Persönlichkeits-Quizzen die ein Profil von dir erstellen, bis hin zu reisserischen Schlagzeilen oder veränderten Fotos, die dich von einer völlig anderen Realität überzeugen können – was du online siehst ist nicht immer das, was es zu sein scheint.

In diesem Daten-Detox erfährst du mehr zu Themen und Schlagwörtern rund um Falschinformationen und bekommst Ratschläge, wie du dir deinen Weg durch all das bahnen kannst, was es dort draußen gibt.

Los geht's!

1.

## DEINE MACHT WELLEN ZU SCHLAGEN

Nimm dir einen Moment Zeit und frage dich einmal Folgendes: **„Welchen Einfluss habe ich online?“** Wann war das letzte Mal, dass du einen schockierenden oder lustigen Artikel, eine Schlagzeile, ein Video oder Bild gesehen hast, und diesen Inhalt innerhalb von Sekunden an deine Freunde weitergeleitet hast? Forscher haben herausgefunden, dass die Geschichten und Bilder die am wahrscheinlichsten viral werden, diejenigen sind, die in dir Gefühle wie Angst, Abscheu, Schrecken, Wut oder Sorge auslösen. Fühle dich jetzt aber nicht schlecht, wenn du genau das erst heute Morgen getan hast!


2.

## DENKE ZWEIMAL DARÜBER NACH, OB DU AN DIESEM PERSÖNLICHKEITSTEST TEILNIMMST

Wann hast du das letzte Mal ein Quiz gesehen (entweder als Text oder Fotofilter), das so oder ähnlich hieß:

- Was ist dein spirituelles Tier?
- Wie sieht dein perfekter Urlaub aus?
- … Und die Liste lässt sich beliebig fortsetzen!

Deine Antworten bei einem Quiz wie „Welcher Simpsons-Charakter bist du?“ zusammen mit deinen anderen Angewohnheiten, die eventuell durch deinen Browser, Apps oder ähnliche Dinge wie Kundenkarten verfolgt werden, können Datenanalysten ein Bild davon vermitteln, was für ein Typ Mensch du bist. Was dir am Herzen liegt und wie du dich dazu beeinflussen lassen kannst, zum Beispiel ein Paar Schuhe zu kaufen … Oder Sie erstellen damit sogar ein Profil von dir, auf dessen Grundlage sie versuchen dich zu beeinflussen bei den nächsten Wahlen eine bestimmte Entscheidung zu treffen.

**Teilen bedeutet, sich zu kümmern**
Teilen ist eine Form der Teilnahme. Wenn du etwas teilst, ganz egal was, spielst du eine Rolle bei der Möglichkeit, dass es viral werden könnte. Und wenn es sich dann beispielsweise als Fake herausstellt, soll dann wirklich dein Name und dein Ruf damit in Zusammenhang gebracht werden? Bevor du etwas teilst, solltest du darüber nachdenken, ob du damit vielleicht eine Unwahrheit, etwas Destruktives oder Toxisches verbreitest.

**Verrate weniger von dir**
Wenn du an **private** Information denkst, kommen dir wahrscheinlich als Erstes deine Passwörter, IDs und Bankverbindung in den Sinn. Aber Informationen zum Beispiel darüber, wovor du Angst hast, was dich nervt oder deine Ambitionen sind ebenso persönlich. Diese Details können für Datenanalysten sehr wertvoll sein, da sie ihnen verraten, was dich als Menschen ausmacht. Denke gut darüber nach, bevor du solche Informationen in einer Umfrage oder einem Quiz preisgibst.

3.

## LASS DICH NICHT KÖDERN

**Klick-Köder** (Clickbait) ist ein Begriff, der zur Beschreibung von sensationslüsternen, unehrlichen oder frei erfundenen Überschriften verwendet wird, die das Ziel verfolgen, Leute dazu zu verleiten, auf die Überschrift oder den Link zu klicken. Je mehr Aufmerksamkeit ein Artikel, Video oder Bild erzeugt, desto mehr Geld kann damit verdient werden. Das bedeutet, dass die Verantwortlichen eine Motivation haben, alles zu behaupten, was nötig ist, damit du auf ihren Content klickst oder ihn teilst.

Basierend auf dem Persönlichkeitsprofil, das die Plattformen, die du nutzt (wie Facebook und Instagram), von dir erstellen, kannst du auf dich zugeschnittene Überschriften zu sehen bekommen, die **deine Emotionen** auf eine Weise auslösen, die dich zum Anklicken bringt.

**Gehe ihnen auf den Grund**
Wenn Dir Klick-Köder begegnen, dann mache nicht bei der Überschrift halt. Wenn es wie ein sicherer Link aussieht, klick Dich doch einmal in den Artikel und finde heraus, wer der Autor ist, wann er veröffentlicht wurde, und auf welche Quellen er sich stützt. Es kann auch sein, dass Du in dem Artikel einen Hinweis darauf findest, dass es sich um bezahlten Inhalt oder Werbung handelt; vielleicht ist er auch als Stellungnahme kategorisiert. Diese Informationen können Dir dabei helfen zu beurteilen, ob er Deine Energie wert ist.

4.

## ACHTE AUF FAKES

Deepfakes sind Videos, Audioclips oder Bilder, die digital verändert wurden, typischerweise um jemandes Gesicht oder Bewegungen zu ersetzen, oder seine Worte zu ändern. Obwohl „Deepfakes“ ein relativ neuer Begriff ist, gibt es sie tatsächlich in der ein oder anderen Form schon seit langer Zeit. Noch einfacher ist es, sogenannte **Cheap Fakes** zu erstellen – irreführende Inhalte, die keine anspruchsvolle Technologie benötigen, sondern ganz einfach fabriziert werden können, indem man einem Foto oder Video eine falsche Überschrift gibt, oder veraltetes Material benutzt, um ein aktuelles Geschehnis darzustellen.

Es mag als unmöglich erscheinen, Fakes wirkungsvoll zu bekämpfen, aber es gibt etwas Wesentliches, was du tun kannst: Lass dich nicht mitreißen.

**Lass dich nicht mitreißen und forsche nach**
Es ist genau wie bei Klick-Ködern: **Nimm nichts einfach so als Fakt hin.** Wenn ein Video oder Foto, das du gesehen hast, überraschend oder unfassbar erscheint, dann werde dir dieses Gefühls bewusst und frage dich, ob nicht mehr dahinter stecken könnte. Andernfalls kannst du es als Anstoß nehmen, zur Quelle vorzudringen, wenn du bemerkst, dass dasselbe Bild deinen Feed flutet oder mehrfach mit dir geteilt wurde.

**Dann wirst du weitere Fragen stellen:** Wer hat es veröffentlicht? (Welche Webseite, wer war der Autor?) Wann wurde es veröffentlicht? Wenn es sich um ein Bild handelt, kannst du auf TinEye eine umgekehrte Bildsuche starten und sehen, wo du es sonst noch finden kannst.

Überprüfe auch andere vertrauenswürdige Nachrichtenquellen, bevor du es als echt einstufst und mit deinen Freunden und deiner Familie teilst.

5.

## SUCHE DIE WAHRHEIT IM INTERNET

Der Begriff „Fake News“ beschreibt eine ganze Bandbreite an ungenauen oder irreführenden Informationen, welche auch Satire, schlecht recherchierten oder nicht verifizierten Inhalt, Täuschungen und Betrug beinhalten.

Im besten Fall ist es ein lustiges Meme. Im schlimmsten Fall ist es ein falscher Gesundheitshinweis oder eine unwahre politische Information.

Auch wenn du dein Bestes unternimmst, die Artikel die du liest zurückzuverfolgen und kritisch zu hinterfragen, kann es sein, dass ein Gefühl der Verwirrung zurück bleibt. Aber vergiss nicht: Damit bist du nicht allein!

**Alle müssen mit anpacken**
Nur weil eine Webseite nicht zu ihren Fehlern steht, bedeutet das nicht, dass keine Fehler gemacht werden. Tatsächlich sind die verlässlichsten Veröffentlichungen diejenigen, die besonders vorsichtig im Umgang mit der Wahrheit sind und Leute oder ganze Abteilungen einstellen, deren einzige Rolle darin besteht, Fakten zu überprüfen.

**Suche nach Quellen, die Korrekturen herausgeben, wenn ihnen ein Fehler unterlaufen ist.** Noch besser ist es, wenn die Korrektur direkt über dem Artikel zusammengefasst und in den sozialen Medien geteilt wird, damit du nicht allzu lange danach suchen musst.

6.

## LASS DEINE FILTERBLASE PLATZEN

Nachdem Webseiten ein Profil von deinen Interessen erstellt haben, kann es sein, dass du dich in einer Filterblase wiederfindest. Das ist der Fall, wenn Dienste dir weitere Geschichten anbieten wie die, die dich bereits anklicken. Inwiefern beschränkt oder verändert das, was du mitbekommst?

In einer Filterblasen zu sein, kann dazu führen, dass Menschen völlig verschiedene Geschichten, Nachrichten, Artikel und Werbung zu sehen bekommen, wie der interaktive Artikel Blue Feed, Red Feed (graphics.wsj.com/blue-feed-red-feed) verdeutlicht. Im schlimmsten Fall können Filterblasen Nachbar- und Gemeinschaften und sogar ganze Nationen polarisieren.

**Bringe frischen Wind in deine Nachrichten**
Eine gute Möglichkeit, deine Filterblase zum Platzen zu bringen, ist es, Dienste zu abonnieren, die Neuigkeiten und Informationen aus unterschiedlichen Quellen zusammentragen und **sich eines Pools verschiedener Perspektiven bedienen.** RSS-Feeds, Foren und Mailinglisten, die eine Bandbreite an Meinungen und Themen ansprechen, können dir dabei helfen, deine Blase zu überwinden.

**datadetoxkit.org** **#datadetox**

Ein Produkt von TACTICAL TECH

Projektpartner Save the Children 100 ANNI IFLA

Finanziert von der Europäischen Union

Aktualisiert: März 2020