

UPDATE 2022

DANN HABEN DIE HALT
MEINE DATEN.

NA UND?

ARBEITSBLÄTTER

Ein Buch für
alle, die nichts
zu verbergen
haben.

30

Arbeitsblätter
& Checklisten

KLAUDIA ZOTZMANN-KOCH

edition sil|ben|reich

4. AUFLAGE

ZITRONENFALTER FALTEN KEINE ZITRONEN

WICHTIG: DU BIST NICHT ZU DOOF, ES WIRD DIR ABSICHTLICH SCHWER GEMACHT.

Notiere, was Du in diesem Kapitel gelernt hast.

Mach eine Liste, welche Dinge Du an Deinem Internetverhalten ändern möchtest.

-
-
-
-

NOTIZEN UND WAS DU WEITER RECHERCHIEREN MÖCHTEST:



AUF DER DATENAUTOBAHN

Notiere, was Du in diesem Kapitel gelernt hast.

To-Dos, die sich aus diesem Kapitel für Dich ergeben:

-
-
-
-
-
-



DAS INTERNET HINTER DEN DISPLAYS

Notiere, was Du in diesem Kapitel gelernt hast.

To-Dos, die sich aus diesem Kapitel für Dich ergeben:

-
-
-
-
-
-



Alles, was Du in weniger als 30 Minuten tun kannst, um das Internet sicherer und datenschutzfreundlicher zu nutzen.

TRACKING – DIE TÄGLICHE JAGD

ALLGEMEINE GESCHÄFTSBEDINGUNGEN (AGB)

Lies die AGB einiger Deiner meistgenutzten Plattformen und Services. Markiere, was Dir auffällt und notiere, was Du vorhast, zu tun (z.B. Anfrage stellen, Service nicht mehr nutzen, Alternative suchen ...)

AGB, DIE DU LESEN WILLST:

Erledigt

[Redacted text area]

To do

[Redacted text area]

Erledigt

[Redacted text area]

To do

[Redacted text area]

Erledigt

[Redacted text area]

To do

[Redacted text area]

Erledigt

[Redacted text area]

To do

[Redacted text area]



Alles, was Du in weniger als 30 Minuten tun kannst, um das Internet sicherer und datenschutzfreundlicher zu nutzen.

TRACKING – DIE TÄGLICHE JAGD

Notiere, was Du in diesem Kapitel gelernt hast, insbesondere, warum Tracking ein Problem sein kann.

To-Dos, die sich aus diesem Kapitel für Dich ergeben:



ALGORITHMEN & "KI"

Notiere, was Du in diesem Kapitel gelernt hast, insbesondere über Profiling.

To-Dos, die sich aus diesem Kapitel für Dich ergeben:



SOCIAL MEDIA

Notiere, was Du in diesem Kapitel gelernt hast, insbesondere über Profiling.

To-Dos, die sich aus diesem Kapitel für Dich ergeben:



WEB 3.0, NFT & BLOCKCHAIN

Notiere, was Du in diesem Kapitel gelernt hast, insbesondere über Profiling.

To-Dos, die sich aus diesem Kapitel für Dich ergeben:



GESELLSCHAFTLICHES

WICHTIG: DATENSCHUTZ IST DER SCHUTZ VON MINDERHEITEN UND EIN GRUNDLEGENDES MENSCHENRECHT.

Notiere, was Du in diesem Kapitel gelernt hast.

To-Dos, die sich aus diesem Kapitel für Dich ergeben:



FRAGEN, FRAGEN FRAGEN

Notiere, was Du in diesem Kapitel gelernt hast.

DATENAUSKUNFTS-ANFRAGEN GEMÄSS ART. 15 DSGVO

Vielleicht hast Du schon einige Firmen oder Institutionen im Kopf, denen Du Deine ersten Anfragen gemäß Artikel 15 DSGVO schicken möchtest? Großartig! Notiere sie hier.

FIRMEN, DENEN DU ANFRAGEN SCHICKEN MÖCHTEST

Erledigt

To do

Erledigt

To do

Erledigt

To do



IN TROCKENEN BÜCHERN

Notiere, was Du in diesem Kapitel gelernt hast, vor allem über die rechtlichen Hintergründe, warum Datentransfers möglich sind.

To-Dos, die sich aus diesem Kapitel für Dich ergeben:



DAS OFFLINE

Notiere, was Du in diesem Kapitel gelernt hast, vor allem, was Du für Deine eigene Privatsphäre auch offline tun kannst.

To-Dos, die sich aus diesem Kapitel für Dich ergeben:



WAS DU IN UNTER 30 MIN TUN KANNST

WOVON BRAUCHST DU BACKUPS?

Okay, Zeit für eine Inventur: Wovon solltest Du Backups haben? Desktop Computer? Laptop? Tablet? Smartphone? Sonst noch was?

GERÄTE & DATEN, VON DENEN DU EIN BACKUP BRAUCHST

Erledigt

Die wichtigsten Daten auf diesem Gerät



BROWSER PRIVATSPHÄRE & SICHERHEIT

Lass uns einen Blick auf Deinen Browser werfen. Ich empfehle Mozilla Firefox. Vielleicht magst Du Dir Alternativen wie Chromium oder Vivaldi ansehen. Lade Dir gern testweise alle davon herunter. Prüfe und passe die Einstellungen zuerst an und dann probiere aus, welcher Dir in der täglichen Benutzung am besten liegt.

BROWSER EINSTELLUNGEN & ADD-ONS

Einstellungen geprüft und angepasst (Datenschutz "streng")

"Alle Cookies beim Beenden des Browsers löschen" eingestellt

Add-on "https everywhere"

Add-on "uBlock origin"

Add-on "EFF Privacy Badger"

Was möchtest Du noch ausprobieren?



PRIVATSPHÄRE & SICHERHEIT AUF MOBILGERÄTEN

Weiter zum Mobilgerät. Auch dies ist ein kleiner Computer, ein sehr leistungsstarkes Gerät in der Größe Deiner Handfläche. Schauen wir uns die Sicherheits- und Privatsphäre-Einstellungen an und setzen die Advertising-ID der Herstellerfirma zurück.

EINSTELLUNGEN AUF MOBILGERÄTEN

Überprüfe alle Apps auf Deinen Geräten und lösche alle, die Du nicht mehr brauchst

Setze die Advertising-ID zurück

Analyse & Verbesserungen ausschalten

Deaktiviere GPS Tracking ("Wichtige Orte bei iOS, bei Android leider sehr verteilt)

INHALTSBLOCKER FÜR MOBILGERÄTE

Firefox Klar (Firefox Focus)

Blokada (Android) oder 1Blocker (iOS)

Was möchtest Du noch ausprobieren?



PASSWÖRTER, PASSWORD-SAFES & 2FA

Dies ist das Wichtigste von allem: Nutze starke Passwords. Stark heißt lang: mehr als 14 Zeichen. Verwende überall ein eigenes Passwort und einen Password-Safe, der Dir hilft, all die Passwörter für Logins und Programme im Auge zu behalten. Dies ist ein großer Schritt. Ich freue mich sehr, dass Du ihn machst! Fang mit einem Lock-Screen, also PIN-Abfrage (besser: Passwort) auf all Deinen Geräten an.

Lockscreen und PIN (noch besser: Passphrase) auf Mobilgerät(en)

PASSWORD SAFE

Such Dir einen Password-Safe aus, der für Dich funktioniert (e.g. KeepassXC).



Was möchtest Du noch ausprobieren?

Installier einen Password-Safe auf Deinem Mobilgerät (z.B. KeePass2Android oder Strongbox für iOS).



Erledigt

2-FAKTOR-AUTHENTIFIZIERUNG

Mach Dich mit Deinem Password-Safe vertraut und finde die Funktion "2FA", also 2-Faktor-Authentifizierung. Die meisten Password-Safes bieten mindestens TOTP-Funktion an. Fang an, Deine Passwörter eins nach dem anderen zu tauschen, wenn Du die Plattform oder den Service das nächste Mal nutzt. Aktiviere 2FA, wo möglich. Starte mit Deinem eMail-Account.

WICHTIG: DEIN E-MAIL-ACCOUNT IST DEIN ALLERWICHTIGSTER ACCOUNT. HIER SOLLTEST DU EIN STARKES PASSWORT UND ZUSÄTZLICH 2FA AKTIVIERT HABEN.



PASSWÖRTER, PASSWORD-SAFES & 2FA

Notiere Deine Accounts, bei denen Du anfangen möchtest, die Passwörter zu tauschen und 2FA zu aktivieren.

Dein eMail-Account

IOT

Denk auch an vernetzte Geräte in Deinem Haushalt und Deinem Rucksack. Tausche schwache und auch Standard-Passwörter gegen starke und lange Passwörter aus. Schieb es nicht auf die lange Bank.



WLAN & BLUETOOTH

Schalte WLAN an den Geräten ab, die Du mit Dir rumträgst, wenn Du das Haus verlässt. Mach eine Gewohnheit draus, dann wird es sehr leicht für Dich.

Bluetooth wird für die meisten Corona-Kontaktverfolgungs-Apps gebraucht. Dies könntest Du für den Moment anlassen und die Bluetooth-Einstellungen überprüfen, wenn Corona vorbei ist.



Ändere Deine Geräte-Namen in etwas, das nicht Deinen Namen, Adresse, Geburtstag oder andere persönliche Daten preisgibt.



WLAN ZU HAUSE ABSICHERN

Überprüfe Deinen WLAN-Router zu Hause, ob der Admin-Bereich schon ein starkes Passwort hat. Falls nicht, ändere es.



Setze ein starkes Passwort für Dein WLAN zu Hause und trag es in Deinen Password-Safe ein.



Falls der Netzwerkname persönliche Daten preisgibt, ändere ihn zu einem nicht-sprechenden Namen (oder zumindest irgendwas ohne persönliche Daten drin). Trag ihn in Deinem Password-Safe ein.



Richte ein eigenes Gäste-WLAN ein, damit Deine Gäste nicht dasselbe Netzwerk nutzen wie Du und alle Deine Geräte im Haus. Falls Du Geräte hast, die Deine Gäste nutzen können sollen, verbinde sie für die Zeit des Besuchs mit dem Gästenetzwerk. Gib dem Gästenetzwerk ein starkes Passwort und trag es in Deinen Password-Safe ein.



APP EINSTELLUNGEN & BERECHTIGUNGEN

Zu Beginn stelle sicher, dass das Betriebssystem Deiner Geräte und alle Programme und Apps up-to-date sind. Updates sind wichtig, da sie immer wichtige Sicherheitsupdates mitbringen. Aktualisiere alles.

Betriebssystem, alle Programme und alle Apps sind aktualisiert

Geh alle Apps auf Deinem Mobilgerät durch und überprüfe die App-Berechtigungen. Keine Taschenlampen-App braucht Zugang zu Deinem Adressbuch, Deiner Kamera oder Deinem Mikrofon. Hinterfrage alle mit Deinem Hausverstand. Notiere, welche App Du bereits überprüft und nötigenfalls angepasst hast.



SICHERE MESSENGER

Wenn Du zu einem sicheren Messenger wechseln möchtest, gibt es ein paar Dinge zu tun, damit Menschen wissen, wo sie Dich erreichen.

MESSENGER WECHSELN

Erledigt

To do

Erledigt

To do

Erledigt

To do

DIE WICHTIGSTEN MENSCHEN, DIE DU INFORMIEREN MÖCHTEST

Erledigt



Alles, was Du in weniger als 30 Minuten tun kannst, um das Internet sicherer und datenschutzfreundlicher zu nutzen.

SICHERE MESSENGER

Wenn Du zu einem sicheren Messenger wechseln möchtest, gibt es ein paar Dinge zu tun, damit Menschen wissen, wo sie Dich erreichen.

1

ENTSCHEIDE DICH FÜR EINEN MESSENGER

Lies das Kapitel ggf nochmal und entscheide Dich für einen Messenger, der zu Deinen Anforderungen passt. Ein Kriterium ist, ob Du große Gruppen brauchst oder nicht.

2

INFORMIERE DEINE KONTAKTE

Informiere Deine Kontakte in Deinem aktuellen Messenger über den geplanten Wechsel.

3

SETZ EINE STATUSMELDUNG

Du kannst Deine Statusmitteilung im alten Messenger nutzen, um die Information gut sichtbar für all Deine Kontakte zu platzieren.

4

RICHE DEIN PROFIL EIN

Pass Dein Profil im neuen Messenger an. Wenn Du möchtest, dass Deine Kontakte Dich leicht finden, nutze den selben (oder wiedererkennbaren) Nickname und das selbe Profilbild.

5

GIB MENSCHEN ZEIT, SICH UMZUGEWÖHNEN

Lösche Deinen alten Messenger und Deinen Account dort nicht sofort. Menschen brauchen Zeit, sich umzugewöhnen. Gib ihnen eine Woche oder auch zwei, ehe Du den Account löschst.

6

LÖSCHE DEN ALTEN ACCOUNT

Lösche den alten Account nach einer Weile. Deinstalliere nicht einfach nur den alten Messenger! Um sicher zu gehen, dass Dein alter Account nicht übernommen werden und jemand sich als Du ausgeben kann, lösche den alten Account. Dann erst deinstalliere die App.

DIE WICHTIGSTEN MENSCHEN, DIE DU INFORMIEREN MÖCHTEST

Erledigt



E-MAIL ACCOUNTS

Deinen eMail-Account wechseln ist an sich leicht. Einige der sichereren Anbieter bieten sogar einen "Umzugsservice" an.

- 1 **ENTSCHEIDE DICH FÜR EINEN ANBIETER**
Lies das Kapitel ggf. noch einmal und entscheide Dich für einen eMail-Anbieter, der zu Deinen Anforderungen passt.
- 2 **TAUSCHE DEINE KONTAKT-INFORMATIONEN AUS**
Passe Deine Kontakt-Infos auf Deinen üblichen Plattformen an, sodass automatisierte eMails an Deinen neuen Account gehen.
- 3 **INFORMIERE DEINE KONTAKTE**
Lass Menschen wissen, dass Du eine neue eMail-Adresse hast. Du kannst auch einen Autoresponder für Deinen alten Account einrichten. Antworte immer vom neuen Account.
- 4 **PASSE NEWSLETTER-ABOS AN**
Ob Du Newsletters auf Deine alte oder neue eMail-Adresse haben möchtest, ist Dir überlassen. Wenn sie beim neuen Account ankommen sollen, passe die Abos an. Bei der Gelegenheit bestelle alles ab, was Du nicht wirklich brauchst oder haben möchtest.
- 5 **DIE ALTE ADRESSE NICHT LÖSCHEN**
Dein eMail-Account ist der wichtigste von allen, da Du Reset-Anweisungen und Benachrichtigungen zu allen anderen Accounts per eMail bekommst. Gib Deinem alten eMail-Account ein gutes langes Password und 2FA und behalte ihn, falls Du einige alte Social Media oder Shop-Accounts zurücksetzen musst.

WICHTIG: DEIN E-MAIL-ACCOUNT IST DEIN ALLER-WICHTIGSTER ACCOUNT. GIB IHM EIN STARKES PASSWORD UND 2FA.

DIE WICHTIGSTEN MENSCHEN, DIE DU INFORMIEREN MÖCHTEST



Erledigt



DEINE EIGENE NEXTCLOUD

Einen eigenen Cloudspeicher zu haben, ist recht einfach und erschlägt viele Probleme mit einer Klatsche: Speicherplatz, Dateien mit anderen teilen, Foto- und Dateien-Backup, Kalender, Adressbuch und vieles mehr.

1

ENTSCHEIDE DICH FÜR EINEN ANBIETER

Suche im Internet nach einem Owncloud- oder Nextcloud-Anbieter in Deinem Land – das macht das Rechtliche einfach.

2

KLICK DIR DEIN CLOUD-PAKET

Die meisten Anbieter haben verschiedene Pakete, die sich meist nach Speicherplatz unterscheiden. Für etwa 3 bis 5 Euro oder Dollar pro Monat solltest Du alles finden, was Du brauchst.

3

RICHTE NEXTCLOUD AUF DEINEN GERÄTEN EIN

Lade die Nextcloud Desktop App auf Deinen Computer. Log Dich darin in Deinen Account bei Deinem Anbieter ein. Such die Ordner aus, die automatisch synchronisiert werden sollen.

4

RICHTE NEXTCLOUD AUF DEINEM MOBILGERÄT EIN

Lade die Nextcloud App auf Dein Telefon und/oder Tablet. Log Dich darin in Deinen Nextcloud-Account ein und richte den automatischen Bildupload und die Backup-Funktion ein.

5

ADRESSBUCH & KALENDER

Anstatt den eingebauten Kalender und das Adressbuch Deines Telefon- oder Laptopherstellers zu verwenden, kannst Du auch Kalender und Adressbuch verwenden, die in Deiner eigenen Nextcloud liegen.

- Richte einen oder mehrere Kalender in Deiner Nextcloud ein
- Exportiere Deine(n) alten Kalender
- Importiere ihn/sie in den/die Nextcloud Kalender
- Ändere den Standard-Kalender in den Geräteeinstellungen auf den/die neuen Kalender

Genauso funktioniert es auch für das Adressbuch: Export – Import – Standard ändern. Danach lösche die Kontakte aus Deinem alten Adressbuch, damit sie nicht länger beim Gerätehersteller liegen. (Geh sicher, dass Du ein Backup des Adressbuchs hast, falls etwas schiefgehen sollte.)



SOCIAL MEDIA ALTERNATIVEN

Notiere, was Du in diesem Kapitel gelernt hast.

SOCIAL MEDIA

Gibt es etwas, das Du bezüglich Deiner Social Media Nutzung überdenken möchtest? Vielleicht eine freie Alternative wie Mastodon ausprobieren? Notiere, was Du tun möchtest und auch weitere To-Dos, die sich aus Deinen Experimenten ergeben.

DINGE ZUM AUSPROBIEREN & VERÄNDERN

Erledigt

To do

Erledigt

To do

Wenn Du jetzt ein Mastodon-Konto hast, schreib mich gern an!
-> @viennawriter@literatur.social



FORTGESCHRITTEN

Notiere, was Du in diesem Kapitel gelernt hast, insbesondere darüber, wie Verschlüsselung funktioniert.

To-Dos, die sich aus diesem Kapitel für Dich ergeben:



ETWAS WEITER FORTGESCHRITTEN

Notiere, was Du in diesem Kapitel gelernt hast.

To-Dos, die sich aus diesem Kapitel für Dich ergeben:

-
-
-
-



DINGE, DIE DU SELBST HERAUSGEFUNDEN HAST

Du hast es bis zum Ende des Buchs geschafft. Mach weiter und recherchiere selbst weiter zu den Themen, die Du auf den Arbeitsblättern am Ende jedes Kapitels notiert hast. Schreib auf, was Du beim tieferen Bohren entdeckt hast.

Notiere Deine weiteren To-Dos.



DINGE, DIE DU SELBST HERAUSGEFUNDEN HAST

Deine weiteren To-Dos:

-
-
-
-
-
-
-
-



NOTIZEN

Alles, was Du in weniger als 30 Minuten tun kannst, um das Internet sicherer und datenschutzfreundlicher zu nutzen.



RESSOURCEN

Alle Infos zum Buch "Dann haben die halt meine Daten. Na und?" sowie eine Leseprobe, Poster und mehr gibt es auf

<https://www.zotzmann-koch.com/book/na-und>



Eine herunterladbare Leseprobe "Dann haben die halt meine Daten. Na und?" als PDF gibt es unter:

<https://www.zotzmann-koch.com/book/na-und/leseprobe>



Eine aktuelle Liste mit Empfehlungen und Updates zum Buch gibt es auf:

<https://www.zotzmann-koch.com/empfehlungen/>

