

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 **punktueller Reinigung** eignet sich hervorragend, wenn Du ein paar schnelle Verbesserungen bei einer Tasse Kaffee erreichen willst. Suche dafür nach bestimmten Informationen 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.



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!

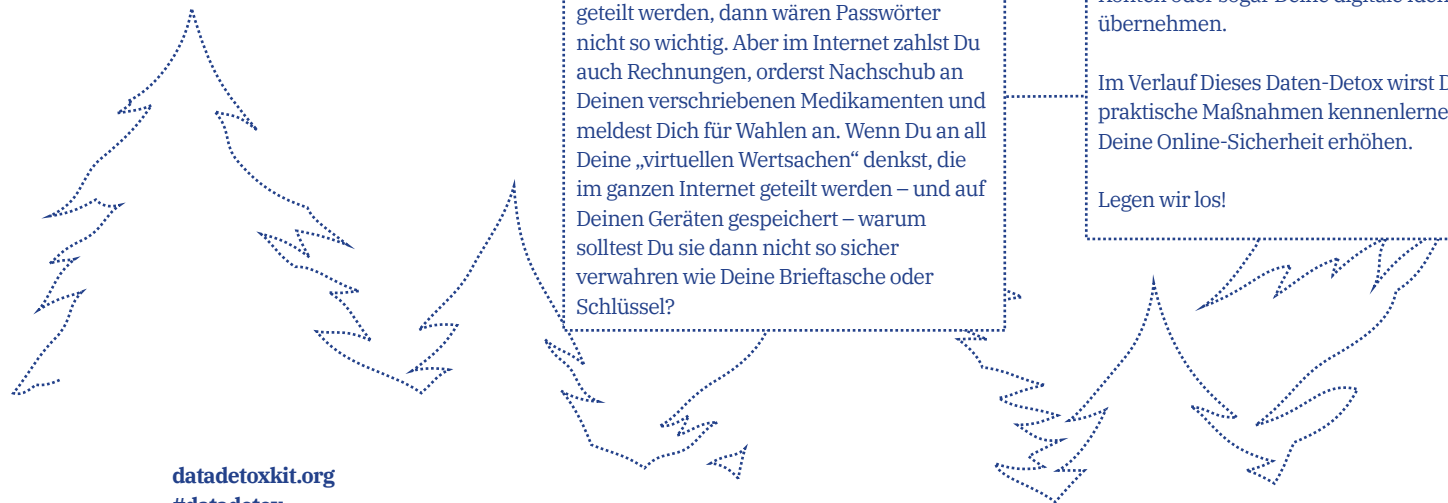
Ein Produkt von

**TACTICAL
TECH**

Unterstützt durch



datadetoxkit.org
#datadetox



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 8 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 Passwortssysteme lassen leider keine Sonderzeichen (wie @#\$%-+=) zu, aber eine längere Kombination aus Buchstaben und Zahlen ist immer noch besser als eine kurze.

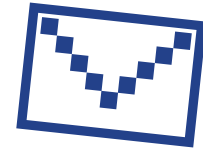
Im Idealfall solltest Du einen **speziellen Passwortmanager** benutzen, um all Deine Passwörter zu generieren und zu speichern. Ein Passwortmanager – wie 1Password und KeePassXC, die oft von Sicherheitsexperten empfohlen werden – ist im Grunde genommen eine App, deren einziger Zweck darin besteht Deine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