In sieben Schritten zu mehr Sicherheit im Netz

Daten sind heutzutage von großem Interesse für Konzerne geworden. Egal ob Google, Facebook oder Amazon: (fast) alle Unternehmen haben das Ziel, so viele Daten wie möglich zu erfassen und so viel wie möglich über ihre Nutzer:innen zu erfahren.

Auf rechtlicher Ebene gibt es die europäische Datenschutzgrundverordnung, die versucht, der permanenten Überwachung von Unternehmen einen Riegel vorzuschieben. Auf zivilgesellschaftlicher Ebene gibt es wichtige Akteur:innen, wie zum Beispiel netzpolitik.org, die Electronic Frontier Foundation oder digitalcourage e.V., die sich für Privatsphäre von Bürger:innen einsetzen.

Aber auch auf individueller Ebene und in der zivilgesellschaftlichen Arbeit kann man mit ein bisschen Zeit sicherer im Netz unterwegs sein. Diese Anleitung in sieben Schritten soll dir dabei helfen.

Mach' dir ein Heißgetränk, hol' dir deine Endgeräte, leg' dir alle Unterlagen zurecht und nimm' dir ein paar Stunden Zeit. Denke einfach an Marie Kondo und sieh' das Ganze als "digitales Ausmisten". Los geht's!

1. Verschaffe dir einen Überblick

Verschaffe dir zunächst einen groben Überblick über deine Aktivitäten im Internet. Auf welchen Social Media Plattformen hast du eigentlich Accounts? Welche Online-Shops, Streaming-Anbieter und weitere digitale Dienstleister verwendest du? Welche Informationen hast du mit ihnen geteilt? Welche Newsletter hast du abonniert? Welche Apps hast du installiert, und worauf haben sie Zugriff? Falls du die Accounts einer zivilgesellschaftlichen Organisation betreust: Wo haben deine Vorgänger:innen überall Profile angelegt?

Der erste Schritt folgt dem Motto: *Take back control!*

Entwickle zunächst ein Gespür dafür, wo du überall deine Daten hergibst und wie du dich im Netz bewegst.

2. Löschen, löschen, löschen – und löschen

Jetzt heißt es tapfer sein und etwas Zeit mitbringen. Beginne nach und nach deine Profile und Informationen, die du nicht mehr online haben möchtest, zu löschen. Denke an Marie Kondo und frage dich: Macht es mir noch immer Freude, diese Informationen zu zeigen? Benutze ich dieses Profil wirklich noch in meinem Alltag?

Mögliche To Do's (die Liste ist sicher nicht vollständig) in diesem Schritt können sein:

- Geh' in dein E-Mail-Postfach und melde dich von Newslettern ab, die du sowieso nie liest. Wenn du schon dabei bist, kannst du gleich prüfen, ob du beim Absender des Newsletters mal ein Nutzerkonto angelegt hast und das auch direkt löschen.

- Lösche Fotos (z.B. Partyfotos von 2009), Kontaktdaten (z.B. nicht mehr aktueller Mitglieder) und deine alten Posts (z.B. die Einladungen vergangener Veranstaltungen) auf Facebook, Instagram und Co. – also die, die du nicht mehr öffentlich zeigen möchtest.

- Gehe durch deine Smartphone-Apps und überlege, welche du eigentlich nicht wirklich verwendest. Lösche die, die du nicht brauchst, und mit ihnen gleich deine Profile.

- Checke auf deinem Smartphone die Privatsphäre-Einstellungen und minimiere die Zugangserlaubnis für Apps (z.B. zu Location-Services)

- Schaue in deinen Browserverlauf: Wo hast du dich noch so angemeldet in den letzten Monaten, welche Cookies kannst du löschen?
  Ein guter Tipp kann hier auch der Schlüsselbund im Browser sein, mit dem du dich sicher mal schnell bei dem einen oder anderen Service angemeldet hast.

- PS: Stelle unter "Einstellungen" deinen Browserverlauf so ein, dass zum Beispiel nach jeder Session oder ein Mal pro Monat deine Cookies und Einträge automatisch gelöscht werden.

3. Lege dir sichere Passwörter und einen guten Passwort-Manager zu

Im dritten Schritt geht es darum, die Dienste, die du wirklich verwenden möchtest, sicherer zu gestalten. Sicherheit einerseits vor Konzernen, andererseits aber auch vor alten Bekannten, denen du vielleicht mal ein (unsicheres?) Passwort zu einem Account gegeben hast, auf den sie jetzt noch immer Zugriff haben.

Sichere Passwörter sind ein absolutes Must-Have. Passwörter sollten immer

- mindestens 8-10 Zeichen lang sein
- eine Kombination aus Zahlen und Buchstaben enthalten
- keine Namen enthalten
- idealerweise aus Sätzen oder mehreren Sprachen bestehen
- nirgends notiert sein
- nicht mehrfach für unterschiedliche Dienste verwendet werden

Ein gutes Hilfsmittel, um den Überblick zu behalten, kann ein Passwort-Manager sein – zum Beispiel der kostenlose KeePassXC, LastPass oder 1Password (auch für Teams geeignet). Diese Manager helfen dir übrigens auch, knifflige Passwörter zu generieren, wenn du ein bisschen Inspiration suchst.

4. Aktiviere wo möglich die 2-Faktor-Authentifizierung

2-Faktor-Authentifizierung bedeutet, dass du dich bei einer Anmeldung mit einem weiteren Gerät (also zwei Mal) authentifizieren musst. Das TAN-Verfahren bei der Bank ist ein klassisches Beispiel dafür. Viele Services bieten in der Zwischenzeit 2-Faktor-Authentifizierung an (ja, sogar Facebook!). Entscheide, wo du besonders sicher sein möchtest und setze eine 2-Faktor-Authentifizierung auf. Die Anleitung dazu findest du im Regelfall in deinen Privatsphäre-Einstellungen im jeweiligen Service, häufig musst du dazu eine App installieren.

5. Sichere E-Mails mit Verschlüsselung

Jetzt geht es darum, auch für die Zukunft eine sichere Infrastruktur zur Kommunikation zur Verfügung zu haben. Ein möglicher erster Schritt, der nicht allzu viel Zeit in Anspruch nimmt, ist ein sicherer E-Mail-Dienst wie zum Beispiel posteo.de oder protonmail.com. Diese Dienste haben ihre Server in Europa und bieten je nach Bezahlmodell eine automatische Verschlüsselung an. Für Menschen mit etwas mehr IT-Expertise kann auch

eine PGP-Verschlüsselung eine kostenlose Alternative darstellen. Wenn du dich erst mal an PGP-Verschlüsselungen herantasten willst, kann Mailvelope eine browserbasierte Alternative für Verschlüsselung sein, für die du keine weitere Software installieren musst.

Hier noch ein freundlicher Reminder: Niemals Anhänge oder E-Mails öffnen, die du nicht kennst.

6. Sicheres Surfen mit einem VPN-Dienst und einem sicheren Internet-Browser

Wenn du viel in öffentlichen WLANs unterwegs bist, kann sich eine Investition in einen guten VPN-Dienst lohnen. VPNs können die IP-Adresse deines Endgeräts verändern und somit sicherstellen, dass du nicht zurückverfolgt werden kannst. Wenn dir VPN-Dienste zu teuer sind (bei kostenlosen VPNs bitte skeptisch sein, meist ist da jemand an deinem gebündelten Internet-Verhalten interessiert), können auch sichere Browser einen wichtigen Beitrag zu mehr Privatsphäre leisten. Der Tor Browser wird von vielen Netzaktivist:innen empfohlen, aber auch Firefox bietet bereits einige Einstellungs-möglichkeiten, die dir ein sichereres Surfen im Netz ermöglichen.

7. Sichere Messenger-Dienste installieren und weiterempfehlen

Im letzten Schritt kannst du dir einen sicheren Messenger-Dienst installieren. Hierbei solltest du auf Ende-zu-Ende-Verschlüsselung, aber auch weitere Privatsphäre-Einstellungen wie etwa den Zugriff auf deine Fotos achten. Signal oder der Element-Chat können gute Alternativen zu herkömmlichen Messenger-Diensten sein. Am Besten ist, wenn du deine Freund:innen oder Team-Kolleg:innen auch gleich dazu ermunterst, auf einen sicheren Messenger-Dienst umzusteigen. So ermöglichst du auch anderen eine sichere Kommunikation.

> *Generell gilt: Privatsphäre-Einstellungen und Services ändern sich leider sehr häufig. Deshalb kann ein “Digitales Ausmisten” ein Mal pro Jahr nie schaden. So behältst du nicht nur Kontrolle über alte Informationen im Netz, sondern auch über die digitalen Spuren, die du hinterlässt.*

Weiterführende Links

Kleines Einmaleins der Digitalen Selbstverteidigung von netzpolitik.org

Protect Your Digital Identity

Digitale Selbstverteidigung von Digitalcourage e.V.

Digital Detox Kit von Tactical Technology Collective *(auf Englisch)*