

Dein Leben. Deine Daten.

Praktische Tipps für mehr Datenschutz, zusammengestellt von der AG Digital der glp Kanton Zürich.

Welche Spuren hinterlässt du im Internet?

Unternehmen wie Google, Facebook, Apple und Microsoft wissen einiges über dich. Durch die Nutzung ihrer Dienste stimmst du zu, dass sie über dich sammeln wo du dich befindest, was du im Internet anschaust, welche Musik du hörst, was du gekauft hast, mit wem du befreundet bist, etc. Kurzum: so ziemlich alles, was du je im Internet gesucht oder angeschaut hast, ist gespeichert. Und spätestens nach dem „Cambridge Analytica“-Skandal (Daten-Leak bei Facebook) wissen wir auch, dass unsere Daten bei genannten Unternehmen leider nicht immer sicher sind.

Du hast nichts zu verbergen?

Viele Dienste sind heute nur darum so praktisch und «auf uns zugeschnitten», weil wir Unternehmen dafür Daten über uns zur Verfügung stellen. Warum sollte dich Datensammlung also stören?

„Wenn man sagt, die Privatsphäre ist mir egal, ich habe nichts zu verbergen, dann ist das so, wie wenn man sagt, die Redefreiheit ist mir egal, ich habe nichts zu sagen.“ E.Snowden, Amerikanischer Whistleblower

Wir sollten entscheiden können, welche Informationen über uns wir teilen wollen und was privat bleibt. Dies ist ein wichtiges Element unserer Selbstbestimmung! Leider wird Datensammlung aber heute grösstenteils nicht transparent betrieben: Entsprechende Bestimmungen sind meist in AGBs versteckt und es ist nur selten möglich, einen Dienst zu nutzen, wenn man der Sammlung nicht zustimmt. Diese Daten stellen auch ein mögliches Sicherheitsrisiko dar: Datenspuren können es für kriminelle einfacher machen, deine Identität zu fälschen und dir (finanziellen) Schaden zuzufügen.

Wie weisst du, ob deine Daten verwendet werden?

„There is no such thing as a free lunch“. Gratis Apps und Dienste gibt es im Allgemeinen nicht, ausser sie sind durch Spenden finanziert (zum Beispiel Wikipedia). Es gilt: Wenn du für einen Service nichts bezahlen musst, bist du höchstwahrscheinlich das (Werbe-)Produkt.

Datenschutzgesetz....da war doch was?

Die neue EU-Datenschutzgrundverordnung (DSGVO/GDPR) verpflichtet viele Unternehmen dazu, die Zustimmung zur Verwendung deiner Daten erneut einzuholen. Aber: Auch die neuen Bestimmungen hindern Unternehmen nicht daran deine Daten zu verwenden, solange du der Sammlung erneut zustimmst. Und meistens musst du das tun, um den Dienst nutzen zu können.

Gibt es Alternativen?

Willst du gar keine Daten mehr teilen, musst du Einsiedler werden. Es gibt jedoch simple Tricks, mit welchen du die Sicherheit deiner Daten erhöhen und kontrollieren kannst, was du über dich preis gibst:

- **Datenschutz beginnt bei dir!** Entscheide bewusst, was du auf Sozialen Medien etc. veröffentlichst.
- **Kommuniziere verschlüsselt:** Siehst du in der Adresszeile des Browsers „https“, ist der Transport der Seite verschlüsselt und die Daten somit während der Übertragung vor Angriffen geschützt. Auch die meisten E-Mail-Anbieter bieten verschlüsselte Kommunikation an. Nutze dieses Angebot.
- **Surfe im Private-Modus**, insbesondere für E-Banking (bei den meisten Browsern mittels Shift+Ctrl+P) oder lösche regelmässig den Browser-Cache und die Cookies (Shift+Ctrl+Delete).
- **Überlegte App-Installation:** achte darauf, welche Berechtigungen eine App wirklich braucht und verweigere alle anderen.
- **Vorsicht bei öffentlichen WLANs.** Der nächste kann deine Spuren lesen. Logge dich nur in vertrauenswürdige WLANs ein und logge dich am Schluss wieder aus.
- **WLAN nur bei Bedarf.** Wenn du nicht im WLAN bist, schalte die Funktion an deinem Handy aus. Ansonsten weiss der WLAN-Betreiber, dass du da bist, auch wenn du das Netz nicht nutzt.
- **Decke deine Kamera ab** um ungewünschte Einblicke in dein Privatleben zu verhindern. Du kannst ein Webcam-Cover kaufen, zur Not tut's aber auch ein Post-It oder ein Stück Isolierband.
- **Benutze Wegwerf-E-Mailadressen** wenn z.B. für eine Webseite eine E-Mail-Adresse benötigt wird nur um die Registrierung zu bestätigen (z.B. tenminutemail.com).
- **Werde aktiv!** Werde Teil der Arbeitsgruppe Digital der glp Kanton Zürich und unterstütze Organisationen wie die „Digitale Gesellschaft“ (www.digitale-gesellschaft.ch) oder den Chaos Computer Club welche sich für mehr Datenschutz und andere digitale Anliegen einsetzen.

Empfehlenswerte Anwendungen

Suchmaschine: DuckDuckGo.com
Mobile messenger: Threema, Signal
Browser: Mozilla Firefox und Opera
E-Mail: Protonmail oder Thunderbird

Das ist dir alles zu «basic»?

Nutze einen vertrauenswürdigen VPN-Service
Betriebssystem: Linux
Anonymisiertes Netzwerk: Tor-Browser
Gesonderte Accounts/Computer z.B. für E-Banking
Boote deinen Computer vom USB-Stick

Die AG Digital diskutiert Digitalthemen, erarbeitet politische Vorstösse und organisiert Veranstaltungen. Fokus ist der Kanton Zürich.
Diskutiere mit! Melde dich bei Simon Schlauri simon@schlauri.name