## Ich möchte Fördermitglied werden

denn Digitalcourage braucht meine Unterstützung

Firma | Organisation

Titel | Vorname

Name

Straße | Hausnummer

PLZ

Ort

E-Mail

Konto

BLZ

Bank

☐ **Ich zahle den normalen Mitgliedsbeitrag von 10 Euro pro Monat.**

☐ **Ich zahle den ermäßigten Mitgliedsbeitrag von 2,50 Euro pro Monat.**

**Mein Beitrag soll** ☐ **monatlich** ☐ **vierteljährlich** ☐ **jährlich von meinem Konto eingezogen werden.**

Hiermit ermächtige ich digitalcourage e.V. bis auf Widerruf, den genannten Mitgliedsbeitragbetrag regelmäßig von meinem/unseren Konto mittels Lastschrift einzuziehen. Weist mein/unser Konto keine Deckung auf, besteht für das kontoführende Institut keine Verpflichtung zur Einlösung. Die Erlaubnis kann ich jederzeit formlos widerrufen. Teileinlösungen werden nicht vorgenommen. Meine/unsere Daten werden elektronisch verarbeitet und nicht weitergegeben.

Ort | Datum

Unterschrift

Digitalcourage e.V. ist gemeinnützig. Mitgliedsbeiträge und Spenden können beim Finanzamt geltend gemacht werden. Anfang des Folgejahres versenden wir eine Bescheinigung über alle Mitgliedsbeiträge und Spenden aus dem jeweiligen Vorjahr.
Bitte schicken Sie dieses Formular als Brief an:
**Digitalcourage e.V. | Marktstraße 18 | 33602 Bielefeld**

digitalcourage

Marktstraße 18 | 33602 Bielefeld

### Einbruch in unseren inneren Garten

Wer schon einmal einen Einbruch in den eigenen vier Wänden erleben musste, kennt es: Das Gefühl der Ohnmacht und des Ekels. Man fühlt sich ausgeliefert, hilflos. Zu Recht.

Ein Einbruch in unsere digitale Privatsphäre und intimsten Gedanken ist nicht unmittelbar wahrnehmbar. Unsere Sorge davor verdrängen wir gerne. Aber tief in uns wissen wir, dass wir niemandem das Recht einräumen wollen, heimlich unseren „inneren Garten“ zu betreten.

Gegen das Gefühl der Ohnmacht können Sie etwas tun. Denn nicht nur Sie selbst, sondern auch die Gemeinschaft braucht Privatsphäre, um sich frei zu entfalten. Wir brauchen unsere kleinen Geheimnisse. Überwachung und Kontrolle schaden uns selbst, der Demokratie und der Freiheit.

Wir müssen das Mitschnüffeln technisch und juristisch unmöglich machen. Dafür braucht es eine Politik, die Freiheit statt Machtinteressen in den Mittelpunkt stellt. Bis es so weit ist, müssen wir uns selber schützen. Dieses Faltblatt soll ein erster Einstieg sein.

## Wir mischen uns mit charmanten und wirksamen Aktionen ein


Wir sind nicht gläsern - wir sind nackt. Dies stellten wir als lebendes Bild bei der Übergabe eines offenen Briefs an das Bundesinnenministerium dar: Wir fordern eine europäische Datenschutzverordnung, die ihrem Namen gerecht wird.
(Foto: photocube | Verena Hornung)

**Kontakt**

**Digitalcourage e.V.**
Marktstraße 18
33602 Bielefeld

Telefon: 0521-1639 1639
Telefax: 0521-61172

Mail: mail@digitalcourage.de
Web: https://digitalcourage.de
https://bigbrotherawards.de
Twitter: @digitalcourage
Shop: https://shop.digitalcourage.de

Unterstützen Sie uns per SMS mit 5 Euro: Senden Sie „courage“ an die **81190** (17 Cent behält der Anbieter)

Spendenkonto: 2129799 | Sparkasse Bielefeld | BLZ 480 501 61
oder online unter https://digitalcourage.de/spenden

Unsere Arbeit wird durch Mitgliedsbeiträge und Spenden finanziert.
Digitalcourage wirkt. Wirken Sie mit.

Bilder: Panthermedia (1), photocube (1), Photocase.com (5): kallejipp, zettberlin, view7, jingz
Wir danken Edward Snowden und seinen Helferinnen und Helfern.
V.i.S.d.P.: padeluun | Digitalcourage e.V. | V4-14|5

**Internet-Überwachung:**

# Digitale Selbstverteidigung

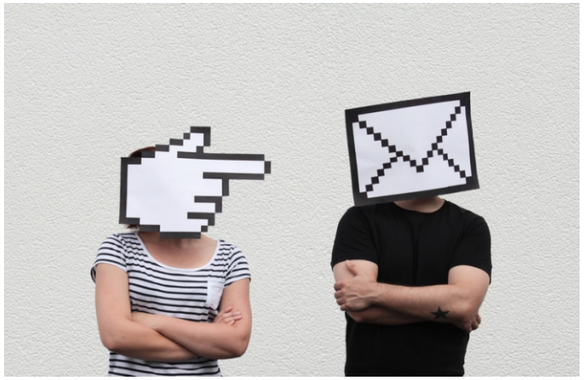
**Kleine Anleitung zur Selbsthilfe**

Die Spähaffaire zeigt, dass große amerikanische Firmen (wie zum Beispiel **Google, Facebook, Yahoo, Amazon, Microsoft** und weitere) unsere privaten Daten an **Geheimdienste** – und wer weiß an wen noch – weitergeben. **Schützen Sie sich.** Wir helfen Ihnen beim Einstieg in den Selbstschutz.

stiftung bridge Bürgerrechte in der digitalen Gesellschaft

digitalcourage

# Was Sie tun können:



## E-Mail und Chat

- **Benutzen Sie ein sicheres E-Mail-Postfach,** nutzen Sie kleine, europäische Anbieter wie etwa posteo.de, mykolab.com oder mailbox.org
- **Verwalten Sie Ihre Mails nicht im Browser,** sondern installieren Sie auf Ihrem Rechner einen E-Mail-Client wie z. B. Thunderbird.

  https://www.mozilla.org/de/thunderbird/
- **Verschlüsseln Sie Ihre E-Mails**. Wie das geht, haben wir schon in den 90er Jahren mit dem ersten deutschsprachigen PGP-Handbuch erklärt. In der Zwischenzeit ist es sogar noch einfacher geworden:

  https://www.thunderbird-mail.de/wiki/Enigmail_OpenPGP
- **Chatten Sie nicht über Facebook oder WhatsApp,** sondern benutzen Sie freie dezentrale Dienste, wie Jabber - auf Ihrem PC und auch auf Ihrem Mobilgerät. Dienste wie Threema und TextSecure wollen wir nicht empfehlen, können aber eine erste Alternative sein.

Aktualisierte Tipps und Hinweise (Download-Links, empfohlene Einstellungen) zu diesem Faltblatt sammeln wir für Sie auf unseren Webseiten.

https://digitalcourage.de/selbstverteidigung

## Suchmaschinen

Es gibt nicht nur Google. Viele andere Suchmaschinen gehen mit Ihren Daten umsichtiger um.

- Probieren Sie statt Google einmal ixquick.com, metager.de, duckduckgo.com, startpage.com, yandex.com oder yacy.net.
- Statt auf Google Maps können Sie sich auf openstreetmap.org orientieren.

## Werden Sie politisch aktiv

Individuelle Maßnahmen zum Schutz sind wichtig. Trotzdem müssen wir jetzt unsere Kräfte bündeln, damit sich das politische Klima ändert.

- Organisieren Sie mit Freunden und Bekannten Gesprächskreise.
- Schauen Sie sich nach „Cryptopartys“ in Ihrer Nähe um. Helfen Sie sich gegenseitig!
- Unterstützen Sie Organisationen, die in diesem Themenfeld arbeiten. Zum Beispiel uns: Digitalcourage setzt sich seit 25 Jahren für eine lebenswerte Welt im digitalen Zeitalter ein.

  https://digitalcourage.de/mitglied

## Anonym und sicher surfen

- Was beim Onlinebanking funktioniert, ist auch woanders möglich: **Achten Sie beim Surfen darauf, dass hinter dem „http“ in der Adresszeile immer ein „s“ steht.** Schreiben Sie es bei Bedarf dazu: „https“. Dann kann niemand „unterwegs“ Ihre Daten mitschnüffeln – „s“ steht für *secure* – die Verbindung ist verschlüsselt.

  https://de.wikipedia.org/wiki/HTTPS_Everywhere
- **Schauen Sie sich an, wie viele Websites Ihnen hinterherschnüffeln.** Installieren Sie Ghostery in Ihrem Browser. Das zeigt Ihnen bei jeder Internetseite an, wer daran interessiert ist, dass Sie dort surfen. Und blockiert gleich noch Ihre Erfassung in den großen Datenbanken, wie Google Analytics.

  https://de.wikipedia.org/wiki/Ghostery
- **Sind Sie über Ihren Browser wiedererkennbar?** Testen Sie Ihren Browserfingerabdruck. Ist er einzigartig, können Sie leicht wiedererkannt werden:

  https://panopticlick.eff.org/
- **Deaktivieren Sie Cookies**, wenn Sie darauf verzichten möchten. Verbieten Sie in jedem Fall, dass Cookies „von Drittanbietern“ akzeptiert werden.
- **Blockieren Sie Werbung,** da Werbeanzeigen Ihre Daten ausspionieren.

  https://de.wikipedia.org/wiki/Adblock_Plus
- **Nutzen Sie das Anonymisierungsnetzwerk Tor.** Sie können sich die benötigte Software kostenlos beim Torprojekt herunterladen. Ist Ihnen das zu umständlich, können Sie bei uns einen „PrivacyDongle“ kaufen, auf dem die Software bereits installiert ist.

## Digitale Mündigkeit

- Hinterfragen Sie Ihre digitalen Handlungen. Stellen Sie sich immer die Frage: Wenn ich das jetzt mache, wer hat außer mir einen Nutzen davon? Möchte ich das wirklich? Und warum ist das so schwer zu erkennen?
- Nutzen Sie möglichst wenige kostenlose Dienste. Machen Sie sich stets bewusst, dass Sie hier meist in einer anderen Währung bezahlen: mit Ihren Daten und Ihrer Freiheit.
- Behalten Sie die Kontrolle über Ihre Daten. Speichern Sie auf eigene Datenträger, Ihre Festplatte oder Ihrem Heimserver, statt in der „Cloud“.
- Nutzen Sie freie Software Linux (z.B. Ubuntu oder Mint) statt Apple oder Windows, LibreOffice statt Microsoft Office, Firefox statt Internet Explorer, Thunderbird statt Outlook.

  https://prism-break.org/#de
- Seien Sie immer vorsichtig: Hunderprozentige Sicherheit wird es nie geben.


Das Wichtigste ist, dass Sie politischen Einfluss nehmen. Sprechen Sie mit Ihrer Bundestagsabgeordneten oder Ihrem Europaabgeordneten. Sagen Sie klar und eindeutig NEIN zu Überwachung.