

Vorname: _____ Name: _____

Straße / Postfach: _____

Postleitzahl: _____ Ort: _____

E-Mail (für den Digitalcourage-Newsletter): _____

Ja, ich möchte Fördermitglied von Digitalcourage e.V. werden.

Mein Monatsbeitrag soll sein:

Ermäßigter Beitrag (2,50 Euro monatlich)

Normaler Beitrag (10 Euro monatlich)

Soli-Beitrag (20 Euro monatlich)

Eigener Soli-Beitrag: _____

IBAN oder Kontonr.: _____ Bank: _____

BIC oder BLZ: _____

Hiermit ermächtige ich Digitalcourage e.V., die Zahlungen von meinem Konto mittels Lastschrift einzuziehen. Zugleich weise ich mein Kreditinstitut an, die von Digitalcourage e.V. von meinem Konto eingezogenen Lastschriften einzulösen. Die Lastschriften sind mit der Gläubiger-ID DE07ZZZ00000323047 gekennzeichnet. Ich kann innerhalb von acht Wochen, beginnend mit dem Belastungsdatum, die Erstattung des belasteten Betrages verlangen. Es gelten dabei die mit meinem Kreditinstitut vereinbarten Bedingungen. Der Einzug einer einmaligen Spende sowie ggf. die erstmalige Zahlung bei wiederkehrenden Spenden und Beiträgen erfolgt zum nächstmöglichen Zeitpunkt. Künftige Zahlungseinzüge erfolgen dann immer am gleichen Kalendertag.

Ort, Datum: _____ Unterschrift: _____

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.



100.000 Unterschriften gegen die Vorratsdatenspeicherung werden in Brüssel übergeben (Foto: campact · CC BY-NC 2.0)

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 Falblatt soll ein erster Einstieg sein.

Digitalcourage wirkt. Wirken Sie mit!

- ▶ Sprechen Sie mit anderen über Datenschutz und Grundrechte.
- ▶ Lernen Sie digitale Selbstverteidigung. Bleiben Sie wachsam.
- ▶ Bestellen Sie unseren Newsletter. Verteilen Sie Infomaterial.
- ▶ Organisieren Sie Infostände und Aktionen in Ihrer Stadt.
- ▶ Sprechen Sie mit Ihren Bundestagsabgeordneten.
- ▶ Engagieren Sie sich in einer unserer AGs.
- ▶ Unterstützen Sie unsere Arbeit mit Geldspenden.
- ▶ Geben Sie uns Ihr Mandat: werden Sie Fördermitglied.



Wir mischen uns ein – mit charmanten und wirksamen Aktionen. (Foto: photocube · Verena Horning)

„Je mehr Bürgerinnen und Bürger mit Zivilcourage ein Land hat, desto weniger Helden wird es einmal brauchen.“

Franca Magnani, italienische Journalistin

Digitalcourage e.V.
 Marktstraße 18
 33602 Bielefeld

Web: digitalcourage.de
 bigbrotherawards.de

Mail: mail@digitalcourage.de
PGP: 8BCD A349 2DC2 A7D0

Twitter: @digitalcourage

Telefon: 0521 1639 1639
Telefax: 0521 61172

Spendenkonto:
 IBAN: DE69 3702 0500 5459 5459 20 · BIC: BFSWDE33XXX · Sozialbank
 oder online unter: digitalcourage.de/spende

Wir danken Edward Snowden und seinen Helferinnen und Helfern.

Foto Cover: Auremar, PantherMedia
Gestaltung: Jens Reimerdes

Foto Einbrecher: view7, photocase.com

Flyer Digitale Selbstverteidigung v1.2 - 03.2018



Internet-Überwachung:
Digitale Selbstverteidigung
 Kleine Anleitung zur Selbsthilfe

Fast im Wochentakt werden neue Ungeheuerlichkeiten offenbart, wie Geheimdienste und Großkonzerne sich intimste Informationen über uns zusammenstellen. Schützen Sie sich. Wir helfen Ihnen beim Einstieg in den Selbstschutz.

▶ digitalcourage

WAS SIE TUN KÖNNEN:

E-Mail und Chat

- ▶ **Benutzen Sie ein sicheres E-Mail-Postfach.** Nutzen Sie kleine, europäische Anbieter wie posteo.de oder mailbox.org, die in Transparenzberichten Behördenanfragen offenlegen und die Sicherheitsrichtlinie BSI TR-03108 umgesetzt haben.
posteo.de, mailbox.org
- ▶ **Verwalten Sie Ihre Mails nicht im Browser.** Installieren Sie einen E-Mail-Client wie z.B. Thunderbird (PC) oder K-9 Mail (mobil).
mozilla.org/thunderbird, github.com/k9mail/k-9
- ▶ **Verschlüsseln Sie Ihre E-Mails.** Wie das geht, haben wir schon in den 1990er-Jahren mit dem ersten deutschsprachigen PGP-Handbuch erklärt. In der Zwischenzeit ist diese Technik deutlich einfacher geworden:
thunderbird-mail.de/lexicon/entry/17-enigmail
- ▶ **Chatten Sie nicht über Facebook, WhatsApp, Telegram oder Threema.** Nur quelloffene Software verdient Ihr Vertrauen. Benutzen Sie am besten das dezentrale Protokoll XMPP (Jabber) mit OTR- oder besser OMEMO-Verschlüsselung, z.B. mit Gajim (Windows/Linux), Adium (Mac), Conversations (Android) oder ChatSecure (iOS). Bequemer ist Signal, das allerdings Ihr Adressbuch auf einem zentralen Server abgleicht.
digitalcourage.de/messenger
jabber.de, gajim.org, conversations.im

Aktualisierte Tipps und Hinweise ...

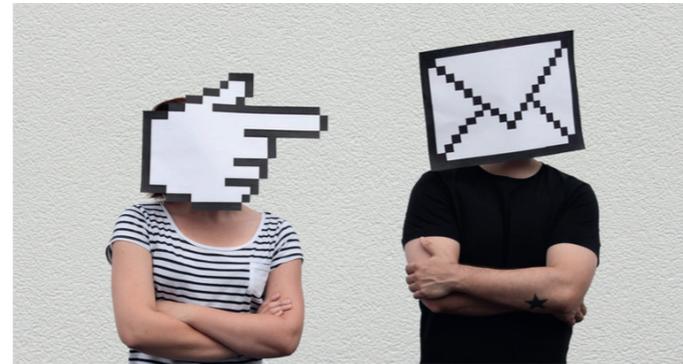
... zu diesem Faltblatt (Download-Links, empfohlene Einstellungen) sammeln wir für Sie auf unseren Webseiten.

digitalcourage.de/digitale-selbstverteidigung

Suchmaschinen

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

- ▶ Probieren Sie statt Google einmal startpage.com, ixquick.eu, metager.de oder searx.info!
- ▶ Statt auf Google Maps können Sie sich mit OpenStreetMap orientieren.
openstreetmap.org



Kommunizieren mit Herz, Hand und Hirn. (Foto: Sebastian Thanner · photocase.com)

Werden Sie politisch aktiv

Individuelle Schutzmaßnahmen sind wichtig. Trotzdem müssen wir unsere Kräfte bündeln, damit sich das politische Klima ändert.

- ▶ Organisieren Sie mit Freund:innen und Bekannten Gesprächskreise.
- ▶ Gehen Sie mit Ihrem Laptop zu einer „Cryptoparty“ in Ihrer Nähe. Geben Sie Ihr neues Wissen weiter!
cryptoparty.in
- ▶ Unterstützen Sie Organisationen, die in diesem Themenfeld arbeiten. Zum Beispiel uns: Digitalcourage setzt sich seit 1987 für eine lebenswerte Welt im digitalen Zeitalter ein.
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.
eff.org/https-everywhere
- ▶ **Hindern Sie Websites daran, Ihnen hinterherzuschnüffeln.** Der Privacy Badger erlernt schnüffelnde Drittwebsites und blockiert diese, ohne Ihr Surferlebnis zu beeinträchtigen. Fortgeschrittene haben mit NoScript die Kontrolle über nachgeladene Programme (JavaScript).
eff.org/privacybadger, noscript.net
- ▶ **Sind Sie über Ihren Browser wiedererkennbar?** Testen Sie Ihren Browser-Fingerabdruck. Ist er einzigartig, können Sie leicht wiedererkannt werden.
panopticklick.eff.org
- ▶ **Beschränken Sie Cookies.** Verboten Sie in jedem Fall, dass Cookies „von Drittanbietern“ akzeptiert werden. Am besten stellen Sie Ihren Browser so ein, dass beim Beenden alle Cookies gelöscht werden. Das Add-on „Cookie AutoDelete“ löscht sie, sobald sie nicht mehr benötigt werden.
addons.mozilla.org/de/firefox/addon/cookie-autodelete
- ▶ **Blockieren Sie Werbung,** da Werbeanzeigen Ihre Daten ausspionieren. Z.B. mit dem Add-on uBlock Origin.
addons.mozilla.org/de/firefox/addon/ublock-origin
- ▶ **Nutzen Sie das Anonymisierungsnetzwerk Tor.** Sie können sich den Tor-Browser kostenlos beim Tor-Projekt herunterladen. Ist Ihnen das zu umständlich, können Sie bei uns einen „PrivacyDongle“ kaufen, auf dem die Tor-Software bereits installiert ist.
torproject.org, shop.digitalcourage.de

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 – am besten verschlüsselt – auf eigenen Datenträgern, Ihrer Festplatte oder Ihrem Heimserver statt in der „Cloud“.
- ▶ Nutzen Sie freie Software: Linux statt Apple oder Windows, LibreOffice statt Microsoft Office, Firefox statt Internet Explorer, Thunderbird statt Outlook.
prism-break.org/de
- ▶ Seien Sie immer vorsichtig: Hundertprozentige 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.

(Foto: zettberlin · photocase.com)

