Wir arbeiten in 5 AGs an diesen Themen:

Flucht & Migration

- Die Visa Warndatei
- Die europäische Fluggastdatenbank
- FRONTEX, die EU-Grenzschutzagentur
- Europol-Novelle
- Schengen-Informationssystem II

Polizei, Geheimdienste & Militär

- Vorratsdatenspeicherung
- Video- und Lauschangriff auf Wohnungen
- Datenabgleich zwischen Polizei und Geheimdiensten (GTAZ)
- Das zentrale Bundesmelderegister BZR
- Rasterfahndung in zentralen Datenbanken
- Biometrische Daten im elektronischen Ausweis und Pass
- Keine Online Durchsuchung privater PCs, weg mit dem Staatstrojaner

SchülerInnen-Themen

- Baby-Datei, Schüler-Datei,
- Kein Militär an Schulen
- Zivilklauseln an die Unis
- Persönlichkeitsprofile, lebenslang abgestempelt

Verbraucher- und ArbeitnehmerInnen-Datenschutz

- Gläserner Bürger, Kundenkarten, Scoring
- Die elektronische Gesundheitskarte
- Für Datenschutz auch am Arbeitsplatz
- Gegen den elektronischen Einkommens-nachweis ELENA … und Nachfolger
- Die bundeseinheitliche Steuernummer

Zensur & Informationsfreiheit

- Gegen Internetsperren und Zensur
- Für Netzneutralität & Informationsfreiheit
- Stopp ACTA
- Open Source statt Kommerzialisierung

Verteidigen wir gemeinsam unser Grundgesetz, unser Recht auf informationelle Selbstbestimmung und die Menschenwürde!

Jede/r kann mitmachen und sich mit uns für seine Bürgerrechte einsetzen.

Die nächsten Termine unserer regelmäßigenTreffen im Berliner Antikriegs-Café COOP, Rochstr. 3, Nähe Alexanderplatz, werden auf unseren Webseiten unter dem Punkt **Aktivengruppen** angekündigt.

Aktion Freiheit statt Angst e.V.
Rochstr. 3,
D-10178 Berlin
Tel: +49-30-69209922-1
Fax: +49-30-69209922-9
Mail: kontakt@aktion-fsa.de
Web: aktion-freiheitstattangst.org

Freiheit statt Angst
AKTIONSBÜNDNIS
Bündnis für Freiheitsrechte, gegen Massen-Überwachung und Sicherheitswahn

Spendenkonto:

Aktion Freiheit statt Angst e.V.
Triodos Bank
IBAN: DE72 5003 1000 1060 9910 02
BIC: TRODDEF1

Der Verein ist ab 01.01.2011 nach §§ 52 1(2) Nr. 24 AO als gemeinnützig anerkannt, Spenden sind steuerlich absetzbar.

Freiheit statt Angst
AKTIONSBÜNDNIS

Aktion Freiheit statt Angst e.V.

Bündnis für Freiheitsrechte, gegen Massen-Überwachung und Sicherheitswahn

Anonym und sicher im Internet

Tipps & Tricks

Was soll dieser Flyer?

Wir möchten damit ein paar Hinweise geben, wie man sich mit einfachen Mitteln gegen das Ausschnüffeln im Internet wehren kann. Gefahren drohen durch Viren und Trojaner aber auch durch die Datensammelgier der großen Medienanbieter wie Google, Facebook, Microsoft, u.a., sowie diverser Geheimdienste.

Grundsätzliches

95% aller Viren werden für Windows Rechner geschrieben, weil die Bösewichter damit die große Mehrheit der PCs erreichen können. Nutzt man stattdessen ein freies (kostenloses) Linuxsystem oder einen Apple Mac ist die Wahr scheinlichkeit von einem Virus befallen zu wer den viel geringer. Ein weiterer Vorteil eines offe nen Systems (**Open Source**) liegt darin, dass in den Systemen weniger Fehler und Hintertüren enthalten sein sollten, da die Software von vie-len Menschen unabhängig voneinander unter-sucht und getestet wird. Inzwi-schen sind auch fast alle An-wendungen als Open Source verfügbar, z. B. http://de.libreoffice.org

Mit, z.B. dem Programm Virtual Box, kann man auf einem PC auch mehrere (virtuelle) Systeme nebeneinander laufen lassen, ein System zum Spielen, eins fürs Mailen und … - ohne, dass eines von den Daten des anderen weiß.
https://www.virtualbox.org/

Ab ins Internet

Der Zugang zum Internet sollte durch eine Fire wall geschützt sein. Nur die wirklich genutzten Anwendungen dürfen ins Internet und eigentlich auch nur, wenn man sie nutzt. Der Ein-/Aus-Schalter für das Netzwerk in der Menuleiste kann sehr hilfreich sein.

- Für das Surfen eignet sich wieder am besten ein OpenSource-Browser, wie Mozilla Firefox. Hände weg vom Internet-Explorer oder Google Chrome.
  https://www.mozilla.org/de/firefox/new/

- Zusätzlich sollte der Browser durch Plugins wie NoScript, AdBlock-Plus, BetterPrivacy, Flashblock, Ghostery, https-everywhere u.ä. geschützt werden.
  https://addons. mozilla.org/de/firefox/
- „Googeln“, also suchen im Internet, muss man nicht mit Google, besser für den Schutz der eigenen Daten ist z.B. Ixquick oder DuckDuckGo. Ixquick kann standardmäßig mit verschlüsselter Übertragung (https statt http) suchen und findet auch alles. https://www.ixquick.com
  http://duckduckgo.com/

Anonym im Internet

Jede/r hat nach deutschem Telemediengesetz (TDG) das Recht sich im Internet anonym zu bewegen. Wenn man sicher sein will, kann man das kostenlose aber auch langsame „Tor-Netz-werk“ nutzen. Einen vorinstallierten Firefox-Browser für Tor gibt es hier:
https://www.torproject.org/

Kostenlos ist nicht umsonst

Viele Angebote im Internet werden als „kosten los“ beworben. Die Anbieter leben dann von un seren Daten, indem sie unsere Persönlichkeits profile an die Werbeindustrie verkaufen – also möglichst anonym bleiben … oder möglichst gleich auf diese a-sozialen Netzwerke, wie z.B. Facebook, Google und Twitter verzichten.

E-Mails verschlüsseln

Auch für Mails ist die Nutzung eines OpenSource Programms, wie z.B. Thunderbird sinnvoll.
https://www. mozilla.org/de/thunderbird/
Es kann mehrere E-Mail- Adressen verwalten. Nach dem Motto „Ich bin viele“ lohnt es sich für verschiedene Bereiche, auch verschiede Adressen zu verwenden. Thunderbird unterstützt mit dem Plugin Enigmail

Mit GnuPG auch verschlüsselte E-Mail.
http://enigmail.mozdev.org/

E-Mail Knigge-Tipp: Wenn du nicht willst, dass alle dein Adressbuch kennen lernen, so schreibe keine Massenmails mit den Adressen im „To:“ oder „Cc:“ - dafür gibt es die Blindkopie „Bcc:“.

Sichere Passwörter – und nicht vergessen

- Passwörter sollten mindestens 8 Zeichen lang sein, möglichst mehr und neben großen und kleinen Buchstaben auch Zahlen und Sonderzeichen enthalten.
- Für verschiedene Anwendungen nicht die gleichen Passwörter verwenden!
- Wer soll sich die alle merken? Wenn's trotz „Eselsbrücken“ nicht im Kopf bleiben will, dann hilft das Open Source Programm KeePassX, das für alle Betriebssysteme zur Verfügung steht. https://www.keepassx.org/
- Passwörter, die die meisten Browser für uns „netterweise“ speichern wollen, sind leicht zu knacken, da nur schlecht ver-schlüsselt – also nicht benutzen.
- Wer nicht nur verschlüsselt mailen möchte, kann auch seine Daten auf dem PC oder USB-Stick mit Truecrypt verschlüsselt speichern. http://www.truecrypt.org/
- Trotzdem bedenken: **Jede** (!) Verschlüsselung lässt sich mit genügend Aufwand in ferner Zukunft mal knacken!

Viel mehr zu diesen endlosen Themen findet sich auf unseren Webseiten unter „Verbraucher-datenschutz“ und „Anti-Überwachung“.
https://www.aktion-freiheitstattangst.org/

Haben Sie weitere Fragen?
Schreiben Sie uns kontakt@aktion-fsa.de
www.aktion-freiheitstattangst.org

Engagieren Sie sich für Ihre Bürgerrechte!
Bürgerrechtsarbeit kostet – Spenden Sie!