

Datenschutzfreundliche Suchmaschinen benutzen

Anstelle von Google z.B. Ixquick. Auch die deutsche Wikipedia eignet sich hervorragend zur Suche. Beide Dienste lassen sich mit standardmäßig verschlüsselter Übertragung als Ein-Tasten-Kurzbefehl oder in der Suchleiste im Firefox-Browser einrichten, was die Arbeit sehr erleichtert. Siehe: <https://www.ixquick.com/deu/> und: <https://de.wikipedia.org/> oder auch: <https://duckduckgo.com/>



Noch mehr Hinweise

Sicherungskopien anlegen

Die für einen persönlich wichtigsten Daten möglichst regelmäßig sichern (auf externen Laufwerken oder – platzsparender – auf Speicherkarten) und an anderen Stellen sicher verwahren.

Kostenlose und offene Software benutzen

Firefox und Thunderbird (s.o.), LibreOffice (früher: OpenOffice) statt Word, Exel und PowerPoint. Gimp und Inkscape zur Grafikverarbeitung, Blender zum Videoschnitt und für 3D-Animationen. Siehe <http://de.libreoffice.org/> und <http://www.gimp.org/> und <http://www.inkscape.org/> und www.blender.org



Metadaten in Dokumenten bedenken

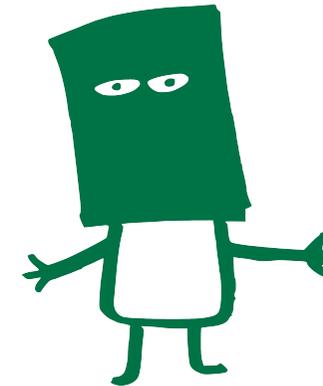
Fotos, Videos, Textdokumente, PDF-Dokumente, E-Mails – alle enthalten so genannte „Meta-Daten“ oder andere nicht sichtbare Informationen, die darüber Auskunft geben können, wann, von wem, an welchem Ort, mit welchem Gerät Fotos aufgenommen, Texte usw. geschrieben worden sind. Gleiches gilt für Ausdrücke von Druckern und Kopierern.

Verzicht/Beschränkung bei (a)sozialen Netzwerken

Facebook, Twitter, Google & Co. leben von der Sammlung und Verwertung eurer persönlichen Daten und machen damit Geld und Profit. Verzichtet darauf oder macht euch intensiv bewusst, was das bedeutet und ob bzw. wie ihr damit umgehen möchtet. Zum Anhören: <http://devianzen.de/20110401-bba-laudatio-rena-tangens-facebook.mp3> und <http://devianzen.de/20120204-DigitalerTsunami-RenaTangens.mp3>

Umgang mit Mobiltelefonen

Smartphones sind grundsätzlich unkontrollierbar – die Wahrung der Privatsphäre und die Benutzung von Smartphones stehen einander im Widerspruch. Ältere Handys sind dagegen tendentiell „sicherer“. Stille SMS zur Lokalisierung von Mobilfunkgeräten und Überwachung durch IMSI-Catcher sind nur mittels komplexer Hardware erkennbar. Handys können auch nach dem Ausschalten weiter aktiv sein und eventuell als Mikrofon-Wanze fungieren. Da hilft nur: Akku raus! Siehe auch <http://www.daten-speicherung.de/index.php/kartentausch/> oder <http://wiki.freieitsfoo.de/pmwiki.php?n=Main.Handytauschboerse>



Weiterlesen

Informationen über sichere Kommunikation:

https://wiki.vorratsdatenspeicherung.de/Sichere_Kommunikation

Ein taz-Beitrag über technische Gegenmaßnahmen:

<https://www.taz.de/!86966/>

Welche Methoden die Staatsanwaltschaften anwenden:

<https://www.vorratsdatenspeicherung.de/content/view/494/79/lang/de/>

Sammlung von Software-Empfehlungen für sichereres Arbeiten am und im Netz:

<https://prism-break.org/>

Wie schütze ich meine Privatsphäre im Netz?

Über diesen Flyer

Wir sind der Meinung, dass jeder Mensch prinzipiell das Recht und die Möglichkeit haben sollte, sich auf seinen Wunsch hin anonym fortzubewegen. Sei es im realen Leben in Stadt und auf Land, sei es im Internet oder in anderen virtuellen Räumen jetzt und in Zukunft.

Anonymität eröffnet allerdings auch die Möglichkeit, diese missbräuchlich zu benutzen. Das, was unsere Gesellschaft als normabweichend oder Verbrechen definiert, kann mit Hilfe von Anonymität ermöglicht oder erleichtert werden. Nach unserer Überzeugung überwiegen jedoch die Vorteile, die sich aus den Möglichkeiten anonymer Fortbewegung und Meinungsäußerungen für den Menschen der ihn umgebenden Gemeinschaft:

Erst das gesicherte Vorhandensein und die Nutzung privater und unbeobachteter Räume ermöglicht dem Menschen eine vielfältige und reflektierte Entwicklung seiner Persönlichkeit. Nur eine vom Überwachungsdruck befreite und unbeschwerte Umgebung lässt einen Austausch von Meinungen und Ideen sowie die Reifung eines gesunden, frohen und produktiven Charakters zu, der einer menschlichen und kreativen Weiterentwicklung der Gesellschaft behilflich sein kann.

Dieses Blatt gibt nicht mehr als ein paar erste technische Anregungen zur Schaffung und Förderung privater und geschützter Kommunikation und möglichst anonymer Bewegung in den Netzen. Die Hinweise sind nicht mehr als lose Bruchstücke - der Versuch einer lückenlosen und umfangreichen Darstellung wäre von Anfang an aussichtslos.

Betriebssystem und Browser

Computer-Betriebssystem

Falls möglich ein freies Linux-Betriebssystem benutzen (z.B. LUbuntu, XUbuntu oder Debian). So etwas ist immer sicherer, und freier als jedes Windows- oder Apple-OS-Betriebssystem (stellt für sich alleine aber noch keinerlei Gewähr dar!) Bei der Installation möglichst die „Alternate“-Version verwenden, mit der die komplette Verschlüsselung der Computer-Festplatte auf einfache Art und Weise in einem Rutsch erledigt wird. <http://www.lubuntu.net/> und <http://xubuntu.org/> und <http://www.debian.org/>



Internet-Browser

Den OpenSource-Browser Mozilla Firefox verwenden statt Internet-Explorer oder GoogleChrome! <https://www.mozilla.org/de/firefox/new/>



Browser-Einstellungen

Unter Extras/Einstellungen/Datenschutz entweder auf permanent privaten Modus umschalten oder aber so, dass keine Chroniken gespeichert werden und Cookies nach jedem Schließen des Firefox gelöscht werden (und dementsprechend ab und zu mal den Firefox schließen und wieder neustarten).

Firefox-Browser-AddOns

Empfehlenswert sind folgende zusätzlichen AddOns: AdBlock-Plus (mit abonniertes Privacy-Blocklist), BetterPrivacy, Flashblock, Ghostery, HTTPS-everywhere, NoScript, Stealther, Cookie Monster, RequestPolicy

Google-„Safebrowsing“ ausschalten

Standardmäßig ist eine Funktion eingeschaltet, die die Übertragung bestimmter Verhaltensdaten an Google beinhaltet. Diese Funktion kann man deaktivieren: <https://wiki.vorratsdatenspeicherung.de/Googlesafebrowsing>

Anonym surfen

Dafür gibt es mehrere Möglichkeiten. Kostenlos und nicht nur deswegen empfehlenswert ist das so genannte „Tor-Netzwerk“. Dort gibt es ein Komplet-Paket, in dem ein bereits vorinstallierter Firefox-Browser die Nutzung dieses Services sehr einfach macht. Wichtiger Hinweis: Durch die Übertragung von Computer- und Browser-Einstellungs-Daten ist eine 100%ige Anonymisierung nicht oder nur schwer möglich. Aber die Verwendung von Tor ist ein sehr großer Schritt in diese Richtung. Siehe <https://www.torproject.org/projects/torbrowser.html.en> oder auch <http://www.daten-speicherung.de/index.php/test-internet-anonymisierungsdienste/>



E-Mails

E-Mail

Keine E-Mails von „Kostenlos-Anbietern“ verwenden. Umsonst ist das nicht, ihr bezahlt mit euren Daten und Informationen über euer Wesen, euer Verhalten, eure Persönlichkeit. Nicht nur Gmail erlaubt sich (und anderen!?) das Durchsuchen eurer Mails nach interessanten Stichworten und Inhalten! Vertrauenswürdige E-Mail-Anbieter, die sich über eine Spende in der Größe eurer Wahl (am besten: weniger, aber dafür als Dauerauftragsspende!) freuen oder den E-Mail-Dienst sehr günstig anbieten, sind: <https://so36.net/> oder <https://riseup.net/> oder <http://nadir.org/> oder <http://privatemail.net/> oder <https://posteo.de/> oder <https://www.mtmedia.org/>

E-Mail-Verwaltung

Nicht nur einfacher, sondern auch sicherer und übersichtlicher ist die Nutzung des OpenSource Programms Thunderbird (ein so genannter „E-Mail-Client“), mit dem ihr auch mehrere E-Mail-Adressen verwalten könnt. <https://www.mozilla.org/de/thunderbird/>



E-Mails verschlüsseln

Mit Thunderbird lässt sich auch die E-Mail-Verschlüsselung einfach und anwenderfreundlich durchführen. Mit dem AddOn namens „Enigmail“ könnt ihr somit dafür sorgen, dass niemand anderes außer der Empfänger in der Lage ist, den Inhalt eurer E-Mails zu lesen. Oft wird diese Verschlüsselung auch als „PGP“ oder „GnuPG“ bezeichnet. Wichtiger Hinweis: Nicht verschlüsselt wird die Betreffzeile!



E-Mails schreiben und weiterleiten

Bitte leite keine dir zugeordnete E-Mail an andere Menschen weiter, ohne dir sicher zu sein, dass der Verfasser dieser Mail damit einverstanden ist/wäre. Und bitte schreibe keine Massenmails, bei denen die Empfänger-E-Mail-Adressen allen anderen Empfängern offenbart wird. Nutze die „Bcc“-Versendefunktion, die als „Blindkopie“ die E-Mails-Daten nicht weiterleitet.

Verschlüsselung & Co.

Daten verschlüsseln

Dateien und ganze oder Teile von Computern bzw. ihrer Festplatten können hochgradig sicher verschlüsselt werden. Ein gutes Programm dafür ist Truecrypt. <http://www.truecrypt.org/downloads>



Halbwertzeit von Verschlüsselung

Bedenke, dass es keine Verschlüsselung gibt, die eine 100%ige und dauerhafte Sicherheit gewähren kann. Bislang wurde jede, als noch so sicher dahingestellte Verschlüsselungsmethode irgendwann mal „geknackt“. Darum: Sei dir dessen bewusst. Sei dir mit allem, was du tust und lässt im Reinen und tue nichts, was du mit deinem Gewissen nicht vereinbaren kannst.

Sichere Passwörter

Möglichst niemals gleiche Passwörter für mehrere Zwecke einsetzen. Das Bekanntwerden an einer Stelle kann sonst zu größten Problemen führen. Ausreichend lange Passwörter mit Zeichen, Zahlen und möglichst ohne Wörter, die in Lexikas zu finden sind. Eselsbrücken bauen. Beispiel „Das ist mein Passwort für das blöde Google-Netzwerk.“ wird zu „D1mPw>d:(G00gle-Nw.“

Vorsicht mit der „Cloud“

Bei in der so genannten Cloud abgelegten Daten gibst du die Herrschaft über diese Daten grundsätzlich an andere ab. Noch viel weniger als sonst schon kannst du erkennen, wer diese Informationen abgreift, beobachtet, benutzt oder manipuliert. Gute Sicherheitskonzepte mögen die Gefahr etwas minimieren, aber niemals aufheben können. Je glänzender und begeisterter die Versprechungen der Unternehmen und der Anbieter sind, umso misstrauischer und kritischer sollte man dem begegnen.