Jason Mason: Sicherheit bei Nutzung des Internets Teil 3 – Hier findet ihr einfache und kostenlose Methoden sowie Werkzeuge, um eure Computer, Laptops, Tablets und eure Privatsphäre vor Gefahren aus dem Internet zu schützen

„Ich kann nicht guten Gewissens zulassen, dass die US-Regierung mit dieser massiven Überwachungsmaschine, die sie heimlich baut, die Privatsphäre, die Internetfreiheit und die Grundfreiheiten der Menschen auf der ganzen Welt zerstört.“ Edward Snowden, Whistleblower Quelle

Spätestens dann, wenn man von der Corona-App und weiteren geplanten Aktionen, wie z.B. die Einführung des digitalen Euro, Supercomputern, Digitalisierung von Schulen, Künstlicher Intelligenz und digitaler Identität liest, wird einem wieder bewusst, wie wichtig die eigene Absicherung gegen die externe Kontrolle und das Ausspionieren ist.

Dank Jasons freundlicher Bereitschaft zur Zusammenarbeit mit Transinformation können wir euch seinen aktuellen Artikel zu dieser Thematik anbieten, der aus drei Teilen besteht. Hier findet ihr Teil 1 und Teil 2.

Gerne könnt ihr auch unser mehrteiliges Interview mit Jason lesen, von dem bereits Teil 1, Teil 2, Teil 3a und Teil 3b veröffentlicht wurden. Weitere werden noch folgen.

Ich habe mich aufgrund einiger Anfragen zu diesem Thema entschlossen, einen neuen Artikel zu verfassen, bei dem sich alles um die Sicherheit im Internet bei Computern und Smartphones dreht.

Der Fokus liegt dabei auf den verbreiteten Windows-Rechnern und Android-Geräten. Ich stelle hier eine Reihe von Tools vor, die es ermöglichen, sicherer im Netz unterwegs zu sein und die eigene Privatsphäre vor Spähangriffen zu beschützen.

Datenschützer weisen ausdrücklich darauf hin, dass man von diesen meist einfach zu installierenden Tools Gebrauch machen sollte, um der vollständigen Überwachung aller Aktivitäten am Computer, Smartphone und im Netz entgegenzuwirken.

Sichere Suchmaschinen

Es folgt nun eine Aufzählung einer Reihe von sicheren Suchmaschinen, die man aus Datenschutzgründen Google vorziehen und sie daher als Standardsuchmaschine im jeweiligen Browser festlegen sollte.

DuckDuckGo

https://duckduckgo.com/

https://3g2upl4pq6kufc4m.onion/?t=h_

Da wäre einmal DuckDuckGo, eine Suchmaschine, die besonderen Wert auf Privatsphäre legt.

Das Hauptaugenmerk bei DuckDuckGo wurde auf das Thema Datenschutz und Privatsphäre gelegt. Die Suchmaschine speichert keine IP-Adressen, protokolliert keine Informationen über Besucher und verwendet Cookies nur in überschaubaren Massen. DuckDuckGo hat sich im Laufe der letzten Jahre zu einer konkurrenzfähigen Suchmaschine zu Google entwickelt und verfügt auch über eine .onion Seite für den anonymen Tor Browser.

Startpage

https://www.startpage.com/

Eine andere Alternative ist die Suchmaschine Startpage. Mit Startpage nutzt ihr die Suchmaschine Google, ohne dass der Internetkonzern euch verfolgen kann. Dafür anonymisiert der Dienst eure Suchanfragen und schickt sie dann erst an Google weiter.

Somit profitiert ihr von dem starken Google-Suchalgorithmus und schützt gleichzeitig eure Privatsphäre. Mittlerweile hat sich der Funktionsumfang von Startpage noch einmal vergrössert. Die anonyme Suchmaschine kommt jetzt auch mit interaktiven Karten zurecht und liefert euch Wikipedia-Sofortantworten.

MetaGer

https://metager.de/

http://metagerv65pwclop2rsfzg4jwowpavpwd6grhhlvdgsswvo6ii4akgyd.onion/

MetaGer ist eine Open-Source-Metasuchmaschine mit Sitz in Deutschland, die Suchergebnisse von Bing, Yandex, Yahoo und anderen Suchmaschinen erhält und über einen eigenen

Web-Crawler verfügt.

Ähnlich wie bei Startpage konvertiert MetaGer Suchanfragen in anonyme Abfragen über einen Proxyserver, der auch die anonyme Anzeigeoption mit allen Ergebnissen bereitstellt. Benutzer-IP-Adressen werden aus Datenschutzgründen abgeschnitten, obwohl Benutzer-Agent-Informationen an die Suchpartner weitergegeben werden.

MetaGer verwendet keine Cookies oder andere Tracking-Methoden. Wenn ihr jedoch eine Mitgliedschaft erwerbt, könnt ihr völlig werbefreie Suchergebnisse erhalten. Ohne Mitgliedschaften und persönliche Spenden kann MetaGer den Betrieb nicht fortsetzen. Für diejenigen im Tor-Netzwerk betreibt MetaGer auch eine .onion Website.

Searx

https://searx.info/

Searx ist freie Software, bei der der Code 100% Open Source ist, so dass jeder dazu beitragen kann, ihn zu verbessern. Searx ist eine Metasuchmaschine, was bedeutet, dass es Ergebnisse von beliebten Suchmaschinen sammelt und kombiniert.

Searx entfernt alle identifizierenden Daten aus eurer Anfrage, sodass Google, Yahoo und andere Suchmaschinen den Suchbegriff als anonyme Anfrage erhalten. Es speichert keine Daten über eure Suche und gibt niemals etwas an einen Dritten weiter.

Disconnect Search

https://search.disconnect.me/

Disconnect Search ist ein weiteres nützliches privates Suchmaschinentool, das die Hilfe bei der Inhaltssuche von grossen Suchmaschinen wie Google, Yahoo und Bing verwendet. Diese Suchmaschine verfolgt niemals eure Online-Suchen, Aktivitäten oder IP-Adresse. Disconnect Search ermöglicht es euch, eure Abfrage anonym zu übermitteln.

Gibiru

https://gibiru.com/

Gibiru ist eine weniger bekannte Option für die private Suche. Es verwendet auch Google, um zu suchen und entfernt Tracking-Daten, bevor das Ergebnis zu euch kommt.

Der Entwickler hinter dieser Suchmaschine sagt, er habe Gibiru entworfen, um genau so zu arbeiten, wie Google es in jenen idealistischen Tagen vor Tracking und Monetarisierung getan hat. Er sagt, Gibiru ist schneller als NSA-Suchmaschinen, weil es alles – ausser dem, was für die Suche benötigt wird – entfernt.

Quelle

Verschlüsselung von Ordnern, Partitionen, Betriebssystemen und Festplatten

Besonderen Wert legt Edward Snowden auch auf die komplette Verschlüsselung des ganzen Computersystems.

Es gibt hier verschiedene Möglichkeiten, je nachdem, welches Betriebssystem man nutzt. Am

besten ist es, die ganze Festplatte bzw. das ganze System zu verschlüsseln. Wenn der Computer gestohlen oder konfisziert wird, ist es fast unmöglich, an eure privaten Daten zu gelangen.

Da die meisten Leute immer noch ein Windows-Betriebssystem nutzen, bieten sich hier folgende Möglichkeiten:

TrueCrypt

TrueCrypt ist eine Software zur Datenverschlüsselung, insbesondere zur vollständigen oder partiellen Verschlüsselung von Festplatten und Wechseldatenträgern.

Das Programm läuft unter Windows ab der Version 2000 bis zur Version Windows 8. Laut einer Meldung auf der offiziellen Website wurde die Entwicklung von TrueCrypt im Mai 2014 eingestellt.

Bei TrueCrypt wurden anscheinend Sicherheitslücken entdeckt. Viele Benutzer schwören heute immer noch auf die sichere Version TrueCrypt 7.1a.

https://www.chip.de/downloads/TrueCrypt_13015067.html

VeraCrypt

Veracrypt ist ein Nachfolger von TrueCrypt. Die Entwickler behaupten, die bisher entdeckten Sicherheitslücken behoben zu haben. VeraCrypt wird laufend weiterentwickelt. VeraCrypt bietet die Möglichkeit, gesamte Systeme, einzelne Partitionen oder sogenannte „Container“ zu verschlüsseln.

Bei Letzterem handelt es sich um spezielle Dateien mit fester Grösse, die nach dem Entschlüsseln wie virtuelle Laufwerke behandelt werden. Durch die Verschlüsselung eures Systems mit Veracrypt seid ihr gegen Ausspähungen von Regierungen und Konzernen gewappnet.

Im Zweifelsfall fällt die Wahl immer auf VeraCrypt. Es wird ständig weiterentwickelt und ist als sicher eingestuft. Hier ein paar Informationen zu den Funktionen von VeraCrypt.

https://www.chip.de/downloads/VeraCrypt_70310496.html

https://veracrypt.de.uptodown.com/windows

Anleitung Software Daten sichern VeraCrypt kostenlos

Anleitung Veracrypt

USB Crypt

https://www.usbcrypt.com/

USBCrypt ist der Name einer hochentwickelten Verschlüsselungssoftware, die das zweistufige

Verifizierungssystem an USB-Inhaber liefert, um eure Daten vor unbefugtem und unerwünschtem Zugriff zu schützen.

Es wird euch in die Lage versetzen, eure Daten die ganze Zeit auf tragbare Weise zu sichern. Es ist eine völlig kostenlose portable Anwendung für das Windows-Betriebssystem.

Das neue Verschlüsselungssystem von USBCrypt basiert auf einem militärischen Schutzsystem, so dass niemand den Zugriff auf eure persönlichen Daten erhalten kann. USBCrypt versetzt euch in die Lage, die externen Laufwerke durch die starken Verschlüsselungsalgorithmen von USBCrypt wie AES zu verschlüsseln und die Schlüssellängen 128 und 256 Bit zu verwenden, um absolute Vertraulichkeit der Daten zu gewährleisten.

Das Verschlüsselungssystem basiert auf einem Passwortsystem, so dass jeder ein gültiges Passwort hat, um Zugriff auf die gespeicherten Daten zu erhalten.

Cypherix Encryption Software

https://cypherix.com/

http://www.cypherix.de/data_encryption_software.htm

Cypherix Encryption Software ist eine Datenschutz- und Verschlüsselungssoftware, die zum Schutz von USB- und anderen Speichermedien entwickelt wurde, die eure persönlichen Daten enthalten.

Es richtet sich sowohl an Einzel- als auch an Unternehmensbenutzer, um digitale Geräte zu schützen und den unbefugten Zugriff durch Unberechtigte zu beschränken. Das Beste an dieser Software ist, dass sie für die Verschlüsselung von USB-Sticks, Festplatten, Wechselmedien und sogar von Speicherkarten verwendet werden kann.

Die wichtigsten Funktionen in der Cypherix Verschlüsselungssoftware sind ein Datenverschlüsselungssystem, ein Festplattenverschlüsselungssystem, ein Verschlüsselungssystem für Dateien und Ordner, ein mobiles Verschlüsselungssystem, ein Passwortschutz-Ordnersystem, keine Einschränkung bei der Verschlüsselung von Daten, ein verschlüsseltes Backup-System, sichere E-Mails und noch vieles mehr.

Darüber hinaus ist es auch ein Multi-Plattform-Verschlüsselungssystem. Cypherix Encryption Software ist die einzige Antwort auf alle eure Sicherheits- und Datenschutzanforderungen. Seine Benutzeroberfläche ist so anwenderfreundlich, dass keine besonderen technischen Fähigkeiten erforderlich sind.

Android System verschlüsseln

Hier eine Reihe von Links mit Anleitungen zur Verschlüsselung von Android Handys.

Android-Daten verschlüsseln – so gehts

Android verschlüsseln Smartphone, Datenschutz, Tipp

Android Verschlüsselung aktivieren und wieder aufheben – so gehts

Der Tor-Browser und das Darknet

Wem die bisher aufgezählten Sicherheitsmassnahmen noch nicht ausreichen, der kann noch schwerere Geschütze auffahren.

Das Tor-Browser-Paket ermöglicht anonymes Surfen im Internet mit dem Open-Source-Browser Firefox. Sobald ihr im Internet unterwegs sind, hinterlasst ihr jede Menge Spuren. Das kostenlose Tor-Browser-Paket beugt dem vor, indem es euch über das verschlüsselte Tor-Netzwerk ins Internet bringt.

Tor steht für „The Onion Router“ (der Zwiebel Router). Er wurde so benannt, weil er mehrere Sicherheitsebenen besitzt. Ist der Tor-Browser installiert, könnt ihr nicht nur das „normale“ Internet (Clearnet bzw. Klarnetz) besuchen, sondern ganz einfach Webseiten im Darknet aufrufen.

Im Darknet benötigt man spezielle und aktuelle Linklisten, um zu den jeweiligen Darknet-Webseiten zu finden. Hilfe zur Installation findet ihr hier. Mit dem Tor-Browser seid ihr immer anonym im Internet unterwegs.

https://www.torproject.org/

https://www.chip.de/downloads/Tor-Browser_22479695.html

Wenn ihr die Sicherheit noch weiter erhöhen wollt, benutzt beim Tor Browser und auch bei anderen Browsern einen zusätzlichen VPN-Dienst. Diese Software leitet euren Datenverkehr auf verschiedene Server im Ausland um, und ihr erhaltet automatisch eine andere IP-Adresse.

Wenn ihr VPN aktiviert und erst danach den Tor-Browser startet, bemerkt niemand, dass ihr das Tor-Netzwerk benutzt. Da das Unternehmen CyberGhost mittlerweile keinen kostenlosen VPN-Client mehr anbietet, kann man auf verschiedene andere kostenlose VPN-Clients zurückgreifen, um mit einem Browser sicherer und anonym im Netz zu surfen

1. **Proton VPN**: https://www.chip.de/downloads/ProtonVPN_117295735.html
2. **Windscribe VPN**: https://www.chip.de/downloads/Windscribe-VPN_103913796.html
3. **OkayFreedom VPN**: https://www.chip.de/downloads/OkayFreedom-VPN_56143203.html
4. **Hotspot Shield VPN**: https://www.chip.de/downloads/Hotspot-Shield-VPN_30200785.html
5. **TunnelBear**: https://www.chip.de/downloads/TunnelBear_62024790.html

Nützliche Dienste des Darknets

Ihr könnt das Darknet nur über das Tor-Netzwerk bzw. den Tor-Browser erreichen. Durch die anonyme Nutzung ergeben sich jedoch viele Vorteile in Bezug auf die Sicherheit im Netz.

Leider werden im Darknet sehr viele Verbrechen abgewickelt. Man kann es aber auch für sehr sichere Kommunikation nutzen. Einen Leitfaden für den Einstieg ins Darknet gibt es hier.

Anonyme E-Mail-Konten sorgen im Darknet für eine sichere Kommunikation und man kann sie nur mit dem Tor Browser erreichen:

OnionMail

http://en.onionmail.info/

OnionMail ist ein anonymer und verschlüsselter E-Mail-Anbieter, der nur im Tor-Netzwerk erreichbar ist.

Gewöhnlich kann man mit solchen Mailservern nur innerhalb des anonymen Tor-Netzwerks kommunizieren. OnionMail bietet darüber hinaus die Möglichkeit, mit dem normalen Internet zu kommunizieren. Solche E-Mail-Konten sind sehr sicher und können nicht über das normale Internet erreicht oder überwacht werden.

secMail

http://secmail63sex4dfw6h2nsrbmfz2z6alwxe4e3adtkpd4pcvkhht4jdad.onion/src/login.php

secMail ist ein weiterer anonymer, kostenloser E-Mail-Dienst, mit dem man im Darknet E-Mails versenden und empfangen kann.

Die Registrierung ist einfach und es wird nicht nach persönlichen Daten gefragt. secMail nutzt ebenfalls die besten Sicherheitsprotokolle.

Ein Nachteil, den man in Kauf nehmen muss, ist das geringe Datenvolumen eines Kontos. Hier liegt es bei 25 MB. Mehr gibt es gegen einen Aufpreis.

Mail2Tor

http://mail2tor2zyjdctd.onion/

Mail2Tor ist ein kostenloser anonymer E-Mail-Dienst zum Schutz eurer Privatsphäre. Es ermöglicht jedem, E-Mails anonym per Webmail oder mit einem E-Mail-Client zu senden und zu empfangen. Ihr müsst Tor-Browser auf eurem Computer installiert haben, um auf Mail2Tor zuzugreifen.

TorBox

http://torbox36ijlcevujx7mjb4oiusvwgvmue7jfn2cvutwa6kl6to3uyqad.onion/

TorBox ist ein versteckter Postfachdienst, auf den nur von TOR zugegriffen werden kann. Es besteht keine Verbindung zwischen TorBox und dem öffentlichen Internet. Alle Nachrichten werden in TorBox gesendet und empfangen.

Ctemplar – Armored Email

http://ctemplarpizuduxk3fkwrieizstx33kg5chlvrh37nz73pv5smsvl6ad.onion/

Ein weiterer Postfachdienst im Tor-Netzwerk, der in Island betrieben wird, wo es die stärksten Gesetze für Netzsicherheit gibt.

ProtonMail

https://protonmail.com/

https://protonirockerxow.onion/

Auch im normalen Internet gibt es die Möglichkeit, verschlüsselte Online-Konten zu benutzen. Viele Tor-Nutzer vertrauen auf ProtonMail, einem Unternehmen in der Schweiz, das kostenlose Konten anbietet. Protonmail kann auch mit allen anderen Browsern genutzt werden.

ProtonMail hat den Hauptsitz in Genf und wird von Proton Technologies geführt. Ihre Server befinden sich an zwei Standorten in der Schweiz, und somit ausserhalb der EU- und US-Rechtsprechung.

ProtonMail wurde im Jahr 2013 wegen der Enthüllung der Snowden-Affäre gegründet. Ende 2016 lag die Nutzerzahl bei rund fünf Millionen. In den Jahren 2015/2016 wurde ProtonMail bereits in Suchresultaten von Google unterdrückt, wodurch ProtonMail weniger zahlende neue Nutzer gewann als geplant.

Wenn ihr ein sicheres E-Mail-Konto benötigt, wählt das kostenlose ProtonMail, das jetzt über einen eigenen Tor-Zugang mit einer .onion Adresse verfügt.

Edward Snowden glaubt, dass Tor die derzeit wichtigste Technologie zum Schutz der Privatsphäre im Netz darstellt. Er selbst nutzt laut eigenen Angaben ausschliesslich Tor. Er meint, dass man, wenn man jetzt selbst noch kein Tor nutzt, das schleunigst ändern sollte.

Es wird in naher Zukunft voraussichtlich zu schweren repressiven Massnahmen im Netz kommen. Jede Webseite, die man heute aufruft, stiehlt Nutzerdaten von euch. Diese Informationen werden abgefangen, gesammelt, analysiert und von in- und ausländischen Regierungen, Unternehmen sowie Geheimdiensten gespeichert und verkauft.

Indem man sich durch ein paar einfache Schritte schützt, kann man dieser Entwicklung entgegenwirken, seine Privatsphäre schützen und zu keinem gläsernen Bürger werden. Hier noch eine Reihe von kostenlosen E-Mail-Anbietern mit integrierter Verschlüsselungs-Technologie.

Weitere kostenlose E-Mail-Anbieter mit integrierter Verschlüsselungs-Technologie

Mailfence

https://mailfence.com/

Mailfence ist ein anständiger, auf den Datenschutz ausgerichteter E-Mail-Dienst, der OpenPGP-Ende-zu-Ende-Verschlüsselung erzwingt. Ihr könnt es kostenlos mit begrenztem Speicher (500 MB) und eingeschränkten Funktionen verwenden.

Zoho Mail

https://www.zoho.com/mail/

Zoho Mail ist ein Service, der von Indien aus entwickelt wurde und dort seinen Sitz hat, mit Rechenzentren, die über die USA, Europa, China und Indien verteilt sind.

Ihre Rechenzentren verfügen über ausfallsichere Server an unbekannten Standorten mit strenger 24/7-Überwachung und einem biometrischen Siegel für die Einreise. Neben der Ende-zu-Ende-Verschlüsselung hält Zoho Mail auch E-Mails während der Übertragung verschlüsselt. Die kostenlosen Konten verfügen sogar über einen Speicher von 5GB pro Nutzer!

Es gibt auch Möglichkeiten, verschlüsselte Nachrichten im Netz auszutauschen, ohne über ein E-Mail-Konto zu verfügen. Dazu sind spezielle Dienste und ein Passwort nötig.

Infoencrypt

https://www.infoencrypt.com/

Infoencrypt ist ein kostenloser, webbasierter Dienst zum einfachen Sichern eurer Nachrichten.

Gebt einfach den Text eurer Nachricht und das Verschlüsselungskennwort ein, das sowohl für die Verschlüsselung als auch für die Entschlüsselung verwendet wird.

Das Programm verschlüsselt eure Nachricht mit einem starken Verschlüsselungsalgorithmus, so dass es sicher ist, zu senden. Wer die verschlüsselte Nachricht ohne Kennwort abfängt, kann die ursprüngliche Nachricht nicht lesen.

Infoencrypt erfordert keine Installation auf eurem PC. Ausserdem gibt es Möglichkeiten, anonym E-Mails zu versenden, ohne über ein E-Mail-Konto zu verfügen.

Free File Camouflage

http://www.myportablesoftware.com/freefilecamouflage.aspx#

Free File Camouflage ist ein kostenloses Programm, mit dem ihr eure Dateien in einem JPEG-Bild verstecken könnt.

Die Software kann mit der Hauptschnittstelle oder über das Windows Explorer-Kontextmenü “senden an” verwendet werden (das erste Mal, dass ihr nur ein Verzeichnis mit einigen Bildern auswählen müsst).

Alle Dateien werden mit dem Verschlüsselungssystem AES verschlüsselt und in einem Bild versteckt. Wenn jemand versucht, das getarntes Bild zu öffnen, sieht er nur das Bild, aber keine Daten.

Wenn ihr diese Methode verwendet, um jemandem eine private Textnachricht in einer in einem Bild versteckten Datei zu senden, muss der Empfänger die Datei mit dem Programm “Free File Camouflage” enttarnen, um sie zu verwenden.

Wenn ihr das getarnte Bild per E-Mail sendet, wird empfohlen, beim Verschlüsseln der Datei in ein Bild zusätzlich ein Kennwort einzufügen.

Send-Email.org

http://send-email.org/

Wenn ihr eine sofortige E-Mail mit höchster Genauigkeit anonym senden möchtet, ist dieses kostenlose anonyme E-Mail-Dienstanbieter-Tool genau das Richtige.

Send-email.org verfügt über eine einfache und gut strukturierte Benutzeroberfläche, die euch Raum gibt, die E-Mail-Adresse des Empfängers, den Betreff der E-Mail und dann den Inhalt einzugeben.

Im Gegensatz zu den meisten anonymen E-Mail-Dienstanbietern könnt ihr dort auch eure echte E-Mail-Adresse angeben, um die Antwort von anderen zu erhalten.

AnonymousEmail.me

https://anonymousemail.me/

AnonymousEmail.me ist eine perfekte Option unter verschiedenen anonymen E-Mail-Dienstanbietern für euch, wenn ihr euch nirgendwo anmelden wollt, um ein E-Mail-Konto zu erstellen. Man kann von dort aus unkompliziert und schnell anonyme E-Mails versenden.

Dieses Tool bietet einfache Formulare, in die ihr die E-Mail-Adresse des Empfängers, den Betreff und den Inhalt der E-Mail schreiben könnt.

CyberAtlantis

https://cyberatlantis.com/anonymous_email.php

CyberAtlantis ist ein einzigartiges Tool, mit dem ihr eure IP-Adresse verbergen könnt. Es ist so strukturiert, dass, sobald ihr eine E-Mail sendet, die IP-Adresse entfernt wird und ihr unauffindbar werdet.

Es erfordert nicht, dass ihr eure persönlichen Daten eingeben müsst, ausser die E-Mail-Adresse des Empfängers, den Betreff und eure Inhalte.

W3 Anonymous Remailer

http://gilc.org/speech/anonymous/remailer.html

W3 Anonymous Remailer ermöglicht es euch, eine kostenlose anonyme E-Mail zusammen mit Anhang (nur mit Anmeldung) zu senden.

Im Gegensatz zu so vielen anderen anonymen E-Mail-Dienstanbietern oder Absendern, die nur das Senden von E-Mails erlauben, bietet W3 Anonymous Retailer euch eine Schnittstelle, um auch eine Datei-Anlage hinzuzufügen. Diese Anhänge in Verbindung mit dem Namen, dem

Betreff und dem Inhalt werden nicht nachverfolgt.

Secure Email

http://www.secure-email.org/index.php

Secure Email ist ein weiterer anonymer E-Mail-Dienstanbieter, um erweiterte geschützte anonyme E-Mails kostenlos zu senden. Mit diesem Dienst werden eure E-Mails mit 4096-Bit-Schlüssel verschlüsselt. Es ist also sehr sicher und völlig anonym.

Mit dem grossen Verschlüsselungsschlüssel ist es für jede andere Person ausser euch unmöglich, eure E-Mails zu lesen. Secure Email erfordert keine persönlichen Daten oder IP-Adresse.

AnonEmail

http://anonymouse.org/anonemail.html

Mit AnonEmail ist es möglich, E-Mails zu versenden, ohne eure E-Mail-Adresse oder Informationen über eure Identität anzugeben. Dadurch könnt ihr freier kommunizieren und ihr müsst euch keine Sorgen machen, dass dies Konsequenzen für euch haben könnte.

Mit diesem Service können ihr E-Mails versenden, ohne persönliche Informationen preiszugeben.

Dienste zum Erstellen von anonymen E-Mail-Adressen

Es gibt im Netz eigene Dienste zur Erstellung und Nutzung von temporären anonymen E-Mail-Adressen, die man als Sicherheit zur Anmeldung bei anderen E-Mail-Diensten oder sozialen Netzwerken nutzen kann, ohne seine persönliche E-Mail-Adresse verwenden zu müssen.

Gebt in eurer Suchmaschine einfach den englischen Begriff „temporary email adress“ oder „trash mail“ ein und ihr erhaltet eine Auflistung derartiger Dienste. Dasselbe funktioniert auch mit internationalen Mobiltelefonnummern „temporary mobile number“ oder „trash mobile“, falls ihr eure persönliche Telefonnummer nicht benutzen wollt oder über gar kein Mobiltelefon oder eine gültige E-Mail-Adresse verfügt.

https://tempail.com/en/

https://trashmail.com/

https://receive-smss.com/

https://www.mytrashmobile.com/

https://www.spoofbox.com/en/tool/trash-mobile

Personenbezogene Google-Daten löschen

Es folgen hier zum Abschluss noch ein paar Informationen und Weblinks mit Anleitungen, die es ermöglichen, personenbezogene Daten bei Google zu löschen.

Ihr solltet diese Möglichkeit nutzen, wenn ihr wollt, dass die auf den Servern gesammelten Daten über euch gelöscht werden, damit sie das Unternehmen nicht mehr für kommerzielle Zwecke verwenden kann.

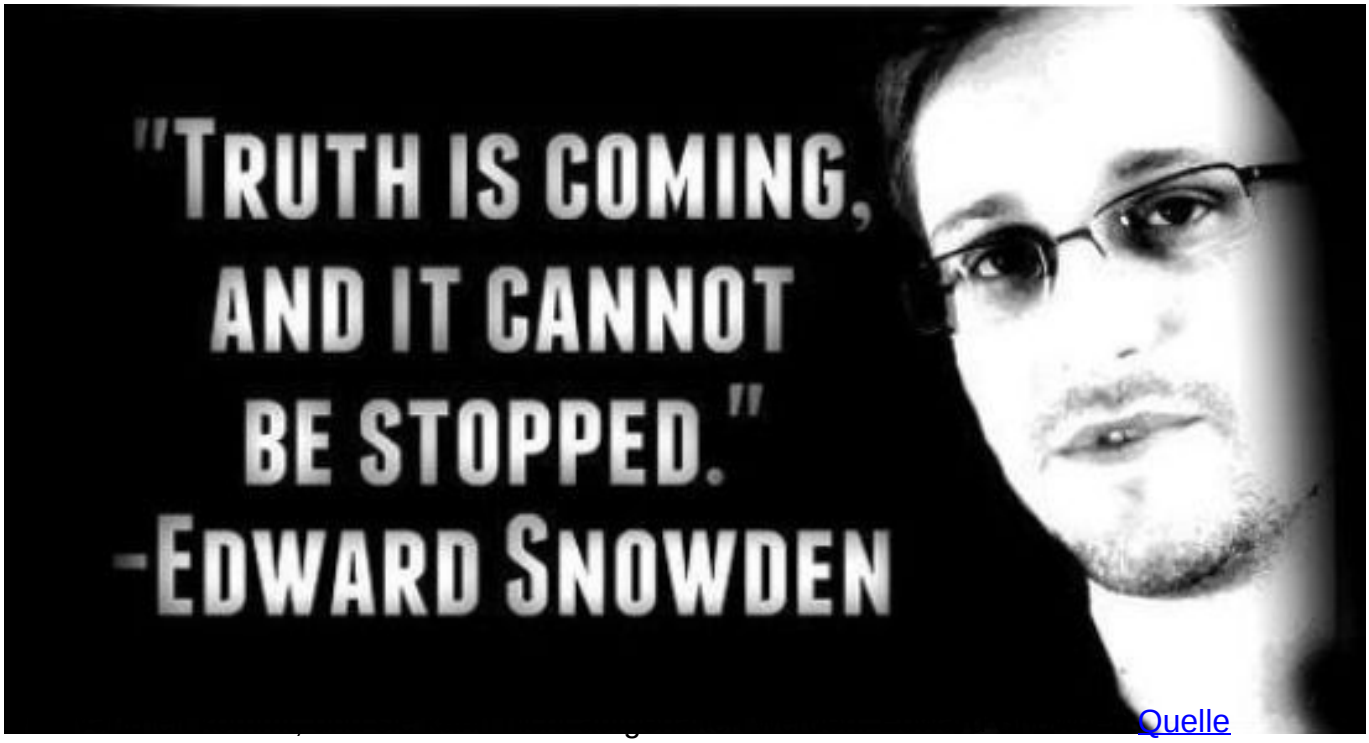
Google-Daten löschen – Tipps, Privatsphäre, Datenschutz

Google-Daten löschen so geht es.

https://support.google.com/accounts/answer/3024190?hl=de

Google Einträge löschen lassen – so gehts.

Google collects a frightening amount of data about you you can find and delete it now



Quelle