Sicheres Surfen und Anonymität

Hier erfährst du:

- Hintergründe zu Privatsphäre und Sicherheit im Netz.
- Wie du den Firefox-Browser verwendest.
- Wie du den anonymisierende Tor Browser verwenden kannst.
- Wie du das portable Betriebssystem Tails einsetzen kannst.

Viele Menschen glauben, dass das Surfen im Internet anonym sei und die abgerufenen und gesendeten Informationen sicher übertragen werden. Das ist falsch: Jede:r Internetbenutzer:in hinterlässt andauernd Spuren im Netz und genau genommen kannst du dir oft nicht sicher sein, mit wem du da gerade Daten austauschst und, dass diese Daten unterwegs – aber auch nach dem sie schon angekommen sind – niemand anderes mehr zu Gesicht bekommt. Willst du ganz sicher gehen, dass eine Information nicht in falsche Hände gerät, ist unter Umständen ein persönliches Gespräch sinnvoller, als eine Kommunikation über das Internet.

Privatsphäre und Sicherheit
Grundsätzlich sollte zwischen Privatsphäre und Sicherheit unterschieden werden. Zur Privatsphäre zählt, zum Beispiel, die Möglichkeit, sich pseudoanonym oder gar anonym im Netz zu bewegen. Die Möglichkeit Informationen auf sicherem Weg zu übertragen – das heißt, die Informationen können unterwegs nicht verändert oder abgehört werden –, gehört hingegen zum Bereich der Informationssicherheit.

Für Aktivist:innen ist je nach Anwendungsfall beides wichtig. So kann die Exekutive durch Anfragen bei Serverbetreiber:innen und Internetanbieter:innen herausfinden, ob von einem bestimmten Internetzugang auf bestimmte Webseiten zugegriffen wurde. Teilweise ist auch aus den Protkollen des Servers ersichtlich, welche Daten durch jemanden dorthin geschickt wurden. Wer Dateien ins Internet hochlädt sollte sich ausserdem bewusst sein, dass diese häufig auf den ersten Blick nicht sichtbare zusätzliche Daten (Metadaten) enthalten, die mitunter Rückschlüsse auf den:die Urheber:in zulassen.

Browser

Browser sind Programme mit denen Webseiten im World Wide Web abgerufen werden können, z.B. Firefox, Tor-Browser, Chrome, Chromium. Browser werden daher sehr viel verwendet. Damit bekommen Browser auch immer mehr Informationen über dich und deine Aktivitäten. Das macht es umso wichtiger, sich hier Gedanken über Sicherheit und Datenschutz zu machen.

Unsere Empfehlungen:

- Firefox: Der Browser für den Alltag
- Tor-Browser - der Browser für mehr Anonymität

Firefox: Der Browser für den Alltag

Mozilla Firefox gilt als die datenschutzfreundlichste Alternative zu Chrome und Microsoft Edge. Der Browser der gemeinnützigen Mozilla Foundation hat sich dem «sicheren Surfen» und Datenschutz verschrieben. Er ist schnell und vielseitig. Der Quellcode ist offen und wird von einer aktiven Community ständig weiterentwickelt. Zudem können zahllose Erweiterungen (Add-ons) installiert werden, um den Datenschutz zu erhöhen. Du kannst den Firefox-Browser auf allen gängigen Betriebssystemen einfach installieren.

Weiterlesen: Genaueres zum Firefox und seinen Erweiterungen, sowie allgemein zu Browsern kannst du in dieser Artikelserie vom Kuketz-Blog nachlesen.

Um die Sicherheit und den Datenschutz noch zu erhöhen, kannst du noch einige Änderungen vornehmen.

Suchmaschine ändern

Im Auslieferungszustand ist bei Firefox, als Suchmaschine Google festgelegt. Dies lässt sich ganz einfach in den Einstellungen ändern: Einstellungen → Suche → Standardsuchmaschine mehr zu "Sucheinstellungen in Firefox ändern" findest du direkt bei Mozilla. Wir würden hier Starpage oder DuckDuckGo empfehlen.

Erweiterungen (Add-Ons) installieren

o uBlock-Origin
Bei uBlock-Origin handelt es sich um einen Adblocker. Ein Adblocker sollte zu deiner Grundausstattung gehören, denn das Internet ist voll von Werbung, was ziemlich nervig sein kann und kann au. Insbesondere ist „Malvertising“ ein Problem. „Malvertising“ ist die Auslieferung von Werbung, welche Schadcode beinhaltet und damit ein Risiko für dich und deine Daten darstellt.

o HTTPS Everywhere
sofern eine Webseite via HTTPS (also verschlüsselt) erreichbar ist, wird das Addon eine Umleitung zur »geschützten« Variante vornehmen.

o Privacy Badger soll Tracking möglichst verhindern.

o NoScript
soll JavaScripte blockieren. JavaScripte werden mittlerweile vor allem in der Werbe- und Trackingbranche verwendet. Das Addon erhöht den Datenschutz deutlich, einige Seiten werden so aber leider nicht mehr funktionieren.

o Cookie AutoDelete

Cookies werden gerne als Tracking-Merkmal eingesetzt. Alle Cookies, die ihr nicht auf eine Whitelist setzt, löscht das Addon nach einer vorgegebenen Zeit oder bis die Seite/der Browser geschlossen wird.

Weiterführende Links

- Eine ausführliche Artikelreihe über Firefox und Erweiterungen: Firefox by Kuketz-Blog
- Artikel zu Suchmaschinen: Suchmaschinen by Kuketz-Blog

Tor-Browser - der Browser für mehr Anonymität

Was ist Tor?
Der Tor-Browser baut auf dem Firefox auf, ist jedoch weiter im Sinne von Datenschutz und Anonymität optimiert. Er schickt deinen Internetverkehr über das Tor-Netzwerk. Dabei wird deine Identität versteckt, indem deine Webanfragen - in verschiedenen Schichten verschlüsselt - über Knotenpunkte in der ganzen Welt geleitet, bevor deine Zielwebseite sie erhält. Dadurch gibt es fast keine Möglichkeit, eine Webanfrage zu seiner Quelle zurückzuverfolgen. Das Netz hostet auch Webseiten (die “onion sites” genannt werden), welche durch das „normale“ Internet gar nicht erreichbar sind: Das können regierungskritische Webseiten sein, Foren von und für Opfer von Missbrauch, über Drogenmarktplätze bis hin zu einfachen, „langweiligen“ Seiten.

Um deine Netzaktivität durch das Tor Netzwerk zu leiten, musst du nur den *Tor Browser herunterladen* und dann benutzt du ihn so wie jeden anderen Browser.

Was heißt anonym?
Der Tor Browser anonymisiert dich, du bist aber nicht privat. Obwohl Anfragen anonym sind, bist du immer noch als „du“ identifizierbar, solltest du dich bei Facebook anmelden oder eine Mail mit Gmail senden.
Wenn du versuchst anonym zu sein, solltest du dich nie bei Diensten anmelden oder Seiten besuchen, die mit deinen persönlichen Daten in Verbindung stehen. Solltest du einen Service benötigen, der solche Daten braucht, dann verwende bei der Registrierung gefälschte Daten und stelle sicher, dass du die Seite nur mit dem Tor Browser aufrufst.
Anleitung:
Hier findest du eine auführliche Anleitung zum Tor-Browser [en] von "security in a box" unter Windows

Tails: Ein Betriebssystem für maximale Sicherheit

Tails ist ein portables, Linux-basiertes Betriebssystem, das speziell zum Schutz der Anonymität entworfen wurde. Du installierst es auf einem USB-Stick und kannst es damit auf fast jedem Computer der Welt starten - egal, ob es ein Windowsrechner, ein Apple oder ein Linuxsystem ist. Es muss dann nur noch beim hochfahren ausgewählt werden, dass vom USB-Stick gestartet werden soll. Warum ist das so nützlich?

- Tails ist ein „amnestisches“ System: Das heißt, dass keine Daten zwischen Sitzungen gespeichert werden. Jedes Mal, wenn du es benutzt, kannst du ein komplett frisches digitales

Umfeld ohne persönlich zuordenbare Informationen laden, unabhängig davon wessen Computer du benutzt. Nach dem Herunterfahren (oder abziehen des USB-Sticks) sind normalerweise keine Daten mehr vorhanden. Falls du aber Daten hast, die du behalten möchtest, bietet Tails die Möglichkeit eine dauerhafte Speichermöglichkeit („persistence Storage“) anzulegen. Dann kannst du deine Emails, Email-Verschlüsselung, Daten und Dateien ganz normal einrichten und speichern.

- Standardmäßig wird jede Internetverbindung, die auf Tails benutzt wird, durch das Tor Netzwerk geschickt. Damit kann deine IP Adresse, dein Standort und deine Aktivitäten nicht einfach von Dritten überwacht werden. Dein Internetprovider kann hier nur sehen, dass du Tor benutzt, aber nicht, was du damit tust.
  Nur eine staatliche Institution, die wirklich hinter dir her ist, könnte deine Tor Nutzung mit sehr viel Aufwand noch nachverfolgen.
- Die standardmäßige Nutzung vom Tor Netzwerk ermöglicht es recht einfach anonym Emails zu schreiben oder andere Anwendungen anonym zu nutzen.
- Tails hat einige tolle Programme und Erweiterungen vorinstalliert, die deine Privatsphäre schützen. Zum Beispiel Mat, um Metadaten per Rechtsklick löschen zu können.

Tails-Anleitungen:
Auf der Webseite findest du **hervorragende mehrsprachige Anleitungen**, die dich Schritt für Schritt mit Bildern und Videos bei der Installation begleiten. Tails kann von Windows, MAC, Linux oder einem anderen Tails aus eingerichtet werden.

Anleitungen auf der offiziellen Tails Webseite

Es gibt auch ein sehr ausführliches Tails Handbuch [PDF-Download]

VPN

Ein VPN erzeugt eine private, verschlüsselte Verbindung zwischen dir und einem VPN Server und alles was du im Netz tust, wird durch dieses private Netzwerk getunnelt, bevor es vom VPN Server in die offene Welt geht. Wenn du dich mit einer VPN Verbindung bei einer Seite anmeldest, dann sieht die Webseite, dass deine Anfrage vom VPN Server kommt, nicht von dir. Jemand der versucht in das, was zwischen dir und der Seite gesendet wird Einblick zu bekommen, kann nicht sehen, was das ist, weil alles verschlüsselt wird. Stelle dir das vor, wie einen privaten Tunnel von dir zum VPN Server. Der Server lässt das, oder das, was du anforderst, in und aus dem Tunnel, aber niemand außer dir kann sehen, was im Inneren ist. Besonders praktisch ist, dass ein VPN Server irgendwo in der Welt stehen kann! Benutzt du einen VPN Server in der Schweiz, werden alle denken, du bist in der Schweiz, weil alle deine Anfragen von dem VPN Server in der Schweiz kommen. Manche Personen haben ihre eigenen VPN Server. Die meisten Leute benutzen aber stattdessen lieber VPN Anbieter. Das sind Firmen oder Organisationen die VPN Server betreiben und verwalten, damit du dich nicht mit den technischen Details auseinandersetzen musst: Du benutzt sie einfach. Manche VPN Anbieter können deine Aktivitäten sogar noch weiter anonymisieren, indem sie sie über Proxies (andere Server) weiterleiten. Leider sind VPN Dienste in aller Regel nicht kostenfrei. Du musst entweder irgendwo deinen eigenen Server aufsetzen oder, was allgemein gebräuchlicher ist, eine monatliche Gebühr an einen VPN Anbieter bezahlen.

Wähle einen vertrauensvollen Dienst
VPN kann deine Anonymität/Privatsphäre erhöhen. Wichtig dabei ist aber dass du dem VPN-Anbieter vertraust, sonst bewirkt es das Gegenteil!

Wir empfehlen:

- Mullvad VPN (kostenpflichtig)
- Riseup VPN (gratis, von einem linken kollektiv)

Guide to Choose a VPN [English]

From:
https://www.fit-fuer-aktion.wiki/ - **Selbstverteidigung im (anti-)politischen Alltag**

Permanent link:
https://www.fit-fuer-aktion.wiki/digitale-sicherheit/sicheres-surfen_anonymitaet/index

Last update: **2022/07/25 15:31**