How to Digitale Sicherheit

-

Eine kleiner Guide zum Schutz vor den Behörden

Für Fragen, Anmerkungen, Anfragen zu Erweiterungen und co., meldet euch bei uns, Mail und PGP-Key findet ihr am Ende des Dokuments!

First off: Wir können (leider) nicht zu 100% sicher und anonym sein. Denn es gibt eine Vielzahl von Interessen, die wollen, dass wir es nicht sind. Trotzdem können wir es diesen Interessen dabei so schwer wie möglich machen und uns selbst mit kleinen Tools gegen staatliche Überwachung & Co. verteidigen.

Es gibt viele Linksammlungen und Tipps & Tricks, wir sammeln hier einfach mal jene, die für uns spezifisch von Bedeutung sind. Welche für euch und eure "Eskalationsstufen" Sinn machen, müsst ihr letztenendes natürlich selbst entscheiden. Unser Tipp: Je weiter ihr es treibt, desto besser!

Inhaltsverzeichnis

Zu Beginn könnt ihr vielleicht mal einen kleinen Test machen, wie 'unsichtbar' ihr, bzw. euer Browser, bereits im Netz unterwegs seid. Vielleicht ganz interessant zum Schauen wie's vorher und wie's nachher aussieht.

---

1. Das Browsen im Internet

Hier seid ihr den größten "Gefahren" und kapitalistischen Absichten ausgesetzt. Mit ein paar Handgriffen lassen sich viele der Gefahren allerdings leicht umgehen und machen darüber hinaus euer "Surferlebnis" viel angenehmer. Zuerst geht's um die richtige **Browserwahl**, dann um die **Suchmaschine**.

Der Browser

Über euren Browser gelangt ihr auf Websites und habt den meisten Kontakt mit anderen digitalen Kontaktpunkten, die Websites speichern Cookies und haben Tracker mit drinnen, die dazu dienen eure Daten zu sammeln und ein Bild von euch anzulegen. Meist zu (aggressiven) Marketingzwecken (s.u. ***Surveillance Capitalism***), aber oft auch zum Verkauf von Datan á la Google. Zudem können Menschen und Institutionen über euren Traffic extrem viele Infos zu euch herauszufinden, z.B. welches Gerät ihr benutzt, wo ihr seid, euer Surfverhalten und wo ihr sonst noch so aktiv seid.

Mit einem guten auf Privatsphäre bedachten Browser könnt ihr schonmal einiges an Sicherheit und Anonymität herstellen. Es gibt für die bekannten Browser Chrome und Firefox einige Add-Ons die eure Spuren verwischen sollen, aber beide haben, wie immer einige Lücken. Bei Chrome ist es vor allem, eh klar, weil's von Google ist... und Google Geld mit unseren Daten macht. Zudem sind viele Einstellungen, wie bei Firefox, nicht darauf ausgelegt, oder nicht direkt einsichtig, um Sicherheit zu garantieren. So können 3rd Party Sachen oftmals nur über Add-Ons, meist von Freiwilligen

geschrieben, geblockt werden. Ebenso 'fingerprints' und andere Scripts, die eure Daten sammeln und weitergeben. Viele dieser Add-Ons können nicht lückenlos gepflegt werden (weil dafür die Leute fehlen) und sicherheitsrelevante Updates dieser Add-Ons brauchen meist eine Weile. Trotzdem ist Firefox unter den Browsern das geringste Übel und daher eine wichtige Anlaufstelle für anonymeres Surfen.

Für eine umfangreiche Auseinandersetzung mit Firefox hier entlang.

(Kommentar Kümmel: Firefox lässt m.E. schon umfangreiche Änderungen zu und bietet auch gute default Einstellungen. Gerade durch "about:config" in der Adresszeile lassen sich auch (sicherheitsrelevante) Einstellungen ansteuern, die in den normalen Einstellungen nicht verfügbar sind. Allerdings muss klar sein, nach was gesucht wird und was in den Konfigurationen verändert werden kann, ohne dass die Änderungen selbst wieder zur Sicherheitslücke werden. Ein umfangreiches Kompendium für Interessierte findet sich dazu hier)

Eine Empfehlung hier ist der Brave Browser, ein Projekt von einem ehemaligen Firefox-Mitarbeiter. Von der Installation an habt ihr Tracker und Ads blockiert (auch Youtube-Werbung) und könnt zB eingebettete Soziale Medien-Felder auf Websites blocken, einstellen wie aggressiv geblockt wird, so weit, dass der Browser versucht überhaupt keine Infos an Websites weiterzugeben, was aber dazu führen kann, dass die Websiten nicht funktionieren oder extrem langsam sind (teils Taktik, teils dem Code geschuldet). Zusätzlich könnt ihr einstellen, dass wenn eine Website eine .onion (Darknet) Adresse hat, ihr direkt über das TOR-Netzwerk auf diese geleitet werdet. Mehr zu TOR gleich.

Es gibt 1000 Add-Ons die für Privatsphäre und Security Sachen gedacht sind. Eine kleine Liste:

- uBlock Origin: Ad- und Track-Blocker
- HTTPS Everywhere: Sichere Verbindung
    - Verschlüsselt die Verbindungen zu vielen großen Websites und schafft daher mehr Sicherheit. Coop zwischen Tor Project und EFF
- NoScript: Dient dazu die von der Website verlangten Skripte zu blockieren (kann die Funktionalität des Browsers schon seeehr einschränken, bietet aber auch die Möglichkeit nur einzelne Skripte zuzulassen und zu schauen, was notwendig ist bzw. was nicht, damit die Seite läuft). Crasht möglicherweise mit anderen Add-Ons und kann Sicherheit dadurch komprimieren.
- PrivacyBadger: blockt zuverlässig Tracking, EFF-Projekt
- Decentraleyes
    - Leitet Anfragen um und spuckt andere Daten aus, geht damit direkt gegen tracking
- ClearURLs
    - löscht automatisch Tracker aus kopierten URLs
- Terms of service Didn't read

TOR Browser

https://www.torproject.org/

Wikipedia: "**Tor** ist ein Netzwerk zur Anonymisierung von Verbindungsdaten. Es wird für TCP-Verbindungen eingesetzt und kann beispielsweise im Internet für Browsing, Instant Messaging, IRC, SSH, E-Mail oder P2P benutzt werden. Tor schützt seine Nutzer vor der Analyse des Datenverkehrs. Es basiert auf der Idee des Onion-Routings."

-> Zwiebelschichten, ihr werdet über verschiedene Server verbunden und seid damit durch die Anzahl der Router (das sind quasi neben eurem Pc noch weitere Verbindungspunkte, bevor ihr mit dem eigentlichen Ziel verbindet) nicht oder schwer zu finden.

Über den Tor Browser, aber auch über Brave, könnt ihr Websites ansteuern, die nicht über normale Browser ansteuerbar sind (wie das genau funktioniert erfahrt ihr hier: YouTube-Link), also Dark- und Deepweb. Zum Bestellen von Drogen, Waffen, Fake-IDs, oder für spezielle Foren, Informationen, elektronische Ressourcen... Alles erfordert ne Menge reinarbeiten und zu positiv, dass man ja eh nicht getrackt wird, solltet ihr nicht sein. Gibt ultraviele Fake-Seiten und -Märkte und dazu einen Haufen Leute die eben darauf aus sind andere Leute abzuziehen.

Wie auch immer, Über das Tor Netzwerk könnt ihr auch "Clearnet"-Seiten, also normale Websites, ansteuern und seid dabei wesentlich anonymer, als ihr es ohne seid. Downside ist, dass der Browser durch das viele "Re-Routing" suuuper langsam ist und im Alltagsgebrauch einfach nervt. Für empfindliche Sachen aber klar zu empfehlen.

Die Suchmaschine

Moment, was? Google hat böse Absichten und ist nicht vertrauenswürdig?

Schade eigentlich. Google hat mit Abstand die beste "Search Engine".

Eine coole, naja, "Alternative" bietet https://www.startpage.com/. Diese Seite benutzt Google im Prinzip, aber entfernt bei der Suchanfrage alle persönlichen Daten durch Server in den Niederlanden, greift über weitere Server auf Suchergebnisse zu und gibt sie euch weiter. Keine Spuren werden hinterlassen und ihr seid anonym unterwegs. Google denkt bei jeder Anfrage ihr greift zum ersten Mal auf Google zu.

Populär ist auch DuckDuckGo. Schreibt sich Privacy auf die Fahne und bietet dazu auch einiges. Doof ist, aber, dass die Suchmaschine bei weitem nicht an die von Google herankommt. Aber: Kann auch im darknet verwendet werden ;)

Bei Qwant handelt es sich um eine Suchmaschine, die dem europäischem Datenschutzrecht unterliegt und in Frankreich entwickelt worden ist. Seit neustem bietet Qwant auch eine Kartenfunktion an (das Design orientiert sich dabei an Google Maps), diese basiert auf den bekannten OpenStreetMaps.

---

2. Passwort-Manager

Um einen Passwort-Manager kommt ihr nicht drum herum, und das sollte auch eines der ersten Dinge sein, die ihr installiert. Immer wieder werden Websites oder User gehackt und - teils sensible - Login-Daten veröffentlicht. Nutzt ihr für diverse Seiten dasselbe Passwort, dann bedeutet ein Leak eine Gefahr für viele euerer Accounts. Dabei reicht es jedoch nicht, nur unterschiedliche Passwörter zu verwenden, diese sollten auch stark sein. Es gibt z.B. eine Unmenge an Paypal-Accounts, die (illegal) im Internet gekauft werden können, einfach, weil es super easy ist, die Passwörter mancher Accounts zu erraten. Sprich ihr solltet ein Passwort niemals doppelt verwenden und immer ein langes, starkes Passwort anlegen. Klingt nach 1000, komplizierten, random Ziffernreihenfolgen, die sich eh niemensch merken kann? Das muss nicht unbedingt sein, aber euer Passwort-Manager packt auch das!

Aber was sind denn jetzt schlechte Passwörter und wie lege ich gute Passwörter an?

Wir wollen gar nicht so viel Zeit damit verlieren, viel darüber zu sprechen, was schlechte Passwörter sind, trotzdem noch einmal zur Erinnerung besonders schlecht sind: einfache Zahlenreihenfolgen (1234, 123456, etc.), einzelne Wörter (ganz schlecht: passwort, *name*, etc.), Passwörter bei denen lediglich einzelne Buchstaben durch Zahlen/ Zeichen ausgetauscht werden (eine "3" für ein "E" oder ein "@" für ein "a" - easy guess) oder Passwörter die =/< 8 Zeichen haben.

Gute Passwörter können sehr einfach über Passwort-Generatoren erstellt werden, meist kann dort eingestellt werden, ob das Passwort bspw. aus einer Passphrase bestehen soll, wie lang es sein soll und ob noch zusätzlich Zahlen/ Sonderzeichen eingebaut werden sollen. Die meisten Passwort-Manager (PM) haben eine solche Funktion bereits integriert (nach Installation des PM könnt ihr so ganz automatisch, z.B. 20-stellige, zufällige Ziffern, als neues Passwort einspeichern). Gute Passwörter müssen allerdings nicht immer so aussehen, als hätte ich dabei wild auf die Tastatur gehauen.

Wichtig: Wie erstelle ich ein sicheres Master-Passwort für den PM?

Vielleicht das wichtigste Passwort, das ihr erstellen werdet und eines der wenigen, wenn nicht sogar das EINZIGE, das ihr euch merken müsst, ist das Passwort eures PM-Tresors. Dieses Passwort sollte sehr stark, gleichzeitig aber auch gut einprägsam sein (allerdings gebt ihr dieses Passwort meist mehrmals am Tag ein und daher ist es eh schnell drin).

Zu einem solchen Passwort könnt ihr wie folgt gelangen:

1. sucht euch 3-4 Worte aus, die nicht sonderlich geläufig sind, die ihr euch aber gut merken könnt. Der Name eures Lieblingsspiels oder iwelche Fantasieworte (darunter können auch Wörter aus anderen Sprachen sein -> macht das Erraten nochmal schwerer)
2. wählt 2-3 Buchstaben aus, die ihr GROß schreibt (random verteilt, auch mitten im Wort)
3. fügt random eine Zahl hinzu
4. fügt random ein Sonderzeichen hinzu

Teilt dieses Passwort nie! Verwendet es nirgendwo anders! Notiert es nicht dauerhaft auf einem Zettel oder auf eurem PC! Nur gut merken.

Welchen Passwort-Manager soll ich wählen?

Eine Übersicht gängiger, kommerzieller Anwendungen mit einem kurzen Abriss über Vor- und Nachteile gibt es hier.

Ich (Kümmel) nutze Bitwarden & Keepass (weil ich paranoid bin und beides Vor-/ Nachteile hat). Die Browsereinbindung von Bitwarden klappt in der Praxis bei allen Browsern, die ich nutze ziemlich gut, die Anwendung wirkt nicht überladen, macht was sie soll und die Synchronisation mit meinem Passwortspeicher hat auch noch keine Probleme gemacht. Bitwarden ist für alle gängien Distributionen verfügbar. Findet einen Passwort-Manager, dessen Integration in die Anwendungen, die ihr nutzt einwandfrei funktioniert, schließlich wollt ihr den Manager jeden Tag nutzen und nicht wieder in alte Verhaltenmuster zurückfallen. [Kommentar mike: Probiere Bitwarden momentan aus, gibt ein plus :) Da das Autofill anders funktioniert: *strg+shift+L* füllt automatisch den auf der jeweiligen Website zuletzt genutzten login]

KeePassXC ist ein community, open-source Projekt mit hohem Sicherheits- und Funktionsumfang, das komplett offline arbeitet (es wird also kein externer Server zum Speichern deines Tresors benötigt). KeePass bedarf allerdings ein bisschen mehr technisches Know-How/ Interesse und die Usability ist nicht immer so flüssig, wie bei den Anwendungen oben. Dafür bietet die Anwendung aber auch mehr Möglichkeiten für erweiterte Sicherheitsfeatures.

---

3. E-Mail

Hier gibt's auch bissl was zu. Immer wieder gibt's Berichte, dass von verschiedenen großen Mail-Providern Daten geleaked werden und Passwörter herausgefunden wurden. Ob eure Daten/ Passwörter sich bereits im Umlauf befinden, könnt ihr hier abchecken: haveibeenpwned?

In Aktivistikreisen benutzen viele riseup, sehr viele safety-measures in Benutzung, niemand hat Zugriff auf Daten. Braucht eine Einladung, die wir ausstellen können. Riseup ist eine gute Option, aber (wie alles) auch keine 100%ige Lösung, denn die Server stehen z.B. außerhalb unserer Reichweite in den USA.

Protonmail hat Server in der Schweiz und arbeitet verschlüsselt, von Haus aus einige coole Sachen (z.B. Website mit .onion-Adresse), free-version nur als Web-App oder mobile Version unter Google-Android/ iOS.

Größere Liste mit weiteren Optionen hier: https://prxbx.com/email/

Thunderbird!

Thunderbird ist ein Mail-Programm, das euch dabei helfen kann eure Mail-Accounts zu verwalten. Anders als die vorinstallierten Standardanwendungen (wie Apple Mail oder Outlook) ist Thunderbird quelloffen bzw. open source (Code des Programms kann eingesehen werden), kostenlos und wird ebenso von Mozilla weiterentwickelt. Thunderbird bietet eine Reihe an Möglichkeiten Sicherheitsfeatures zu aktivieren oder zu integrieren, so z.B. die Verschlüsselung von Mails mittels PGP.

Schritt 1: Thunderbird Installieren!

(Eine Anleitung wie ihr von eurem alten Mail-Programm wechselt findet ihr hier)

Schritt 2: Accounts in Thunderbird hinzufügen.

(Für Tipps & Tricks, Fragen und Tutorials hier die Hilfe Seite)

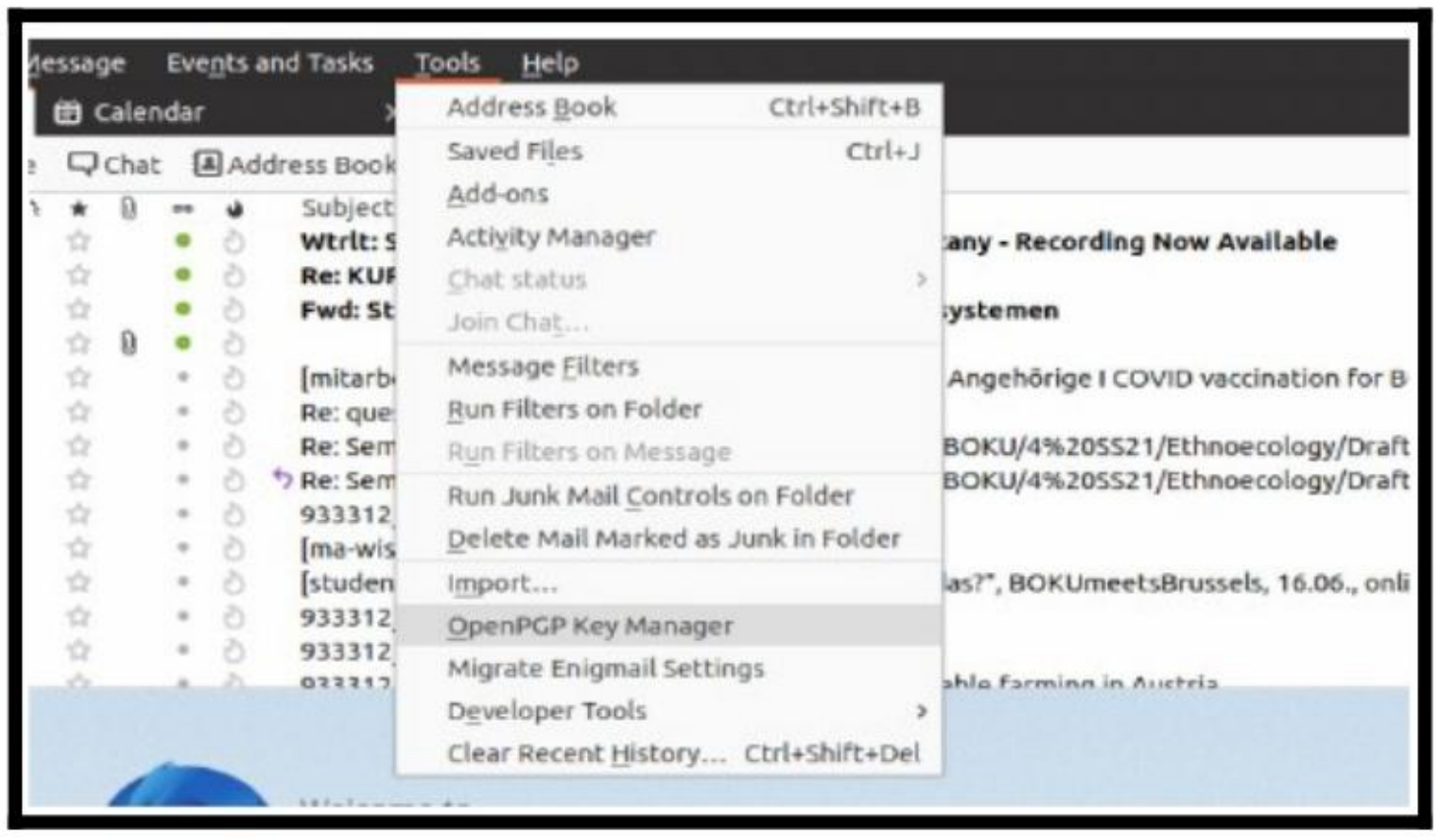
Schritt 3: Sichere Verschlüsselung von Mails einrichten. Dazu:

How to PGP

PGP (Pretty Good Privacy) ist eine Methode Mails, Nachrichten und Dokumente zu verschlüsseln.

Ihr habt dazu einen "Privaten Schlüssel" (Private Key), der lokal auf dem PC gespeichert ist - diesen kennt nur ihr bzw. euer PC - , und einen "Öffentlichen Schlüssel" (Public Key), den ihr an Kontaktpersonen leitet. Der Public Key *ver*schlüsselt, der Private Key *ent*schlüsselt.

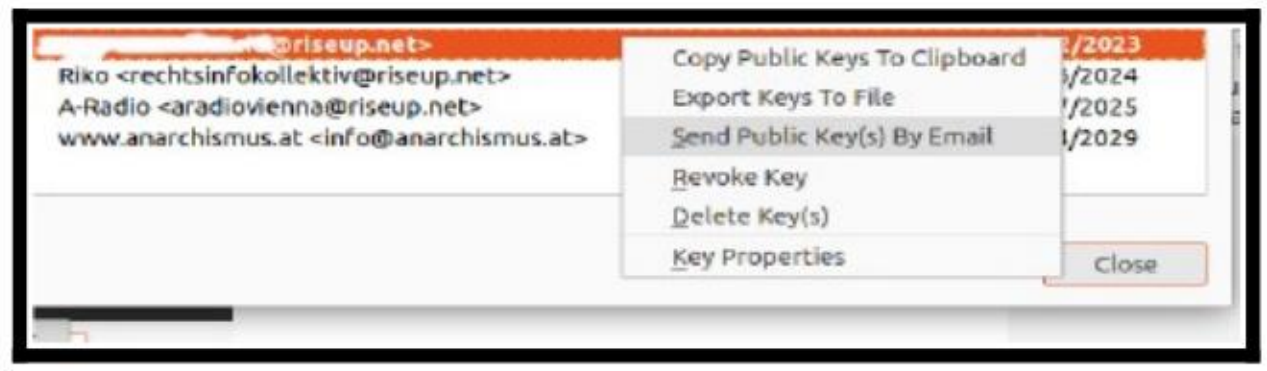
Thunderbird & PGP



Hier einfach dann die gewünsche Mailadresse auswählen, Keys generieren und voila! Ihr habt nun einen *Private* und einen *Public Key*!

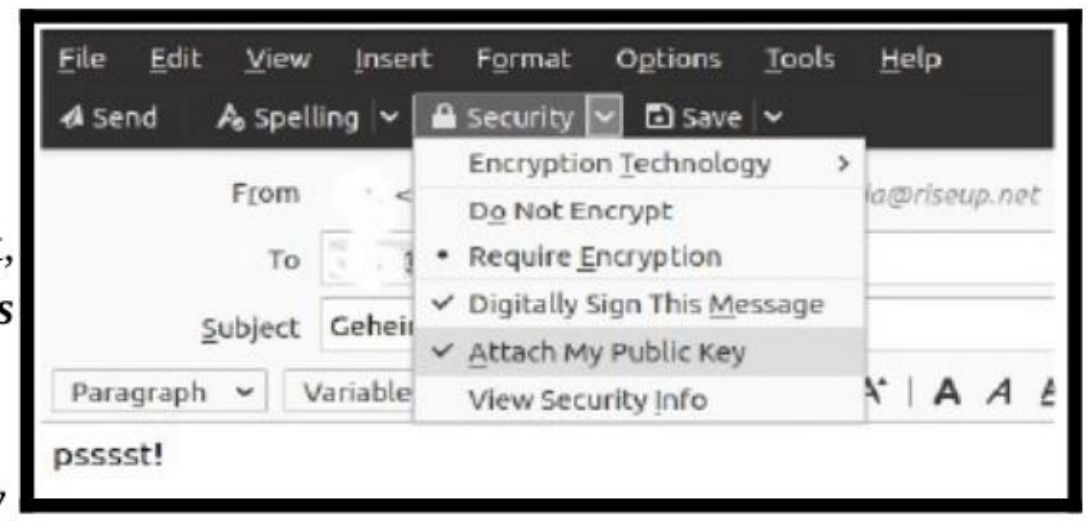
Doch Wie schickt ihr den Public Key an eure Freund*innen und Genoss*innen?

4 Möglichkeiten!



1. Copy to Clipboard. Damit könnt ihr es in einen Chat, eine Mail, auf eine Website copy-pasten. Ist ein viele Zeilen langes Ding, das ihr in der Form häufig auf Webseiten finden werdet.
2. Export keys to file. Damit bekommt ihr ein file mit der Endung ".asc". Den könnt ihr dann einfach wo abspeichern, schicken, whatever! Wenn ihr auf diese Weise einen Key geschickt bekommt, könnt ihr den einfach im Thunderbird "OpenPGP Manager" unter ***Edit -> Import Public Key(s) from File*** hinzufügen. Private Keys haben dieselbe Endung und können auch so eingefügt werden. z.B. wenn ihr migriert oder den Key auch auf dem Smartphone oder einem anderen PC haben wollt zum Mails lesen.
3. Send public key(s) by Email. Erklärt sich von selbst, ihr könnt auch bei jeder Mail die ihr schickt den Key anhängen.
4. Wenn ihr eine Mail schickt könnt ihr unter ***Security*** die Option ***Attach my Public Key*** auswählen und der key wird direkt in den Anhang gepackt.

Basics sind klar? *Sehr cool!*



Dann habt ihr nun Genoss*innen die unbedingt ne geheime Mail bekommen sollen. Wie geht das?

Ganz einfach: ***Require Encryption*** heißt, dass ihr verschlüsselt. ***Digitally Sign this Message*** heißt, dass die empfangende Person sicher sein kann, dass die Absende-Adresse stimmt und ***Attach my Public Key*** bedeutet, dass die andere Person euren Key bekommt und ins Mailprogramm aufnehmen kann.

Wenn ihr die Public Key(s) der anderen Person in eurem **OpenPGP Manager** gespeichert habt, werden die verschlüsselten Mails automatisch entschlüsselt. Aber eben nur im Mailprogramm auf eurem Computer! Die Mails, die mit eurem Public Key verschlüsselt wurden, können nur mit eurem lokal gespeicherten Private Key entschlüsselt werden. Mails abfangen oder euren Account hacken macht das Lesen der Mails also unmöglich.

Kleiner Tipp: Macht euch backups von eurem "Key Pair", also sowohl vom Private, als auch vom Public Key. Diese unverschlüsselt auf eurem Desktop rumliegen lassen, sie an euch selbst per Mail schicken oder sie in einer Cloud speichern sind definitiv schlechte Ideen. Diese Backups direkt auf einem verschlüsselten USB-Stick zu speichern, also ohne Zwischenspeichern am PC, könnte schon etwas besser funktionieren. Falls ihr ernsthafter mit Tails arbeiten wollt, wäre eine Möglichkeit die Backups im Persistent Storage abzulegen.

Alles nicht so romantisch wie die RAF-Methode, aber durchaus sicherer.

Genauerer Überblick: https://www.varonis.com/blog/pgp-encryption/

Wen Näheres interessiert, YouTube Video to E2EE & Key-Exchange:

Teil I: https://www.youtube.com/watch?v=jkV1KEJGKRA

Teil II: https://www.youtube.com/watch?v=NmM9HA2MQGI

---

4. VPN

VPN steht für **Virtual Private Network** und ist ganz grob eine 'Umleitung', über die ihr euch mit Internetdiensten verbindet. Wenn wir auf eine Internetseite zugreifen wollen, dann schreien wir normalerweise metaporisch gesprochen, quasi aus dem Fenster. Alle können dadurch wissen, wo wir wohnen, wo wir hinwollen und was wir machen. Mit der Nutzung des VPNs hören wir nicht unbedingt auf, damit das wer-was-wann-wo herauszuposaunen, aber es ist stark vereinfacht erstmal nur der VPN-Dienst, der uns hört und unsere Anfrage weiterleitet. Für alle anderen erscheint es, als ob wir nur eine Nummer aus einem Wohnblock sind. VPN-Dienste bieten meist mehrere Wohnblocks (Server) mit (IP-)Adressen an, aus denen wir wählen können. Anonym sind wir damit aber noch lange nicht, je nachdem, wo der Server liegt oder welches Recht für den VPN-Dienst gilt, können die Cops den Client Hops nehmen oder unsere richtige Adresse einfordern. Besser ist es, wenn selbst der VPN-Dienst keinen Plan hat, welche Personen den Server gerade nutzen, weil z.B. bei der Registrierung keine individuellen Ident.-Daten notwendig sind und keine Listen (logs) darüber geführt werden, wer was wann macht. Schlussendlich gilt auch hier: Auch VPNs muss ich vertrauen... Die Unternehmen können viel versprechen und sagen, sie speichern nix, was sie am Ende tatsächlich machen und ob sie mit Geheimdiensten kooperieren, ist schwer nachzuvollziehen. Aber: lieber Wohnblock als aus dem Fenster des Einfamilienhauses schreien :P

Welcher VPN passt für mich?

Es gibt gefühlt tausende kommerzielle Anbieter, ein Überblick ist schwer: Save **That One Privacy Guy's VPN Comparison Chart.xlsx**.

Einige Websites machen regelmäßig Vergleiche.

Ein paar Fragen für euch zum langhangeln:

- Was will ich mit dem VPN machen?
- Auf welchen Geräten/Betriebssystemen benutze ich ihn?
- Wie fallen Rezensionen aus?
- Wieviele Zugänge bekomme ich? Kann ich diese mit Freund*innen teilen?

Ich (mike) benutze PrivateVPN, funktioniert über graphische Clients auf Windows, Mac und Android und über OpenVPN auch auf allen Linux-Distributionen. Es sind 5 Zugänge dabei, alle zwar mit selbem Passwort, aber sollte in den meisten Fällen eh wurscht sein, v.a. da lokal eingestellt wird. > 200 Server stehen in > 60 Ländern, daher extrem praktisch für verschiedenste Anwendungen, andere Anbieter haben noch mehr. Wenn ihr viel in bestimmten Kontexten arbeiten wollt, schaut euch Serverlisten durch!

Ich (Kümmel), habe auch gute Erfahrungen gemacht mit Mullvad, IVPN, AzireVPN und unter Vorbehalt NordVPN (da nutze ich einen geteilten Account mit anderen, NordVPN ist der einzige Client mit bekanntem security breach und der Umgang damals mit dem Leak war auch nicht astrein... war natürlich ein riesiger Aufschrei und sie sagen, sie haben nachgebessert, aber ja...). (addendum v. mike: NordVPN wird wieder relativ hoch geratet was security angeht)

Ein kleiner Überblick über Pro & Contra, den ich dazu für mich mal angelegt hatte:

Client	+	-
AzireVPN	Streaming möglich, relativ günstig, Server nicht gemietet, anonymer Account (aber mit user name + password), 5 Geräte in Basis Paket	Funktionsumfang (z.B. Multi-Hop, Standorte), Android Client sehr simpel (geringe Einstellungmög.)
IVPN	Streaming möglich, Preis fair (fixes Modell), guter support, anonymer Account	jurisdiction?, nur 2 Geräte in Basis Paket (+ kein Multi-Hop)
Mullvad	Preis fair, guter Client, viele Protokolle, umfangreicher Service, anonymer Account (zufällige Nummer dient als ID)	kein Streaming, jurisdiction?
NordVPN	Streaming möglich, viele Standorte, Funktionsumfang prinzipiell hoch	Buisness Ethics, einziger Client mit bekanntem breach, Wireguard Protocol nicht unterstützt
ProtonVPN	freie Version (eingeschränkte Serverstandorte), Android Client gut	relativ teuer

Es gibt natürlich auch kostenlose VPN Services, die sind allerdings oft fragwürdig, teils mit begrenztem Traffic, keine oder geringe Serverwahl und der Sicherheitsaspekt sollte hinterfragt werden.

`Kommentar Kümmel: Kostenpflichtige Angebote müssen nicht vertrauenswürdig sein, kostenlose VPNs sind es garantiert nicht.`

---

5. Messenger-Dienste

WhatsApp und Facebook-Messenger sind es nicht, da sind wir uns einig, aber was sind sichere Alternativen?

Telegram hat nach den WhatsApp Datenschutz-Neuerungen extremen Zulauf bekommen. Die dubiosen Verschlüsselungspraktiken und die per default deaktivierte Ende-zu-Ende-Verschlüsselung in privaten Chats (die muss extra aktiviert werden, Gruppennachrichten sind in Telegram **derzeit immer unverschlüsselt**) machen diesen Dienst zu **keiner** sicheren Alternative.

Threema aus der Schweiz bietet prinzipiell ein feines Datenschutzkonzept und ist seit kurzem auch open-source. Der Dienst muss einmalig gekauft werden (good old times) und hat den Funktionsumfang moderner Konkurrenzapps. Threema benötigt allerdings im Gegensatz zu anderen Diensten keine Telefonnummer oder andere Identifikationsmerkmale. Ein kleines Problem ist, dass Android Nachrichten des Messengers verzögert zustellt, weil Apps von Google, Facebook & Co priorisiert werden (Quelle).

Da die meisten von uns **Signal** nutzen hier ein paar hilfreiche Tipps:

iOS (englisch)/ Android (deutsch): Es macht Sinn unter

> settings - notifications - notification content/ Einstellungen - Benachrichtigungen - Anzeigen

die Option zu *No Name or Content* auszuwählen (zumindest vor Aktionen! M.E. macht es aber immer Sinn, schließlich ist es manchmal nicht mehr möglich die Einstellungen zu ändern). Push-Nachrichten erscheinen damit nur noch als neutrale Signal-Notifications ohne Hinweise auf Wer oder Was.

Unter

> *Privacy - Disappearing Messages/ Datenschutz - Verschwindende Nachrichten*

könnt ihr Voreinstellungen für neue Chats auswählen, die für jeden von euch eröffneten Chat gelten. Der Timer gibt an wie lange Nachrichten für alle Beteiligten sichtbar sein sollen.

> *Privacy - App Security/ Datenschutz - App-Sicherheit*

ermöglicht euch die Screenvorschau während des Multitaskings zu unterbinden und eine Bildschirmsperre nach einer gewissen Abwesenheit (Signal fordert dann die Eingabe des Passwortes) einzurichten. Beides macht Sinn, wobei ihr das Timeout natürlich nach eigenem Ermessen einstellen könnt.

Unter

> *Privacy - Advanced/ Datenschutz - Erweitert*

gibt es auch die Möglichkeit jeden Anruf über den Signal Server laufen zu lassen, sodass die eigene IP-Adresse nicht der angerufenen Person preisgeben wird (Kann die Anrufqualität schmälern, nicht unbedingt notwendig und relevant, da hoffentlich eh auch VPN).

Wenn ihr mit euerer normalen Handynummer angemeldet seit macht es davon abgesehen natürlich Sinn euren Namen im Profil zu ändern (vllt. iwelche Kürzel) und das auch bei anderen Messenger-Diensten so zu handhaben.

Alternativen zu Signal

Signal hat einen entscheidenden Nachteil: Ihr müsst eure Telefonnummer teilen um mit Menschen in Kontakt zu treten. Daher wäre es eine Überlegung wert zusätzlich noch andere Messenger zu nutzen. Alternativen sind z.B. DeltaChat oder Briar. Diese anderen Systeme sind zwar weniger verbreitet, haben aber meist eine starke Entwickler:innen-Community und können daher u.U. Alternativen darstellen. Die Kommunikation über einen (firmeneigenen) Server wie bei Signal oder

Threema setzt immer auch die Bindung an dieses Unternehmen voraus. Andere Projekte wie bspw. der Client Element basieren hingegen auf Matrix. Der Vorteil könnte hier sein, dass das Matrix Netzwerk über dezentralisierte Server arbeitet, keine Registrierung voraussetzt und plattformübergreifende Kommunikation zulässt (auch z.B. zu Signal). Nicht alle Clients, die verfügbar sind bieten hohe Sicherheitsstandards, **Element** arbeitet aber mit E2EE. Eine gute Dokumentation von Matrix findet sich bei der TU Dresden, hier. Andere Stimmen betonen wiederum, das Matrix eklatante Sicherheitslücken hat und keine sichere Alternative im aktivistischen Kontext ist. Die föderale Struktur der Software-Architektur wird z.B. für die Speicherung etlicher Kopien auf anderen Servern kritisiert. Hier braucht es noch mehr Research, um herauszufinden wie und ob diese Anwendungen unseren Anforderungen entsprechen können.

---

6. Dateien und Systeme verschlüsseln (Behörden hassen diesen Trick!!)

Wir haben nun über Plattformen gesprochen, die zum Austausch dienen können. Jetzt soll es ein bisschen darum gehen wie wir das, was wir versenden wollen verschlüsseln können und den Zugang zu den Dateien erschweren, wenn der Channel über den wir teilen vielleicht doch kompromittiert ist oder die Datei(en) in die falschen Hände geraten könnte(n).

Wir könnten natürlich alles wild verschlüsseln, unser Betriebssystem doppelt und dreifach absichern, versteckte Orte auf der Festplatte anlegen oder Hardware Tokens besorgen. In der Praxis gibt es da umfangreiche Möglichkeiten, die hier aber etwas zu weit führen würden. Wir konzentrieren uns zunächst einmal darauf wie wir einzelne Dateien verschlüsseln können und die Festplatte gegen unauthorisierte Zugriffe schützen.

Dateien/ Dokumente verschlüsseln:

Verschlüsseln per PGP: Basic und sehr sicher: dieses bissl umständliche **PGP**. Ein paar kleine Tutorials zum lokalen verschlüsseln mit PGP: Windows & Linux & iOS. Damit verschlüsselt ihr ± manuell die Dateien und leitet sie dann weiter. Es gibt hier einige Methoden, z.B. direkt über ein Eingabe-Terminal (Sieht stark nach hacken wie im Film aus) oder aber auch über graphische Benutzeroberflächen, in das die Schlüssel direkt importiert werden können, was Handhabung und Übersicht definitiv erleichtert.

Andere Verschlüsselungsmöglichkeiten:

Dateityp	How to (genauere Infos unter den genannten Links)
PDF	So gut wie jeder PDF-Viewer bietet die Möglichkeit an, das Dokument mit einem Passwort zu schützen. Leider sind die Sicherheitssignaturen des Formats kaputt by Design. Passwörter in den PDFs direkt verhindern zwar zunächst den Zugriff von Lai*inn*en auf das Dokument, wer es ernst meint kann allerdings die Dateien frei modifizieren und sich z.B. Inhalte via Internet anzeigen lassen (Quelle).
Textdokumente	Verschlüsselung über interne Fuktion in Word. --> alle anderen Texttypen lassen sich auch über die nachfolgende Methode verschlüsseln.

Videos/ Bilder/ Verzeichnisse/ Textdok.	Ordner mit Dateien (aller möglichen Art) lassen sich unter Windows über Zip-Dateien verschlüsseln. Im MacOS gelingt das ebenso easy über .dmg-Dateien. Eine kurze Anleitung dazu findet ihr hier. Eine umfangreiche Liste an Möglichkeiten unter Ubuntu (und anderen Distributionen) findet sich in diesem Forum.
Partitionen, USB-Sticks, Imagedateien	dm-crypt (wiki-link, Linux), Veracrypt (Linux, Mac, Windows) --> beide Programme ermöglichen das Anlegen eines verschlüsselten Containers, der auf der Festplatte immer gleich viel Platz einnimmt. Verschlossen kommt niemensch an die Daten ran. Es ist auch möglich einen "doppelten Boden" einzubauen und so einen zweiten versteckten Container anzulegen. Wie sinnvoll das ist hängt davon ab, welche Daten vor wem geschützt werden sollen; FileVault (verschlüsselt die Festplatte auf Mac, siehe unten)
Dateien in die Cloud hochladen	Boxcryptor ist ein Programm, das es ermöglicht Dateien E2E verschlüsselt in die jeweilige Cloud hochzuladen. Wenn ihr also einen Cloud-Dienst verwendet, dem ihr eure Bilder, Videos, Dokumente, etc. anvertraut, dort die Dateien aber unverschlüsselt hochgeladen werden, kann dieses Programm dafür sorgen, dass der Zugriff tatsächlich nur mit euerer Passphrase möglich ist. Ein Tutorial für Windows, MacOS, iOS und Android findet ihr hier. In der Basis-Version (alles andere kostet leider) habt ihr die Möglichkeit mit einem Cloud-Dienst und zwei Geräten, auf denen synchronisiert wird, zu arbeiten. Eine kostenlose Option für Dropbox-Konten ist Cryptomator.

Wie immer ist es natürlich besser Dinge lokal auf euerem Rechner zu verschlüsseln und dann direkt über einen sicheren Kanal weiterzuleiten (USB, **offline**). Ermöglicht der Kanal über den ihr kommuniziert allerdings nur eine gewisse Dateigröße und ihr seid auf eine Cloud angewiesen (Systemli & Cryptpad für Dateien unter 1 GB), dann könnt ihr z.B. über Tresorit Dateien bis zu 5 GB bereitstellen. Ihr müsst dazu eine E-Mail Adresse angeben (Vorsicht, Tresorit schickt euch eine unverschlüsselte Mail, in der ist zwar nicht der Zugriff auf den Link möglich, aber ihr/alle die mitlesen könnt die Mail-Notifications abbestellen), aber es ist möglich die Dateien zusätzlich mit einem Passwort zu sichern, sodass nur Personen mit Link *und* Passwort die Datei herunterladen können. In der Basisversion könnt ihr euch noch über Zugriffe per Mail informieren lassen. Der Link läuft nach 7 Tagen oder 10 Zugriffen automatisch ab. Teilt Passwort und Link immer über unterschiedliche Kanäle (das gilt allgemein!).

Weitere kostenlose, quelloffene und sehr einfach gestaltete Optionen, über die Dateien bis zu 2 GB geteilt werden können, die keine Identifikationsmarker von euch verlangen, euch aber die Möglichkeit bieten Passwörter und Verfallszeiten des Links festzulegen sind: NowTransfer, Disroot und Anoxinon.

... und dann vielleicht doch in ner Cloud speichern?

... oder direkt in der Cloud arbeiten!

Bei Festplatten haben wir folgendes Problem: Bei moderneren SSDs ist es fast unmöglich eine Datei restlos zu löschen, Dateien werden gestückelt in verschiedenen Parts der Festplatte gespeichert und es ist ohne riesigen Aufwand möglich herauszufinden wo sie im Endeffekt verstreut sind, was restloses Löschen über die gewöhnlichen Wege erheblich erschwert. Das Löschen von Dateien unter Windows über den Papierkorb ist dabei auch irreführend, denn die Dateien werden nicht tatsächlich gelöscht, sondern nur prinzipiell zum Überschreiben freigegeben (das kann per

Zufall passieren, die Wahrscheinlichkeit ist aber erstmal relativ gering) und können daher mit hoher Wahrscheinlichkeit rekonstruiert werden. Die einzige Möglichkeit Dateien von einer SSD komplett zu löschen ist die ganze Festplatte zu "wipen". Bei alten HDDs, die mit der Scheibe drin, ist das Ganze sehr viel einfacher und "wipen" ist mit einfachen Tools möglich (Windows & Linux & Mac). Wenn ihr also noch eine alte Festplatte verbaut habt, habt ihr in diesem Fall einen Vorteil.

Da das allerdings seit einigen Jahren nicht mehr dem Standard entspricht, müssen wir uns Alternativen zum Arbeiten mit kritischen Daten überlegen. Die naheliegendste Möglichkeit ist ohne Digitalisierung zu arbeiten. Da das allerdings nicht immer möglich ist, wäre für das gemeinschaftliche Arbeiten an Themen **ohne strafrechtliche Konsequenzen** naheliegend direkt in der (verschlüsselten) Cloud zu arbeiten. Da wir uns ja schon mit Online-Sicherheit auseinandergesetzt haben und für sensibles Arbeiten auf das im nächsten Kapitel erwähnte ***Tails*** zurückgreifen, dürfte das in den meisten Fällen das Mittel der Wahl sein. Bei strafrechtlich relevanten Sachen --> unbedingt offline bleiben, nichts aufschreiben und eine gewisse Sicherheitskultur beachten!

Welche Möglichkeiten in der Cloud zu arbeiten gibt es?

Klar, Google Drive/ Docs/ etc. ist super praktisch und es wirkt oft als wäre das die einzige Möglichkeit gemeinsam an Dokumenten, Präsentationen und Tabellen zu arbeiten. Die Bandbreite an Alternativen, vorallem an sicheren (!), ist aber sehr groß.

Viele der *open source* online Clouds und Pads basieren auf *EtherPad* und bauen einen größeren Sicherheitsapparat um diese Basis. Im Prinzip ist die Funktion genau wie bei Google Drive. Beliebt sind z.B. cryptpad.fr, limonade.cc, pads.c3w.at. Teilweise gibt es Probleme mit der Servergeschwindigkeit bei einigen Hosts, daher am besten vorher ausprobieren! Die Funktionen sind bei allen *EtherPad* basierten Methoden sehr ähnlich. Ihr könnt hier so vorgehen, dass alle beteiligten Personen einen eigenen Account anlegen, oder aber, dass ihr gemeinsam einen Account nutzt, was eben anonymer ist.

Eine offline-Variante für Linux stellt EncryptPad dar, ein offline-Texteditor mit eingebauter Verschlüsselung für eure Dokumente. Es benutzt eine symmetrische Verschlüsselung basierend auf dem im Mail-Teil erwähnten PGP, kombiniert mit einem Passwort. Vorsicht: Wenn ihr das gewählte Passwort vergesst oder den Schlüssel verliert habt ihr keinen Zugriff mehr, es gibt keine Möglichkeit drum herum zu arbeiten! Mit einer sicheren Schlüssel- und Passwort-Weitergabe könnt ihr die geupdateten Versionen immer über einen Cryptdrive oder ähnlichem teilen und so gemeinsam, aber zeitversetzt, daran arbeiten.

Ganze Festplatten verschlüsseln

Klare Empfehlung! Es ist nicht nur extrem schwer bis quasi unmöglich für Behörden eine verschlüsselte Festplatte zu entschlüsseln, sondern auch extrem teuer! Es gibt hier viele kostenlose und kostenpflichtige Programme für alle Plattformen (inklusive Smartphone), hier werden erstmal nur die default-Lösungen präsentiert. Standardmäßig vorinstalliert gibt es in Windows den BitLocker zum verschlüsseln der gesamten Festplatte, FileVault bei MacOS und verschiedenste Tools bei den jeweiligen Linux-Distributionen (z.B. für Ubuntu ist es direkt bei der Installation möglich, aber auch im Terminal möglich, die Anleitung ist etwas kompliziert und erfordert ein wenig reinarbeiten. Andere Billo-Anleitung). Bei Tails wird der erwähnte *Persistent Storage* beim Erstellen automatisch verschlüsselt!

Zusatz: Bilder/ Videos um Metadaten bereinigen + Gesichter unkenntlich machen

Metadaten sind Informationen, die sich in Dateien (meist auf den ersten Blick unsichtbar) verstecken können. Das können Infos über die Kamera, mit der aufgenommen worden ist, oder das Gerät im Allgemeinen sein, aber auch z.B. sehr genaue Standortangaben. Systemli bietet ein Web-Interface zur Bereiningung von veräterischen Informationen.

Grundsätzlich ist es besser vertrauliches Material direkt auf dem eigenen Computer zu bereinigen und keiner externen Plattform zu vertrauen. Das bei Systemli verwendete Programm lässt sich mit etwas Technikgeschick als Terminal-Tool lokal auf dem PC installieren. Hier ist dazu die Dokumentation. Unter Linux gibt es dazu noch das gut integrierte *mat2*, welches in euren File-Browser integriert ist. Es ist standardmäßig bei Tails vorinstalliert und kann bei z.B. Ubuntu einfach mit `sudo apt install mat2` installiert werden. Mit diesem Tool könnt ihr einfach im Ordner per Rechtsklick die Metadaten bereinigen, wodurch eine "saubere" Kopie der Datei erstellt wird (Denkt daran die Original-Datei zu löschen bzw. darauf zu achten die cleane Variante weiterzuleiten).

Eine weitere Alternative dazu ist Exiv2.

Für Android gibt es außerdem die App ObscuraCam. Mit Hilfe dieser App können Gesichter unkenntlich gemacht werden und gleichzeitig Bilder um Metadaten bereinigt werden.

Für iOS gibt es zum Cleanen u.a. die App "ViewExif".

---

7. Betriebssysteme

Windows ist nicht nur auf vielen Ebenen extrem anstrengend, sondern auch extrem anfällig für Attacken. Das hat mehrere Gründe, einer davon ist natürlich, dass es von einer riesigen Menge an Menschen benutzt wird und daher ein sinnvolles Ziel darstellt. Es ist das Standard-Betriebssystem für Computer und wird daher viel von wenig versierten Nutzer*innen genutzt, wodurch Attacken schnell gelingen können. Dadurch und die in Linux-Distributionen integrierten Sicherheitskonzepte, braucht ihr keine schlecht-funktionierenden Anti-Viren-Programme, sondern seid von Beginn an sicherer.

Hauptalternative sind die vielen Linux-Distributionen, ausgelegt auf ebenso viele verschiedene Nutzungsarten und -Geschmäcker.

Die verschiedenen Linux-Distributionen haben eine Menge Vorteile, aber auch einen entscheidenden Nachteil: Es lassen sich keine Windows-Programme abspielen (außer man nutzt Umwege, die wenig stabil sind). Alternativen für diese Programme gibt es aber zuhauf. Großer Vorteil in puncto Sicherheit ist, dass die Systeme open source sind und von einer großen Community geschrieben werden. Kapitalinteressen gibt es hier idR keine und die meisten Distributionen fallen unter eine "Schenk-Ökonomie".

Ihr werdet, sofern ihr nicht schon einiges an Erfahrungen mitbringt, zu Beginn öfters denken "Wow schaut der Mist kompliziert aus", aber ebenso schnell merken, dass ihr zu jedem Problem extrem schnell Hilfe findet. Die Communities sind sehr groß, sehr versiert und sehr freundlich und zuvorkommend. Nichts was euch begegnet, ist nicht schon wem anderes begegnet ;)

Ubuntu

Ubuntu ist die populärste Linux-Distribution und auf Benutzerfreundlichkeit ausgelegt. Hat ein freundliches Design und viele Möglichkeiten es anzupassen durch verschiedenste Oberflächen. Es ist eine der besten Distributionen für den Einstieg und erlaubt einiges an rumexperimentieren. Es gibt viele Wege Ubuntu sicher zu gestalten, wobei die Sicherheit von Haus aus schon relativ hoch ist: Fast jeden Tag kommen Sicherheitsupdates heraus, an der die riesige Community schreibt.

Ein kleiner Auszug von der Ubuntu-Website: "use your common sense. The biggest security threat is generally found between keyboard and chair."

TailsOS

Von Tails habt ihr bestimmt schonmal gehört. Es wird nicht direkt auf dem PC installiert, sondern läuft live über einen USB-Stick. Das hat den Vorteil, dass nichts am PC gespeichert wird und ihr ihn schnell rausziehen und wegrennen könnt. TailsOS ist auf Sicherheit und Privatsphäre ausgelegt, verbindet zum Beispiel direkt über das Onion-Netzwerk, das auch von Tor genutzt wird. Ihr könnt Dinge dauerhaft auf dem Stick speichern, dazu wird ein verschlüsselter "persistent storage" angelegt (unter "configuring persistant storage" gibt es eine detaillierte Anleitung).

Dieses Betriebssystem ist perfekt wenn ihr illegales tun wollt, on the run in nem Internet-Cafe oder auf fremden Computern etwas seid oder einfach keine Spuren hinterlassen wollt. Außerdem easy to do und zum rumexperimentieren, wenn ihr euren PC nicht neu aufsetzen wollt: ein 8GB USB-Stick reicht. Standardmäßig sind neben dem Tor Browser auch noch ***Thunderbird***, ***KeePassXC*** (Passwort Manager), ***Metadaten-Bereiniger*** (Kapitel 6), ***LibreOffice*** (open source Alternative zu Microsoft Office) und ***Bild-, Ton- und Grafikbearbeitungsprogramme*** inkludiert. Quasi alles was ihr für einen mobilen Workspace braucht!

Kleine Anleitung für den Start.

Arch-Linux

Archlinux ist eine Linux-Distribution für den normalen Gebrauch, sofern ihr euch auskennt. Super personalisierbar und wenig Zeug drauf, über das Angriffe gelingen könnten. Ihr habt komplett in der Hand wie das Betriebssystem aussieht.

---

8. Common Sense mit dem Smartphone

Sobald das Plenum beginnt, werden alle Handys rausgelegt und in Gegenwart eines Handys versucht nichts von Bedeutung laut auszusprechen. Doch... sind wir immer so vorsichtig? Und warum gehen wir das Ganze nicht ein wenig radikaler an? Tech-Konzerne sammeln fleißig Daten und auch andere Institutionen, wie zB der Staat (buh!), können unsere Smartphones knacken und 2500 Beidl-Fotos veröffentlichen. Unsere Privatsphäre können wir aber recht einfach besser schützen. Wieder nicht komplett, zumindest nicht solange wir spezielle Hardware dazupacken und ohne SIM fahren, aber ein heftig erhebliches Stück besser zumindest!

Beginnen wir einfach mal mit dem Radikaleren:

Google-freies Betriebssystem

Die meisten von uns benutzen wohl Android-Smartphones. Geschrieben von Google und damit durchsetzt von Wegen eure Daten zu sammeln. Dazu Bindung an eine Gmail-Adresse und meist auch mit Chrome als Browser. Das macht das Telefon schon ab Vertrieb zur Datenkralle. Ob über GPS-Tracker, angezapftes Mikrofon, oder Tracking eures Online-Verhaltens. Doch hier gibt es super Alternativen, mit denen ihr zudem der geplanten Obsoleszenz entgegenwirken könnt und ausbleibende Security Updates (ich glaube die meisten Modelle werden nur 2-3 Jahre mit Updates versorgt) reaktivieren. Auch der Akku läuft länger und Ruckler können beseitigt werden.

Dazu wird das "normale" Android vom Handy runtergeschmissen und ein "Custom OS" draufgespielt. Das populärste ist LineageOS. Nicht jedes Smartphone wird unterstützt, eine Liste gibt es hier. Ihr könnt euch aussuchen ob ihr trotzdem Google Play oder Google Services dabeihaben wollt, damit ist zwar das installieren von Apps einfacher, aber der urprüngliche Beweggrund ein bisschen verraten. Apps können auch von den Websites der jeweiligen App als *.apk*-Datei heruntergeladen und manuell installiert werden. Ein paar Apps werden nicht funktionieren, alle gängigen schon. Außerdem ist LineageOS mit der aktuellen Version auf Android 10, was das installieren aller Apps erlaubt. Es gibt einige Sicherheits-Features und viele Möglichkeiten euer Smartphone euren Wünschen nach einzustellen. Und das alles ohne Google, juhu!

Es gibt noch einige mehr direkt auf Privacy-fokusierte Betriebssysteme, eine kleine Übersicht gibt es hier, vielversprechend scheint GrapheneOS zu sein.

Für Apple-Produkte schaut das Ganze ein wenig komplizierter aus. Es gibt Wege auf dem Iphone Android-basierte Betriebssysteme zu installieren, ich schätze das Risiko das Handy zu zerschießen und unbenutzbar zu machen aber als relativ hoch ein. Ein fertiges Projekt ist nicht zu finden, Project Sandcastle ist noch in der Beta-Phase.

Besonders 'ältere' Smartphones, deren Android/ iOS-Versionen bereits vom Update-Zyklus ausgeschlossen sind, laufen Gefahr sich zu Sicherheitsrisiken zu entwickeln. Erkannte Sicherheitslücken werden bei ihnen nicht durch ein neues Software-Update geschlossen und können so potentiell für einen Angriff ausgenutzt werden. Bei Apple ist diese Geschichte, wie oben beschrieben, recht alternativlos, bei Google macht es Sinn spätestens (!) zu diesem Zeitpunkt auf ein freies OS umzusteigen.

SIM-Tracking

Die Polizei kann jederzeit tracken in welchen Sendemasten-Schnittpunkten ihr euch gerade befindet, was genauer ist, als mensch es zuerst erwarten würde. Außerdem ist Teil der Riot-Control die mobile Überwachung des Funkverkehrs, womit Papa Staat weiß, dass ihr auf Demo X wart. Es gibt wenig was getan werden kann, dem zu entkommen, vorallem, da eure Nummern in der Regel mit euren Namen verknüpft sind. Abhören können die Behörden wie gewohnt alles, eure Signal-Chats mitlesen aber nicht.

Die Lösung? SIM-Karten aus den Niederlanden oder Tschechien. In beiden Ländern sind die SIM-Karten ohne Registrierung nutzbar und durch die neue Roaming-Regeln sind diese auch europaweit benutzbar. Die besseren Tarife haben niederländische Anbieter. Ihr könnt sie frei in den Ländern mit Bargeld kaufen und direkt welche für eure Freund*innen und Genoss*innen mitnehmen. Denkt an Ladekarten! Aber: Aktivieren müsst ihr die Karten meist im jeweiligen Landesnetz.

Auch diese Methode hat seine Grenzen: Die Geräte-ID wird immer mitgesendet. Es gibt Apps zum randomisieren, aber die können scheinbar gut geknackt werden. Trotzdem: Packt die neuen unregistrierten SIM-Karten in eure Demo-Handys und seid erreichbar und besser vernetzt auf Demos, Aktionen und Riots!

Die Sache mit den Apps

Klar sind Facebook App und Messenger, WhatsApp und Co. praktisch und haben Vorteile. Nicht aber für die Privatsphäre. Apps fragen zwar immer nach Befugnissen, aber wann dann wirklich auf Mikrofon, Kamera und Kontakte zugegriffen werden kann, ist unklar. Wir alle haben schon mitbekommen, wie Menschen über etwas nur reden und in den nächsten Stunden die Werbung auf dieses Thema gerichtet war. Ein Freund, der weit weg von Meer, Boots-Community und co wohnt, hat mal über Träumereien bezüglich einem kleinen Kajütboot geredet, kurz drauf bekam er Werbung für nahegelegene Bootsanlegestellen in Wiesbaden. Das Smartphone liegt nur nebendran und nimmt fröhlich auf, in dem Fall war es entweder die Facebook-App oder der Messenger. Dabei muss manchmal noch nicht einmal zugehört werden, die Masse an Metadaten die über euch oder eure Bezugspersonen zur Verfügung stehen ermöglicht es jedes erkennbare Muster des Verhaltens genaustens zu tracken und daraus ein passgenaues Profil von eurem Leben zu erstellen.

Es macht daher Sinn zu reflektieren, was ihr auf eurem Smartphone haben wollt und was ihr wirklich braucht. Hier eine kleine Liste:

Apps

- Social Media Apps und Spiele sind komplett aufs Sammeln von Daten ausgelegt und überschreiten durchgehend die "rote Linie".
    - Diese Apps direkt zu löschen gibt euch einen gescheiten Privacy Boost.
- Unnötige und unbenutzte Apps löschen.
- Um auf Demos per Twitter mitlesen zu können was passiert, gibt es zum Beispiel Nitter und Fritter, YouTube anonym(er) nutzen geht über HoloPlay.
- Good to Have
    - Passwortmanager (die in Kapitel 2 erwähnten sind auch mobil verfügbar!)
    - Guten Browser (z.B. Brave, Firefox oder Tor Browser)
    - Mail-App (z.B. K-9-Mail mit integrierten Sicherheitsfeatures)
    - VPN Client
    - Eine App zum Verschlüsseln von Dateien (z.B. OpenKeyChain)
    - Apps zum unkenntlich machen von Gesichtern (z.B. ObscuraCam)

App-Permissions

- Schaut was bei welchen Apps abgefragt wird und deaktiviert im Bestfall einfach alles. Je weniger etwas kann, desto weniger Schaden richtet's auf dem Handy an.

Am einfachsten und sichersten werden in Android Apps über den Google PlayStore gedownloadet, wenn ihr aus verschiedensten Gründen (zB Google fernzubleiben) einen anderen Weg wählen wollt, gibt es F-Droid, ein App-Store über den ihr Free and Open-Source Software recht vertrauenswürdig beziehen könnt.

What else...?

Wenn ihr WiFi und Bluetooth nicht benutzt --> deaktiviert es.

Natürlich alles was mit Tracking zu tun hat, deaktivieren. Dazu zählen automatische Geräte-Backups, GPS History, und die "Google Web and App Activity". Falls ihr ein Samsung-Gerät benutzt: deaktiviert den Samsung Datenaustausch. Das alles bringt nichts, wenn ihr festgenommen werdet und die Cops direkt auf euer Gerät zugreifen können, also Lockscreen sichern!

Sonstiges

Updatet eure Geräte regelmäßig! Damit werden die erkannten Sicherheitslücken geschlossen und wer euch ausspionieren will hat eine schwerere Zeit.

Das ewig leidige Thema **YouTube.** Zum abonnieren von Kanälen und zum Schauen von Ü18 Videos braucht ihr einen Google Account, inzwischen sogar mit eurer Telefonnummer verknüpft, oder sogar mit Perso-Foto. Einfach zu umgehen: **FreeTube**! Client zum runterladen, damit könnt ihr Kanäle abonnieren, Videos schauen und direkt runterladen und co.

2-Faktor-Authentifizierung ist in der Regel immer eine ganz gute Idee, leider wollen viele Dienste dafür eure Handynummer, also gut überlegen.

Glossar (zum schnellen Nachschlagen)

Glossar zum bearbeiten, auch wegen Sortier-Funktion, etc., kann auch mega gut hier reinkopiert werden, ohne dass es blöd ausschaut, hier:
https://cryptpad.fr/sheet/#/2/sheet/edit/FFTt75NaHnQRKj+Phl8uv6KR/

BIOS	Akronym für „Basic Input/Output System“. Dahinter verbirgt sich eine Firmware (*ähnlich Betriebssystem*), die sich auf dem Motherboard (der Hauptplatine) eines Computers in einem nichtflüchtigen Speicher befindet. Im Gegensatz zum normalen Arbeitsspeicher wird der ROM-Baustein, auf dem das BIOS installiert ist, nach dem Ausschalten des PCs nicht gelöscht und steht daher direkt beim Start zur Verfügung. Sobald ein Nutzer einen x64/x86-PC einschaltet, wird das BIOS automatisch gestartet. Anders als Betriebssysteme muss es nicht installiert werden, sondern ist in jedem Fall bereits auf der Hardware des Computers vorhanden.
Browser	Webbrowser oder allgemein auch Browser (engl. to browse, ‚stöbern, schmökern, umsehen‘, auch ‚abgrasen‘) sind spezielle Computerprogramme zur Darstellung von Webseiten im World Wide Web oder allgemein von Dokumenten und Daten. Das Durchstöbern des World Wide Webs beziehungsweise das aufeinanderfolgende Abrufen beliebiger Hyperlinks als Verbindung zwischen Webseiten mit Hilfe solch eines Programms wird auch als Internetsurfen bezeichnet. Neben HTML-Seiten können Webbrowser verschiedene andere Arten von Dokumenten wie zum Beispiel Bilder und PDF-Dokumente anzeigen. Webbrowser stellen die Benutzeroberfläche für Webanwendungen dar.
Clearnet	Öffentlich erreichbares Internet, oder aber auch: Oberflächen-Internet. Umfasst die Websites, die ihr über gängige Suchmaschinen finden.
Code	Ein Set an Anleitungen, die ein Computerprogramm bilden, welches wiederum von einem Computer ausgeführt werden kann.
Cookies	eine Textinformation, die im Browser auf dem Endgerät des Betrachters (Computer, Laptop, Smartphone, Tablet usw.) jeweils zu einer besuchten Website (Webserver, Server) gespeichert werden kann. Das Cookie wird entweder vom Webserver an den Browser gesendet oder im Browser von einem Skript (JavaScript) erzeugt. Der Webserver kann bei späteren, erneuten Besuchen dieser Seite diese Cookie-Information direkt vom Server aus auslesen oder über ein Skript der Website die Cookie-Information an den Server übertragen. Aufgabe dieses Cookies ist beispielsweise die Identifizierung des Surfers (Session ID), das Abspeichern eines Logins bei einer Webanwendung wie Wikipedia, Facebook usw. oder das Abspeichern eines Warenkorbs bei einem Online-Händler. Ein häufiger Einsatzzweck ist das

	Webtracking von Nutzern[1] mit speziell präparierten Seiten. Der Begriff Cookie wird im Datenschutz auch als Synonym für Datenentnahme, Datenspeicherung, Datennutzung, Datenverwertung, Datenweitergabe wie auch Datenmissbrauch verwendet, unabhängig davon, ob dazu tatsächlich ein physisches Cookie verwendet wird oder andere Techniken eingesetzt werden
Darknet	bezeichnet ein abgeschlossenes Netzwerk und beinhaltet abgeschlossene Webseiten, die nicht in normalen Suchmaschinen indexiert sind und über den Tor Browser oder andere Browser, die Tor als lokalen Proxy nutzen, zu finden sind.
Deepweb	Das Deep Web (auch Hidden Web oder Invisible Web) bzw. Verstecktes Web bezeichnet den Teil des World Wide Webs, der bei einer Recherche über normale Suchmaschinen nicht auffindbar ist. Im Gegensatz zum Deep Web werden die über Suchmaschinen zugänglichen Webseiten Clear Web, Visible Web (Sichtbares Web), oder Surface Web (Oberflächenweb) genannt. Das Deep Web besteht zu großen Teilen aus themenspezifischen Datenbanken (Fachdatenbanken) und Webseiten. Zusammengefasst handelt es sich um Inhalte, die nicht frei zugänglich sind, und/oder Inhalte, die nicht von Suchmaschinen indiziert werden oder die nicht indiziert werden sollen.
E2EE	Unter Ende-zu-Ende-Verschlüsselung (englisch „end-to-end encryption“, „E2EE“) versteht man die Verschlüsselung übertragener Daten über alle Übertragungsstationen hinweg. Nur die Kommunikationspartner (die jeweiligen Endpunkte der Kommunikation) können die Nachricht entschlüsseln. Theoretisch verhindert die Ende-zu-Ende-Verschlüsselung das Abhören der Nachricht durch alle anderen, inklusive der Telekommunikationsanbieter, Internetprovider und sogar der Anbieter der genutzten Kommunikationsdienste. Bei Verwendung einer symmetrischen Verschlüsselung darf der Schlüssel zur Sicherstellung der Ende-zu-Ende-Verschlüsselung nur den End-Kommunikationspartnern bekannt sein. Bei Verwendung einer asymmetrischen Verschlüsselung muss sichergestellt sein, dass der geheime Schlüssel (Private Key) ausschließlich im Besitz des Empfängers ist. Die zu übertragenden Daten werden auf Senderseite verschlüsselt und erst beim Empfänger wieder entschlüsselt. Dadurch können Seitenkanalinformationen, wie sie zum Beispiel teils zur Steuerung des Übertragungsprozesses anfallen, nicht mit verschlüsselt werden, andererseits werden mitwissende Zwischenstationen, an denen die übertragenen Inhalte im Klartext vorliegen, eliminiert.
Fingerprint	Eine "Hashfunktion" oder Streuwertfunktion ist eine Abbildung, die eine große Eingabemenge, die Schlüssel, auf eine kleinere Zielmenge, die Hashwerte, abbildet. Ein Hashwert wird deshalb auch als englisch Fingerprint bezeichnet, da er eine nahezu eindeutige Kennzeichnung einer größeren Datenmenge darstellt, so wie ein Fingerabdruck einen Menschen nahezu eindeutig

	identifiziert.
IRC	Internet Relay Chat, kurz IRC, bezeichnet ein textbasiertes Chat-System.
Krypto-Anarchie	Krypto-Anarchisten sehen ein wachsendes Missverhältnis zwischen staatlicher (und neoliberaler) Ermächtigung und Geheimhaltung auf der einen Seite und staatlicher (und kapitalistischer) Entmündigung und Überwachung der Bürger*innen (und Konsument*innen) auf der anderen. Sie versuchen, die Möglichkeiten, die die Kryptographie und Computernetzwerke wie das Internet bieten, zu nutzen, um diese Verhältnisse umzukehren; also Staatsgeheimnisse (und Unternehmensgeheimnisse) zu veröffentlichen, Gesetze zu unterlaufen und freie kryptographische Software zu Verfügung zu stellen, mit der man etwa anonym kommunizieren oder Handel treiben kann.
Linux	Als Linux oder GNU/Linux (siehe GNU/Linux-Namensstreit) bezeichnet man in der Regel freie, unixähnliche Mehrbenutzer-Betriebssysteme, die auf dem Linux-Kernel und wesentlich auf GNU-Software basieren. Die weite, auch kommerzielle Verbreitung wurde ab 1992 durch die Lizenzierung des Linux-Kernels unter der freien Lizenz GPL ermöglicht. Einer der Initiatoren von Linux war der finnische Programmierer Linus Torvalds. Er nimmt bis heute eine koordinierende Rolle bei der Weiterentwicklung des Linux-Kernels ein und wird auch als Benevolent Dictator for Life (deutsch wohlwollender Diktator auf Lebenszeit) bezeichnet. Das modular aufgebaute Betriebssystem wird von Softwareentwicklern auf der ganzen Welt weiterentwickelt, die an den verschiedenen Projekten mitarbeiten. An der Entwicklung sind Unternehmen, Non-Profit-Organisationen und viele Freiwillige beteiligt. Beim Gebrauch auf Computern kommen meist sogenannte Linux-Distributionen zum Einsatz. Eine Distribution fasst den Linux-Kernel mit verschiedener Software zu einem Betriebssystem zusammen, das für die Endnutzung geeignet ist. Dabei passen viele Distributoren und versierte Benutzer den Kernel an ihre eigenen Zwecke an. Linux wird vielfältig und umfassend eingesetzt, beispielsweise auf Arbeitsplatzrechnern, Servern, Mobiltelefonen, Routern, Notebooks, Embedded Systems, Multimedia-Endgeräten und Supercomputern. Dabei wird Linux unterschiedlich häufig genutzt: So ist Linux im Server-Markt wie auch im mobilen Bereich eine feste Größe, während es auf dem Desktop und Laptops eine noch geringe, aber wachsende Rolle spielt. Im März 2021 war es in Deutschland auf 2,19 % Systemen installiert.
Onion	Onion-Routing (englisch onion „Zwiebel“) ist eine Technik zum Erreichen von Anonymität im Internet. Hierbei werden die Webinhalte über ständig wechselnde Routen mehrerer Knoten geleitet. Diese stellen jeweils eine Art verschlüsselnder Proxyserver dar. Dadurch bleibt die wahre Identität desjenigen, der

	die Daten angefordert hat, für den Webserver auf der anderen Seite anonym, und nicht einmal die Betreiber der Knoten selbst können eine Zuordnung zwischen dem Nutzer und seinen angeforderten Webinhalten herstellen, es sei denn, alle Knoten der jeweiligen Route arbeiten zusammen.
Open Source	Als Open Source (offene Quelle) wird Software bezeichnet, deren Quelltext öffentlich und von Dritten eingesehen, geändert und genutzt werden kann. Open-Source-Software kann meistens kostenlos genutzt werden. Software kann sowohl von Einzelpersonen aus altruistischen Motiven zu Open-Source-Software gemacht werden wie auch von Organisationen oder Unternehmen, um Entwicklungskosten zu teilen oder Marktanteile zu gewinnen.
P2P	Peer-to-Peer (kurz meist P2P genannt, von englisch peer „Gleichgestellter“, „Ebenbürtiger“) und Rechner-Rechner-Verbindung sind synonyme Bezeichnungen für eine Kommunikation unter Gleichen, hier bezogen auf ein Rechnernetz. In einigen Kontexten spricht man auch von Querkommunikation. In einem reinen Peer-to-Peer-Netz sind alle Computer gleichberechtigt und können sowohl Dienste in Anspruch nehmen, als auch zur Verfügung stellen. In modernen P2P-Netzwerken werden die Netzwerkteilnehmer jedoch häufig abhängig von ihrer Qualifikation in verschiedene Gruppen eingeteilt, die spezifische Aufgaben übernehmen.
PGP	Verschlüsselungsprogramm, das auf einem "Public Key"-Verfahren basiert, in dem es ein eindeutig zugeordnetes Schlüsselpaar gibt. Dieses besteht aus dem Public Key und dem Private Key, wobei der erstere zum Verschlüsseln verwendet wird, sich daher bei Sender*innen befindet, und der letztere sich nur lokal gespeichert bei der empfangenden Person befindet, da diese den Private Key zum entschlüsseln verwendet.
SSH	Secure Shell oder SSH bezeichnet ein kryptographisches Netzwerkprotokoll für den sicheren Betrieb von Netzwerkdiensten über ungesicherte Netzwerke. Häufig wird es verwendet, um lokal eine entfernte Kommandozeile verfügbar zu machen, d. h., auf einer lokalen Konsole werden die Ausgaben der entfernten Konsole ausgegeben, und die lokalen Tastatureingaben werden an den entfernten Rechner gesendet.
Suchmaschine	Eine Suchmaschine ist ein Programm zur Recherche von Dokumenten, die in einem Computer oder einem Computernetzwerk wie z. B. dem World Wide Web gespeichert sind. Nach Erstellung einer Suchanfrage, oftmals durch Texteingabe eines Suchbegriffs, liefert eine Suchmaschine eine Liste von Verweisen auf möglicherweise relevante Dokumente, meistens dargestellt mit Titel und einem kurzen Auszug des

	jeweiligen Dokuments. Dabei können verschiedene Suchverfahren Anwendung finden. In der Regel erfolgt die Datenbeschaffung automatisch, im Internet durch "Webcrawler", auf einem einzelnen Computer durch regelmäßiges Einlesen aller Dateien in vom Benutzer spezifizierten Verzeichnissen. Gängige Internetsuchmaschinen wie Google zeigen ausschließlich Clearnet-Einträge an, während andere sich ausweiten lassen (DuckDuckGo) oder ausschließlich für das DeepWeb ausgelegt sind (Torch).
Surveillance Capitalism	Surveillance Capitalism "Marktwirtschaftliches, kapitalistisches System, das die mit technischen Mitteln von Menschen abgeschöpften persönlichen Daten dazu benutzt, Informationen über Verhaltensweisen zu sammeln, diese zu analysieren und für marktökonomische Entscheidungsfindungen aufzubereiten, um daraus Verhaltensvorhersagen generieren zu können und über deren Nutzung Gewinne zu erwirtschaften." Das System kann schnell & einfach für andere, unterdrückerische, Zwecke eingesetzt werden. Gute 1-stündige Doku zum Thema.
TCP	Das englisch Transmission Control Protocol (TCP, deutsch Übertragungssteuerungsprotokoll) ist ein Netzwerkprotokoll, das definiert, auf welche Art und Weise Daten zwischen Netzwerkkomponenten ausgetauscht werden sollen. Nahezu sämtliche aktuelle Betriebssysteme moderner Computer beherrschen TCP und nutzen es für den Datenaustausch mit anderen Rechnern. Das Protokoll ist ein zuverlässiges, verbindungsorientiertes, paketvermitteltes[1] Transportprotokoll in Computernetzwerken. Im Unterschied zum verbindungslosen UDP (englisch User Datagram Protocol) stellt TCP eine Verbindung zwischen zwei Endpunkten einer Netzverbindung (Sockets) her. Auf dieser Verbindung können in beide Richtungen Daten übertragen werden.
Tor ...	Tor ist ein Netzwerk zur Anonymisierung von Verbindungsdaten. Es wird für TCP-Verbindungen eingesetzt und kann beispielsweise im Internet für Browsing, Instant Messaging, IRC, SSH, E-Mail oder P2P benutzt werden. Tor schützt seine Nutzer vor der Analyse des Datenverkehrs. Es basiert auf der Idee des Onion-Routings. Der Tor Browser (auch Tor Browser Bundle) enthält eine vorkonfigurierte Kombination aus Tor (Client) und einer modifizierten Version des Browsers Mozilla Firefox ESR (mit NoScript, HTTPS Everywhere, Torbutton und TorLauncher).
Trackers/Tracking	Web Analytics (auch Clickstream-Analyse, Datenverkehrsanalyse, Traffic-Analyse, Web-Analyse, Web-Controlling, Webtracking) ist die Sammlung von Daten und deren Auswertung bzgl. des Verhaltens von Besuchern auf Websites. Ein Analytic-Tool, auch Trackingtool genannt, untersucht typischerweise, woher die Besucher kommen, welche Bereiche auf einer Internetseite aufgesucht werden und wie oft und wie lange welche Unterseiten und Kategorien angesehen werden. In Deutschland ist der Einsatz solcher Werkzeuge aus Datenschutzgründen umstritten.

	Sie wird vor allem zur Optimierung der Website und zur besseren Erreichung von Zielen der Website (z. B. Häufigkeit von Besuchen, Vermehrung von Seitenaufrufen, Bestellungen, Newsletter-Abonnements) eingesetzt. Grundlegend kann bei Web Analytics zwischen Auswertungsverfahren zur permanenten Messung der Site-Effektivität und Methoden zur Auffindung von Schwachpunkten in der Site und Verbesserungsmöglichkeiten unterschieden werden (siehe Methoden). Neben einer Reihe von freien Produkten bieten etwa 150 Unternehmen Lösungen für Web Analytics an.
VPN	VPN funktioniert mithilfe einer freigegebenen öffentlichen Infrastruktur unter Beibehaltung der Privatsphäre. Dies erfolgt durch Sicherheitsverfahren und Tunneling-Protokolle, wie des Layer-Two-Tunneling-Protokolls (L2TP). Die Protokolle konvertieren die Netzwerkpakete in ein VPN-Protokoll und übertragen diese. Dieser Vorgang wird als Tunneling bezeichnet. Die Daten werden auf der Senderseite verschlüsselt und auf der Empfängerseite entschlüsselt. Zusätzlich wird die Sicherheit erhöht, indem neben den Daten auch die aus- und eingehenden Netzwerkadressen verschlüsselt werden.
2-Faktor-Authentifizierung	Die Zwei-Faktor-Authentisierung (2FA), häufig auch als Zwei-Faktor-Authentifizierung bezeichnet, bezeichnet den Identitätsnachweis eines Nutzers mittels der Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren). Typische Beispiele sind Bankkarte plus PIN beim Geldautomaten, Fingerabdruck plus Zugangscode in Gebäuden, oder Passphrase und Transaktionsnummer (TAN) beim Online-Banking. Die Zwei-Faktor-Authentisierung ist ein Spezialfall der Multi-Faktor-Authentisierung.

Checklist

- Ich habe einen der oben angeführten Browser zu meinem Standardbrowser gemacht und Google durch etwas besseres ersetzt
- Ich habe die angeführten Add-Ons & Erweiterungen installiert (und weiß prinzipiell was sie machen)
- Ich habe den TOR-Browser installiert
- Ich verwende einen Password-Manager und habe ein starkes, sicheres Master-Passwort angelegt
- Ich habe einen (mehrere) sicheren E-Mail Account angelegt
- Ich verbinde nur noch über VPN
- Ich weiß was ein PGP-Schlüssel ist und wie ich die Methode verwenden kann, um verschlüsselte Nachrichten zu versenden
- Ich habe mich von Windows verabschiedet und ein anderes Betriebssystem installiert, dazu einen USB-Stick mit TailsOS angefertigt.
- Wenn ich Bilder oder Videos teilen möchte, weiß ich, wie ich zuvor Meta-Daten entferne und Gesichter unkenntlich mache.
- Wenn ich Dateien auf meinem PC verschlüsseln will, weiß ich, wie ich vorgehen muss und habe evtl. dazu eine Programm installiert
- Ich habe verstanden, dass Handys auf Aktionen ne blöde Idee sind, oder ich hab ne neue Nummer und gehe vorsichtig damit um!

 Unsere Kämpfe brauchen in dieser Zeit eine funktionierende Sicherheitskultur; die Unterdrücker*innen kennen sich aus, wir sollten das auch tun.

Wir hoffen dieser Guide hilft euch, euch sicherer und komfortabler in der digitalen, als auch in der realen Welt zu bewegen.

Libertäre Grüße,

Kümmel & Noa

Kontakt

Wir freuen uns über Fragen, Anregungen, Anfragen zu Erweiterungen und co. Schreibt uns einfach (verschlüsselt) eine Mail an: currydigital@riseup.net

-----BEGIN PGP PUBLIC KEY BLOCK-----

xsDNBGEtCiQBDADVFsuQohs0qu1N4+DEeUG2Vf88A0JVt2pydx50VHTFDaE74A4XirZ/sLDzgEHB
bS2VMDvRAO1RsyTBZ5RIxEWJ/5UwuyY995Wa8i7HSZ8G9/bGu8kYjee7G5WEMbeBAFlJjgcZj/Zh
kWFQJnE6XFgS2vGmig+vdIsZkwsa0LNi5rJIlnmJtvUyZHz1/KM9uYAe8tdgUfeoVJfBOUGPKpYs
Rimz58ryzOyWZ1lN4lU/LvvdAE+ML36JfbWFGiWO8YABjMfzL6exKJoWsyZi1pzlRMfZIxQ4mcPK
0vxs6qt/iNet1ybJao43jO3s6IEiGOPiMB5ZIHUJR5N3WRDtPTLTj2S/OyH96Q7jfrD/VZtlBBGU
AYyDovgpmT3YkSMkteVqDpATqfjxTZ1n8PIoUg1N8CjoNY63VfwrVxIC6D6JeI0qX4J/q2iTkfyi
sEZaUUHQbs5ot4X+zasPRJsSGTLWREBPaJz7Q7iAj2AJN6onNucDJPDrQrZO/8LC9Dz7bw0AEQEA
Ac0dTm9hIDxjdXJyeWRpZ2l0YWxAcmlzZXVwLm5ldD7CwQ8EEwEIADkWIQRdH3qn9Si3nzJA4AOA
Q0CMhHNAYwUCYS0KJAUJCWYBgAIbAwULCQgHAgYVCAkKCwIFFgIDAQAACgkQgENAjIRzQGMUsQ
wA
igk9J+qlviFONEbERnC9ZqIhMjrF9BY0swlY2dYyo7Bhb8rn3JrE+XsUVfvP99akNufa4usqqBQH
UU9qVXfKSMZB5i7OhCb/FaOSEPH2Y4esmABbCljLLB8Hm5sSJBI03uuCU9WjCG4EcGw6/3bd1+iC
L0oe9C4zCyFqgU56VZuueaSHfJJK2+Ruv/rhTCSK3/ey/F3M5nnYvpl7JybevMPmYkoiwtcTHnv5
0bxN7IABpLCxlG7iP2Empea9SgxVVV1fU+qgwuJZAs9eqMN9J4YetaF96kYbRhAZuSfpoa/A/zNn
JuBekSVvtqygEd7iYR0Ls4rWwNdBjA4y6Nf6NTNykDhlJ2T92fUkR9GCxP2ZTcwvgqUCgH5h+3eI
l57RCdI83mPyzGbXf/bT3+BGswSRwFejFKvfXEiVMdhcMhC0MPKRtSiUmxZ3njdLwx4Yfv9nXY1V
Amug1ewXmdyK1NBhRg6p7q0+vs4ydoQtJnYpZiSQSG5Vzb5QTOTQ2CD0zsDNBGEtCiQBDAC08h1p
E2yaRiDUrX8IDHjvZFQ9KoB6JgmSsqxL9PkSdW3+QErZrODVXAagAUjAQVjqusHpPnNGWKpAryAO
cAxxNyz32D4IX5yREbMz+VNwgC/ufjHC5ENcyLeH2MfIsUJjE6qpjilzitSTKUaYWsEUB8eLDq5k
fVt1AO2S9cZno3LsHSv/zX5hZqypeQrVGochdTFaFcxUbSMo7kxA0OpvBxIguzzZ7DHS19he7Wgj
GfDDXyxZAazu9ToMXP6Sxpzh70r3T24YU7xmHSOsicWfqDRBIC7IUVu1Oi+guYTUt7w9ax+RYiYm
p+xaWT/TsXjPwnb8FFEpSWBZLlU0HN6d6RiGlvNkksidokAIuKg6jOJufHFglO05WMrQzRJ/DpJ4
ZD0fe7G7kBy+/HnGLjThCozEbgNcIZyOo6AybIu6ReH5CZ6fjSLrfXKIbrRInDCHDkuG19BpI2lf
JGElqLViFytfF8+UhiXI0jiNnW6eCM85rX86jYaXSCUw482qav0AEQEAAcLA/AQYAQgAJhYhBF0f
eqf1KLefMkDgA4BDQIyEc0BjBQJhLQolBQkJZgGAAhsMAAoJEIBDQIyEc0BjDzkL/3fR05dkDI0v
VSYZr78e2hmzd9ulpbEyoelpTSYo2Wg4rMkSmgHi4fgQdCmTLwix6Z6VfHp1apVUM6HJFu3Coifa
cS8USzGcILs6WOvX1AlWWCssOSFDHu7m5XLEjaupBm1E0ZYILq1gQgZZGDNhzR9+101hJ7yPmA4Q
JaO+VvcSCIKco37mVkSpFvxGLFvmYjMm006FPjrHucLcDzulmzANmr//hJZw0jVDOzbbdEgxWRK3
0mW6C8RjN1NiU+kB+OUm2/iLsRl5ggSEB95dEPaeyw8C7x0B7J37V848paz6dU3BuIsJCNQ949Sc
I+XGy4IlLbRyT3QxzIenhr9JpTnhfODIIim9evj6JDD4zke+l5ZMQBLb1Bj7sjOeClT19gLgyGem
oafHDtdd7Im+37b7iSuXvTZaLTWfQBuyaqwCcsB2cZrG7N9F26pxQDT/FAdHUdpCYiV8l4zz/G91
n4c1OYP5MZrSaDB7+7JYcC3iYeCur9H/kv370dhRvJXYVQ==
=WrXT
-----END PGP PUBLIC KEY BLOCK-----