Friedrich / Partner

Stand März 2023

PRIVACY HANDBUCH

„Zu argumentieren, dass Sie keine Privatsphäre brauchen, weil Sie nichts zu verbergen haben, ist so, als würden Sie sagen, dass Sie keine Meinungsfreiheit brauchen, weil Sie nichts zu sagen haben.“

Edward Snowden

INHALT

VORWORT

Liebe Kundinnen, liebe Kunden,

Die Digitalisierung schreitet immer weiter voran. Das Internet ist kaum noch aus unserem modernen Alltag wegzudenken. Doch dafür haben wir einen hohen Preis bezahlt: unsere Privatsphäre.

Fast jeder kennt die Geschichte von Hänsel und Gretel. Und so wie Hänsel und Gretel eine Spur von Brotkrumen im Wald hinterlassen haben, um nach Hause zu finden, hinterlassen wir heute jeden Tag unbemerkt tausende an digitalen Spuren. Und im Durchschnitt verbringt der Deutsche ca. 46 Stunden pro Woche im Internet - das ist sehr viel Lebenszeit.[1]

Dadurch sind wir alle komplett gläsern und leben den feuchten Traum der Stasi. Der komplett transparente Bürger, den man überwachen kann und der freiwillig immer die Wanze dabei hat und seine Stasiakte bereitwillig kostenlos und ständig selbst ausfüllt. Das alles spielerisch verpackt und aus purer Bequemlichkeit. Der Preis hierfür ist hoch. Es werden komplette Profile von uns erstellt, die teils schon vorher wissen, was wir wollen, bevor wir es tun.

Ihre Privatsphäre im Internet ist jeden Tag in Gefahr. Aber Sie können etwas dagegen tun. Das vorliegende Dokument gibt Ihnen einfache Tipps und vor allem leicht umzusetzende Tipps, mit denen Sie sich vor digitaler Überwachung schützen können.

Herzlichst,
Ihr Marc Friedrich

[1] Statista; statista.com/infografik/14362/so-viele-stunden-sind-die-deutschen-pro-woche-online/

01.

WARUM IST PRIVATSPHÄRE SO WICHTIG?

Vielleicht fragen Sie sich jetzt „Warum soll ich denn im Zweifel Geld dafür ausgeben, um ein paar Daten über mich zu schützen? Ich hab doch eh nichts zu verbergen.“ Erstens glaube ich nicht, dass diese Aussage auf jeden zutrifft und zweitens ist Privatsphäre absolut essentiell für die Freiheit.
Edward Snowden hat das treffend auf den Punkt gebracht:

„Zu argumentieren, dass Sie keine Privatsphäre brauchen, weil Sie nichts zu verbergen haben, ist so, als würden Sie sagen, dass Sie keine Meinungsfreiheit brauchen, weil Sie nichts zu sagen haben.“

Das Recht auf Privatsphäre ist sogar in der UN-Menschenrechtscharta hinterlegt und ist somit ein offiziell anerkanntes Menschenrecht.

Heute wissen Konzerne und Staaten alles über Sie. Noch nie waren wir transparenter. Wir alle sind ein offenes Buch, in dem jeder mitlesen kann, wenn er denn die Mittel dazu hat.

Was einmal erfasst ist, ist für immer gespeichert. Ihr Lieblingsessen, Ihr Bewegungsprofil, Ihre Einkäufe, Ihre Vorlieben, Ihre sexuelle Orientierung, wann Sie zur Arbeit gehen oder sogar wo Ihre Smart-Geräte im Haus platziert sind. Das Internet vergisst nichts. Das macht uns angreifbar. Alexa hört mittlerweile jedes Wort mit und auch für Staaten wird es dadurch einfacher, Bürger auszuspähen. Und wir wissen, dass das schon alles vorgekommen ist. Haben Sie sich noch nie gewundert, warum Sie plötzlich eine Werbung erhielten und Sie erst gestern darüber laut nachgedacht bzw. am Telefon mit Ihrer Freundin gesprochen haben? Egal ob eine bestimmte Marke Katzen-futter, eine Reise nach Katar oder einen bestimmten Kinofilm. Konzerne wie Google oder Amazon kennen Sie mittlerweile besser als Sie glauben.

02.
SIE KÖNNEN SICH SCHÜTZEN

Aber jetzt die gute Nachricht: Sie können etwas dagegen tun. So genannte Privacy Tools erlauben es, dass Sie sich dagegen wehren und Ihre Privatsphäre im Netz Stück für Stück wieder zurückgewinnen. Bevor wir in die einzelnen Möglichkeiten einsteigen, ist es wichtig zu verstehen, dass es sich hierbei um einen Prozess handelt, an dem Sie ständig weiterarbeiten und den Sie stets verbessern müssen. Denn die Gegenseite schläft nicht und wird Wege finden, diese Abwehrmaßnahmen mit der Zeit zu umgehen. Daher mein Tipp an dieser Stelle: Bleiben Sie stets auf dem Laufenden und versuchen Sie Schritt für Schritt, sich auf diesem Gebiet vertrauter mit bestimmten Werkzeugen wie z. B. einem VPN zu machen. Aber haben Sie keine Angst: Das ist kein Hexenwerk und man benötigt keinerlei Vorkenntnisse.

Kurz etwas zum Aufbau dieses Handbuchs. Wir haben dieses in drei Teile aufgeteilt:

- **Sicher Surfen im Internet**
- **Sicher Kommunizieren**
- **Sicher Bezahlen**

Im letzten Teil geht es vor allem um das sichere Bezahlen und Transferieren von Geld. Wenn Sie regelmäßig meine Videobeiträge verfolgen, dann wissen Sie, dass ich es für sehr wahrscheinlich halte, dass das Bargeld bald seinem Ende entgegen blicken wird. Ob wir es wollen oder nicht, wir werden schon bald vor diese Wahl gestellt. Doch auch hier gibt es mit Bitcoin eine friedliche Alternative, mit der wir uns unabhängiger machen können. Daher geht es in diesem Teil des Handbuchs vor allem auch um die anonyme Nutzung von Bitcoin. Aber jetzt viel Spaß bei der Lektüre und viel Erfolg bei der Umsetzung!

Anmerkung: Bei den Empfehlungen, die mit * gekennzeichnet sind, handelt es sich um Affiliate-Links.

03.
SICHER SURFEN

VPN

Mit Sicherheit haben Sie schon mal von einem VPN gehört. Falls nicht, ist das auch nicht schlimm. VPN steht für Virtuelles Privates Netzwerk. Mittels eines VPN können Sie eine sichere Netzwerkverbindung aufbauen.

Ein guter VPN erfüllt in der Regel zwei Aufgaben.
Erstens: Er verschlüsselt Ihren Datenverkehr im Internet und verbirgt Ihren Standort und Ihre IP-Adresse. Damit können Sie eine sichere Verbindung zum Internet herstellen, zum Beispiel wenn Sie ein öffentliches Netzwerk nutzen.

Zweitens: Können Sie mit einem VPN Ländersperren umgehen, also z. B. auf Streaming-Inhalte zugreifen, die nicht in Ihrem Land verfügbar sind. Sollten Sie sich in einem Land befinden, welches erhebliche Internetzensur durchführt (z. B. China), dann können Sie mit Hilfe eines VPNs diese Sperren umgehen.

Die Nutzung eines VPNs kann sogar Dinge günstiger machen. Manche Webseiten berechnen Preise nämlich nur aufgrund Ihres Standorts. Hier kann ein VPN durchaus nützlich sein, weil die Webseite nicht den exakten Standort einsehen kann. Ich buche z. B. Flüge und Mietwagen deutlich günstiger über mein VPN. So amortisiert sich der VPN schnell. Der größte Vorteil ist aber, wie gesagt, der zusätzliche Schutz der eigenen Privatsphäre.

Eine wichtige Eigenschaft bei VPNs ist zum Beispiel, ob sie „open source“ sind. Das bedeutet, dass der Programmcode der Software öffentlich einsehbar ist. Natürlich können die meisten Menschen diesen Programmcode nicht verstehen, aber darum geht es auch nicht. Es geht darum, dass es möglich ist, den Code zu verifizieren.

Und das tun in der Tat auch viele Menschen. Somit können schneller Schlupflöcher und Fehler gefunden werden, denn viele Augen sehen mehr. Es ist zudem ein Vertrauensmerkmal, denn bei vielen Anbietern, die nicht open source sind, weiß niemand, was in dem Programm genau passiert, da der Programmcode „verschlossen ist".

Mittlerweile gibt es natürlich eine ganze Heerschar an VPN-Anbieter. Hier gibt es zum Teil erhebliche Unterschiede, auf die man achten sollte. Ich kann hier vier verschiedene Anbieter empfehlen.

NordVPN®

Unsere Empfehlung: NordVPN*

Ich persönlich bin ein großer Fan von NordVPN und nutze ihn auch selbst tagtäglich. Daher kann ich diesen Anbieter jedem nur ans Herz legen.

Kleiner Lifehack: Wenn Sie Nord VPN nutzen, wählen Sie die Ukraine als Ihren Standort und umgehen Sie so sämtliche Paywalls bei Zeit, Spiegel, Welt und Süddeutsche Zeitung.

Hier geht's zum Anbieter: nordvpn.com/marc

Mit dem Coupon-Code „marc" erhalten Sie exklusives Angebot

WEITERE ANBIETER

(Bitcoin als Zahlungsmittel bei allen möglich)

Mullvad VPN	www.mullvad.net/de
Express VPN	www.expressvpn.com/de
Proton VPN	www.protonvpn.com/de

PASSWORTMANAGER

Als nächstes auf unserer Liste: ein Passwortmanager. Jeder von Ihnen kennt es sicherlich. Man hat hunderte Accounts und wohl keiner kann sich zu jedem dieser Accounts jedes Passwort merken. Wenn Sie allerdings “123” oder lediglich Ihr Geburtsdatum als Passwort haben, dann würde ich spätestens jetzt das Passwort ändern. Das ist ein gefundenes Fressen für Hacker.

Hier kann der richtige Passwortmanager Abhilfe schaffen, denn man muss sich nur ein einziges Passwort merken und hat damit schon den Zugriff auf alle Passwörter, die man dort hinterlegt. Passwortmanager haben aber noch deutlich mehr Funktionen:

Man kann sie gemeinsam innerhalb einer Familie oder Firma nutzen. Man kann verschlüsselte Dateispeicher für hochsensible Passwörter erstellen. Man hat eine Zwei-Faktor-Authentifizierung, die zusätzlichen Schutz bietet.

Tipp: Die Zwei-Faktor-Authentifizierung (2FA) ist eine Methode, bei der man sich zusätzlich über ein zweites Geräts einloggen kann, zum Beispiel beim Online-Banking. Somit wird es Betrügern erschwert, sich in Accounts zu hacken, denn dafür brauchen sie Zugang zum zweiten Gerät. Wichtig hierbei: Die 2FA per Telefonnummer (SMS) ist relativ unsicher, denn Handynummern können leicht „gestohlen“ werden. Betrüger haben schon häufig einen sogenannten „Sim-Swap“ durchgeführt, bei dem sie Zugriff auf das Handy kriegen**.** Daher am besten eine Authenticator-App verwenden.

KEEPER®

Unsere Empfehlung: Keeper

Meine Empfehlung an dieser Stelle ist der Passwortmanager Keeper. Die Bedienung ist wirklich kinderleicht und intuitiv.

Hier geht’s zum Anbieter:
https://www.keepersecurity.com

SUCHMASCHINE

In Sachen Sicherheit sollte man auch auf keinen Fall die Suchmaschine vergessen. Denn vor allem Suchmaschinen wie Google sammeln unzählige Daten über Sie und verkaufen diese dann an Unternehmen weiter.

Und ich weiß, **Google** zu nutzen ist unglaublich einfach und vor allem sehr bequem. Aber wer es ernst meint mit der Privatsphäre und sich unabhängiger von Big Tech machen möchte, der sollte unbedingt mal auf Alternativen zurückgreifen. Zum Beispiel **DuckDuckGo**. Auch den Browser **Brave** möchte ich Ihnen unbedingt ans Herz legen. Dieser hat Funktionen wie Werbeblocker, er ist mit vielen Geräten kompatibel und kostenlos.

SOZIALE NETZWERKE

Kommen wir zum nächsten Punkt. Fast jeder von uns ist heute in sozialen Netzwerken wie Facebook, Instagram und Co. unterwegs. Auch hier gibt es Stellschrauben, an denen man drehen kann, um seine Privatsphäre zu verbessern.

Zum Beispiel könnte man einen Alias verwenden statt den richtigen Namen. Seit einiger Zeit gibt es zudem eine interessante Alternative zu zentralisierten Anbietern wie **Twitter**.

Nostr, die Abkürzung steht für Notes and Other Stuff Transmitted by Relays, ist gerade hoch im Kurs bei allen, die genug von Zensur und Unterdrückung der Meinungsfreiheit haben. Dazu zählt im Übrigen auch Edward Snowden, der sich ebenfalls erst kürzlich als Fan von Nostr geoutet hat.

Das Prinzip ist ähnlich wie bei Bitcoin, denn auch hier versucht man mittels eines Protokolls die Probleme und Nachteile von Zentralisierung und somit von Machtkonzentration und Machtmissbrauch zu umgehen. Um Nostr nutzen zu können, muss man einen Client verwenden. Der beliebteste ist aktuell **Damus**. Dieser ist erhältlich im App Store.

Der große Unterschied zu anderen sozialen Netzwerken ist, dass es bei Nostr keine Accounts im klassischen Sinne gibt, sondern alle Teilnehmer erhalten einen öffentlichen und privaten Schlüssel.
Also genau wie bei Bitcoin.

Dann gibt es da noch die sogenannten Relays. Das sind im Grunde genommen Server, die jeder Teilnehmer betreiben kann. Wenn man nun etwas postet, dann schickt man die Nachricht einfach an mehrere Relays.

Fakt ist: Social Media Konzerne sammeln einen Haufen Daten über Sie. Die TikTok-App zum Beispiel ist eine gewaltige Daten-Sammelmaschine. Und wem gehört TikTok? Den Chinesen. Also überlegen Sie sich gut, ob Sie oder Ihre Kinder sich einen Account zulegen. Denn für die chinesische Regierung ist das eine wertvolle Datenquelle.

04
SICHER KOMMUNIZIEREN

Und damit sind wir schon beim nächsten Punkt, nämlich dem sicheren Kommunizieren im Internet.

MESSENGERDIENSTE

Sie nutzen mittlerweile mit großer Wahrscheinlichkeit einen Messenger-Dienst auf Ihrem Smartphone. Bei den meisten wird das sicherlich WhatsApp sein, oder?

WhatsApp gehört allerdings zum Big-Tech-Konzern Meta. Whatsapp, Instagram und Facebook sind also alle Unternehmen unter einem Dach und gehören Mark Zuckerberg. Ein Schelm, wer dabei Böses denkt.

Als Alternative kann ich Ihnen auf jeden Fall verschlüsselte Messenger ans Herz legen. Hier kann ich wärmstens den **Signal-Messenger** empfehlen. Auch gut sind **Telegram, Wire und Threema.**

Anregung:
Haben Sie schonmal daran gedacht, WhatsApp ganz zu löschen? Klar, der soziale Druck ist mit Sicherheit am Anfang sehr groß. Schließlich arbeitet hier der Netzwerk-Effekt gegen Sie. Machen wir an dieser Stelle ein kleines Gedankenexperiment. Wenn alle so denken würden wie Sie, dann wird Whatsapp mit hoher Wahrscheinlichkeit seine Vormachtstellung weiterhin behalten. Hier kann ich Sie nur ermutigen: Wenn Sie genug von der Allmacht von Big Tech haben, dann wagen Sie den Schritt weg von Whatsapp. Ein paar Ihrer Freunde und Bekannten werden es Ihnen gleichtun und wer weiß, vielleicht gerät so ein Stein ins Rollen.

MAIL-PROVIDER

Emails sind mittlerweile nicht mehr aus unserem Alltag wegzudenken. Wussten Sie zum Beispiel, dass der durchschnittliche Mensch rund fünf Stunden am Tag mit dem Abrufen seiner privaten und geschäftlichen E-Mails verbringt? Gerade geschäftliche E-Mails enthalten dabei oft hochsensible Informationen, die Sie eigentlich nicht in den Händen Dritter sehen wollten. Emails sind darüber hinaus nach wie vor der einfachste und sicherste Weg für Hacker, auf die Daten eines Unternehmens zuzugreifen. Fälle, in denen eine Mitarbeiterin oder ein Mitarbeiter versehentlich auf den Anhang in einer Mail klicken, ist mittlerweile zur Normalität geworden.

Was macht einen E-Mail-Anbieter sicher?

Zunächst einmal sollte dieser eine Ende-zu-Ende-Verschlüsselung haben. Ende-zu-Ende-Verschlüsselung bedeutet, dass die E-Mail auf ihrem gesamten Weg vom Absender zum Empfänger verschlüsselt wird. Das Problem bei Anbietern wie beispielsweise Gmail (also Google) ist, dass dieser die Nachrichten nur auf Netzwerkebene verschlüsselt. Sobald diese jedoch den Server von Google erreichen, können diese theoretisch von Google gelesen werden.

Bei der Wahl eines sicheren E-Mail-Providers sollten Sie zudem auf den Standort des Servers achten. Spätestens seit der NSA-Affäre, die von Edward Snowden aufgedeckt wurde, wissen wir zudem, dass insbesondere E-Mail-Provider extrem anfällig sind. Bei der Wahl des E-Mail-Providers sollte man also vor allem auf die Standortwahl von dessen Servern achten. Länder wie Schweiz oder Schweden haben dabei besonders hohe Datenschutzrichtlinien.

Darüber hinaus sollte Ihr Provider unbedingt eine Zwei-Faktor-Authentifizierung anbieten. Dadurch wird eine zusätzliche Sicherheitsstufe eingebaut. Der alleinige Besitz Ihres Passworts reicht also nicht aus, um auf Ihr E-Mail-Postfach zugreifen zu können. Ein weiterer Pluspunkt ist definitiv eine Open-Source-Politik, das heißt der Software-Quellcode ist für jeden einsehbar, wie bereits auf S.6 erklärt.

Machen wir zum Schluss noch einen Schwenk weg von der digitalen in die physische Welt. Wenn Sie nicht wollen, dass man so leicht an Ihre Hausadresse herankommt, dann empfehle ich Ihnen definitiv ein Postfach zu benutzen. So erhalten Sie mehr Diskretion bei der Briefzustellung. Ein Postfach ist auch preislich wirklich kein Ding. Aktuell bekommt man es für gerade einmal 22,90 Euro pro Jahr bei der Deutschen Post.

ProtonMail

Unsere Empfehlung: ProtonMail

ProtonMail ist unserer Einschätzung nach einer der besten Mail-Provider am Markt. Die Server des Unternehmens befinden sich in der Schweiz und man verfolgt zudem einen Open-Source-Ansatz.
Ein weiterer Pluspunkt ist eine sogenannte Zero-Access-Verschlüsselung, mit der ProtonMail Ihre Daten verschlüsselt. Das bedeutet, dass ProtonMail Ihr Passwort nicht kennt und somit auch nicht Ihre E-Mail entschlüsseln kann.

Hier geht's zum Anbieter:
https://proton.me/

ZWISCHENFAZIT

Machen wir ein kleines Zwischenfazit bis hierhin. Sie haben nun einige Tipps bekommen, wie Sie sicher im Internet surfen können. Darüber hinaus wissen Sie nun, welche Möglichkeiten es gibt, sicher im Internet zu kommunizieren.

Jetzt fehlt nur noch das sichere und anonyme Bezahlen und Geld überweisen. Sie wissen ja, das Thema Geld spielt eine große Rolle bezüglich Freiheit, denn Regierungen wollen sogenannte CBDCs einführen, also digitales Zentralbankgeld. Damit wird es für Regierungen noch einfacher sein, Bürger auszuspähen, weil sie jetzt jede Geld-transaktion nachverfolgen können und wissen, was Sie wann gekauft haben.

05
SICHER BEZAHLEN

BARGELD NUTZEN!

Mein Tipp hier: Bargeld nutzen! Dazu habe ich auch einen Beitrag für Focus Online verfasst, den Sie auch auf meinem Blog unter www.friedrich-partner.de finden.

Wer mir schon länger folgt, der kennt meine Meinung zum Thema Bargeld. Das Bargeld ist zwar immer noch Fiat-Geld und das wird früher oder später wertlos werden, aber es ist momentan wenigstens noch die anonymste Form des Bezahlens. Seit Jahren sehen wir jedoch bereits Anstrengungen seitens der Politik und der Wirtschaft, uns das Bargeld immer weiter madig zu machen.

Hierzu kann ich Ihnen auf jeden Fall mein Video zum Bargeldverbot ans Herz legen, in dem ich im Detail erkläre, wieso wir aktuell einen derart rigorosen Kampf gegen das Bargeld sehen und warum ich glaube, dass wir bald schon die Einführung sogenannter CBDCs live miterleben werden. Das Tückische ist hierbei, dass sich für viele in unserem Alltag erstmal nicht viel ändern wird. Wir haben es hierbei schließlich mit einem schleichenden Prozess zu tun.

BITCOIN

Viele von Ihnen wissen, dass ich ein großer Bitcoin-Befürworter bin, und zwar nicht nur, weil ich glaube, dass es die größte Revolution aller Zeiten ist, sondern auch, weil es uns erstmals in der Geschichte der Menschheit die Möglichkeit gibt, Staat und Geld zu trennen.

Grundsätzlich ist auch wichtig: Halten Sie Ihre privaten Schlüssel selber und lassen Sie die Bitcoins nicht auf einer Plattform oder Börse rumliegen. Die jüngsten Ereignisse rund um die Kryptobörse FTX haben eindrucksvoll gezeigt, warum es so wichtig ist, seine Coins niemals einer Drittpartei anzuvertrauen. Wir empfehlen Hardwarewallets und stellen Ihnen im Folgenden zwei Anbieter vor.

→ ***Wichtig: Bitcoin ist nach wie vor eine sehr junge Technologie und gilt daher als Investmentanlage mit extrem hohem Risiko. Bitte investieren Sie nur Geld, was Sie sich leisten können zu verlieren. Es ist auch nicht empfehlenswert Bitcoin auf Kredit oder Schulden zu kaufen.***

Unsere Wallet-Empfehlung: Bitbox*

Das Bitbox Hardware-Wallet BitBox02 ist ein verlässliches Wallet, das in der Schweiz hergestellt wird. Der Fokus von BitBox liegt auf maximaler Sicherheit, so wurde bspw. ein Dual-Chip-System verwendet, um sog. Brut Force Attacken unmöglich zu machen. Backups lassen sich im Handumdrehen auf eine SD-Karte übertragen.

Link zum Shop:
https://shiftcrypto.ch/bitbox02/?ref=W7OpdOrYMT

Weitere Wallet-Empfehlung: Trezor Model One*

Link zum Trezor-Shop:
https://trezor.go2cloud.org/SH8W

Wer gerne Bitcoin ausgibt statt zu hodeln, der sollte definitiv das **Lightning Netzwerk** nutzen. Mittlerweile gibt es dutzende Lightning-Wallets, die man alle einfach mal ausprobieren sollte und dann die beste für sich aussucht. Hier empfehle ich z. B. die **Wallet of Satoshi** oder **Muun Wallet**. Lightning ist ein Bitcoin-Protokoll, das schnelle und sichere Zahlungen ermöglicht. Ist wesentlich schneller und günstiger, als wenn Ihr eine normale Bitcoin Transaktion auf der Blockchain macht. In Echtzeit!

Das Ganze hat jedoch einen Hacken. Deutschland ist nicht El Salvador, wo der Bitcoin bereits zum legalen Zahlungsmittel erklärt wurde. Bis auf wenige Onlinehändler und ein paar Kneipen akzeptiert kaum ein Händler in Deutschland Bitcoin.

Tatsächlich gibt es jedoch Wege, wie Sie in Ihrem Alltag viele Dinge mit Bitcoin zahlen können, z. B. den Einkauf bei **REWE**. Dafür ist nur ein kleiner Umweg nötig. Es gibt Plattformen, wo man mit Bitcoin Guthabenkarten für verschiedene Geschäfte und Dienstleistungen kaufen kann, die man dann im Anschluss einfach an der Kasse als Zahlungsmittel benutzt.

Bitrefill

Unsere Empfehlung: Bitrefill

Ein Anbieter, den ich hierbei empfehlen kann, ist “Bitrefill”. Bitrefill bietet seine Dienstleistungen auch in Deutschland an. Das Angebot umfasst fasst sämtliche großen Händler wie Amazon, Zalando oder REWE. Selbst Prepaid-Telefonkarten lassen sich über Bitrefell erwerben.

Hier geht’s zum Anbieter:
https://www.bitrefill.com/

Man muss dazu aber auch sagen, dass die Bitcoin Blockchain ein öffentliches Kassenbuch ist, wo man Adressen theoretisch verfolgen kann. Und auch mit ein paar Tricks diesen eindeutige Identitäten zuweisen kann. Das ist jetzt vor allem für **Fortgeschrittene**! Eine der besten Möglichkeiten ist ein sogenannter **Coinjoin**. Ganz simpel ausgedrückt ist ein Coinjoin ein simples Tool, bei dem mehrere Teilnehmer eine gemeinsame Transaktion erstellen, die Bitcoin von allen Teilnehmer enthält und sie an neue Adressen dieser Teilnehmer auszahlt. Dadurch lässt sich am Ende nicht mehr genau sagen, welche Adresse zu welchem Teilnehmer gehört.

WASABI WALLET

Unsere Empfehlung: Wasabi

Wasabi Wallet ist kostenlos und open source, das heißt, jeder kann theoretisch den Software Code einsehen und überprüfen. Streng nach dem Grundsatz der Bitcoin-Community „Not Your Keys, not Your Coins“ ist Wasabi Non-Custodial, das heißt, nur Sie allein sind für Ihre Coins verantwortlich. Was uns besonders gut an Wasabi Wallet gefällt, ist die einfache Benutzung. Wasabi ist ein benutzer-freundliches Bitcoin-Wallet, das die Privatsphäre seiner Benutzer automatisch unter der Haube verwaltet, ein-schließlich Netzwerkverbindungen, Auswahl der Eingänge und Coin-Join.

Hier geht’s zum Anbieter:
https://wasabiwallet.io/

06
FAZIT

Wir hoffen, wir konnten Ihnen zeigen, dass es mittlerweile eine ganze Bandbreite an Werkzeugen gibt, mit denen man sich und seine Privatsphäre schützen kann. Die in diesem Handbuch vorgestellten Tools sind dabei nur ein kleiner Ausschnitt dessen, was man tun kann. Privatsphäre ist extrem wichtig und wird aller Voraussicht nach auch immer wichtiger werden. Sich nicht damit zu befassen bzw. darauf zu vertrauen, dass man ja sowieso nichts zu verbergen hat, ist definitiv keine Alternative.

Das Internet vergisst nie. Sie sollten sich immer bewusst sein, was man an Daten preisgibt. Aber auch keine Angst haben, die Möglichkeiten sind da und diese werden immer besser.

Und ganz wichtig, denken Sie immer daran: Das Ganze ist ein Marathon und kein Sprint. Nicht alles auf einmal lösen wollen, sondern in kleinen Schritten vortasten. Es ist noch kein Meister vom Himmel gefallen.

HAFTUNG:

Jede Person ist für seine Geldanlage selbst verantwortlich.
Wir über-nehmen keinerlei Haftung für Schäden, die durch falsche Schlussfolgerungen aus den Hinweisen in diesem Schreiben entstanden sind. Wir schließen Haftungsansprüche jeglicher Natur aus.

Alle Informationen beruhen auf Quellen, die wir für glaubwürdig halten. Trotz sorgfältiger Bearbeitung können wir für die Richtigkeit der An-gaben keine Gewähr übernehmen. Alle enthaltenen Meinungen und Informationen dienen ausschließlich der Information und begründen kein Haftungsobligo. Regressinanspruchnahme, sowohl direkt, wie auch indirekt, und Gewährleistung wird daher ausgeschlossen. Alle enthaltenen Meinungen und Informationen sollen nicht als Aufforderung verstanden werden, ein Geschäft oder eine Transaktion ein-zugehen. Auch stellen die vorgestellten Strategien keinesfalls einen Aufruf zur Nachbildung, auch nicht stillschweigend, dar.

Vor jedem Geschäft bzw. vor jeder Transaktion sollte geprüft werden, ob sie im Hinblick auf die persönlichen und wirtschaftlichen Verhältnisse geeignet ist. Wir weisen ausdrücklich noch einmal darauf hin, dass der Kauf und Handel von Bitcoin mit grundsätzlichen Risiken verbunden ist und der Totalverlust des eingesetzten Kapitals nicht ausgeschlossen werden kann.

Die im Privacy Handbuch vorgestellten Meinungen, Strategien und Informationen dürfen keinesfalls als allgemeine oder persönliche Beratung aufgefasst werden, da die Inhalte des Privacy Handbuchs lediglich die subjektive Meinung der Redaktion widerspiegeln.
Das Privacy Handbuch veröffentlicht gelegentlich Verknüpfungen (Hyperlinks) im Rahmen von Werbeanzeigen, Quellenangaben u. ä.

Dabei gilt, dass der Herausgeber des Privacy Handbuchs, sowie der Betreiber des Internetauftritts der Friedrich Vermögenssicherung GmbH ausdrücklich erklären, keinerlei Einfluss auf die Gestaltung oder Inhalte der verlinkten Seiten zu haben. Der Herausgeber des Bitcoin Handbuchs und der Betreiber des Internet-Auftritts der Friedrich Vermögenssicherung GmbH distanzieren sich daher ausdrücklich von Inhalten verlinkter Seiten. Dies gilt für alle vorhandenen Hyperlinks, sowohl sichtbar wie verborgen, und für alle Inhalte von Seiten, zu denen diese Hyperlinks führen.