

Plausible Abstreitbarkeit

Ein Artikel von mir im [Journalistenblatt](#) 2/2026.



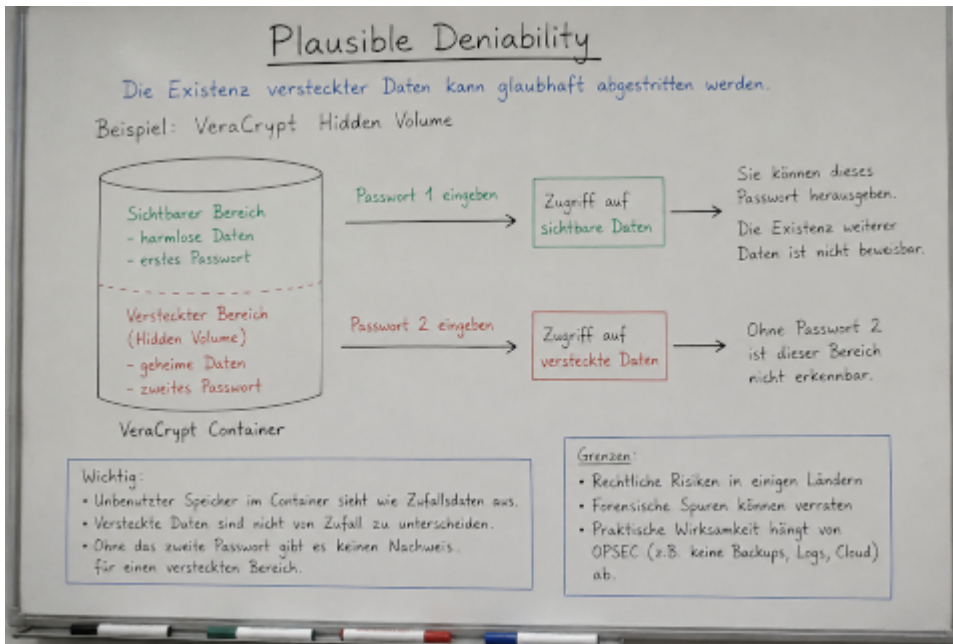
Reisen wir nach Hongkong, China, Neuseeland oder Russland? Es macht keinen Unterschied, was die Neugier der jeweiligen Sicherheitskräfte angeht. Man muss alle elektronischen Geräte bei der Einreise entsperren und alle Passwörter herausrücken. (vgl. Übersicht unten, Stand April 2026). Das gilt nicht nur für Leute, die Ilhan Omar heißen oder einen Islamistenbart tragen.

Das [Konsulat der USA in Hongkong warnt](#) zum Beispiel: Am 23. März 2026 änderte die Regierung von Hongkong die Durchführungsbestimmungen zum National Security Law. Es ist nun strafbar, sich zu weigern, der Hongkonger Polizei Passwörter mitzuteilen oder Entschlüsselungshilfe zu leisten, um Zugriff auf sämtliche persönlichen elektronischen Geräte zu ermöglichen, einschließlich Mobiltelefonen und Laptops. Die Geräte können auch beschlagnahmt werden, sind die Grenzbeamten misstrauisch geworden.

Geschäftsleute und Journalisten, die Daten und Dokumente ungern in falsche Hände sehen wollen, können das Risiko minimieren, indem sie auf einer Auslandsreise ein „leeres“ Laptop mitnehmen und ein Zweithandy benutzen, auf dem nichts

Privates zu finden ist, und dann vor Ort alles neu installieren und von der eigenen Cloud herunterladen. Das ist aber unpraktisch und umständlich.

Kategorie	Staat	Rechtslage	Konsequenz bei Verweigerung	Besonderheiten
Strafbarer Passwort-Zwang	Hongkong	Passwortherausgabe gesetzlich erzwingbar	Geldstrafe oder Haft möglich	Gilt auch bei Transit
Strafbarer Passwort-Zwang	China	Weitreichende Sicherheitsgesetze	Strafverfolgung möglich	Besonders streng bei politischen Inhalten
Strafbarer Passwort-Zwang	Vereinigtes Königreich	Anti-Terror-Gesetze erlauben Passwortforderung	Strafbar bei Verweigerung	Auch ohne konkreten Verdacht möglich
Strafbarer Passwort-Zwang	Neuseeland	Zoll darf Entsperrung verlangen	Geldstrafe bei Weigerung	Gilt speziell bei Einreise
Faktischer Zwang	Vereinigte Staaten	Geräte dürfen durchsucht werden	Einreise kann verweigert werden	Besonders bei Nicht-Staatsbürgern
Faktischer Zwang	Kanada	Grenzbehörden dürfen Geräte prüfen	Probleme/Verzögerung möglich	Rechtslage im Wandel
Faktischer Zwang	Australien	Durchsuchung ohne richterlichen Beschluss	Verweigerung führt zu Problemen	Weitreichende Zollbefugnisse
Faktischer Zwang	Russland	Sicherheitsbehörden mit umfassenden Befugnissen	Einreiseprobleme möglich	Praxis teils streng umgesetzt



Mit dem Zwang, alle Passwörter herauszugeben, verhält es sich wie mit Zensur jedweder Art: Das trifft nur die Dummen und Faulen, nie die Richtigen. Man kann das alles umgehen, und muss noch nicht einmal IT- oder Kryptografie-Experte sein.

Die Aufgabe ist also nicht nur, Inhalte zu verbergen, sondern auch, das Verbergen zu verbergen.

Das Problem: Es dürfte bekannt sein, dass alles, was man schützen will, in verschlüsselte Veracrypt-Container gehört. Dafür gibt es zahllose und sogar leicht verständliche Tutorials. Aber: Weil es jeder weiß, wird ein Grenzbeamter, der sich auskennt, beim Entsperren eines Laptops diese Container entdecken und dann auffordern, ihm den Inhalt zu zeigen. Die Aufgabe ist also nicht nur, Inhalte zu verbergen, sondern auch, das Verbergen zu verbergen.

Das ist gar nicht so kompliziert, wie es sich anhört. Das Prinzip nennt man „Plausible Deniability“ (plausible Abstreitbarkeit). Wenn man mit Veracrypt einen „hidden container“ anlegt, hat man einen sichtbaren Container (der wie eine Dateiordner aussieht), indem sich ein weiterer Ordner (Container) verbirgt, der aber unsichtbar ist und auch ein anderes Passwort hat. Wenn man gezwungen wird, das Passwort herauszugeben, gibt man das des äußeren Containers an, der

legitime, unkritische Daten enthält – der versteckte Dateiordner bleibt unsichtbar. Das funktioniert mit allem Betriebssystemen und auch externen Speichern wie USB-Sticks.

Das Problem sind natürlich die E-Mail-Programme auf Smartphones und Rechnern. Man könnte sogar gezwungen werden, verschlüsselte E-Mails zu öffnen. Noch schlimmer ist, dass alle Kontakte offen gelegt wären.

Auch dafür gibt es eine Lösung – hier eine Übersicht:

System	Anleitung
Windows	<ol style="list-style-type: none">1. VeraCrypt installieren.2. Einen verschlüsselten Container erstellen.3. Den Container als Laufwerk einbinden, zum Beispiel V:.4. Das Mailprofil oder die portable Version des Mailprogramms in den Container verschieben.5. Das Mailprogramm nur starten, wenn der Container eingebunden ist.6. Nach der Nutzung das Mailprogramm schließen und den Container aushängen.
Ubuntu / Linux	<ol style="list-style-type: none">1. VeraCrypt installieren.2. Einen Container anlegen und mounten, zum Beispiel nach /media/veracrypt1.3. Das Thunderbird-Profil in diesen Container verschieben.4. Thunderbird mit dem Profil im Container starten, z. B. mit: thunderbird -profile /media/veracrypt1/thunderbird-profile5. Nach dem Arbeiten Thunderbird beenden und den Container wieder aushängen.

System	Anleitung
macOS	<ol style="list-style-type: none"> 1. VeraCrypt installieren oder alternativ ein verschlüsseltes DMG-Image mit dem Festplattendienstprogramm anlegen. 2. Den Container oder das verschlüsselte Image öffnen. 3. Das Mailprofil in den verschlüsselten Bereich verschieben. 4. Das Mailprogramm nur von dort bzw. mit diesem Profil starten. 5. Nach der Nutzung das Mailprogramm beenden und das Image bzw. den Container schließen.
Hinweis	<p>Der Schutz wirkt nur, solange der Container geschlossen ist. Wenn der Container geöffnet und das Mailprogramm aktiv ist, können die Inhalte natürlich gelesen werden. Für mehr Sicherheit sollten außerdem temporäre Dateien, Suchindizes, Ruhezustand und unverschlüsselte Backups beachtet werden.</p>

Bereich	Anleitung
Ziel	<p>Die lokal gespeicherten E-Mails sollen nicht offen auf dem Smartphone liegen, sondern möglichst in einem verschlüsselten Bereich gespeichert werden.</p>

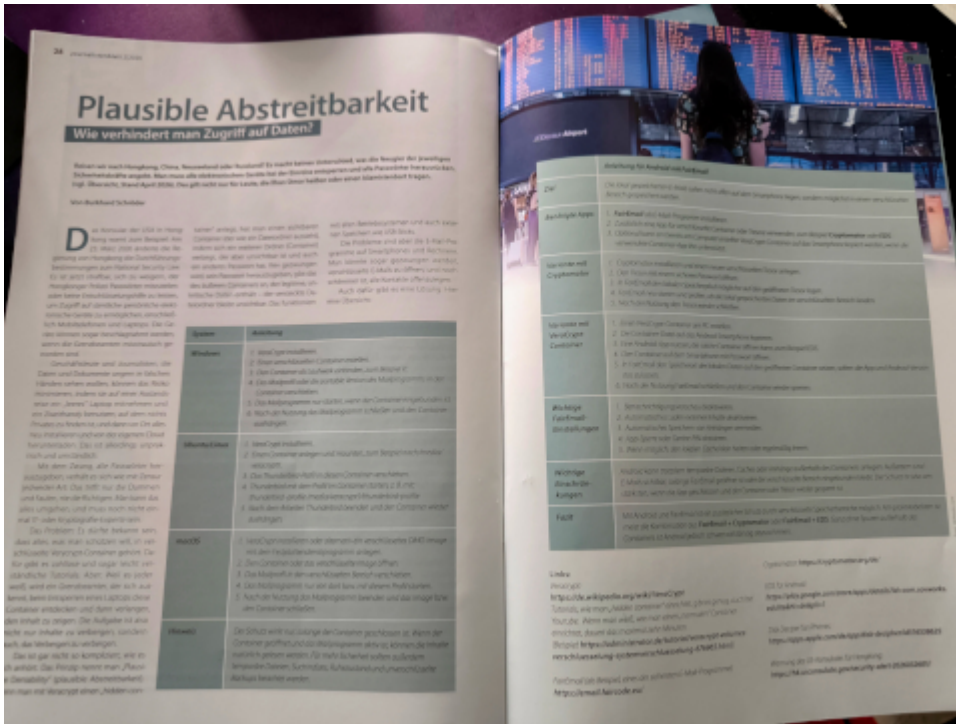
Bereich	Anleitung
Benötigte Apps	<ol style="list-style-type: none">1. FairEmail als E-Mail-Programm installieren.2. Zusätzlich eine App für verschlüsselte Container oder Tresore verwenden, zum Beispiel Cryptomator oder EDS.3. Optional kann ein bereits am Computer erstellter VeraCrypt-Container auf das Smartphone kopiert werden, wenn die verwendete Container-App ihn unterstützt.
Variante mit Cryptomator	<ol style="list-style-type: none">1. Cryptomator installieren und einen neuen verschlüsselten Tresor anlegen.2. Den Tresor mit einem sicheren Passwort öffnen.3. In FairEmail den lokalen Speicherpfad möglichst auf den geöffneten Tresor legen.4. FairEmail neu starten und prüfen, ob die lokal gespeicherten Daten im verschlüsselten Bereich landen.5. Nach der Nutzung den Tresor wieder schließen.

Bereich	Anleitung
Variante mit VeraCrypt-Container	<ol style="list-style-type: none">1. Einen VeraCrypt-Container am PC erstellen.2. Die Container-Datei auf das Android-Smartphone kopieren.3. Eine Android-App nutzen, die solche Container öffnen kann, zum Beispiel EDS.4. Den Container auf dem Smartphone mit Passwort öffnen.5. In FairEmail den Speicherort der lokalen Daten auf den geöffneten Container setzen, sofern die App und Android-Version das zulassen.6. Nach der Nutzung FairEmail schließen und den Container wieder sperren.
Wichtige FairEmail-Einstellungen	<ol style="list-style-type: none">1. Benachrichtigungsvorschau deaktivieren.2. Automatisches Laden externer Inhalte deaktivieren.3. Automatisches Speichern von Anhängen vermeiden.4. App-Sperre oder Geräte-PIN aktivieren.5. Wenn möglich, den lokalen Cache klein halten oder regelmäßig leeren.

Bereich	Anleitung
Wichtige Einschränkungen	<p>Android kann trotzdem temporäre Dateien, Caches oder Anhänge außerhalb des Containers anlegen. Außerdem sind E-Mails sichtbar, solange FairEmail geöffnet ist oder der verschlüsselte Bereich eingebunden bleibt. Der Schutz ist also am stärksten, wenn die App geschlossen und der Container oder Tresor wieder gesperrt ist.</p>
Fazit	<p>Mit Android und FairEmail ist ein zusätzlicher Schutz durch verschlüsselte Speicherbereiche möglich. Am praktikabelsten ist meist die Kombination aus FairEmail + Cryptomator oder FairEmail + EDS. Ganz ohne Spuren außerhalb des Containers ist Android jedoch schwer vollständig abzuschirmen.</p>

Wer nichts zu verbergen und eine Webcam im Schlafzimmer installiert hat, muss nichts tun.

Gute Reise!



Links:

- [Veracrypt](#)
- Tutorials, wie man *hidden container* einrichtet, gibt es genug, auch bei Youtube. Wenn man weiß, wie man einen „normalen“ Container einrichtet, dauert das maximal zehn Minuten. Beispiel: [Vollständiges Veracrypt Tutorial: Volumes – Hidden Volumes – Systemverschlüsselung](#).
- [FairEMail](#) – als Beispiel, eines der sichersten E-Mail-Programme)
- [Cryptomator](#)
- [EDS für Android](#)
- [Disk Deciper für iPhones](#)