

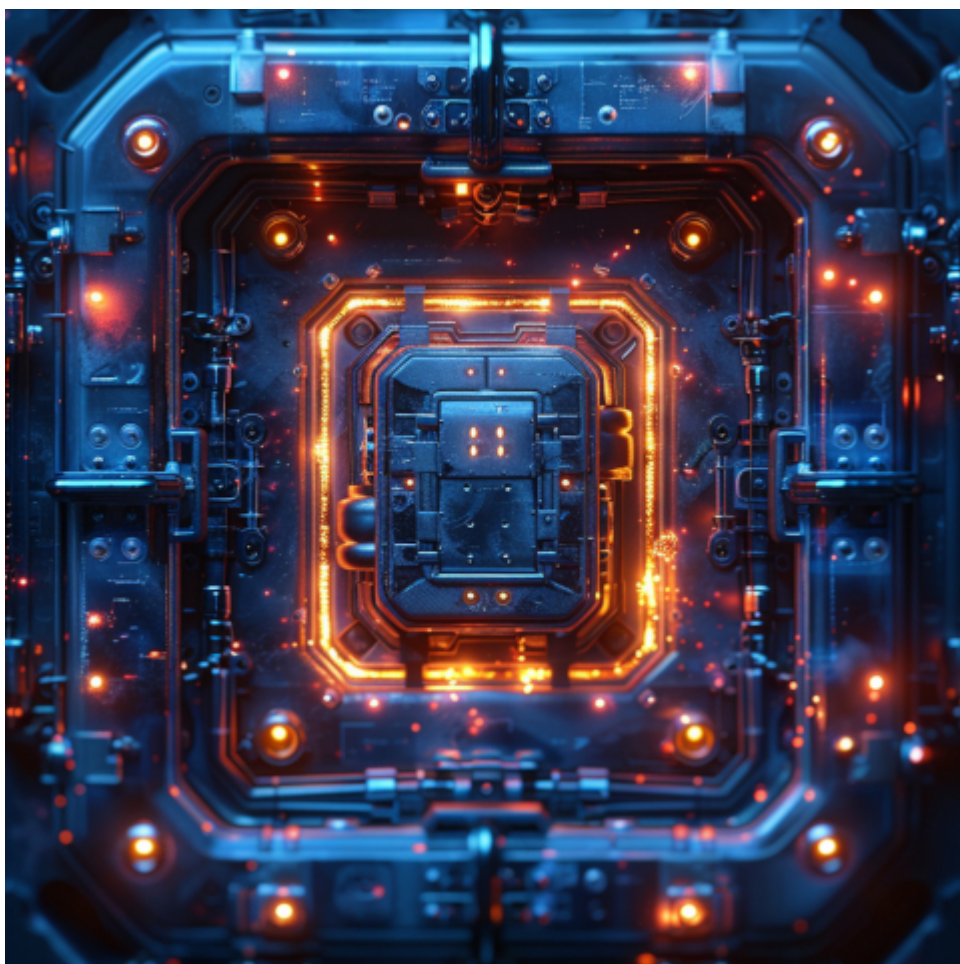
In versteckten Containern



Das [Konsulat der USA](#) in Hongkong warnt: „On March 23, 2026, the Hong Kong government changed the implementing rules relating to the National Security Law. It is now a criminal offense to refuse to give the Hong Kong police the passwords or decryption assistance to access all personal electronic devices including cellphones and laptops. This legal change applies to everyone, including U.S. citizens, in Hong Kong, arriving or just transiting Hong Kong International Airport. In addition, the Hong Kong government also has more authority to take and keep any personal devices, as evidence, that they claim are linked to national security offenses.“

([Wir hatten das](#) schon 2017.) Auf einem Laptop kann man das Geschnüffel „von außen“ natürlich einigermaßen vermeiden. Man richtet einfach ein [Hidden Volume](#) mit Veracrypt ein, und hat alle Daten, die niemanden etwas angehen, geschützt.

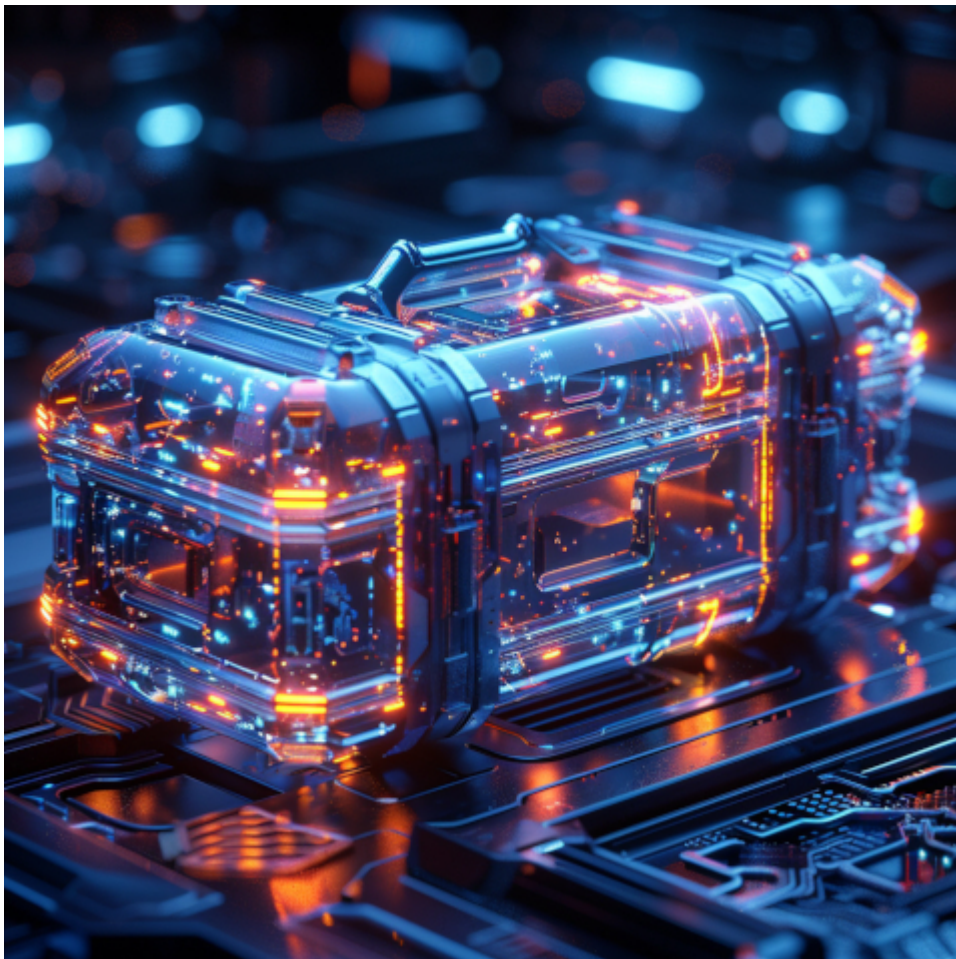
Das Problem sind natürlich die E-Mail-Programme auf Smartphones und Rechnern. Man könnte sogar gezwungen werden, verschlüsselte E-Mails zu öffnen, und noch schlimmer ist, dass alle Kontakte offengelegt wären. Da haben wir aber noch etwas in petto, wie man so sagt...



Wie macht man das?

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.
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.
Wichtiger 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>



Und zum Beispiel für ein Android-Smartphone?

Bereich	Anleitung für Android mit FairEmail
Ziel	Die lokal gespeicherten E-Mails sollen nicht offen auf dem Smartphone liegen, sondern möglichst in einem verschlüsselten Bereich gespeichert werden.
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.
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.

<p>Wichtige FairEmail-Einstellungen</p>	<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.
<p>Wichtige Einschränkungen</p>	<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>
<p>Fazit</p>	<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>

Bonus: Nur eine [portable Version](#) auf einem USB-Stick mitnehmen. Die Gefahr besteht natürlich, dass übereifrige Zoll- oder Grenzbeamte den beschlagnahmen... Wer auf Nummer Sicher gehen will, nutzt während eines Auslandsaufenthalts in den Ländern, in denen das Obige verlangt wird, nur Webmail per VPN.