

Aufbewahrung von Daten und Verschlüsselung

Hier erfährst du:

- Konkrete Anleitungen und Hilfestellungen zum verschlüsseln deines Computers, deiner externen Festplatten und USB-Sticks.
- Du erfährst wie du Daten für immer löschen kannst.
- Wie du ein sicheres Passwort auswählst
- Wie du deine Datensicherung gestalten kannst.

Du findest Argumente für einen gründlichen und sicheren Umgang mit deinen Geräten und Daten. Wir setzen uns damit auseinander, warum ein unverschlüsseltes Gerät eine Gefahr darstellt, welche Sicherheit eine Verschlüsselung bietet und auch warum gelöschte Informationen trotzdem nicht weg sind.

Wie Verschlüsselung prinzipiell funktioniert, welche verschiedenen Verschlüsselungsarten es gibt und wie sie sich historisch entwickelt hat, findest du in unserem [Grundlagentext zu Verschlüsselungstechnologie](#).

Anleitungen und konkrete Tipps

[Computer verschlüsseln](#)

[Verschlüsselung externer Speicher und Ordner](#)

[Sicheres Backup deiner Daten](#)

[Passwortsicherheit](#)

[Handy verschlüsseln](#)

[Daten löschen](#)

Warum Computer verschlüsseln echt wichtig ist und was du dabei beachten musst

Mit der Aussage mensch habe einen verschlüsselten Computer ist meist gemeint, dass der Speicher auf dem das Betriebssystem eines Rechners liegt, verschlüsselt ist. Bei einer Standardinstallation werden bei den meisten Betriebssystemen die Daten unverschlüsselt auf die Festplatte geschrieben. Das User:innen-Passwort, das du auf deinem Computer eingibst, ist oft nicht viel mehr als eine Sperre des Bildschirms und soll nur verhindern, dass wer anderer schnell auf deine Daten zugreifen kann. Dieses User:innenpasswort ist aber kein wirkliches Hindernis, um fähige Leute davon abzuhalten zu deinen Daten zu kommen.

Empfehlung

Verschlüssele den Speicher, auf dem dein Betriebssystem installiert ist und den dein Betriebssystem nutzt!

Wir sagen „Computer verschlüsseln“, weil das oft so genannt wird. Korrekt wäre, dass wir es **Speicher verschlüsseln** nennen, weil ein Computer eine oder mehrere Festplatten hat (oder auch andere Speicherformen) und diese Festplatten sind mit verschiedenen Unterteilungen (Partitionen) versehen. Zur Veranschaulichung kannst du dir die Festplatte, als einen Schrank vorstellen und die Partitionen als unterschiedliche Schubladen in diesem Schrank. Wichtig ist, dass alle Schubladen gut geschützt sind. Mehr dazu dann in den einzelnen Anleitungen.

Wie Verschlüsselung grundsätzlich funktioniert, kannst du in unseren Überblicksartikeln nachlesen: Der Text "[Verschlüsselung](#)" gibt dir einen allgemeinen Überblick wie das Verschlüsselungsverfahren funktioniert und welche verschiedenen Verschlüsselungsarten bei Kommunikation und Speicher zum Einsatz kommen.

In aller Kürze: Wichtige Hinweise zur Verschlüsselung deines Computers

- **Deine Daten sind durch die Verschlüsselung nur geschützt, wenn der Computer ausgeschaltet ist!** Daher: Wenn du nicht Zuhause bist schalte den Computer aus. Auch über Nacht bzw. wenn du schläfst, empfehlen wir den Computer auszuschalten.
 - **Deine Verschlüsselung ist nur so gut wie dein Passwort!** Lies dir unsere Tipps zum Thema [Passwortsicherheit](#) durch.
 - Es heißt immer, dass Verschlüsselung einen Computer langsam macht. Das kann stimmen bei älteren Modellen - moderne Rechner (Prozessoren) sind immer mehr auf die Unterstützung von Verschlüsselung ausgelegt und haben keinen signifikanten Nachteil. Aber auch bei älteren Computern musst du dir die Frage zwischen Bequemlichkeit und Sicherheit stellen!
 - Mit einem verschlüsselten Computer sind nicht nur deine Daten, sondern auch die Daten in installierten Programmen geschützt: Chatverläufe, Browserhistory, etc. und du musst nicht aufpassen, wo genau du deine Dateien abspeicherst.
 - Betriebssystemverschlüsselung/Computerverschlüsselung schließt eine sehr große Sicherheitslücke! Aber es ist nicht die einzige Möglichkeit für Angreifer:innen an deine Daten zu kommen, daher sei weiterhin vorsichtig was du aus dem Internet herunterlädst, welche Anhänge in Emails du öffnest, wessen USB-Sticks ansteckst,...
 - Computer zu verschlüsseln wird immer mehr zum Standard und ist längst keine Nische mehr für „Leute die etwas zu verbergen haben“. Auch die großen Computerfirmen wie Apple und Microsoft bieten inzwischen Lösungen für Verschlüsselung des eigenen Computers an, weil die meisten Firmen und Nutzer:innen ein starkes Interesse an Datenschutz haben.
-

Warum ein unverschlüsseltes Betriebssystem unsicher ist

Bei einer Standardinstallation werden bei den meisten Betriebssystemen die Daten unverschlüsselt auf die Festplatte geschrieben. Wenn die Bullen bei euch auftauchen und euren Computer

mitnehmen, können sie zum Beispiel die Festplatte ausbauen und in einen anderen Computer einbauen und sich alle Daten ansehen, die auf dem Computer abgespeichert sind. Und das sind einerseits alle Dokumente die ihr abgespeichert habt (Flyer, Logos, Texte, Fotos ...) und andererseits auch Protokolle von Chatsitzungen, der Verlauf eures Browsers (also wann ihr welche Internetseiten angesurft habt) oder vielleicht auch alle eure Emails. Heutzutage werden bei der Arbeit im Netz so viele Daten auf eurem Computer zwischengespeichert, dass kein Mensch darüber einen Überblick haben kann. Das heißt, wir sehen uns nicht einfach nur Inhalte auf Webseiten an, sondern Teile der Daten auf Webseiten finden auch den Weg auf unsere Festplatte.

Die Verschlüsselung macht die Daten nur mit dem passenden Schlüssel lesbar. Ein User:innenpasswort heißt nicht, dass das Gerät verschlüsselt ist und stellt eine geringe Hürde beim Zugriff auf die Daten dar.

Bei Aktivist:innen, die so unvorsichtig sind und Passwörter unverschlüsselt abspeichern, kann die Beschlagnahmung von Computern natürlich noch weitreichendere Folgen haben.

Auch gelöschte Daten sind immer noch wiederherstellbar!

Wenn ich ein Protokoll zum Beispiel als PDF heruntergeladen und angesehen habe, wird es auf der Festplatte abgelegt. Sogar wenn ich es nach dem Lesen lösche, verbleibt es auf der Platte: Wenn ihr eine Datei in den, auf den meisten Systemen vorhandenen, Papierkorb schiebt, ist sie nicht gelöscht sondern nur verschoben. Wenn ihr eine Datei wirklich löscht, dann ist die Datei auch nicht verloren, sondern es wird nur in einer Tabelle auf dem Dateisystem der Ort wo sich die Daten befinden, als leer markiert. Es gibt genug Programme mit denen diese Dateien wieder hergestellt werden können. Es gibt natürlich die Möglichkeit, den Speicherbereich, wo die ursprüngliche Datei lag mit anderen Daten zu überschreiben. Jedoch wird dabei nur der Teil der Festplatte überschrieben, wo die Datei abgespeichert war- viele Programme speichern temporäre Sicherheitskopien der bearbeiteten Daten irgendwo anders ab, auch wenn wir etwa Text- oder Worddateien öffnen, wird stets eine solche temporäre Datei angelegt. Hier findest du unsere Tipps wie du [Dateien sicher löschen](#) kannst.

Warum ich mein System verschlüsseln sollte

- Weil du mit Verschlüsselung dich und auch andere schützen kannst.
- Weil du es damit Repressionsbehörden und allen anderen die an deine Daten wollen so schwer wie möglich machst. Auch wenn du denkst, dass du nichts „Problematisches“ auf deinem Computer hast: Wenn Verschlüsselung weit verbreitet ist, kann das auch die Leute schützen die vielleicht berechtigterweise „etwas zu verbergen“ haben.
- Weil auf einem verschlüsselten Computer/Betriebssystem nicht nur deine Daten, sondern auch die Daten von installierten Programmen geschützt sind: Chatverläufe, Browserhistory, Bearbeitungsgeschichten von Dokumenten,
- Weil auf deinem Computer so viele Daten abgespeichert sind, dass mensch selbst kaum mehr Überblick hat (denke etwa an die berühmten „Cookies“).
- Weil deine Privatsphäre geschützt ist: Wird dein Computer gestohlen oder geht verloren, wenn

du ihn verkaufst oder verschenkst oder er geht einfach kaputt und funktioniert nicht mehr:
Niemand kann ansehen, was du auf dem Computer gespeichert oder gemacht hast.

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

Permanent link:
<https://www.fit-fuer-aktion.wiki/digitale-sicherheit/aufbewahrung-verschluesselung-daten/index>

Last update: **2022/05/10 20:04**

