



# Verschlüsselung von Daten

Wenn vertrauliche Daten gespeichert, transportiert oder weitergegeben werden, macht es Sinn, diese Daten bzw. Datenträger zu verschlüsseln. Wenn die Verschlüsselung gut ist, können die Daten ohne den Schlüssel nicht wiederhergestellt werden.

Aktuelle Empfehlungen finden Sie unter:

<https://www.bsi-fuer-buerger.de/Passwoerter>

Download Faktenblatt „Sichere Passwörter“:

[https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSIFB/sichere\\_passwoerter\\_faktenblatt.pdf?\\_\\_blob=publicationFile&v=12](https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSIFB/sichere_passwoerter_faktenblatt.pdf?__blob=publicationFile&v=12)

## Tipps für gute Passwörter

### Was hat Ihr Passwort mit Pizza zu tun?

Denken Sie sich einen Satz aus, der mindestens eine Zahl enthält, zum Beispiel:

**„Am liebsten esse ich Pizza mit vier Zutaten und extra Käse!“**

Merken Sie sich nun den ersten Buchstaben eines jeden Wortes und Sie erhalten ein starkes und sicheres Passwort.

**AleiPm4Z+eK!**

Tipps:  
Nutzen Sie Passwort-Manager!  
Das sind Apps oder Software-Programme, die alle Ihre Passwörter und die zugehörigen Benutzernamen sicher verwahren. Sie brauchen sich dann nur ein sicheres Masterpasswort für den Passwort-Manager merken.

© Bundesamt für Sicherheit in der Informationstechnik (BSI) [www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de)

### Ein sicheres Passwort – einfach erstellen

Passwörter etwa für E-Mail-, Social Media- und Cloud-Accounts schützen sensible persönliche Daten vor unerlaubtem Zugriff. Deshalb sollten sie besonders komplex und schwierig zu erraten sein.

**Dos**

- ✓ Je länger, desto besser: Passwortlänge von mindestens acht Zeichen wählen
- ✓ Groß- und Kleinbuchstaben verwenden
- ✓ Sonderzeichen wie ?, !, %, +, \_ etc. nutzen
- ✓ Mehrere Ziffern hinzufügen

**Don'ts**

- ✗ Passwort-Kombinationen vermeiden, die Geburtstage bzw. Namen des Haustiers enthalten oder in einem Wörterbuch stehen.
- ✗ Auf gängige Wiederholungs- und Tastaturmuster wie asdf, 1234, abcd, 666 etc. verzichten.
- ✗ Nicht ein simples Passwort wählen, das nur um ein Sonderzeichen am Wortanfang oder -ende ergänzt ist, zum Beispiel: !Pizza.

Bei Reisen ins Ausland können Umlaute auf landestypischen Tastaturen eventuell nicht genutzt werden.

© Bundesamt für Sicherheit in der Informationstechnik (BSI) [www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de)

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Auf <https://howsecureismypassword.net/> können Sie testen, wie lange es dauern würde, Ihr Passwort zu knacken.

## Verschlüsselungsmöglichkeiten

### ▪ Verschlüsselung einzelner Dateien

Nahezu alle Office-Programme bieten die Option „Kennwortschutz“.

Dabei wird die jeweilige Datei mit einem Passwort geschützt und verschlüsselt.

Anleitung: <https://schulamt-muenchen.musin.de/attachments/article/330/Verschl%C3%BCsslung%20von%20Dokumenten.pdf>

### ▪ Verschlüsselung von Datenträgern mit Bitlocker

Bitlocker ist ein Windows-Programm, das Datenträger wie z. B. USB-Sticks, verschlüsselt. Es funktioniert unter Win 10 und Win 7.

Anleitung: siehe nächste Seite

Tutorial: <https://www.youtube.com/watch?v=KVEDQCCVDK0&feature=youtu.be>



### ▪ Verschlüsselung mehrerer Dateien und Ordner mit 7-Zip

7-Zip ist ein Open Source Programm, das für alle Betriebssysteme erhältlich ist. Dateien oder Ordner können komprimiert in einer Datei gespeichert und optional auch verschlüsselt werden.

Anleitung:

<https://www.heise.de/tipps-tricks/ZIP-Archiv-mit-einem-Passwort-schuetzen-So-geht-s-3907870.html>

Download: <https://www.7-zip.de/>



### ▪ Verschlüsselung von Festplatten und Wechseldatenträgern mit VeraCrypt

VeraCrypt ist eine Open-Source-Software zur Datenverschlüsselung, insbesondere zur vollständigen oder partiellen Verschlüsselung von Festplatten und Wechseldatenträgern.

Als Nachfolgeprogramm von Truecrypt ist es in der Bedienung und Anwendung nahezu identisch.

Es arbeitet mit verschlüsselten Containern, die beim Öffnen ein Passwort erfordern.

Ausführliche Anleitung: <https://www.kuketz-blog.de/veracrypt-daten-auf-usb-stick-sicher-verschluesseln/>

Download: <https://www.veracrypt.fr/en/Downloads.html>

Tutorials:

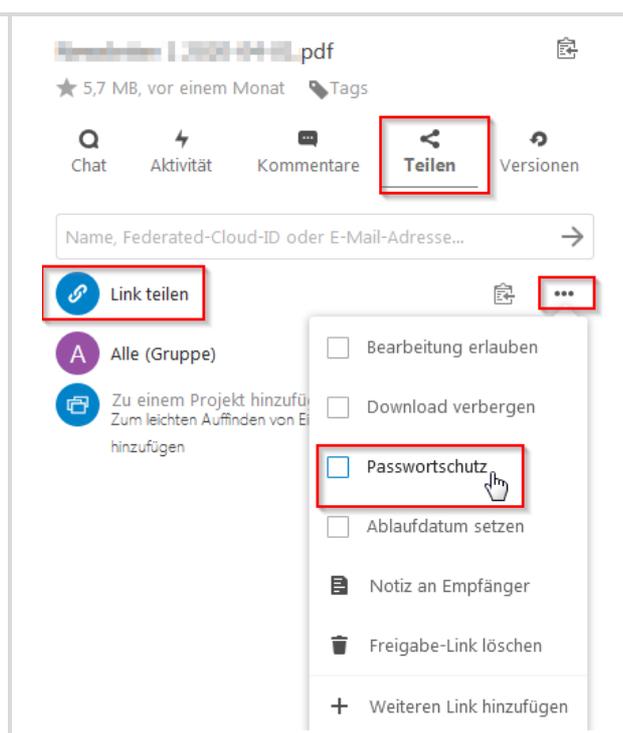
▪ <https://www.youtube.com/watch?v=gUbgrow3Od0>

▪ <https://www.youtube.com/watch?v=jPRkPwM2uvo&feature=youtu.be>



### ▪ Verschlüsselung von Freigabelinks mit nextcloud

Dateien, die in nextcloud abgespeichert sind, können über Links inkl. Passwortschutz freigegeben werden. Um die Datei über den Link öffnen zu können, ist die Eingabe des Passwortes erforderlich.

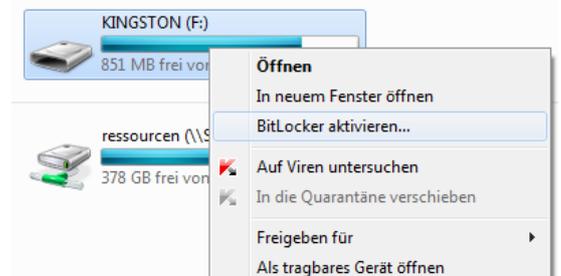


The screenshot shows a file named '123456789.pdf' in Nextcloud. The 'Teilen' (Share) button is highlighted with a red box. Below it, the 'Link teilen' (Share link) option is selected and also highlighted with a red box. In the resulting share menu, the 'Passwortschutz' (Password protection) checkbox is checked and highlighted with a red box. Other options in the menu include 'Bearbeitung erlauben', 'Download verbergen', 'Ablaufdatum setzen', 'Notiz an Empfänger', 'Freigabe-Link löschen', and 'Weiteren Link hinzufügen'.

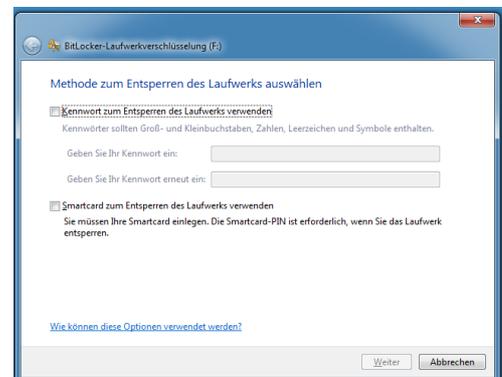


# Verschlüsselung eines USB-Sticks mit BitLocker

- ① USB-Stick einstecken
- ② rechte Maustaste - BitLocker aktivieren
- ③ BitLocker wird gestartet



- ④ Methode zum Verschlüsseln wählen (Kennwort vergeben)



- ⑤ Die Verschlüsselung wird gestartet und dauert einige Minuten.
- Der USB-Stick ist nun verschlüsselt und kann nach dem Einstecken nur mit dem Kennwort gelesen werden.

