

## Anleitung zur Verschlüsselung Ihrer E-Mail mit 7Zip

1. **Laden Sie sich ein passendes Programm herunter**, wie etwa 7-Zip. Einen sicheren Download finden Sie direkt beim Hersteller unter <http://www.7-zip.de/download.html> . Setzen Sie andere Programme wie beispielsweise Winzip oder Winrar ein, erhalten Sie ein gleich gutes Ergebnis. Es besteht dann kein Grund, auf 7Zip zurück zu greifen. Auch die Vorgehensweise ist ähnlich. Wichtig ist, dass Sie die Regeln für die Wahl eines geeigneten Passworts beachten.
2. Klicken Sie mit der rechten Maustaste auf den zu archivierenden Ordner oder die zu archivierende Datei und wählen Sie die Menüpunkte „**7-Zip**“ und dann „**Zu einem Archiv hinzufügen**“ aus.
3. Es öffnet sich ein neues Fenster, in welchem Sie nun im unteren rechten Bereich „**Verschlüsselung ein Passwort und ein Verschlüsselungsformat einstellen**“ können. Hier sollte **das Format „AES-256“ gewählt werden**, weil es als sicherer ist.
4. Achten Sie darauf, dass Sie bei „**Archivformat**“ die **richtige Dateiendung** auswählen. Im Dropdown-Menü wählen Sie dazu die Option „**zip**“ aus, wenn diese nicht schon vorselektiert ist.
5. Klicken Sie nun auf „**OK**“, um den Ordner zu einem gesicherten ZIP-Archiv zu komprimieren.

## Regeln zur Wahl eines geeigneten Passworts

Damit das Passwort nicht sofort geknackt werden kann, empfiehlt es sich, einige Regeln einzuhalten:

1. Das Passwort sollte mindestens acht Zeichen lang sein – mehr ist besser: Je weniger Zeichen ein Passwort hat, desto schneller kann es geknackt werden. Deshalb sind besonders sensible Bereiche auch mit Passwörtern geschützt, die über 20 Zeichen lang sind.
2. Verwenden Sie Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern: Das erhöht die Zahl der möglichen Kombinationen um ein Vielfaches. Und je mehr Möglichkeiten es gibt, desto schwerer wird es, den Code zu knacken. Deshalb sind gerade Sonderzeichen sehr wichtig für ein gutes Passwort. Diese positionieren Sie am besten innerhalb des Passworts und nicht am Anfang oder Ende.
3. Das Passwort sollte keinen logischen Bezug haben: Ihr Passwort sollte keinen persönlichen Bezug enthalten - zum Beispiel keine Namen oder Geburtstage.
4. Das Passwort sollte keine Muster beinhalten: Kombinationen wie "987654321" oder achtmal der gleiche Buchstabe sollten nicht als Passwort eingesetzt werden. Auch „qwertzuio“ - also nebeneinander liegende Tasten - müssen vermieden werden.
5. Am besten sind Passwörter ohne jeglichen Sinn, wie beispielsweise „Vb\_\*413Frda“. Die sind aber natürlich schwerer zu merken. Sie können sich deshalb Eselsbrücken bauen - zum Beispiel als Satz: „Mein Kater will mindestens 1 mal am Tag fressen“ wird zum Passwort „MKwm1\*aTf.“