# FAQ: Passwortsicherheit

Passwörter dienen nicht nur dem Schutz vertraulicher Daten, sondern auch als Authentifizierungsmerkmal bei der Verwendung von Nutzerkonten. Umso wichtiger ist es daher, dass die eigens gewählten Passwörter einen hohen Schutzstandard aufweisen. Betrachtet man jedoch die Rangliste der beliebtesten Passwörter in Deutschland, so handelt es sich bei der Zeichenfolge „123456“ nach wie vor um eines der am meisten genutzten Passwörter deutscher Internetnutzer.

### *Was zeichnet ein sicheres Passwort aus?*

Ein sicheres Passwort sollte über mindestens zehn bis zwölf Zeichen verfügen und dabei Groß- und Kleinschreibung, Ziffern sowie Sonderzeichen enthalten. Auch wenn unter diesen Umständen die Verlockung groß ist: Vermeiden Sie es unbedingt, sich Ihre Passwörter zu notieren. Um sich komplexe Passwörter dennoch gut einprägen zu können, eignen sich unterschiedliche Hilfsstrategien: Zum einen kann ein beliebiger Satz gebildet werden, von dem die Anfangsbuchstaben eines jeden Wortes das Grundgerüst bilden. Im Anschluss können bestimmte Buchstaben in sich ähnelnde Ziffern oder Sonderzeichen umgewandelt werden. Zum anderen können aber auch einzelne, durch Ziffern und Sonderzeichen verbundene Wortgruppen ein sicheres Passwort darstellen.

Die Ergänzung von einfachen Ziffern oder üblichen Sonderzeichen am Anfang oder Ende eines einfachen Passwortes ist hingegen nicht empfehlenswert. Als Passwort gänzlich ungeeignet sind Namen von Bekannten, Freunden und Familienmitgliedern, Geburtsdaten oder gängige Wiederholungs- und Tastaturmuster, wie beispielsweise „1234abcd“oder „asdfgh“. Auch sollte das vollständige Passwort möglichst in keinem Wörterbuch vorkommen.

Darüber hinaus sollten Passwörter nur einmalig vergeben werden. Eine regelmäßige anlasslose Änderung ist hingegen nach Ansicht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bei sicheren Passwörtern nicht mehr erforderlich.

| Zeichen | 6-stellig | 8-stellig | 10-stellig | 12-stellig | 14-stellig |
|---|---|---|---|---|---|
| 0 - 9 | 0 Sekunden | 0 Sekunden | 10 Sekunden | 1.000 Sekunden | Ein Tag |
| A - Z | 0 Sekunden | 209 Sekunden | 39 Stunden | 3 Jahre | 2.046 Jahre |
| a - z A - Z | 20 Sekunden | 15 Stunden | 5 Tage | 12.395 Jahre | 33.515.076 Jahre |
| a - z A - Z 0 - 9 | 57 Sekunden | 61 Stunden | 27 Jahre | 102.304 Jahre | 393.257.529 Jahre |
| a - z A - Z 0 - 9 ! - # | 783 Sekunden | 83 Tage | 2.108 Jahre | 19.482.899 Jahre | Sehr lange |

*„Knack-Geschwindigkeit“ bei ungefähr einer Milliarde Passwörter pro Sekunde*

### *Ändern Sie voreingestellte Passwörter umgehend*

Diverse Hardware- und Softwarelösungen verfügen über allgemein bekannte voreingestellte oder „leere“ Passwörter. Diese stellen ein besonderes Sicherheitsrisiko dar und sind aus diesem Grund umgehend abzuändern. In diesem Zusammenhang sei noch erwähnt, dass Router stets über ein mindestens 20-stelliges Passwort verfügen sollten.

### *Sichern Sie Ihre Endgeräte per Sperrbildschirm*

Sämtliche gängigen Betriebssysteme bieten automatische Bildschirm-Timeouts in Verbindung mit der Eingabe eines Passwortes bei Reaktivierung an. Diese Funktion sollte abhängig vom jeweiligen Endgerät, spätestens jedoch fünf Minuten nach der letzten Benutzeraktivität den Zugang sperren. Bei kürzerer Abwesenheit ist auch eine Sperrung per Tastenkombination, beispielsweise durch Windows-Taste + L möglich. Dies verhindert, dass unbefugte Dritte während Ihrer Abwesenheit Zugang zu personenbezogenen Daten sowie anderen vertraulichen Informationen erhalten.

### *Geben Sie Passwörter nur auf eigenen Geräten ein*

Oftmals ist nicht bekannt, ob fremde Endgeräte über einen ausreichenden Schutz vor Schadprogrammen verfügen. Demnach kann auch nicht ausgeschlossen werden, dass mittels sogenannter „Keylogger" sämtliche Tastatur- und Bildschirmeingaben aufgezeichnet werden. Vermeiden Sie aus diesem Grund auf die Eingabe Ihrer Zugangsdaten bei der Nutzung fremder Endgeräte. Sofern Sie beispielsweise während einer Dienstreise gezwungenermaßen ausschließlich über fremde Geräte Ihre Zugangsdaten eingeben können, empfiehlt sich für diese Zeit die Nutzung eines temporären Ersatzpasswortes.

### *Geben Sie Passwörter niemals weiter*

Wie eingangs erwähnt, handelt es sich bei Passwörtern auch um ein Authentifizierungsmerkmal Ihrer Person. Geben Sie aus diesem Grund Passwörter niemals weiter, weder an Familienangehörige noch an Vorgesetzte oder Kolleginnen und Kollegen. Ändern Sie Ihr Passwort umgehend, wenn Sie mitbekommen haben, dass ein anderer Ihre Zugangsdaten in Erfahrung bringen konnte.

### *Trennen Sie berufliche und private Passwörter*

Verwenden Sie für berufliche und private Zwecke stets unterschiedliche Passwörter. So vermeiden Sie, dass berufliche Passwörter durch das Ausspähen von Zugangsdaten bei privaten Dienstanbietern bekannt werden.

### *Nutzen Sie die Zwei-Faktor-Authentisierung*

Verschiedene Dienstanbieter bieten zusätzlich zum Passwortschutz eine sogenannte „Zwei-Faktor-Authentisierung" an. Dabei wird nach der erfolgreichen Eingabe der Zugangsdaten zunächst ein zufällig generierter Code per SMS an eine zuvor festgelegte Telefonnummer gesendet. Erst mit der Eingabe dieses Codes erhält der jeweilige Nutzer einen Zugang. Alternativ wird dieses Verfahren teilweise auch mit speziellen Code-Generatoren angeboten.