Bitte ändern Sie schnellstmöglich das Voreingestellte Passwort unter der Verwendung der folgenden Tipps.

## Tipps für sichere Passwörter nach BSI

Schlecht gewählte Passwörter sind nach wie vor eines der häufigsten Defizite bei der IT-Sicherheit. Oft wählen die Nutzer zu kurze oder zu wenig komplexe Zeichenkombinationen oder nutzen dasselbe Passwort für mehrere Anwendungen.

1. **Ein komplexes Passwort wählen**: Ein gutes Passwort (zum Beispiel für ein Benutzerkonto im Internet) sollte mindestens acht Zeichen lang sein und nicht im Wörterbuch stehen. Neben Groß- und Kleinbuchstaben sollte es auch Ziffern und Sonderzeichen enthalten.
2. **Keine Namen verwenden**: Tabu sind Namen von Familienmitgliedern, des Haustieres, des besten Freundes oder des Lieblingsstars oder deren Geburtsdaten. Wenn möglich sollte es nicht in Wörterbüchern vorkommen.
3. **Kreativ werden**: Um ein komplexes und dennoch leicht zu merkendes Passwort zu konstruieren, empfiehlt sich ein Merksatz als Eselsbrücke. Dabei denkt sich der Nutzer einen Satz aus und benutzt von jedem Wort beispielsweise nur den ersten Buchstaben. Anschließend verwandelt man bestimmte Buchstaben in Zahlen oder Sonderzeichen. So wird zum Beispiel aus dem Merksatz "Morgens stehe ich auf und putze meine Zähne." das Passwort "Ms1a&pmZ". Es soll nicht aus gängigen Varianten und Wiederholungs- oder Tastaturmustern bestehen, also nicht asdfghoder 1234abcd und so weiter. Einfache Ziffern am Ende des Passwortes anzuhängen oder eines der üblichen Sonderzeichen $ ! ? #, am Anfang oder Ende eines ansonsten simplen Passwortes zu ergänzen ist auch nicht empfehlenswert.
4. **Passwörter regelmäßig ändern**: Jedes Passwort sollte in regelmäßigen Zeitabständen geändert werden. Viele Programme erinnern automatisch daran, wenn das Passwort schon ein halbes Jahr benutzt wird.
5. **Passwörter nicht aufschreiben**: Auch wenn es bei selten genutzen Zugangsdaten schwerfällt: Grundsätzlich sollten Nutzer sich Passwörter nicht notieren. Passwörter dürfen Dritten nicht weitergegeben oder weitergesagt werden.
6. **Unterschiedliche Passwörter verwenden**: Problematisch ist die Gewohnheit, einheitliche Passwörter für viele verschiedene Zwecke zu verwenden. Denn gerät das Passwort einer einzelnen Anwendung in falsche Hände, sind auch die anderen Anwendungen nicht mehr geschützt.

***Quelle:*** *www.bsi-fuer-buerger.de/Passwoerter*