

Richtlinien zum Erstellen sicherer Passwörter

Inhaltsverzeichnis

- 1. Passwortrichtlinien an der KSZ
 - 1.1. Windows Komplexitätsanforderungen
- 2. Einige Grundsätze die sie beim Erstellen von Passwörtern beachten müssen:
- 3. Damit ihre Passwörter sicher sind, müssen sie sich an gewisse Regeln halten. Folgende Fehler sollte man bei der Wahl eines Passwortes nie machen:
- 4. Wie bilden Sie einfach sichere Passwörter die man sich auch merken kann? Einige Tipps:
- 5. Bekannte Probleme im Zusammenhang mit dem Passwortwechsel

1. Passwortrichtlinien an der KSZ

- Passwortlänge: Mindestens 12 Zeichen
- Komplexität: Das Passwort muss die Windows Komplexitätsanforderungen erfüllen, siehe Punkt 1.1
- Wiederverwendung: Die letzten 4 Passwörter werden gespeichert, das Passwort muss sich also deutlich von den 4 Letzten unterscheiden.

1.1. Windows Komplexitätsanforderungen

Das Passwort

- darf weder Benutzernamen noch Teile von Vor- und Nachnamen enthalten.
- muss Gross- und Kleinbuchstaben enthalten
- muss Ziffern (0 bis 9) enthalten
- muss Sonderzeichen enthalten (~!@#%&*_+="{\|} {} [] ;: " <> , . ? /)

2. Einige Grundsätze die sie beim Erstellen von Passwörtern beachten müssen:

- Verwenden Sie einen Passwortmanager (z.B. KeePass).
- Längere Passwörter sind sicherer als komplizierte Passwörter (einem Computer ist egal wie kompliziert die Zeichenreihenfolge ist).
- Das Passwort muss man sich merken können. Es darf nicht aufgeschrieben werden.
- Platzieren Sie Zahlen und Sonderzeichen nicht nur am Anfang und am Schluss von Passwörtern.
- Passwörter können nicht wiederverwendet werden. Es muss jedes mal ein neues Passwort gewählt werden.

3. Damit ihre Passwörter sicher sind, müssen sie sich an gewisse Regeln halten. Folgende Fehler sollte man bei der Wahl eines Passwortes nie machen:

- Verwenden Sie niemals ein Wort welches einen Bezug auf Sie herstellt (2. Vorname, Name eines Verwandten, Geburtsort etc.).
- Einzelne Worte aus dem täglichen Wortschatz und aus dem Duden sind tabu.
- Keine Passwörter die nur Zahlen enthalten.

4. Wie bilden Sie einfach sichere Passwörter die man sich auch merken kann? Einige Tipps:

- Verwenden sie diverse nicht zusammenhängende Worte und formen sie daraus ein Passwort mit über 20 Zeichen. (z.B. DaumenCroissant5Kreise!nachts).
- Überlegen sie sich einen langen Satz und verwenden sie von jedem Wort nur die ersten 2-3 Buchstaben. Beispiel: "Ist das Leben zu hart, hilft vielleicht ein Luftballon." wird zu "IsdaLezuha,hivi1Lu". Verwendet wurden die ersten zwei Buchstaben jedes Wortes, das Komma wurde beibehalten und "ein" wurde durch 1 ersetzt.
- Denken Sie sich eine E-Mailadresse aus. Verwenden Sie dazu irgendwelche Worte die Sie zu einer E-Mailadresse formen (z.B. morgens@halb10.deutschland).

Kombinieren Sie oben genannte Tipps um ein möglichst sicheres Passwort zu erhalten. Verwenden Sie auf keinen Fall eines der hier erwähnten Beispiele als Passwort.

5. Bekannte Probleme im Zusammenhang mit dem Passwortwechsel

- Outlook unter Windows funktioniert nicht mehr [FAQ - Outlook funktioniert nach Passwortwechsel nicht mehr](#)