

## Anwendungsaufgabe: Büro - Bestellung

### Die Sicherheit von Passwörtern

Sie können noch einmal das interaktive Video ansehen, um die Aufgabe zu lösen:

[https://www.digidazu.at/start/buero/bestellung/#interaktives\\_video\\_1](https://www.digidazu.at/start/buero/bestellung/#interaktives_video_1)

### Elemente eines sicheren Passworts:

1. Lesen Sie hier einige Aussagen über Passwörter und ihre Sicherheit.

Welche Aussagen stimmen? Kreuzen Sie diese Aussagen an!

- Ein Passwort sollte eher kurz sein. Dann kann man es sich besser merken.
- Ein Passwort sollte Sonderzeichen enthalten.
- Es ist gut, wenn man immer dasselbe Passwort verwendet.
- Das eigene Geburtsdatum, der Name aber auch einfache Wörter sind als Passwort nicht so sicher.
- Ein Passwort sollte mindestens 12 Zeichen haben. Je länger desto sicherer.
- Ein gutes Passwort enthält Zahlen, Groß- und Kleinbuchstaben.
- Zahlenfolgen (z.B. 45678) als Passwort sind schwer zu knacken.

### Passwörter testen:

2. Sehen Sie sich nun einige Passwörter an.

Wie sicher schätzen sie diese Passwörter ein? Kreuzen Sie an!

	<i>unsicher</i>	<i>schwach</i>	<i>mittelmäßig</i>	<i>sicher</i>
a) 102090290	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
b) 1978ISweIM!06	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
c) lloveyou	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
d) 2506-Wien-2022	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
e) ABCDE12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
f) W1nt3r§onn3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

	<i>unsicher</i>	<i>schwach</i>	<i>mittelmäßig</i>	<i>sicher</i>
g) M.VUCIC	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
h) abc123	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
i) 12Sommerregen=?45	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
j) !?"\$?%\$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

3. Man kann die Sicherheit von Passwörtern auch testen. Im Internet gibt es dazu mehrere Seiten. Eine solche Seite ist <https://checkdeinpasswort.de/>  
Testen Sie diese Passwörter! Wie sicher sind sie laut dieser Seite?

	<i>unsicher</i>	<i>schwach</i>	<i>mittelmäßig</i>	<i>sicher</i>
a) 102090290	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
b) 1978ISweIM!06	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
c) lloveyou	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
d) 2506-Wien-2022	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
e) ABCDE12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
f) W1nt3r§onn3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
g) M.VUCIC	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
h) abc123	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
i) 12Sommerregen=?45	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
j) !?"\$?%\$	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**ACHTUNG:**

Testen Sie auf solchen Seiten sicherheitshalber nicht Ihre richtigen Passwörter!

**Passwörter aufbewahren:**

4. Auch bei der Aufbewahrung von Passwörtern gibt es einiges zu beachten. Lesen Sie dazu die Tipps von Saferinternet unter diesem Link:  
<https://www.saferinternet.at/faq/datenschutz/wie-kann-ich-passwoerter-sicher-aufbewahren/>

Schreiben Sie nun die fehlenden Wörter in die Lücken!

- a) Halten Sie Ihre Passwörter \_\_\_\_\_.
- b) Geben Sie Passwörter stets \_\_\_\_\_ von Dritten ein.
- c) Speichern Sie Passwörter nicht im \_\_\_\_\_ ab.
- d) Verwenden Sie \_\_\_\_\_ Passwörter für unterschiedliche Benutzerkonten.
- e) Alternativ dazu können Sie auch einen Passwort-Safe bzw. \_\_\_\_\_ benutzen. Dieser speichert viele verschiedene Passwörter hinter einem Master-Passwort ab. So brauchen Sie sich nur noch ein einziges Passwort zu merken. Bekannte Passwort-Manager sind etwa *LastPass*, *1Password*, *Keeper*, oder *KeePass*.
- f) Beim Aufschreiben Passwort nicht als Passwort bezeichnen.
- g) Nicht zusammen mit ergänzenden \_\_\_\_\_ hinterlegen.
- h) Keinesfalls direkt am \_\_\_\_\_ oder \_\_\_\_\_ aufbewahren.
- i) Wenn Ihr Service-Anbieter gehackt wurde oder Sie glauben, dass eine unbefugte Person Ihr Passwort herausgefunden hat – \_\_\_\_\_ Sie es sofort!

## Lösungen

1.

- Ein Passwort sollte eher kurz sein. Dann kann man es sich besser merken.
- Ein Passwort sollte Sonderzeichen enthalten.
- Es ist sicher, wenn man immer dasselbe Passwort verwendet.
- Das eigene Geburtsdatum, der Name aber auch einfache Wörter sind als Passwort nicht so sicher.
- Ein Passwort sollte mindestens 12 Zeichen haben. Je länger desto sicherer.
- Ein gutes Passwort enthält Zahlen, Groß- und Kleinbuchstaben.
- Zahlenfolgen sind leicht zu merken und schwer zu knacken.

3.

	<i>unsicher</i>	<i>schwach</i>	<i>mittel</i>	<i>sicher</i>
a) 102090290	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
b) 1978ISweIM!06	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
c) Iloveyou	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
d) 2506-Wien-2022	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
e) ABCDE12	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
f) W1nt3r§onn3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
g) M.VUCIC	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
h) abc123	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
i) 12Sommerregen=?45	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
j) !?"§?%\$	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

4.

- a) Halten Sie Ihre Passwörter **geheim**.
- b) Geben Sie Passwörter stets **unbeobachtet** von Dritten ein.
- c) Speichern Sie Passwörter nicht im **Browser** ab.
- d) Verwenden Sie **unterschiedliche** Passwörter für unterschiedliche Benutzerkonten.

- e) Alternativ dazu können Sie auch einen Passwort-Safe bzw. **Passwort-Manager** benutzen. Dieser speichert viele verschiedene Passwörter hinter einem Master-Passwort ab. So brauchen Sie sich nur noch ein einziges Passwort zu merken. Bekannte Passwort-Manager sind etwa *LastPass*, *1Password*, *Keeper*, oder *KeePass*.
- f) Beim Aufschreiben Passwort nicht als Passwort bezeichnen.
- g) Nicht zusammen mit ergänzenden **Zugangsdaten** hinterlegen.
- h) Keinesfalls direkt am **Computer** oder **Handy** aufbewahren.
- i) Wenn Ihr Service-Anbieter gehackt wurde oder Sie glauben, dass eine unbefugte Person Ihr Passwort herausgefunden hat – **ändern** Sie es sofort!