Passworttipps

Mit Passwörtern zeigen wir z.B. einer Website, dass wir wirklich wir selbst sind. Die Idee dahinter ist, dass nur wir und diese Website das Passwort kennen. Aber ist das immer so?

Zu einfache Passwörter können schnell erraten werden. Daher ist es wichtig, **komplexe** und vor allem **lange Passwörter** zu verwenden. Für Passwörter, die man sich selbst merken muss, hat sich das so genannte **"Diceware"**-Verfahren[1] mit **5 oder mehr Wörtern** bewährt. Es bietet gleichzeitig sichere und gut zu merkende Passwörter.

Wenn Passwörter z.B. auf einer anderen Website wieder verwendet werden, muss nun auch diese Website das Passwort kennen. Die Prämisse „nur wir kennen das Passwort" stimmt also nicht mehr. Denn selbst große Webseiten können gehackt und Passwörter gestohlen werden[2]. Man sollte daher **für jeden Zugang ein separates, sicheres Passwort** verwenden!

Mit einem **Passwortmanager** wie z.B. **KeePass**[3] kann man eine Vielzahl von Passwörtern bequem und sicher verwalten. Hier ist natürlich auf ein besonders langes und sicheres Passwort zu achten!

1 https://de.wikipedia.org/wiki/Diceware
2 Überprüfbar z.B. auf https://HaveIBeenPwned.com
3 KeePass 2 http://keepass.info

Sicherheitstipps

1. E-Mails

- Keine Links in E-Mails anklicken. Wenn doch notwendig, besonders auf die URL achten!
- Unteradressen für verschiedene Dienste verwenden, um die Herkunft einer E-Mail erkennen zu können. Viele E-Mailanbieter leiten automatisch zur Originaladresse weiter:

  ich+meineBank@example.com → ich@example.com

2. Software

- Software am besten von der Herstellerwebsite. Diese findet man z.B. über Wikipedia.
- Updates zügig installieren
- Sicherheitslücken in Adobe Flash und Java sind extrem häufig: deaktivieren oder deinstallieren!
- Selbst ein aktueller Virenscanner hilft oft nicht genug – mitdenken und hinterfragen wichtiger!

3. Backups

Von wichtigen Daten sollte regelmäßig ein Backup auf einem USB-Stick oder einer externen Festplatte angefertigt werden.