bzi Bildungszentrum Interlaken

Sicherer Umgang mit den Zugangsdaten

Für Lehrpersonen und Verwaltungsangestellte

Alle Mitarbeitenden des bzi erhalten Zugangsdaten für die Computersysteme. Die Daten gelten für den Zugang zum Schulnetz, E-Mail-Server, Intranet, Office 365 und den Remotezugang von externen Standorten via Citrix VDesk. Den korrekten Umgang mit den Logindaten für die Systeme regelt die ICT-Nutzungsordnung.

Die Zugangsdaten für die Lehrpersonen und das Verwaltungspersonal lauten:

Benutzername: **name.vorname@bzi.ch** (gleiche Schreibweise wie E-Mail-Adresse)

Kennwort: *******

Das Startkennwort muss bei der ersten Anmeldung gemäss Passwortrichtlinie geändert werden. Achtung! Nach der Registrierung der erforderlichen Sicherheitsinformationen kann ein vergessenes Kennwort selber zurückgesetzt werden. Informationen und die entsprechenden Links sind auf **password.bzi.ch** zu finden. Neuen Mitarbeitenden wird das Startkennwort per Post zugeschickt. Verwaltungsmitarbeitende müssen das Passwort anschliessend alle 90 Tage ändern, Lehrpersonen alle 180 Tage.

Wichtige Regeln und Sicherheitsvorkehrungen sind:

- **Die persönlichen Zugangsdaten dürfen auf keinen Fall anderen Personen (Lernenden, Lehrpersonen, Externen) mitgeteilt werden.** Für Handlungen mit den persönlichen Zugangsdaten ist immer der Inhaber/die Inhaberin verantwortlich. Stellvertreter/innen und externe Referenten erhalten auf Anfrage temporäre Logindaten vom Informatikdienst. Lernende und Kursteilnehmende haben eigene Zugangsdaten.

- Das Passwort nicht unter die Tastatur, hinter den Monitor kleben oder an die Pinnwand heften! Wenn man es überhaupt aufschreibt, dann den Zettel zumindest sicher aufbewahren.

- Beim Verlassen des PC-Arbeitsplatzes **immer** den Computer sperren (**CTRL + ALT + DELETE --> SPERREN**). Per Sicherheitsrichtlinie wird die Sperrung der Arbeitsstation vom Server nach 10 Minuten Inaktivität automatisch aktiviert. Diese Massnahme ist in den Schulzimmern und PC-Räumen äusserst wichtig, da die Lernenden an diesem PC sonst Zugang zu den Daten der Lehrkraft erhalten.

- Die Passwortlänge und Komplexität wird per Sicherheitsrichtlinie vom Informatikdienst vorgegeben. Die Vorgaben sind

  → Das Kennwort muss mindestens acht Zeichen lang sein.
  → Das Kennwort darf keine drei oder mehr Zeichen aus dem Kontonamen des Benutzers enthalten.
  → Das Kennwort enthält Zeichen aus mindestens drei der folgenden fünf Kategorien: Deutsche Großbuchstaben (A - Z), Deutsche Kleinbuchstaben (a - z), Arabische Ziffern (0 - 9), Nicht-alphanumerische Zeichen (Beispiel: !, $, # oder %)

- Tipps für die Wahl eines sicheren Passwortes:

  - Kombination aus Kleinbuchstaben, Zahlen und Sonderzeichen nutzen, deutsche Umlaute meiden.

Version vom: 18.06.2019
Hanspeter Rasch

- Wörter aus dem persönlichen Umfeld (Eigennamen, Kosenamen, Haustiernamen etc.) sind tabu.
- Keine Wörter aussuchen, die im Duden oder irgendeinem (Fremdsprachen-)Lexikon stehen. Also auch keine Comicfiguren oder Herr-der-Ringe-Helden.
- Geburtstage oder andere personenbezogene Daten vermeiden.
- Nicht einfach nur Sonderzeichen anhängen, sondern sie in das Passwort integrieren.
- Keine Wörter obiger Kategorien einfach nur rückwärts schreiben oder anders verfremden.

Ein recht sicheres Kennwort könnte sein: **0aJ/4%(hGs$df"Y!** (16 Zeichen). Die Problematik solcher Zufallszeichenfolgen ist jedoch, dass sie schwer zu merken sind und deshalb irgendwo notiert werden.

Gut geeignet ist die Verwendung der Anfangsbuchstaben eines Satzes "Hd7B%sd7Z" gebildet aus den **fett** hervorgehobenen Zeichen von "**H**inter **d**en **7** **B**ergen **%** **s**ind **d**ie **7** **Z**werge", mit eingestreutem Sonderzeichen).

Einige unbrauchbare Passwörter:

- 123456
- passwort
- God oder Gott
- Peter1
- Triviale Tastaturzeichenfolgen (1qay2wsx, asdf, qwert...)

Wer sich viele unterschiedliche Passwörter merken muss, kann mit einem Passwortverwaltungsprogramm (Passworttresor) seine Logindaten verwalten (auf dem Schul-PC installiert). Ein sehr empfehlenswertes Programm ist die OpenSource-Software "**KeePass**". Das Programm gibt es auch in einer portablen Version für USB-Sticks. Download:

Programm: https://keepass.info/download.html

Deutsches Sprachpaket: https://keepass.info/translations.html

---

Achtung!

Transportiere wichtige Daten wie Prüfungsunterlagen, vertrauliche Dokumente, etc. immer verschlüsselt auf dem USB-Stick oder auf dem Notebook. Ein ausgezeichnetes OpenSource-Programm ist "VeraCrypt". Verfügbar für Windows, OSx und Linux. Download:

Programm: https://www.veracrypt.fr/en/Home.html

Mehr Informationen zum sicheren Umgang mit dem PC und den Daten bietet das CBT-Lernprogramm "Datenschutz": https://review.datenschutz.ch/datenschutz/

Wie sicher ist mein Passwort? Dein Passwort kannst du auf folgender Website auf die Sicherheit überprüfen: https://www.passwortcheck.ch/passwortcheck/