Passwort ändern

Wo kann ich mein Passwort ändern?

Sie finden die Seite, mit der Sie Ihr Passwort ändern können, auf der Homepage des Gauß-IT-Zentrums.
Dazu müssen Sie in der Navigationsleiste auf der linken Seite den Punkt „Self-Service“ auswählen.
Anschließend klicken Sie in der Leiste auf „Passwort ändern“.

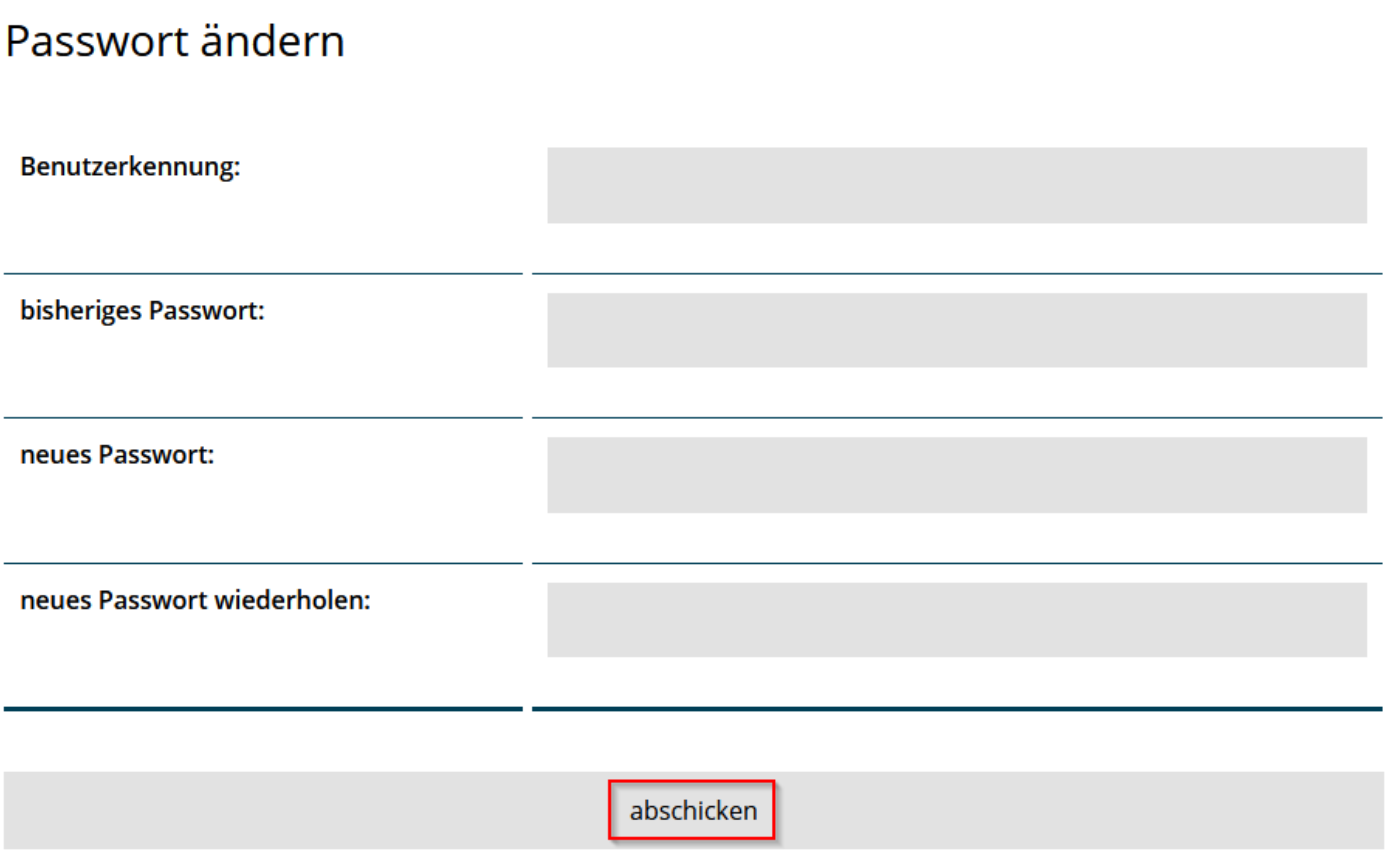
Alternativ können Sie auch den folgenden Link nutzen, welcher zu der selben Seite führt:

https://www.tu-braunschweig.de/it/self-service/passwort-aendern

Wie kann ich mein Passwort ändern?

Um das Passwort zu ändern, müssen Sie bei den Eingabefeldern Ihre TUBS-ID (z.B. y-Nummer) und ihr altes Passwort eingeben.
Anschließend geben Sie ihr neues Passwort ein und wiederholen dieses.

Wenn Sie das neue Passwort eingegeben haben, müssen sie unten auf der Seite auf **[Abschicken]** klicken.



Was muss ich beachten wenn ich mein Passwort ändern will? / Richtlinie für Passwörter

Die aktuelle Richtlinie für Passwörter sowie Hinweise auf den sicheren Umgang mit Passwörtern finden Sie hier:

[DE] https://books.rz.tu-bs.de/books/benutzerkonto/page/richtlinie-fur-passworter

[EN] https://books.rz.tu-bs.de/books/benutzerkonto/page/richtlinie-fur-passworter-guideline-for-passwords-en

Wir möchten Sie daran erinnern, dass Ihnen die IT-Ressourcen auf Basis universitäts-interner Ordnungen bereitgestellt werden.
Hierbei gelten die folgenden Nutzungsbedingungen:

[DE] https://books.rz.tu-bs.de/books/benutzerkonto/page/tubs-id-nutzungsbedingungen

[EN] https://books.rz.tu-bs.de/books/benutzerkonto/page/tubs-id-nutzungsbedingungen-terms-of-use-en

Die aktuelle Fassung der Ordnungen kann auf dieser Seite eingesehen werden.

Zusatzprüfung auf "bekannte" (geleakte) Passwörter

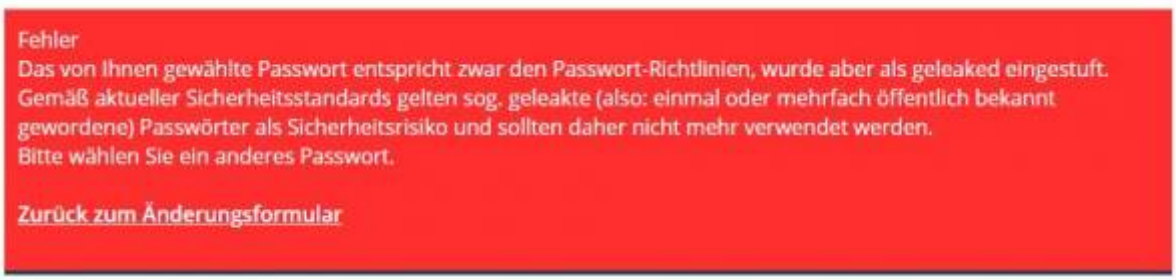
Ab dem 03.05.2018 (Weltpassworttag) erweitert das GITZ die Passwortprüfung auf der „Passwort ändern“-Seite.

Zusätzlich zu der bereits bekannten Prüfung auf Einhaltung der Passwort-Regeln (siehe oben) wird ab dem 3.5.2018 auf der „Passwort ändern“-Seite des GITZ ebenfalls geprüft, ob das gewünschte Passwort eventuell bereits in einer Liste von bereits schon einmal gehackten und bekannt gewordenen Passwörtern enthalten ist. Wenn dies der Fall ist, gilt das Passwort als unsicher, da solche Passwortlisten auch von Hackern für neue Angriffe oftmals verwendet werden.

Das GITZ verwendet dafür den Service der Webseite „have I been pwned“ (HIBP) des unabhängigen Sicherheitsforschers Troy Hunt, bei der es sich um die umfassendste, offen zugängliche Sammlung von unsicheren, „geleakten“ Passwörtern handelt. Die Seite wird auch von mehreren Regierungen als Prüfinstanz verwendet (Heise Newsticker, Engadget).

Der online verfügbare Service von HIBP verwendet einen ausgeklügelten Mechanismus, der sicherstellt, dass das eingegebene Passwort bzw. der daraus erzeugte sog. „Hash“ in keinem Fall vom GITZ an HIBP weiter gegeben wird .

Falls das Passwort bereits in der Liste vorkommt, wird eine Fehlermeldung ausgegeben und das Passwort wird nicht für die Verwendung an der TU Braunschweig akzeptiert:



In diesem Fall muss man ein anderes Passwort verwenden.

Allgemeine Hinweise zur Passwortlänge

Folgende einfache Merkhilfe kann bei der Wahl des Passwortes sehr hilfreich sein:
Man denkt sich einen Satz aus, in dem auch eine Zahl vorkommt:
Wir **h**aben **4** **A**utos **i**n **u**nserer **G**arage **s**tehen.
Nun nimmt man von jedem Wort den Anfangsbuchstaben und schon hat man ein relativ sicheres Passwort:

Wh4AiuGs
Bei der nächsten Passwortänderung kann dann z. B. heruntergezählt werden.
Dadurch erhält man ein (für Computer) völlig neues Passwort und muss sich dabei gar nicht viel merken.

Created 2024-05-22 13:24:10 UTC by Dennis Lukas
Updated 2026-08-27 13:16:37 UTC by Lasse Braun