# Sicherer Umgang mit dem eigenen Account

Anleitung für Studierende
Stand: Oktober 2018

## Inhalt



## Geben Sie nie Ihre Accountdaten an Dritte weiter!

! **Wie Sie es nicht machen sollten:** Sie sind im Urlaub und Ihr Kollege benötigt dringend eine Datei, die Sie auf Ihrem Arbeitsplatzcomputer abgelegt haben. Sie geben Ihm Ihre Zugangsdaten, damit er sich die Datei herunterladen kann.

**Warum nicht?** Sie haben keinen Einfluss darauf, wie andere Personen oder Systeme mit Ihren Daten umgehen (womöglich werden diese aufgeschrieben und zugänglich abgelegt). Dritte könnten Einsicht in Ihre Daten oder Manipulationen daran vornehmen, ohne dass Sie es überhaupt bemerken. Reagieren Sie deshalb auch nie auf Accountdatenabfragen per E-Mail (Phishing).

☑ **Nutzen Sie für den Zugriff von außerhalb der Universität unsere dafür vorgesehen Angebote** für Bedienstete oder Studierende (z.B. Outlook WebAccess oder WebDAV), für gemeinsam genutzte Dateien das Gruppenfileservice. Der Servicedesk berät Sie im Zweifelsfall gerne.

## „Verleihen“ Sie nie Ihre Zugangsdaten an andere Personen!

! **Wie Sie es nicht machen sollten:** Sie ermöglichen einer Person den Zugang zum Universitäts-WLAN, indem Sie auf deren Notebook Ihre Zugangsdaten eingeben.

**Warum nicht?**

- Diese Zugangsdaten werden unter Umständen dauerhaft im fremden System gespeichert – wenn Sie Ihr Passwort ändern, versucht das Fremdgerät weiterhin, sich mit Ihren alten Zugangsdaten einzuloggen, und verursacht so eine Sperrung Ihres Accounts.
- Sie kennen den Sicherheitszustand des fremden Geräts nicht – vielleicht sind Viren oder Keylogger darauf installiert, die in weiterer Folge Ihre Zugangsdaten Unbefugten zugänglich machen.

☑ **Nutzen Sie für Externe und Gäste die von der UNI-IT angebotenen Alternativen**, wie z. B. das Tagungsnetzwerk (lokale WLAN-Freischaltung für Gäste) oder Eduroam (d. h. Angehörige teilnehmender Hochschulen loggen sich mit den Zugangsdaten ihrer Heimatuniversität in unser WLAN/eduroam ein). Der Servicedesk gibt Ihnen gerne Auskunft über alle Möglichkeiten.

## Verwahren Sie Ihre Passwörter an einem sicheren Ort!

! **Wie Sie es nicht machen sollten:** Sie schreiben alle Usernamen und Passwörter in eine Textdatei, die Sie auf dem Desktop Ihres Computers abspeichern. Das Passwort für Ihren Arbeitsplatz-PC notieren Sie sich auf einem Zettel, den Sie unter der Tastatur aufbewahren.
**Warum nicht?** Dateien, die unverschlüsselt auf einem IT-Gerät abgelegt werden, sind dort im Klartext verfügbar und damit relativ leicht zugänglich.

☑ **Sichere Ablage von Passwörtern**: Legen Sie aufgeschriebene Passwörter an einem sicheren Ort ab (z. B. verklebtes Kuvert in einem verschlossenen Schrank). Wenn Sie Passwörter am PC abspeichern möchten, verschlüsseln Sie die Datei. Passwort-Tresors-Software seriöser Anbieter (z. B. KeePass) ist eine sinnvolle Alternative.

## Verwenden Sie gute Passwörter!

! **Wie Sie es nicht machen sollten:** Damit Sie sich Ihr Passwort einfach merken können, verwenden Sie den Namen Ihres Haustiers.
**Warum nicht?** Möchte jemand Ihr Passwort herausfinden, kann er/sie unterschiedliche Methoden verwenden:

- Kennt Sie der Angreifer/die Angreiferin, kann er/sie vielleicht schon mit gezieltem Probieren Ihr Passwort erraten (z. B. Geburtstage, Namen von PartnerIn, Kindern, Haustieren, Hobbies etc.).
- Bei sogenannten Brute-Force-Attacken probiert der Angreifer/die Angreiferin einfach alle möglichen Kombinationen aus – zum Beispiel von 0000 bis 9999. Sie machen es sehr einfach, wenn Sie ein kurzes Passwort wählen oder eines, das es tatsächlich als Wort gibt – bei einer Wörterbuchattacke werden einfach sämtliche Wörter durchprobiert.

☑ **Kriterien für ein gutes Passwort:**

- mindestens 10 Zeichen
- Zeichen aus mindestens zwei der folgenden Kategorien: Kleinbuchstaben, Großbuchstaben, Ziffern und Symbole (UNIGRAZonline verlangt mindestens drei Buchstaben, eine Ziffer und ein Sonderzeichen)
- darf nicht Ihren Vornamen, Familiennamen oder Usernamen enthalten
- Auch Teile von Vor- oder Familiennamen sollten nicht verwendet werden.

Weiterführende Informationen und Tipps für sichere Passwörter finden Sie z. B. auf

- https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html
- https://www.luis.uni-hannover.de/pw_used.html

## Verwenden Sie nicht das gleiche Passwort für unterschiedliche Dienste!

! **Wie Sie es nicht machen sollten:** Damit Sie sich nicht so viele Passwörter merken müssen, verwenden Sie das gleiche Passwort für die Uni, Ihr eBay-Konto und Ihren privates E-Mail-Konto (z. B. GMX, Gmail etc.).

**Warum nicht?** Die Zugangsdaten Ihres privaten E-Mail-Providers werden womöglich gestohlen. In Folge wird versucht, ob Ihre gestohlenen Zugangsdaten auch bei anderen Systemen funktionieren.

☑ **Verwenden Sie für jeden Account ein eigenes Passwort, das Sie regelmäßig ändern.** Sie können sich die unterschiedlichen Passwörter leichter merken, wenn Sie diese nach einer Systematik erstellen. Haben Sie bis dato Passwörter mehrfach verwendet, so können Sie möglicherweise auf der Webseite von haveibeenpwned erkennen, ob ein Account mit diesem Passwort gestohlen wurde. In allen Accounts, die dasselbe Passwort enthalten, muss dann ein individuelles Passwort gesetzt werden.

## Geben Sie keine Passwörter in nicht vertrauenswürdige Systeme ein!

! **Wie Sie es nicht machen sollten:** Sie möchten im Urlaub Ihre E-Mails lesen und loggen sich deshalb über den öffentlichen PC der Frühstückspension in Ihr Postfach ein.

**Warum nicht?** Sie haben keinerlei Informationen über den Sicherheitszustand des Systems. Es könnte virenverseucht sein und Ihre eingegebenen Zugangsdaten an Unbefugte übermitteln. Vielleicht hat auch jemand bewusst ein Programm installiert, um die Daten der Reisenden auszuspionieren.

☑ **Sollten Sie gezwungen gewesen sein, Ihr Passwort in ein nicht vertrauenswürdiges System einzugeben, so ändern Sie das Passwort umgehend, sobald sie wieder ein vertrauenswürdiges System zur Verfügung haben.**