

# Sicherer Umgang mit dem eigenen Account

---

RedakteurIn: Barbara Unger

Version:1.0

Gespeichert: 31.10.2011

Zielgruppe(n): Bedienstete, Studierende

Zusammenfassung: *Dieses Dokument gibt Ihnen einfache Verhaltens-Tipps, mit denen Sie Ihre Accountdaten (Username und Passwort) vor dem unerwünschten Zugriff Dritter schützen können.*

## Inhalt

Geben Sie nie Ihre Accountdaten an Dritte weiter!.....	2
„Verleihen“ Sie nie Ihre Zugangsdaten an andere Personen!.....	2
Verwahren Sie Ihre Passwörter an einem sicheren Ort!.....	2
Verwenden Sie gute Passwörter! .....	3
Verwenden Sie nicht das gleiche Passwort für unterschiedliche Dienste! .....	3
Geben Sie keine Passwörter in nicht vertrauenswürdige Systeme ein! .....	4

## Geben Sie nie Ihre Accountdaten an Dritte weiter!



### **Wie Sie es nicht machen sollten:**

Sie sind in 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 Datenabfragen 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 jemandem den Zugang zum Universitäts-WLAN, indem Sie auf dessen Notebook Ihre Zugangsdaten eingeben.

### **Warum nicht?**

- Diese Zugangsdaten werden unter Umständen dauerhaft im fremden System gespeichert – wenn Sie Ihr Passwort ändern, versucht sich das Fremdgerät weiterhin, 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 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 Benutzernamen 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.



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.

## 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 unterschiedliche Methoden verwenden:

- Kennt Sie der Angreifer, kann er vielleicht schon mit gezieltem Probieren Ihr Passwort erraten (z.B. Geburtstag, Namen von PartnerIn, Kindern, Haustieren, Hobbies etc.).
- Bei sogenannten [Brute-Force-Attacken](#) probiert der Angreifer einfach alle möglichen Kombinationen aus – zum Beispiel von 0000 bis 9999. Sie machen es ihm sehr einfach, wenn Sie ein kurzes Passwort wählen oder eines, das es tatsächlich als Wort gibt – mit einer „Wörterbuchattacke“ probiert er einfach sämtliche Wörter durch und ist so schneller am Ziel.

### Kriterien für ein gutes Passwort:

- mindestens 6 Zeichen
- mindestens ein Buchstabe und eine Ziffer
- darf nicht Ihren Vornamen, Familiennamen oder Benutzernamen enthalten
- Verwendung von Sonderzeichen
- Auch Teile von Vor- oder Familiennamen sollten nicht verwendet werden.
- Generell sollten Sie keine Teile von Wörtern verwenden (mehr als drei Buchstaben), die in (deutschen oder englischen) Wörterbüchern zu finden sind.

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


- [https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2011/Passwortsicherheit\\_27012011.html](https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2011/Passwortsicherheit_27012011.html)
- [http://rrzn10.uni-hannover.de/pw\\_used.html](http://rrzn10.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 privaten Mail-Anbieter (z.B. GMX, Hotmail etc.).*

### Warum nicht?

Ein Datendieb stiehlt womöglich die BenutzerInnen-Daten Ihres privaten E-Mail-Providers. In Folge wird er versuchen, 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 (vgl. „Verwenden Sie gute Passwörter“)

## 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 Geschäftsreisenden 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.