Gute Nutzerpassworte

Ihr Passwort ist Ihr individueller „Schlüssel“ für den Zugang zu verschiedenen Diensten und Anwendungen innerhalb der IT-Infrastruktur der Hochschule. Alles, was für Unbefugte nicht so ohne Weiteres erreichbar ist, zieht aber auch das Interesse auf sich. Moderne Passwort-„Knack“-Programme (Cracker) erleichtern das Herausfinden von Nutzerpassworten.

Sie sind deshalb gut beraten, einige Hinweise und Regeln zur Bildung möglichst sicherer Passworte zu beachten:

- Je mehr (unterschiedliche) Zeichen ein Passwort enthält, desto sicherer wird es. Viele Systeme schreiben Mindestlängen vor; wenn nicht, dann sollte Ihr Passwort mindestens 8 Zeichen lang sein.
- Vermeiden Sie Trivialworte, gängige Begriffe und Bezeichnungen, die ohne großen Aufwand mit Ihrer Person und Ihrem Umfeld in Bezug gebracht werden können (typisches Negativbeispiel: „ich“).
- Verwenden Sie möglichst nicht nur Buchstaben, sondern „mischen“ Sie Buchstaben mit Ziffern und Sonderzeichen – wie Punkt, Komma, Bindestrich usw. Achten Sie darauf, dass nicht mehrere gleiche Zeichen nebeneinander stehen.
- Deutsche Umlaute (ä,ö,ü) und das ß sollten Sie nicht verwenden – verschiedentlich können IT-Systeme nicht damit umgehen, weil sie nicht den deutschen Zeichensatz verwenden.
- Achten Sie auf Groß- und Kleinschreibung! Sie wird oft akribisch unterschieden.

Rein kryptisch (also zufällig) kombinierte Zeichenfolgen ergeben sehr sichere Passworte, sind aber leider nicht gut zu merken.

Eine gute Strategie ist, einen Satz aus mehreren Worten zu bilden, deren Anfangsbuchstaben man sich merken kann. Wenn dann noch Worte wie „ein“ durch die Ziffer 1, „für“ durch 4 usw. ersetzt werden, ergibt sich ein recht sicheres Passwort.

Ein gut gewähltes und weitgehend sicheres Passwort für mehrere Zugänge zu verwenden ist sinnvoller als für jeden Zugang ein eigenes einfaches.

Teilen Sie Ihr Passwort niemandem mit!
Notieren Sie es nicht – auf keinen Fall im Umfeld Ihres Rechners!

Sollte Ihnen trotz aller Sorgfalt der Verdacht kommen, dass Ihr Passwort unberechtigt benutzt oder ausgespäht wurde, dann wenden Sie sich umgehend an Ihren zuständigen Bereichsadministrator oder auch an das Hochschulrechenzentrum.

Gleiches gilt sinngemäß, wenn Sie Ihr Passwort vergessen haben.