Hinweise zu Passwörtern

Mit Ihrem Benutzeraccount (fd-Nummer) erhalten Sie Zugriff auf eine Reihe zentraler Dienste an der Hochschule Fulda. Dazu gehört der Zugriff auf Ihre E-Mail Adresse, der Login in den PC-Pools, sowie im VPN und WLAN der Hochschule Fulda, der Zugang zum eLearning- und zentralen Studiensystem (Prüfungsanmeldung, Notenübersicht, usw.).

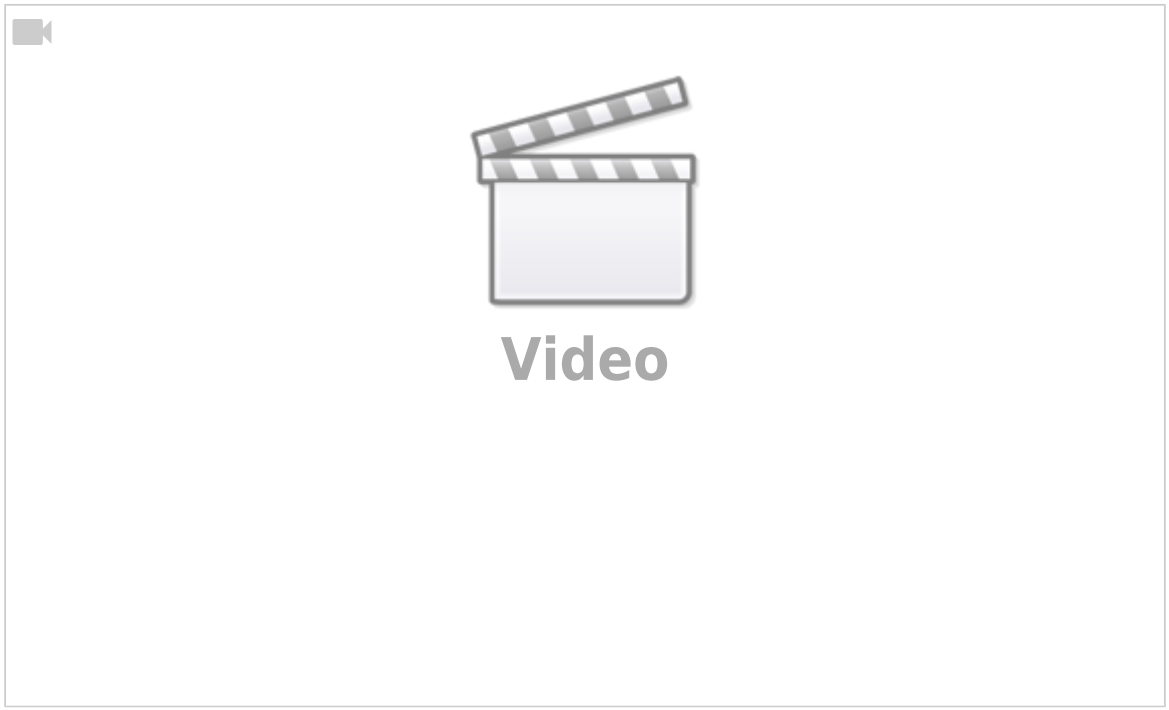
Damit Ihre persönlichen Daten vor dem Zugriff durch Dritte geschützt bleiben, sollten Sie ein sicheres Passwort wählen und dieses ändern, falls Sie den Verdacht haben, dass ein Dritter Kenntniss davon erhalten haben könnte.

Bitte behandeln Sie ihr Passwort streng vertraulich! Geben Sie es unter keinen Umständen an Dritte weiter. Das Rechenzentrum wird Sie nie auffordern, uns oder jemand anderem ihr Passwort zu nennen.

Sicherheit von Passwörtern

Wer die Wahl hat, hat die Qual. Besonders bei der Wahl der richtigen Passwörter tun sich viele PC-Nutzer schwer. Einfache Passwörter lassen sich durch die hohe Leistung heutiger Computer sehr schnell knacken. Sichere Passwörter sind dagegen häufig sehr kompliziert und lassen sich nur schwierig merken. Noch dazu sollte ja idealerweise unterschiedliche Zugänge (E-Mail, Facebook, Shopping, usw.) mit unterschiedlichen Passwörtern gesichert werden, um zu vermeiden, dass ein Sicherheitsvorfall bei einem Unternehmen nicht gleich dazu führt, dass die Angreifer auch auf alle anderen, mit dem gleichen Passwort gesicherten Konten zugriff erhalten.

Klar muss sein, dass *einfache* und *kurze* Passwörter heute in Minuten zu knacken sind. Aus diesem Grund sollte ein Passwort keine im Wörterbuch enthaltenen Begriffe, Namen von Personen oder Geburtsdaten enthalten. Das folgende Video erklärt anschaulich, wie Angriffe auf zu einfache Passwörter aussehen und wie Sie sichere Passwörter wählen können.



Viele weitere Tips zum Thema sichere Passwörter finden Sie beim Bundesamt für Sicherheit in der Informationstechnik.

Wie merkt man sich ein gutes Passwort?

Wie in dem Video zu sehen ist, muss ein Passwort heute eine gewisse Länge aufweisen, damit es trotz der immer schneller werdenden Computer schwer zu knacken ist. Eine Möglichkeit ist daher die Verwendung eines ganzen Satzes als Passwort.

Will man nicht immer einen ganzen Satz tippen, aber trotzdem ein sicheres Passwort wählen, gibt es auch dafür Tricks. Eine beliebte Methode funktioniert so: Man denkt sich einen Satz aus und benutzt von jedem Wort nur den ersten (oder nur den zweiten oder letzten) Buchstaben. Anschließend verwandelt man bestimmte Buchstaben in Zahlen oder Sonderzeichen um. Hier ein Beispiel:

- Gewählt wird der Satz: *Am Sonntag gehe ich um sechs zum Fischmarkt!*
- Nur die ersten Buchstaben: *ASgiuszF!*
- Der Buchstabe *i* sieht der Ziffer *1* ähnlich, also noch das *i* durch eine *1* und das Wort *sechs* durch eine *6* ersetzen: *ASg1u6zF!*

Schon hat man ein sicheres Passwort, das man sich aufgrund der „Eselsbrücke“ gut merken kann. Natürlich gibt es viele andere Tricks und Methoden, die genauso gut funktionieren.

Welche Regeln müssen Passwörter an der Hochschule Fulda erfüllen?

Laut der Sicherheitsrichtlinie der Hochschule Fulda sind Sie verpflichtet, ein Passwort zu wählen, das einige Mindestanforderungen erfüllt.

- Benutzen Sie ein Passwort, das aus **mindestens acht Zeichen** besteht
- Zulässige Zeichentypen sind Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen
- Das Passwort muss aus **mindestens drei** der zulässigen Zeichentypen bestehen
- **Keine Trivialworte** oder anderweitig leicht zu erratende Worte (wie Namen, persönliche Daten, Urlaubsorte, gängige Begriffe oder Zeichenfolgen).
- Verwenden Sie keine Telefonnummern oder Nummernfolgen als Passwort.
- Halten Sie ihr Passwort geheim. Die Weitergabe von Passwörtern an Dritte ist verboten.
- Ändern Sie ihr Passwort bei dem Verdacht, dass Dritte es kennen könnten.

Damit Ihr Passwort auch für die Anmeldung am WLAN (eduroam) funktioniert, darf es keine Umlaute (ä,ö,ü,ß) und nicht die folgenden Sonderzeichen (´,`,^,§,€) enthalten.

Sollte man Passwörter irgendwo aufschreiben?

Passwörter sollten nie unverschlüsselt auf dem PC abgelegt werden, da sonst die Gefahr besteht, dass diese z.B. durch Malware bzw. Trojaner oder im schlimmsten Fall durch Diebstahl des PC bzw. der Festplatte Dritten in die Hände fallen. Auf Papier notierte Passwörter sollten an einem sicheren Ort verwart werden und sich in keinem Fall in der Nähe des PC (z.B. unter der Tastatur) befinden.

Wer sich viele Passworte merken muss, kann einen Passwortmanager wie KeePass einsetzen. Eine

Liste von Passwortmanagern finden Sie hier. Auch die Passwortmanager von Webbrowsern wie Firefox oder Google Chrome speichern Passworte verschlüsselt auf der Festplatte ab. Vorraussetzung ist hier natürlich, dass ein sicheres Master-Passwort gesetzt wird.

Was tun, wenn man sein Passwort vergessen hat?

Wenn Sie Ihr Passwort vergessen haben sollten, können Sie sich im Sekretariat des Rechenzentrum ein neues Passwort aushändigen lassen. Bitte bringen Sie dazu unbedingt Ihren Studierendenausweis bzw. ein Ausweisdokument (z.B. Personalausweis ode Reisepass) mit.