Passwortänderung für Hochschulangehörige und Lehrbeauftragte

Inhalt

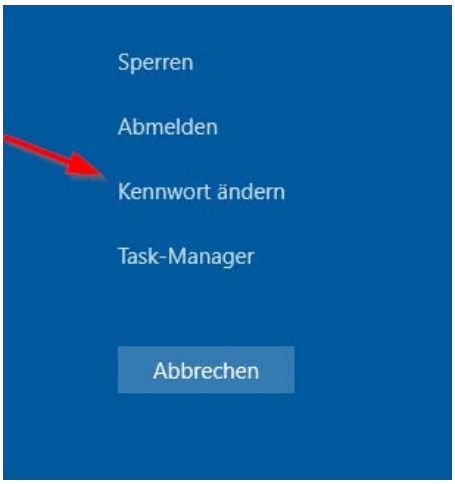
1. Allgemeine Vorbereitung der Passwortänderung

Falls Ihr **Handy** mit dem FHWS WLAN verbunden ist, setzen Sie dieses bitte **vor der Passwortänderung** in den **Flugmodus**. (Andernfalls kann es zu einer **Kontosperrung von einer Stunde** aufgrund von mehrfach fehlgeschlagenen Anmeldeversuchen kommen.)

2. Passwortänderung für Personal/Professoren

2.1. Änderung im FHWS Netz

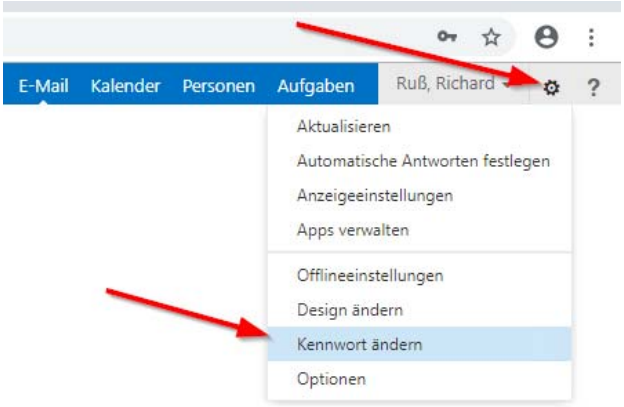
- Passwort ändern mit STRG+ALT+ENTF



- WLAN-Verbindung mit dem **neugesetzten** Passwort anpassen (Laptop + Handy)

2.2. Änderung außerhalb des FHWS Netzes

- Passwort ändern über webmail.fhws.de



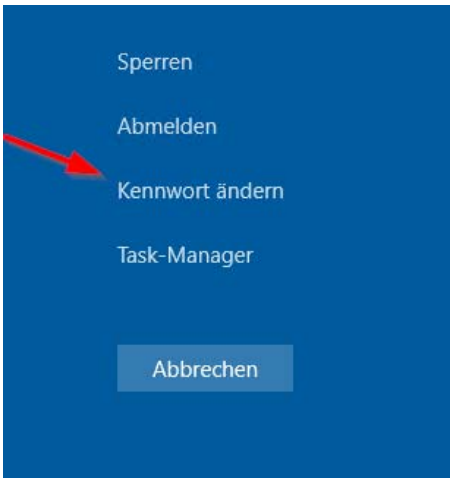
- Nach einem Neustart gilt für die Anmeldung am eigenen Gerät das **alte** Passwort, bei allen anderen FH-Diensten (E-Mail, E-Learning, usw.) das **Neue.**

Sobald das Notebook wieder im FHWS-Netz ist, **vor der Anmeldung** entweder mit dem **WLAN verbinden**, **oder** ein **LAN-Kabel anschließen**, kurz warten und sich mit dem **neugesetzten** Passwort anmelden.

- WLAN-Verbindung mit dem **neugesetzten** Passwort anpassen (Laptop + Handy)

2.3. Änderung außerhalb des FHWS Netzes bei Nutzung des VPN Zugangs

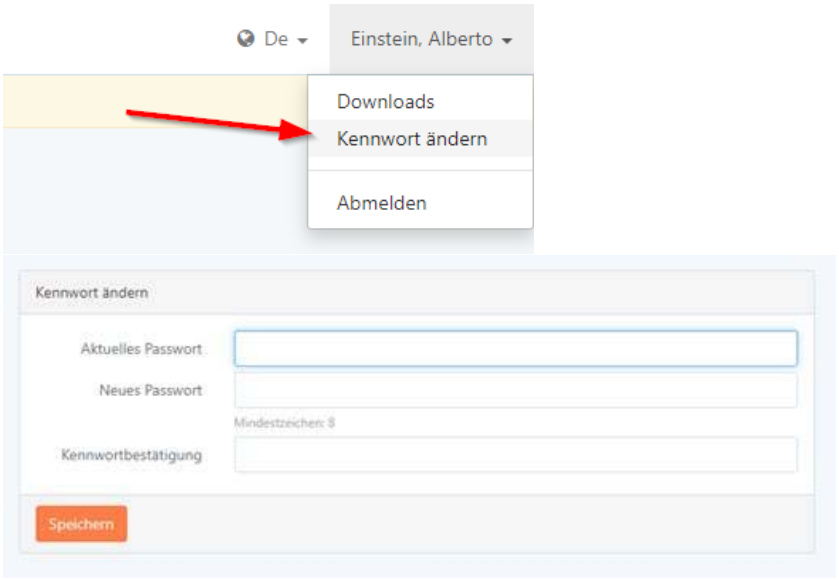
- FortiClient starten
- Passwort ändern mit STRG+ALT+ENTF



- WLAN-Verbindung mit dem **neugesetzten** Passwort anpassen (Laptop + Handy)

3. Passwortänderung für Lehrbeauftragte

- Lehrbeauftragte melden sich im LB-Portal an

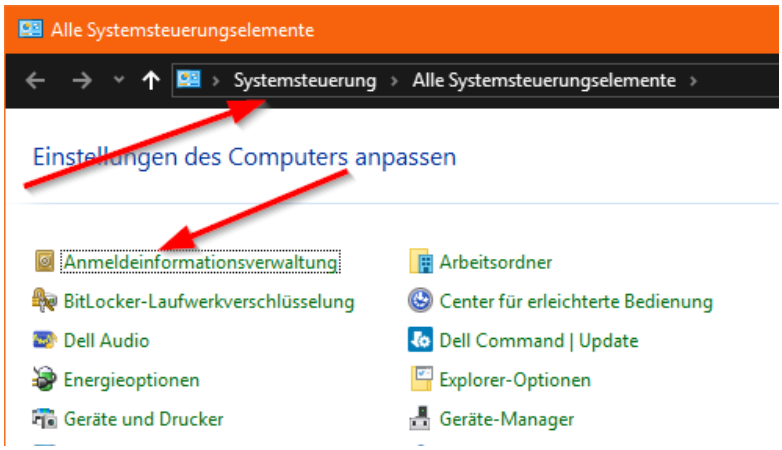


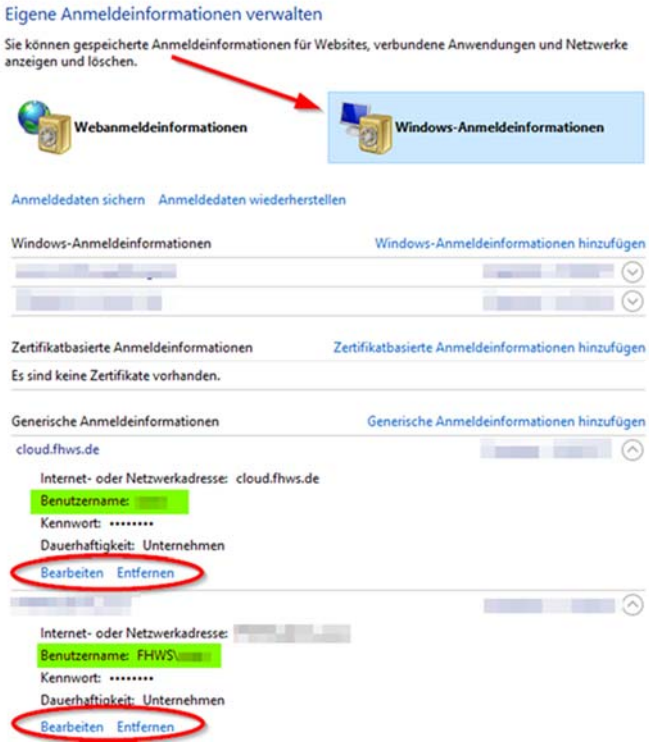
Das Passwort wird sowohl für die FHWS-Kennung, als auch für den Zugang über die private E-Mail-Adresse zum LB-Portal gesetzt!

- WLAN-Verbindung mit dem **neugesetzten** Passwort anpassen (Laptop + Handy)

4. Weitere evtl. notwendige Anpassungen

- NextCloud Client
- WLAN
- Laufwerksverbindungen zu FH-Server
- Druckerverbindungen
- Anmeldeinformationen prüfen (Datum der letzten Änderung)
  - (Systemsteuerung – Anmeldeinformationsverwaltung – Windows Anmeldeinformationen) Entweder bearbeiten oder entfernen.
    Die Einträge werden bei der nächsten Benutzung der Dienste neu angelegt.





Am Handy:

- WLAN
- E-Mail
- NextCloud App

5. Allgemeine Hinweise zur Passwortsicherheit

Das **FHWS Passwort** darf **für keinen anderen Dienst** (z.B. Facebook, private E-Mail Konten etc.) **verwendet** werden!!!

5.1. Mindestanforderung an ein Passwort

- Mindestens 8 Zeichen, wobei sich die Länge nach dem Schutzbedarf der Daten richten sollte
- Kombination aus Groß-, Kleinbuchstaben, Sonderzeichen und Ziffern (3 von 4 Kriterien sollten erfüllt sein)
- Keine Verwendung von Trivialpasswörtern, die leicht zu erraten sind (bspw. fortlaufende Ziffern, Name des Haustieres, Geburtsdatum, oder einer Kombination dieser)
- Passwort sollte nicht im Wörterbuch stehen
- Keine Fortlaufenden Passwörter (bspw. Kennwort1, Kennwort2)
- Keine gängigen Tastaturmuster (bspw. asdf, qwertz)
- Kein simples Passwort, das am Anfang und am Ende um ein Sonderzeichen ergänzt wird

Quelle: https://www.bsi.bund.de

5.2. Gestaltung eines starken Passwortes

Nutzen Sie eine wahllose Kombination aus Groß- sowie Kleinbuchstaben und Zahlen.
Beispiel: Koch + Lampenschirm + Sonne + entsprechende Zahlen = K0chL4mp3nsch1rmS0nn3

Sie können auch selbst einen Satz verschlüsseln.
Beispiel: Der Satz “Ich laufe gern einen Marathon” wird so verschlüsselt, dass von jedem Wort die letzten zwei Buchstaben genutzt und anschließend mit Zahlen kombiniert werden. Daraus ergibt sich “Chf3rn3n0n”.

5.3. Sichere Aufbewahrung

Bedenkt man die schiere Vielzahl der Passwörter, die sich ein normaler Mensch in seinem Alltag – privat und beruflich – merken muss, ist es manchmal schwierig sich alle zu merken. Außerdem ist der Mensch ein Gewohnheitstier und vernachlässigt die Verwendung von unterschiedlichen Passwörtern für jeden Login. Hier kann einem heutzutage die jedoch ebenfalls die Technik zu Hilfe kommen. Passwortsafes**,** wie KeePass**,** 1Password**,** LastPass ermöglichen die sichere Aufbewahrung von zahlreichen Passwörtern. Der Nutzer muss sich hier nur ein „Masterpasswort“ für den Passwortsafe merken und gelangt einfach zu allen anderen Passwörtern. Ansonsten sollte davon abgesehen werden, das Passwort niederzuschreiben.

6. Kontaktinformationen des Helpdesks

helpdesk.itsc@fhws.de

Öffnungszeiten: 08:00 – 16:00 Uhr

- **Helpdesk Würzburg**

  Hotline 0931 - 3511 6260

  Münzstraße 19 - Raum Z.1.07

  Röntgenring 8 - Raum A.3.08

  97070 Würzburg

- **Helpdesk Schweinfurt**

  Hotline 09721- 940 6262

  Ignaz-Schön-Straße 11 – Raum 7.1.07

  97421 Schweinfurt