Sicherheitsrisiken beim Zugang zu myFMH

Liebe myFMH-Nutzerinnen und -Nutzer

Beinahe täglich melden die Medien irgendwelche Sicherheitsvorfälle aus dem Bereich IT (Informationstechnik). Sei es, dass vertrauliche Unternehmensdaten entwendet oder Unternehmenswebseiten lahmgelegt wurden oder, dass Zugangsdaten wie Passwörter und Benutzerkontos in grossem Umfang zum Kauf angeboten werden. Beispielsweise haben Hacker folgenden Unternehmen eine erhebliche Anzahl Passwörter / Benutzerkontos gestohlen:

- Yahoo (über 500 Millionen),
- LinkedIn (über 177 Millionen)
- Dropbox (über 68 Millionen)
- Adobe (über 153 Millionen)

Sie sehen: Das Ausmass ist immens, und dabei handelt es sich hier nur um eine kleine Auswahl von betroffenen Unternehmen. Die Liste könnte beliebig erweitert werden.

Was passiert mit gestohlenen Daten?

Meist handelt es sich bei gestohlenen Daten um scheinbar wenig sensitive Informationen wie Namen, Telefonnummern und E-Mail-Adressen. Kriminelle wissen jedoch sehr wohl mit solchen Daten umzugehen und verkaufen die gestohlenen Daten zum Beispiel im Darknet an dubiose Marketingfirmen. Diese wiederum verwenden die Daten für Spam-Mails, Werbepost oder Telefonmarketing. Gestohlene Daten können auch als Grundlage für Identitätsdiebstahl dienen, indem sie mit anderen Daten (z.B. mit öffentlich zugänglichen Informationen einer betroffenen Person) verknüpft werden. So lässt sich auf einfache Weise eine Identität erstellen, die missbraucht werden kann, um sich zum Beispiel als jemand anderes auszugeben und an sensitive Informationen wie Passwörter zu gelangen.

Was können Sie tun?

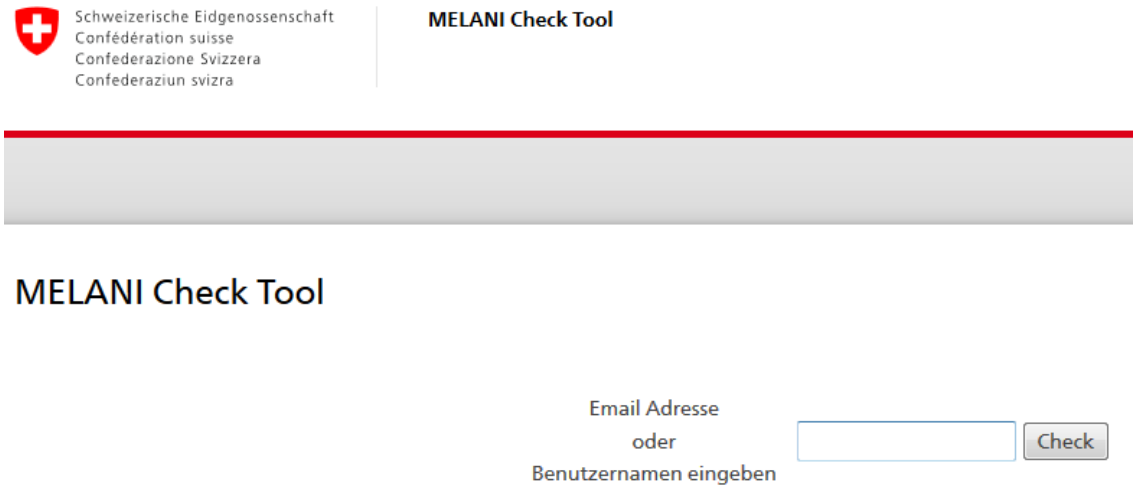
Sie leisten einen wesentlichen Beitrag zur Sicherheit Ihrer Daten, wenn Sie ein gutes Passwort verwenden und möglichst eine 2-Faktoren-Authentifizierung einsetzen. Wird z.B. Ihr Passwort gestohlen, wird noch ein zweiter Faktor benötigt, um an Ihr Benutzerkonto und Ihre Daten zu gelangen.

Ist es möglich zu prüfen, ob bereits eines meiner Benutzerkontos missbraucht wurde?

Ja, es gibt mehrere Möglichkeiten. Geben Sie dazu einen der folgenden Links im Web-Browser (z.B. Internet Explorer oder Firefox) ein:

- https://www.checktool.ch/
  (Melde- und Analysestelle Informationssicherheit Schweiz)

FMH · Verbindung der Schweizer Ärztinnen und Ärzte · Fédération des médecins suisses
Elfenstrasse 18 · Postfach 300 · CH-3000 Bern 15 · Telefon +41 31 359 11 11 · Fax +41 31 359 11 12 · info@fmh.ch · www.fmh.ch



- https://haveibeenpwned.com/
  (Webseite, die es Internetbenutzern erlaubt, zu prüfen, ob ihre Daten entwendet wurden)

Mein Benutzerkonto wurde missbraucht – was nun?

Falls Sie betroffen sind, ist es wichtig, dass Sie sofort das Passwort zum entsprechenden Benutzerkonto (z.B. myFMH oder privat verwendete Dienste wie Facebook, Yahoo oder Dropbox) ändern. **Verwenden Sie nie dasselbe Passwort für mehrere Dienste! Insbesondere darf das für myFMH gewählte Passwort nur hierfür verwendet werden (vgl. die Nutzungsbedingungen myFMH, Ziff. 5.2).**

Sie sind wichtig!

Es geht jedoch nicht nur um Passwörter / Benutzerkontos und E-Mail-Adressen, welche für Hacker interessant sind, sondern auch um andere sensible Daten, welche entwendet werden könnten. Denken Sie dabei an die Daten in myFMH, eLogbuch oder in der Standeskommissions-Datenbank. Wäre es nicht möglich, auch mit diesen Daten Schaden anzurichten? Nein, es muss nicht immer nur ein finanzieller Schaden entstehen. Es könnte sich zum Beispiel auch um einen Image-Schaden handeln. Oder wie würden Sie reagieren, wenn plötzlich auf doctorfmh.ch manipulierte Angaben zu Ihrer Person angezeigt würden?

Es ist deshalb wichtig, dass Sie sich bewusst sind, dass auch Sie ein Sicherheitsrisiko sein können. Warum? Sie besitzen die Zugangsdaten (Benutzername, Passwort) zu Applikationen und Daten. Umso wichtiger ist es, ein sicheres Passwort zu verwenden.

Was ist ein sicheres Passwort?

Folgende Punkte sind für sichere Passwörter wichtig:

- Passwörter sind persönlich und absolut vertraulich,
- werden nicht aufgeschrieben,
- enthalten Gross- und Kleinbuchstaben, Zahlen sowie Sonderzeichen,
- sind mindestens 8 Zeichen lang,
- werden jeweils nur für *einen* bestimmten Zweck eingesetzt (z.B. separate Passwörter für Privat, e-Banking sowie Beruf, etc.).

Zwei-Faktor-Authentifizierung für eine höhere Sicherheit

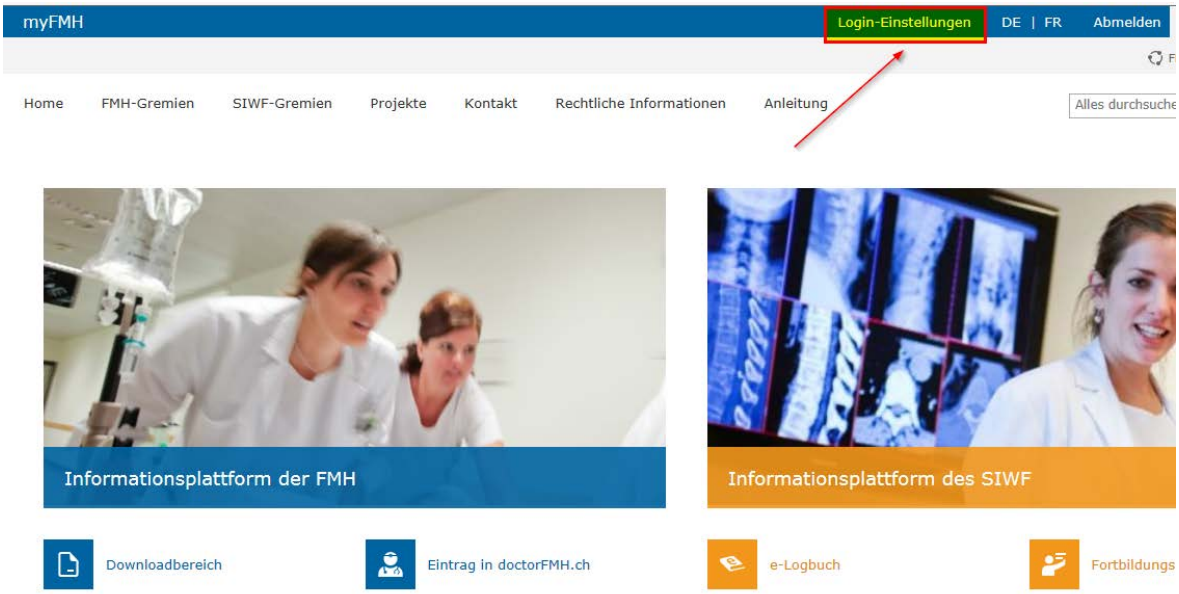
Ein gutes Passwort zu haben, ist wichtig. Besser noch ist ein Zugang mittels Zwei-Faktor-Authentifizierung, welche immer die bevorzugte Login-Variante sein sollte. Dadurch wird der Zugang für unberechtigte Personen und Kriminelle zusätzlich erschwert. Der Zugang zu myFMH ist mit den folgenden Zwei-Faktor-Authentifizierungen möglich (siehe unten):

- Passwort und SMS
- Passwort und Sicherheitscodeliste
- HIN-Client

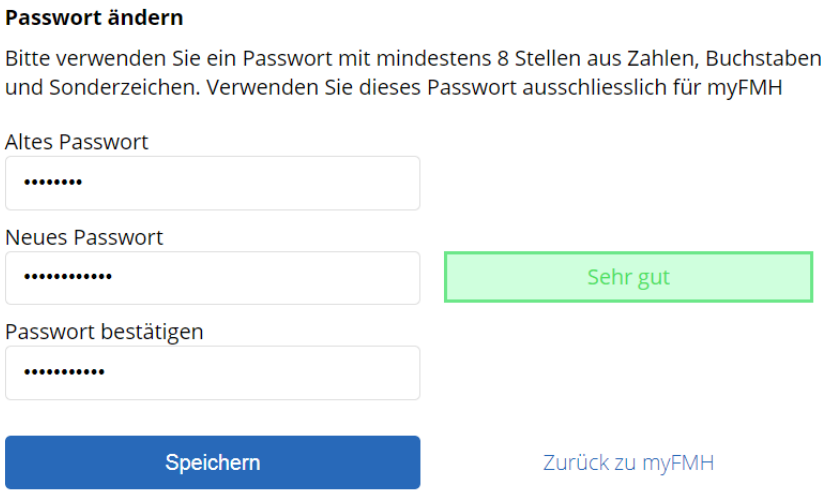
Änderung des Passwortes

Möchten Sie das Passwort auf myFMH ändern? Gehen Sie dazu wie folgt vor:

1) Loggen Sie sich über den Knopf «myFMH» (http://www.fmh.ch) ein. Der Knopf befindet sich ganz rechts und hat einen roten Hintergrund.
2) Wählen Sie den Punkt «Login-Einstellungen» (siehe folgende Abbildung).



3) Navigieren Sie zum Bereich «Passwort wechseln» (auf der Seite ganz nach unten scrollen). Klicken Sie diesen an.
4) Geben Sie ein neues Passwort ein. Die Applikation zeigt Ihnen an, ob es sich um ein gutes Passwort handelt.

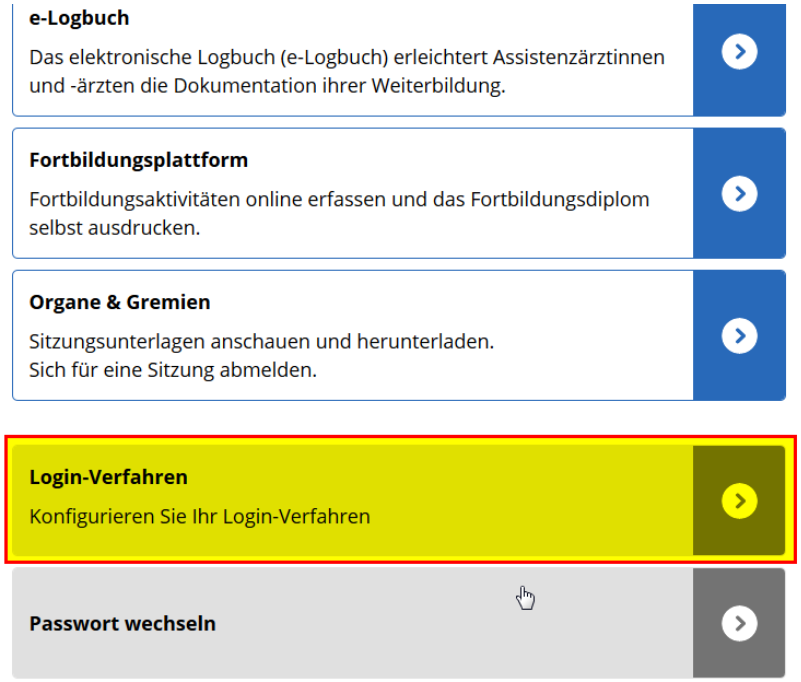


5) Speichern Sie das Passwort.

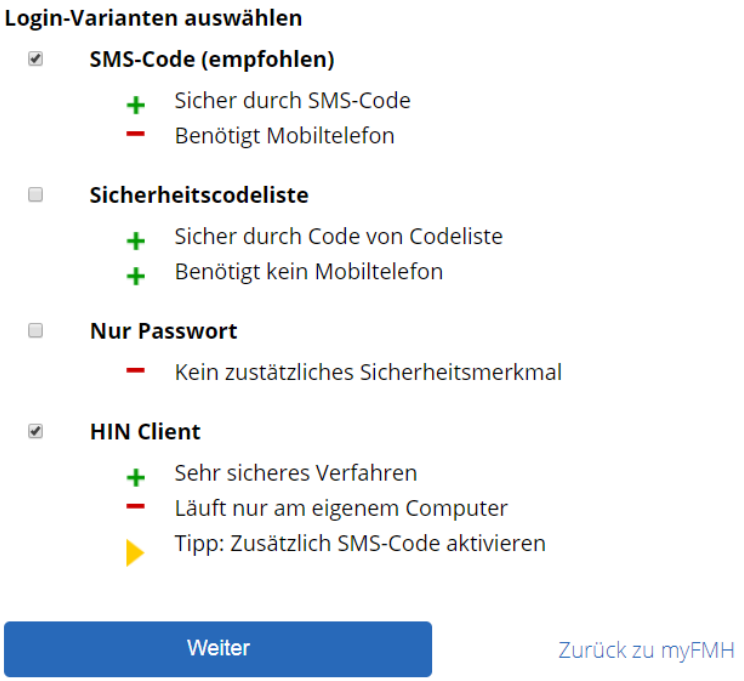
Änderung des Login-Verfahrens

Falls Sie das Login-Verfahren ändern möchten, gehen Sie wie folgt vor:

1) Loggen Sie sich über den Knopf «myFMH» (http://www.fmh.ch) ein. Der Knopf befindet sich ganz rechts und hat einen roten Hintergrund.
2) Wählen Sie den Punkt «Login-Einstellungen».
3) Wählen Sie den Menüpunkt «Login-Verfahren»:



4) Sie gelangen nun zur Seite mit der Übersicht über Ihr aktiviertes Login-Verfahren. Über den Knopf «Login-Verfahren ändern» kommen Sie zur Auswahl der vorhandenen Login-Verfahren (siehe nächste Abbildung). Wählen Sie am besten eine Zwei-Faktor-Authentifizierung.



Nur wer sich mit den Sicherheitsrisiken beschäftigt, trägt dazu bei, dass die Daten in den FMH / SIWF-Applikationen sicher sind. Also packen wir es gemeinsam an.

Kontakt:
FMH
Dienstleistungen und Mitgliedschaft
Elfenstrasse 18, Postfach 300
3000 Bern 15
Tel. 031 359 12 59