

Informationssicherheit

Die Informationssicherheit beschäftigt sich mit der Einhaltung der folgenden Sicherheitsziele: Vertraulichkeit, Verfügbarkeit und Integrität. Das bedeutet,

- dass Informationen (sowohl analoge als auch digitale) vor Einsicht der Daten gegenüber Dritten geschützt werden sollen,
- dass Informationen (möglichst) jederzeit verfügbar sein sollten und
- dass jede Änderung von Informationen nachvollziehbar sein soll.

Fabian Amon
Informationssicherheitsbeauftragter (ISB)
der Hochschule Trier

Setting Secure Passwords

Setting secure passwords isn't just important at home — it also matters at the university. Protect yourself from attacks in the university environment as well. This article covers your options for choosing, storing, and changing passwords.

Choosing a password>>>

Grundsätzlich gilt: Je länger, umso besser. Das bedeutet, dass durch die Auswahl vier verschiedener Zeichenarten (Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen) und mindestens zwölf Zeichen die Komplexität steigt. Seien Sie bei der Auswahl des Passwortes kreativ und nutzen Sie keinesfalls leicht zu erratende Passwörter. Für die Auswahl eines geeigneten Passwortes könnten Sie einen Satz wählen, aus jedem Wort des Satzes den ersten Buchstaben extrahieren und zu einem Passwort formen. Dies erleichtert Ihnen das Merken von Passwörtern.

Beispielsatz:

Ich schaue jeden Sonntagabend
im TV meine Lieblingsserie!

Beispielpasswort:

Isj3AiTmLi3!

Aus dem S wurde noch eine 3 generiert. **(VERWENDEN SIE NICHT DIESES PASSWORT!)**

Passwörter verwalten>>>

Nutzen Sie für jede Anwendung ein eigenes Passwort. Dies birgt zwar die Gefahr das Passwort zu vergessen, schützt jedoch vor systemübergreifenden Angriffen. Falls Sie eine Vielzahl an Passwörtern verwenden, nutzen Sie einen geeigneten Passwortmanager. Ein empfehlenswerter Passwortmanager hierfür ist Keepass. Einen in Internetbrowsern

integrierten Passwortmanager können wir nur empfehlen, wenn ein Master-passwort dafür eingerichtet wird. Wenn Sie sich Passwörter notieren, achten Sie darauf, dass diese nicht einsehbar sind und hinterlegen Sie die Notiz nicht an öffentlich zugänglichen Orten (wie z. B. am Monitor). Verwahren Sie auch temporäre Passwortnotizen immer sicher, z.B. in einem Tresor auf.

Passwort ändern>>>

Falls Sie Auffälligkeiten im Zusammenhang mit Ihrer Hochschulkennung feststellen, ändern Sie unverzüglich Ihr Passwort. Vergessen Sie nicht das Passwort auch zusätzlich im Passwortmanager zu ändern. Informieren Sie in diesen Fällen den untenstehenden Notfallkontakt

**Passwörter sollten mindestens 12 Zeichen lang sein.
Je länger, desto besser!**

Bitte beachten Sie außerdem auch folgende Inhalte auf den Hochschulwebseiten:

[BSI - Umgang mit Passwörtern](#) | [BSI - Passwörter verwalten mit dem Passwort-Manager](#) | [BSI - Sichere Passwörter](#)



Notfallkontakt bei IT-Vorfällen

Bei **Informationssicherheitsvorfällen** wenden Sie sich umgehend telefonisch an die: +49 651 8103-777 oder per E-Mail an: informationssicherheit@hochschule-trier.de