Informations-Sicherheit
...so einfach wie das **ABC**

ALWAYS
BE
CAREFUL

Passwort-Manager

Was starke Passwörter mit Zahnbürsten zu tun haben, konntest du im letzten Newsletter erfahren. In diesem Beitrag widmen wir uns einer Möglichkeit, **wie du Kennwörter sicher aufbewahren kannst**.

Ein wichtiger Schritt, den du zur Absicherung deiner Konten unternehmen kannst ist, dass du **ein jeweils einzigartiges starkes Kennwort für all deine Benutzerkonten und Anwendungen vergibst**. Leider ist sehr wahrscheinlich unmöglich, sich all diese Kennwörter auswendig zu merken. Aus diesem Grund kommt es immer wieder vor, dass viele Menschen nur ein einziges Passwort für alle Dienste nutzen.

Die **einfache Lösung hierfür ist die Verwendung eines Passwort-Managers**, in dem du all deine Kennwörter sicher aufbewahren kannst. Durch die Verwendung eines Passwort-Managers, oder auch Passwort-Safe genannt, ist es gar nicht mehr nötig, dass du all deine Kennwörter kennst. Du hast mit so einem Tool weiters die Möglichkeit, **starke Passwörter generieren zu lassen**.

Tipps zur Auswahl und sicheren Nutzung eines Passwort-Managers:

- Der Passwort-Manager sollte **für dich einfach benutzbar sein**. Kommt dir das jeweilige Tool zu komplex vor, such dir besser ein anderes, das zu deinen Anforderungen passt.
- Der Passwort-Safe sollte auf allen Geräten funktionieren, die du zur Eingabe von Kennwörter nutzt und sollte **eine sichere Möglichkeit bieten**, deine Kennwörter zu synchronisieren. Ob du hier auf Cloud-Provider vertraust, hängt von deinen persönlichen Anforderungen ab.
- Du solltest **nur bekannte und vertrauenswürdige Passwort-Manager nutzen**. Vorsicht also bei Produkten, die sich noch nicht lange am Markt befinden, die schlechte Bewertungen bekommen haben und die damit werben, eine eigene Verschlüsselung zu verwenden oder ein vergessenes Passwort wiederherstellen zu können.
- Wichtig bei der Auswahl des richtigen Tools ist auch, dass **eine fortwährende Wartung durch den Hersteller gewährleistet ist**. Sorg auch dafür, dass **du immer die aktuelle Version** nutzt.
- Der Passwort-Manager sollte über eine **Funktion zur automatischen Generierung** deiner Kennwörter verfügen und sollte auch **die Sicherheit deiner selbst gewählten Passwörter bewerten können**. Weiters sollte er über eine **Option** verfügen, die dir anzeigt, **ob eins deiner Passwörter kompromittiert wurde**, indem ein Abgleich mit Datenbanken wie „have i been pwned“ unterstützt wird.
- Der Passwort-Safe sollte eine **Möglichkeit** bieten, **weitere sensible Informationen** wie deine Kreditkartendaten, Sicherheitsabfragen usw. **zu speichern**.
- **Zur Absicherung des Passwort-Managers solltest du ein gutes Master-Passwort verwenden**, das du dir einfach merken kannst, für Angreifer aber schwer zu erraten ist.
- **Ein guter Passwort-Safe bietet auch die Möglichkeit zur Multi-Faktor-Authentisierung**, was die Sicherheit drastisch erhöht.
- Zu guter Letzt, leg dir **eine Sicherung deiner Passwort Datenbank** an. Denn wenn die Datenbank verloren geht, sind auch all deine Kennwörter verloren!!!

Bitte denk immer daran, **SICHERHEIT GEHT UNS ALLE AN!**