imc part of Scheer

imc My Digital School
Sichere Passwörter

Das A und O in Sachen Datensicherheit

Was haben das Einloggen am PC, die Anmeldung auf dem Social Media Profil oder das Anlegen einer E-Mail-Adresse gemeinsam? Richtig, für alle Anmeldungen braucht es einen Benutzernamen und noch wichtiger: Ein Passwort.

Für Schüler*innen gehört dies längst zur Normalität, wachsen sie doch als Generation Z im digitalen Zeitalter auf. Doch nicht immer sind sie sich den Gefahren bewusst, welchen Schaden ein unsicheres Passwort verursachen kann, sei es auf dem Computer, Smartphone oder sonstigen Accounts. Hacker brauchen oft nur wenige Minuten, um Passwörter zu knacken und an sensible Daten zu gelangen.

Daher hier einige Tipps, wie insbesondere junge Menschen für das Thema Passwörter sensibilisiert werden können und wie ein starkes Passwort aussehen sollte.

Facts

39s. Alle 39 Sekunden findet ein Cyberangriff statt

6,8 Ein 6-stelliges Passwort, das nur aus Kleinbuchstaben besteht, kann in 6,8 Sek. geknackt werden

3,2 3,2 Milliarden E-Mail-Passwort-Kombinationen wurden 2021 durch Datenlecks veröffentlicht

1

Länge

Grundsätzlich gilt: Je länger, desto besser. Ein gutes Passwort sollte mindestens zwischen zehn und zwölf Zeichen lang sein, um Angriffen standhalten zu können.

2

Komplexität

Für ein starkes Passwort sollte man möglichst viele verschiedene Zeichen nutzen. Dazu gehören neben den Sonderzeichen und Ziffern auch ein Mix aus Groß- und Kleinbuchstaben.

Tipp: Bildet einen Satz, der idealerweise Zahlen und Sonderzeichen enthält und den ihr euch leicht merken könnt. Die Anfangsbuchstaben dieses vermeintlich sinnlosen Satzes bilden dann das Passwort. Aus dem Beispielsatz „Ich esse am liebsten Kekse um 4 Uhr mittags!" würde dadurch das Passwort „IealKu4Um!" resultieren. Dieser Merksatz kann dann mit einem Wort oder einer Abkürzung für den jeweiligen Account versehen werden. Der Zugang für TikTok könnte somit aus dem Merksatz plus dem Zusatz TT bestehen, also: IealKu4Um!TT

3

Einzigartigkeit

Passwörter, die auf Namen von Familienmitgliedern, Haustieren oder den Geburtsdaten basieren, gilt es zu meiden. Auch auf gängige Varianten und Wieder-holungsmuster wie „Passwort 123" oder „1234abcd" sollte verzichtet werden.

4

Vielfalt

Für jeden Account sollten idealerweise unterschiedliche Passwörter genutzt werden. So können zum Beispiel Passwörter für verschiedene Anwendungsgruppen wie E-Mail, Streaming Dienste oder Soziale Medien generiert werden, indem die zuvor beschriebene Methode verwendet wird. Aber auch hier gilt:
Je mehr verschiedene Passwörter, desto besser.

Tipp: Es existieren eigens dafür vorgesehene Passwort-Tools, die sichere Passwörter generieren oder die Passwörter verwalten.

Fazit

Schüler*innen sind heute sowohl in der Schule als auch in ihrer Freizeit ständig im Internet unterwegs. Um private Daten zu sichern und sich selbst zu schützen, sollte ihnen der verantwortungsvolle Umgang mit Passwörtern daher möglichst früh vermittelt werden.

Quellen:

https://blog.wwo.de/look-at-it/2021/03/09/cybersicherheit-die-wichtigsten-zahlen-fakten-zu-datenschutz-verletzungen-2021/

https://www.computerwoche.de/a/passwort-vergessen-so-knacken-sie-es,1896154,2

https://www.it-daily.net/shortnews/27192-3-2-milliarden-passwoerter-wurden-gehackt-und-veroeffentlicht

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html#:~:text=Grunds%C3%A4tzlich%20gilt%3A%20Je%20l%C3%A4nger%2C%20desto,mindestens%2020%20Zeichen%20lang%20sein