Infoblatt für Schülerinnen und Schüler

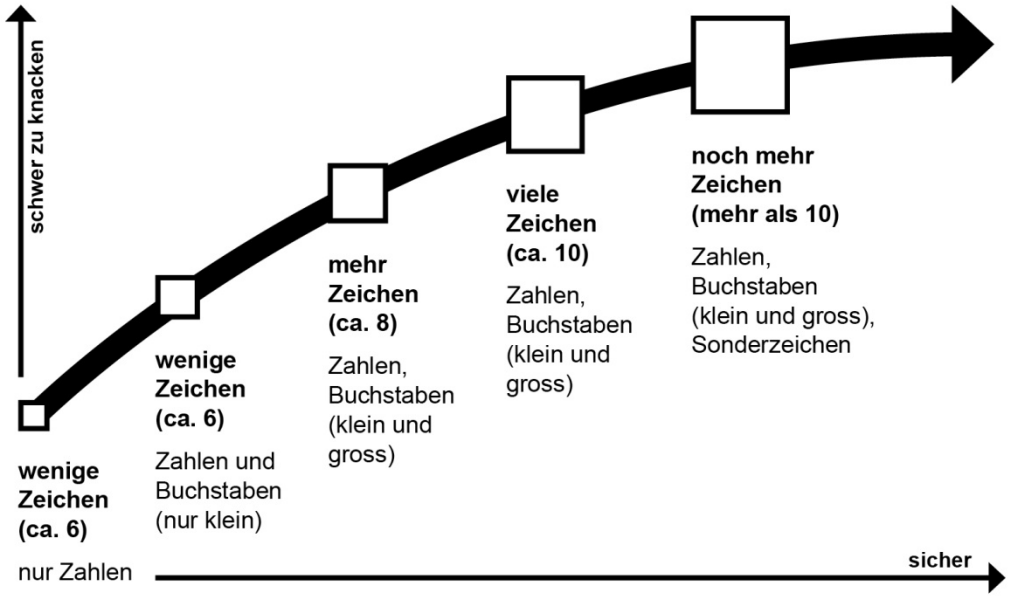
Das sichere Passwort

Bei vielen Internetseiten muss ein Benutzername und ein Passwort erstellt werden, damit man auf deren Dienste (Mail, Onlinespeicher, Fotoplattform usw.) zugreifen kann. Auf diesen Seiten oder Plattformen werden Daten von dir gespeichert, welche du vor dem Zugriff anderer schützen willst und sollst. Ein möglichst sicheres Passwort, das du für dich im Kopf behalten kannst, bietet dir Schutz.

Keinen sicheren Schutz vor Crackern[1] bieten Passwörter, welche mit dir selber zu tun haben. Das können dein Name und das Geburtsjahr oder deine Initialen sein. Ebenfalls keinen sicheren Schutz bieten Passwörter, welche aus Wörtern bestehen, die in Wörterbüchern vorkommen. Cracker lassen Computer diese Wörter durchtesten.

Cracker können aber auch Passwörter einfach knacken, die nur wenige Zeichen umfassen. Dazu nutzen sie leistungsfähige Computer, welche alle möglichen Zeichenkombinationen testen. Wenn du Zahlen, Gross- und Kleinbuchstaben, sowie Sonderzeichen in dein Passwort einbaust, erhöht sich die Anzahl Möglichkeiten rasch und der Hacker benötigt deutlich mehr Zeit, um dein Passwort herauszufinden.

Die untenstehende Abbildung zeigt auf, welche Möglichkeiten du hast, ein Passwort sicherer zu gestalten.



Als Alternative zu einem herkömmlichen Passwort bieten sich biometrische Merkmale, wie zum Beispiel der Fingerabdruck oder das Muster des Auges (Irisscan) an. Die Anmeldung mit einem biometrischen Merkmal erfordert jedoch eine Hardware, die über die entsprechenden Lesegeräte verfügt.

[1] Cracker sind Personen, die versuchen, sich unerlaubterweise Zugang zu Plattformen zu verschaffen. Sie versuchen dein Passwort zu erraten. Fälschlicherweise werden diese Personen oft als Hacker bezeichnet.