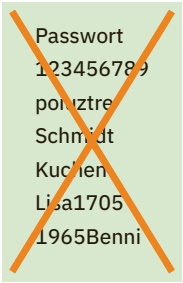
dieser Angriffsmethode der – wörtlich – »rohen Gewalt« probiert ein Programm beliebige Buchstaben- und Zahlenfolgen aus. Je kürzer ein Passwort, desto schneller ist es gehackt.

Aus den beiden genannten Szenarien ergeben sich bereits drei wichtige Regeln für die Passwortwahl:

1. Verwenden Sie keine einfachen Buchstaben- oder Ziffernfolgen wie »asdfgh« oder »12345678«.
2. Wählen Sie als Passwort keinen Begriff, der in einem Wörterbuch zu finden ist.
3. Auch wenn es wunderbar leicht zu merken ist: Ihr Name in Kombination mit dem Geburts- oder Hochzeitstag scheidet als gutes Passwort ebenfalls aus.



Das richtige Passwort finden

Tipp 002

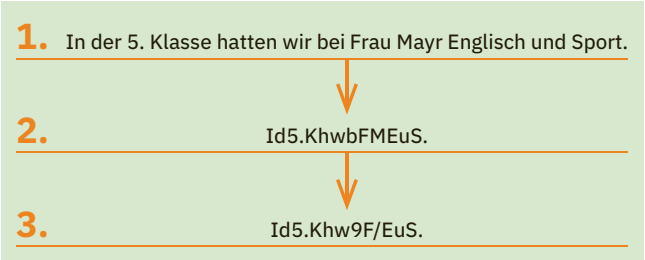
Je länger ein Passwort ist, desto besser. Ein Passwort sollte aus mindestens acht Zeichen bestehen, es dürfen aber auch gerne 14, 27 oder noch mehr Zeichen sein, sofern der jeweilige Onlinedienst, bei dem Sie sich anmelden, dies zulässt. Besonders schwierig machen Sie es Hackern, indem Sie eine Kombination aus Groß- und Kleinbuchstaben, Ziffern sowie Sonderzeichen (»§«, »/« oder auch »+«) wählen. Die Krux bei solchen Kennwörtern ist allerdings, dass man sie sich nur schwer merken kann. Mit einem kleinen Trick lässt sich aber auch dieses Problem lösen:

1. Denken Sie sich zunächst einen beliebigen Satz aus, an den Sie sich gut erinnern können. Ein Beispiel hierfür:

   »In der 5. Klasse hatten wir bei Frau Mayr Englisch und Sport.«

2. Für das Passwort wählen Sie nun z. B. den ersten Buchstaben eines jeden Wortes. Zahl und Satzzeichen behalten Sie bei. Das Ergebnis: »Id5.KhwbFMEuS.«.

3. Um das Passwort noch etwas schwieriger zu machen, können Sie einzelne Buchstaben durch Sonderzeichen oder Ziffern ersetzen, etwa das »b« durch »9« oder das »M« durch »/«. Das Passwort lautet nun: »Id5.Khw9F/EuS.«.



Bei der Passwortwahl sind Ihnen natürlich keinerlei Grenzen gesetzt. Manch einer zieht es vielleicht auch vor, mehrere Wörter einfach aneinanderzuhängen. Man spricht in diesem Fall statt von einem Passwort auch von einer *Passphrase*. Diese Variante können Sie allerdings nur bei Onlinediensten einsetzen, die sehr lange Zeichenfolgen erlauben. Passagen aus bekannten Liedern oder Gedichten sind übrigens nicht empfehlenswert, denn auch diese sind recht schnell geknackt.

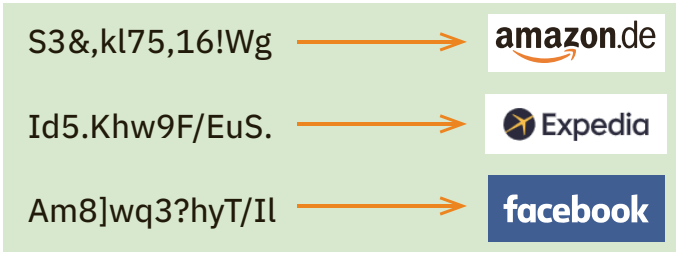
Bei der Passwortwahl Auslandsaufenthalte berücksichtigen

Wer häufig im Ausland ist und dort Computer mit landesüblichen Tastaturen nutzt, sollte dies auch bei der Passwortwahl berücksichtigen. Ein Umlaut wie »ü« oder »ä« eignet sich zwar hervorragend für deutsche Tastaturen, im Ausland gestaltet sich die Eingabe dagegen kompliziert.

Jedes Konto verdient sein eigenes Passwort

Tipp 003

Wenn man endlich ein gutes Passwort gefunden hat, könnte man es doch eigentlich gleich für alle Konten nutzen, die man im Internet anlegt? Nein, dies sollten Sie auf gar keinen Fall tun! Denn wenn es einem Hacker gelingen sollte, einen Anbieter – z. B. einen Onlineshop – zu hacken und so in den Besitz Ihres Passwortes zu gelangen, stehen ihm automatisch die Türen zu all Ihren anderen Konten offen. Da leider tatsächlich viele Anwender ein einziges Passwort für all ihre Internetaktivitäten nutzen, probieren auch Cyberkriminelle gerne aus, zu welchen weiteren Portalen ihnen das Passwort Zugang verschafft. Wählen Sie also für jedes Benutzerkonto, das Sie im Internet anlegen, ein eigenes Passwort.



Passwörter regelmäßig ändern

Tipp 004

Das Knacken eines Passwortes – und damit quasi des Schlüssels innerhalb der digitalen Welt – bleibt zunächst meist unbemerkt. Sie sollten nun nicht darauf warten, bis Sie den sicheren Beweis erhalten, dass eines Ihrer Konten gehackt wurde. Beugen Sie stattdessen lieber vor, indem Sie regelmäßig die Passwörter Ihrer Onlinekonten ändern. Dabei gilt die einfache Regel: Je sensibler die Daten sind, desto häufiger sollte das Passwort

~~Id5.Khw9F/EuS.~~

Hvn4&,L!2g/üx\1J

geändert werden. Bei einem kleinen Onlineshop, in dem Sie vielleicht einmal im Jahr bestellen, ist es ausreichend, auch nur einmal im Jahr das Kennwort zu tauschen. Bei Ihrem Onlinebankkonto sollten Sie hingegen häufiger aktiv werden.

Sinn oder Unsinn: Passwort-Checker?

Im Internet finden sich immer wieder Angebote, die Qualität eines Passwortes zu überprüfen. Solche *Passwort-Checker* sind allerdings mit größter Vorsicht zu genießen, denn es gibt keine Garantie dafür, dass Ihr eingegebenes Passwort auf den Webseiten nicht abgegriffen und anschließend für kriminelle Machenschaften genutzt wird. Geben Sie hier also auf gar keinen Fall Passwörter an, die Sie tatsächlich nutzen, sondern allenfalls abgewandelte Versionen, die den eigentlichen Passwörtern in Aufbau und Länge ähneln.

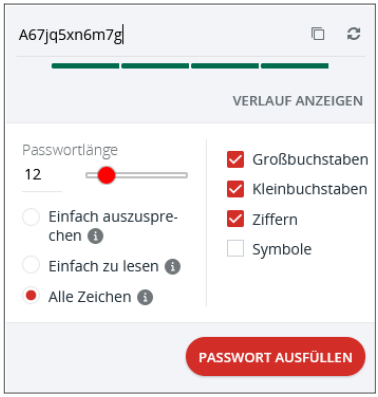
Der Passwort-Manager als Gedächtnisstütze

E-Mail-Konten, diverse Onlineshops, soziale Netzwerke, Reiseportale und dann noch Onlinebanking: Für jedes Benutzerkonto sollte ein eigenes Passwort angelegt werden, das nicht nur kompliziert, sondern auch lang ist und möglichst regelmäßig geändert wird. Hier schlägt so manch einer die Hände über dem Kopf zusammen und fragt sich, wie man sich diese Datenmengen nur merken soll. Denn notieren und als Post-it auf den Bildschirm oder unter die Tastatur kleben ist keine Option, wie Ihnen sicherlich klar ist. Eine wertvolle Hilfe stellt hier ein sogenannter *Passwort-Manager* dar.

Die Vorteile eines Passwort-Managers

Tipp 005

Ein Passwort-Manager unterstützt Sie bereits bei der Generierung sicherer Passwörter und erleichtert Ihnen später auch die Eingabe der Zugangsdaten (Benutzername und Passwort) in den Anmeldeformularen der Onlinedienste. Die Zugangsdaten werden im Passwort-Manager verschlüsselt gespeichert, das Programm wiederum wird mit einem Master-Passwort geschützt. Dieses Passwort ist das einzige, das Sie sich wirklich merken müssen. Vergessen Sie es, haben Sie keinen Zugriff mehr auf die im Passwort-Manager gespeicherten Zugangsdaten. Das Master-Passwort legen Sie selbst direkt nach der Installation des Programms fest. Dabei gelten die bereits zuvor beschriebenen Anforderungen: Das Passwort sollte möglichst kompliziert und lang sein.



Cloudbasiert oder lokal

Tipp 006

Passwort-Manager lassen sich grob in zwei Kategorien aufteilen: Die einen speichern die Datenbank mit den verschlüsselten Passwörtern auf den Servern des Anbieters oder in einer alternativen Cloud. Bei den anderen wird die Passwort-Datenbank (auch *Tresor* oder *Vault* genannt) lokal auf der Festplatte des Geräts gespeichert, auf dem auch der Passwort-Manager installiert ist. Der Vorteil der cloudbasierten Tools ist, dass Sie bequem von verschiedenen Geräten (z. B. PCs, Tablets oder auch Smartphones) aus auf Ihre Zugangsdaten zu den Onlinekonten zugreifen können (lesen Sie hierzu auch den