Foto: stokkete/Adobe Stock

Auch das eigene Lieblingsessen wie eine Pizza Margherita kann als Ideengeber für ein sicheres Passwort herhalten

Was hat Pizza mit Passwort zu tun?

Wer die Wahl hat, hat bekanntlich auch die Qual. Und besonders bei der Wahl von sicheren Passwörtern tun sich viele Internetnutzer schwer. Dabei gibt es zahlreiche Tools und Tipps, die helfen.

Im jährlichen Ranking um das schlechteste Passwort, das die Deutschen trotz aller Warnungen von Experten nach wie vor am häufigsten wählen, lag auch im vergangenen Jahr die Zahlenfolge „123456" klar auf dem ersten Platz. Aber auch die auf Tastaturen aneinandergereihte Buchstabenfolge „qwertz" oder einfach das Wort „Passwort" – gerne auch in der englischen Version „Password" – liegen nach wie vor im Trend. Dass diese Passwörter für den Unternehmenscomputer, aber auch für den E-Mail-Account, das Pay-Pal-Konto oder diverse Online-Shops nicht sicher sind, wissen sicher die meisten Internetnutzer. Und trotzdem hoffen sie einfach – wohl aus Bequemlichkeit –, dass sie ein Hackerangriff nicht trifft.

Das ist aber ein gefährlicher Trugschluss: Hacker haben Werkzeuge, die vollautomatisch alle möglichen Zeichenkombinationen ausprobieren, ganze Wörterbücher einschließlich gängiger Kombinationen aus Worten und angefügten Zahlen testen oder einmal im Internet veröffentlichte Zugangsdaten bei allen möglichen Diensten durchprobieren. Um das zu verhindern, sollte ein Passwort bestimmte Qualitätsanforderungen erfüllen und immer nur für einen Zugang genutzt werden, rät unter anderem das Bundesamt für Sicherheit in der Informationstechnik (BSI). Welche Anforderungen das genau sind, zeigt der Infokasten auf Seite 35.

Lange Zeit galt die Empfehlung, dass Internetnutzer ihre Passwörter in regelmäßigen Abständen ändern sollten, um es Hackern besonders schwer zu machen. Mittlerweile wurde diese Handlungsanweisung aber von den meisten Sicherheitsbehörden wie dem BSI revidiert. Denn durch die regelmäßigen Änderungen hatten viele Nutzer ihre Codes eher geschwächt, um sie sich leichter merken zu können. Besser sei es also, komplizierte Passwörter zu wählen, die man dann auch langfristig nutzen kann.

> Das **Masterpasswort** ist der **Schlüssel** zu allen Log-ins, die der **Nutzer hinterlegt** hat.

Das ist ein sicheres Passwort

Bei der Wahl eines Passwortes sind der eigenen Kreativität keine Grenzen gesetzt. Das BSI gibt hierfür ein eingängiges Beispiel: Wer Pizza mit extra Käse mag, kann sich einen Satz wie „**A**m **l**iebsten **e**sse **i**ch **P**izza **m**it **vier Z**utaten **und e**xtra **K**äse**!**" ausdenken. Denn solche oder ähnliche für den gemeinen „Pizzaliebhaber" einfach zu merkende Sätze können der Schlüssel für ein sicheres Passwort sein. Dafür sollten sich Internetnutzer den ersten Buchstaben eines jeden Wortes merken und siehe da, das sichere Passwort zu diesem Merksatz lautet: AleiPm4Z+eK!. Am besten ist es, so raten es unter anderem auch die Experten der Verbraucherzentrale, solche Sätze frei zu erfinden und keine zu wählen, die man irgendwo vielleicht schon einmal gelesen hat. Ein kleiner Tipp: Als Gedankenstütze können die Passwörter auf Zetteln notiert werden, die jedoch immer an einem geschützten

Ort aufzubewahren sind und für andere – dazu gehören auch die Familienangehörigen – nicht frei zugänglich sein sollten.

Auch wenn das eine oder andere Passwort für den Otto Normalverbraucher durchaus schwer nachzuvollziehen und vor allem zu entschlüsseln ist, sollte man die Codes möglichst nicht für mehrere Dienste gleichzeitig verwenden. Denn ist einmal ein Code entschlüsselt, haben Hacker genug Tools zur Verfügung, um in Windeseile die Passwörter auf allen gängigen Homepages durchzuprobieren.

Passwort-Manager helfen

Sichere Passwörter für alle Online-Konten sind also essenziell, damit hochsensible Unternehmensdaten nicht in die falschen Hände geraten. Dennoch fällt es vielen Menschen im Alltag schwer, sich die komplexen und langen Passwörter zu merken. Klar, Merksätze, wie oben beschrieben, können eine kleine Stütze sein. Sie werden aber dennoch schnell vergessen, wenn man pro Internetdienst ein neues Passwort benötigt.

Abhilfe kann da ein Passwort-Manager schaffen. Er hilft, die Zugangsdaten für die verschiedenen Dienste sicher zu verwalten. Mittels Verschlüsselung und eines komplexen Masterpassworts verwahren die Passwort-Manager alle Passwörter des Nutzers sicher auf. „Sie funktionieren ähnlich wie ein Notizbuch, das in einer Schublade eingeschlossen ist und dessen Inhalte somit nur für den Besitzer einsehbar sind", schreibt das BSI. Dabei liegen die Vorteile solcher Tools klar auf der Hand: Sie verwahren nicht nur die Passwörter, sondern unterstützen auch bei der Passwortvergabe, warnen vor gefährdeten Websites oder möglichen Phishing-Attacken und lassen sich auf mehreren Geräten zur einfacheren Handhabung synchronisieren.

Wenn Fuhrparkleiterinnen oder Fuhrparkleiter einen Passwort-Manager nutzen wollen, müssen sie zunächst ein zentrales Passwort wählen, mit dem sich die Software starten und die gespeicherten Passwörter anzeigen lassen. Dieses sogenannte Masterpasswort ist das einzige, aber auch das wichtigste Passwort, das sich die Nutzer merken müssen. „Es ist quasi der Schlüssel zum digitalen Schlüsselkasten", bringt es die Stiftung Warentest, die im vergangenen Jahr 2020 insgesamt 14 Passwort-Manager getestet hat, auf den Punkt. Der Rest läuft mehr oder weniger automatisch: Ruft der Nutzer eine Homepage auf, vergibt der Passwort-Manager das für diese Internetseite passende Passwort und loggt den Nutzer ein.

> Hacker haben **vielerlei Werkzeuge**, um leichte Passwörter schnell zu **entschlüsseln**.

Empfehlenswerte Systeme

Das Ergebnis des Stiftung Wartentest-Tests spricht eine klare Sprache: Schon kostenlose Dienste schnitten gut ab, aber wer mehr bezahlt, bekommt in der Regel auch mehr geboten.

Dennoch hat es ein komplett kostenloses Tool in die Top drei der Bewertung geschafft: **KeePass**. Es bietet laut Testurteil genau das, was man von einem Passwort-Manager erwartet. Als Testsieger bei Stiftung Warentest ging **Keeper** hervor. Kleiner Nachteil: Diesen Manager gibt es nur gebührenpflichtig im Abo. Auf den zweiten Platz hat es im Test das Programm **1Password** geschafft. Es bietet zwar eine kostenlose Variante, allerdings mit einem deutlich geringeren Funktionsumfang, so die Tester. *Theresa Siedler*

Tipp

Sechs Regeln für gute Passwörter

1. Ein Passwort sollte mindestens zehn Zeichen lang sein.
2. Es sollte aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen und nicht in einem Wörterbuch zu finden sein oder mit Ihnen und Ihrer Familie in Zusammenhang stehen. Verwenden Sie also keine Namen, Geburtsdaten, Telefonnummern oder Ähnliches.
3. Es sollte keine bloße Zahlenfolge, alphabetische Buchstabenfolge oder eine Reihe benachbarter Tasten auf der Tastatur darstellen.
4. Je sensibler ein Zugang ist (etwa beim Online-Banking), umso mehr Sorgfalt sollten Sie bei der Auswahl eines starken Passwortes walten lassen. Falls der Anbieter keine Zeichenbegrenzung für das Passwort vorsieht, gilt: Je länger, desto besser!
5. Wählen Sie nicht ein Passwort für alle Portale, sondern legen Sie mindestens für die wichtigsten und meist genutzten Dienste eigene Passwörter an.
6. Ändern Sie das Passwort, wenn es Ihnen von einem Anbieter übermittelt wurde und Sie sich das erste Mal dort angemeldet haben. Weitere Gründe zum Ändern des Codes wären, dass Ihr Online-Dienstleister Sie dazu auffordert, große Datenlecks öffentlich werden oder Ihr Gerät mit Schadsoftware infiziert worden ist.

Quelle: Verbraucherzentrale