



Zu viele nutzen dasselbe Passwort für mehrere Dienste

Viele Internetnutzer setzen in Bezug auf Passwörter mehr auf Bequemlichkeit als auf Sicherheit. So nutzen 36 Prozent in Deutschland für mehrere Online-Dienste das gleiche Passwort.

Die Mehrheit beschäftigt sich aber damit, sichere Passwörter zu verwenden. Fast zwei Drittel sagen: Ich achte bei der Erstellung neuer Passwörter auf einen Mix aus Buchstaben, Zahlen und Sonderzeichen.

Drei von zehn Internetnutzern (31 Prozent) ändern ihre Passwörter in regelmäßigen Abständen.

Acht Prozent sagen, dass sie einen Passwort-Generator beziehungsweise einen Passwort-Safe zur Erstellung und Verwaltung ihrer Passwörter nutzen.

Teresa Ritter, Bitkom-Expertin für IT-Sicherheit, erklärt:

🗨️ **Lange Wörter mit unterschiedlichen Zeichen – das ist eine einfache Faustregel für gute Passwörter.“**

Einen perfekten Schutz vor Cyberkriminellen bieten auch die längsten Passwörter nicht. Doch Cyberattacken werden deutlich erschwert.

Trick für sichere Passwörter

Je komplexer das Passwort, desto höher der Schutz. Trotzdem werden im Alltag oft simple Passwörter genutzt. Mit einem Trick lassen sich auch schwierige Passwörter leicht merken, indem clevere Eselsbrücken eingesetzt werden. Um Passwörter mit Buchstaben, Zahlen und Sonderzeichen

zu generieren, werden dafür die Anfangsbuchstaben von ausgedachten Sätzen genommen, etwa: „Mein Verein gewann das entscheidende Spiel mit 3 zu 2!“ Daraus lässt sich ein sicheres und gut zu merkendes Passwort erstellen: „MVgdeSm3z2!“.

Der Passwort-Manager als Kennwort-Tresor

Passwort-Manager speichern alle genutzten Kennwörter in einer verschlüsselten Datei. Nutzer müssen sich nur noch ein Passwort merken, das Master-Passwort. Dieses Passwort sollte höchste Standards erfüllen. Einmal eingegeben, erlangt man Zugang zu allen gespeicherten Kennwörtern.

Einige Programme bieten sogar die Möglichkeit, nicht nur Passwörter, sondern auch die dazugehörigen Benutzernamen zu speichern. Auf Wunsch füllen die Programme die abgefragten Felder beim Login automatisch aus.

Doppelte Sicherheitsstufe

Einige Dienste bieten mittlerweile Mehr-Faktor-Authentifizierungen an. Der Nutzer muss dann mehr als eine Sicherheitsabfrage beantworten, um auf einen Account zuzugreifen. Dazu erhält man nach der Passwortabfrage

beispielsweise eine SMS auf das Mobiltelefon mit einem Code. Parallel erscheint ein Feld, das den übermittelten Code abfragt. Sofern verfügbar, sollte diese Option aktiviert werden.

Updates: Immer auf dem neuesten Stand

Ohne einen aktuellen Virenschanner kann es sehr gefährlich sein, sich im Internet zu bewegen – gleich ob per Desktop-Computer oder Smartphone. Umso wichtiger ist es, die Virensoftware immer aktuell zu halten. Nutzer sollten die Update-Hinweise ihrer Virensoftware ernst nehmen. Gleiches gilt für das Betriebssystem, den Browser, Add-Ons und die anderen Programme.

Augen offen halten

Beim Phishing verschicken Betrüger gefälschte Mails mit Links zu Online-Händlern, Bezahlendiensten, Paketdiensten oder sozialen Netzwerken. Oberstes Gebot: den gesunden Menschenverstand nutzen. Banken und andere Unternehmen bitten ihre Kunden nie per E-Mail, vertrauliche Daten im Netz einzugeben. Diese Mails sind am besten sofort zu löschen. Das Gleiche gilt für E-Mails mit unbekanntem Dateianhang oder verdächtigen Anfragen in sozialen Netzwerken.

Backups einrichten

Durch regelmäßige Sicherungskopien, auch Backups genannt, bleiben persönliche Daten auch dann erhalten, wenn Geräte defekt sind oder verloren gehen. Die gesicherten Daten lassen sich anschließend auf einem neuen Gerät problemlos wiederherstellen. Daten-Backups lassen sich per Synchronisation mit einem Heim-PC aufspielen, mit Hilfe eines Massenspeichers wie einer Micro-SD-Karte oder über Cloud-Speicher.

Versicherungs- und Finanznachrichten

expertenReport



<https://www.experten.de/id/4918854/zu-viele-nutzen-dasselbe-passwort-fuer-mehrere-dienste/>