

# Zahlen bitte! 123456 ... Dein Passwort ist meins!

[Originalartikel](#)

[Backup](#)

<html> <p class=„printversionback-to-article printversion-hide“><a href=„<https://www.heise.de/newsticker/meldung/Zahlen-bitte-123456-Dein-Passwort-ist-meins-3951841.html>“>zur&#252;ck zum Artikel</a></p><figure class=„printversionlogo“><img src=„<https://1.f.ix.de/icons/svg/logos/svg/heiseonline.svg>“ alt=„heise online“ width=„180“ height=„40“/></figure><figure class=„aufmacherbild“><img src=„[https://heise.cloudimg.io/width/700/q75.png-lossy-75.webp-lossy-75.foil1/\\_www-heise-de\\_/imgs/18/2/3/5/9/1/5/3/zahlenbitte\\_123456-af288bbe83b45a5c.png](https://heise.cloudimg.io/width/700/q75.png-lossy-75.webp-lossy-75.foil1/_www-heise-de_/imgs/18/2/3/5/9/1/5/3/zahlenbitte_123456-af288bbe83b45a5c.png)“ alt=„Zahlen bitte! Das Problem mit der &quot;123456&quot;“/></figure><p><strong>Am 1. Februar ist „&#196;ndere-dein-Passwort-Tag“ - ein Tag, der auf die wichtige Passwortsicherheit aufmerksam machen m&#246;chte. Und das ist offenbar auch n&#246;tig, solange „123456“ das beliebteste Passwort der Deutschen ist.</strong></p> <p>Unser Leben verlagert sich zunehmend ins Digitale und findet zu einem gro&#223;en Teil online statt: Wir gehen bei Amazon und Co. shoppen, schauen Serien und Filme bei Netflix und erledigen &#220;berweisungen und Geldgesch&#228;fte online. Immer mehr private Daten sind im Netz unterwegs und somit potenziell aussp&#228;hbar. Sichere Passw&#246;rter zu benutzen, wird daher immer wichtiger.</p> <h5 id=„nav\_1234561“><strong>123456 beliebtestes Passwort der Deutschen</strong></h5> <p><strong>Trotzdem stehen die Passw&#246;rter „123456“, „hallo“ und „passwort“ auch in der j&#252;ngsten Studie des Hasso-Plattner-Instituts (HPI) weiterhin ganz oben auf der Beliebtheitsliste deutscher Internetnutzer[1]</strong>. Auch Namen von Haustieren oder Geburtsdaten sind nach wie vor beliebt, k&#246;nnen aber mit einer W&#246;rterbuchattacke ebenso leicht geknackt werden. Dar&#252;ber hinaus sind durch <strong>Rekorddatenlecks bei Yahoo[2]</strong> &amp; Co. Milliarden Namen/Passwort-Kombinationen ins Netz gesp&#252;lt worden. Ob Ihre Konten betroffen waren, k&#246;nnen Sie zum Beispiel mit dem <strong>Identity Leak Checker des HPI[3]</strong> herausfinden.</p> <p>Da die Menschen auch international wenig kreativ sind, wenn es um die Verschl&#252;sselung Ihrer Online-Accounts geht, riefen die Technik-Blogs Gizmodo und Lifehacker 2012 zum ersten „Change your password“-Tag auf.</p> <h5 id=„nav\_gutes2“><strong>Gutes Passwort, schlechtes Passwort</strong></h5> <p>Denn ein schwer zu knackendes Passwort zu finden, ist gar nicht so kompliziert. Besonders wichtig: Passw&#246;rter d&#252;rfen nicht einfallslos sein. Sie sollten Buchstaben, Ziffern und Zeichen enthalten und m&#246;glichst lang sein. Au&#223;erdem sollte f&#252;r jeden Online-Account ein anderes Passwort verwendet werden &#8211; denn wurde ein Passwort geknackt, dann haben Hacker direkt auch noch Zugriff auf alle Konten, die mit dem gleichen Passwort „gesch&#252;tzt“ sind. Mittlerweile fordern viele Webseiten ein komplexeres Kennwort mit Zeichen, Buchstaben und Ziffern von Ihren Nutzer &#8211; aber eben noch nicht alle. <strong>Wie Sie sich selbst ein gutes Passwort ausdenken, erkl&#228;ren wir Ihnen in dieser Anleitung.[5]</strong></p> <p>Neben unsicheren Passw&#246;rtern birgt auch das Abspeichern der Anmeldedaten auf dem PC oder Smartphone Gefahren. Die Funktion ist zwar praktisch, allerdings k&#246;nnen so auch Unbefugte Zugang zu Ihren Kunden-Konten und wom&#246;glich auch Zahlungsdaten bekommen. Wenn Sie auf das Abspeichern Ihrer Anmeldedaten dennoch nicht verzichten wollen, <strong>sollte die Zwei-Faktor-Authentifizierung genutzt werden, die immer mehr Online-Dienste anbieten.[6]</strong> <strong><br/></strong></p> <h5 id=„nav\_passwort3“><strong>Passwortmanager helfen beim Merken</strong></h5> <p>Wer keine Lust hat, sich f&#252;r jeden Dienst ein einfallsreiches Passwort mit Buchstaben, Ziffern und Zeichen auszudenken, ist ein Kandidat f&#252;r einen Passwortmanager. Dort k&#246;nnen alle Passw&#246;rter wie in einem Tresor abgelegt werden. Der Clou: Man braucht sich nur noch ein

einziges Master-Passwort merken, um Zugriff auf alle anderen Passwörter zu erhalten. Passwortmanager gibt es als Online- oder Offline-Lösung. Wie Passwortmanager funktionieren und wie man sie benutzen kann, haben wir hier zusammengefasst.[7] Aber auch dann ist Vorsicht geboten: Immer wieder werden Schwachstellen in Passwortmanagern gefunden[8], aber die Angreifer Passwörter auslesen können. (anka[9])

URL dieses Artikels: <http://www.heise.de/-3951841>

Links in diesem Artikel:

- [1] <https://www.heise.de/security/meldung/Zahlenfolge-123456-immer-noch-beliebtestes-Passwort-in-Deutschland-3927009.html>
- [2] <https://www.heise.de/meldung/Rekordhack-bei-Yahoo-war-drei-Mal-so-gross-3849303.html>
- [3] <https://sechpi.de/ilc/>
- [4] <http://www.heise.de/thema/Zahlen-bitte!>
- [5] <https://www.heise.de/tipps-tricks/Sicheres-Passwort-finden-so-klappt-s-3836799.html>
- [6] <https://www.heise.de/security/artikel/Uebersicht-Diese-Webseiten-bieten-Zwei-Faktor-Authentifizierung-3940341.html>
- [7] <https://www.heise.de/tipps-tricks/Passwortmanager-So-verwalten-Sie-Ihre-Passwoerter-3934582.html>
- [8] <https://www.heise.de/security/meldung/Windows-10-Luecke-in-vorinstalliertem-Passwort-Manager-Keeper-gibt-Kennwoerter-preis-3921316.html>
- [9] <mailto:anka@heise.de>

Copyright © 2018 Heise Medien

From: <https://schnipsel.qgelm.de/> - Qgelm

Permanent link: [https://schnipsel.qgelm.de/doku.php?id=wallabag:zahlen-bitte\\_-123456-...-dein-passwort-ist-meins](https://schnipsel.qgelm.de/doku.php?id=wallabag:zahlen-bitte_-123456-...-dein-passwort-ist-meins)

Last update: 2021/12/06 15:24

