verbraucherzentrale
Rheinland-Pfalz

PASSWÖRTER BEI ONLINE-DIENSTEN

Marktcheck der Verbraucherzentrale Rheinland-Pfalz, August 2018

PASSWÖRTER BEI ONLINE-DIENSTEN

Informationen und Tipps zu sicheren Passwörtern

Inhalt

1. Einleitung

1,4 Milliarden Nutzernamen mit Klartext-Passwörtern sollen im Darknet aufgetaucht sein, so der Sicherheitsanbieter 4iQ im Dezember 2017[1]. Das bedeutet, dass diese Daten von Nutzerinnen und Nutzern nun für Hacker und Betrüger relativ leicht zugänglich sind.

Sicherheitslecks auf Seiten der Anbieter führen immer wieder zu gestohlenen Zugangsdaten. Gleichzeitig geschieht es aber auch, dass Online-Konten von Verbraucherinnen und Verbrauchern trotz guter Sicherheitseinstellungen geknackt werden. Hier ist die Sicherheitslücke fast immer ein zu schwaches Passwort.

Das Hasso-Plattner-Institut (HPI) der Universität Potsdam forscht intensiv zu IT-Systemen. Regelmäßig analysieren die HPI-Expertinnen und Experten Nutzerdaten von deutschen E-Mail-Adressen und erstellen daraus eine Liste der meistgenutzten Passwörter in Deutschland. Die Untersuchungen zeigen, dass die meisten Nutzerinnen und Nutzer immer noch schwache und unsichere Passwörter verwenden.[2] So belegte beispielsweise die sehr unsichere Ziffernfolge „123456“ auch im Jahr 2017 den ersten Platz dieser Liste.

Laut HPI lauten die zehn beliebtesten Passwörter in Deutschland:

- 123456
- 123456789
- 1234
- 12345
- 12345678
- hallo
- passwort
- 1234567
- 111111
- hallo123

Diese Passwörter sind alle unsicher und schwach und bieten ein Einfallstor für Hacker und Kriminelle. Sie ermöglichen Zugriff auf Online-Konten und damit auf persönliche Informationen. Die Aufklärung von Verbraucherinnen und Verbrauchern über die Wichtigkeit guter Passwörter ist daher unverzichtbar. Zusätzlich ist es nach Auffassung der Verbraucherzentrale aber auch zwingend erforderlich, dass Online-Händler und sonstige Diensteanbieter die Nutzerinnen und Nutzer bei der Auswahl eines sicheren Passwortes unterstützen und sie anleiten, wenn sie ein Nutzerkonto einrichten.

Um zu überprüfen, welche Hilfestellung Verbraucherinnen und Verbraucher hierbei von Diensteanbietern bekommen, hat die Verbraucherzentrale im Frühjahr 2018 die Vorgaben und Empfehlungen bei insgesamt 141 Anbietern untersucht, davon bei

- 95 Online-Shops
- 33 E-Mail-Diensten

---

[1] https://www. zdnet.de/88320851/14-milliarden-nutzernamen-mit-klartext-passwoertern-im-darkweb-aufgetaucht/

[2] https://hpi.de/pressemitteilungen/2017/die-top-ten-deutscher-passwoerter.html

- 13 Social-Media-Anbietern.

Die Verbraucherzentrale hat geprüft, ob diese bei der Einrichtung von Nutzerkonten zwingende Vorgaben hinsichtlich der Länge und Ausgestaltung von Passwörtern machen.

1.1 Paradigmenwechsel bei den Empfehlungen für sichere Passwörter

Werden Passwörter geknackt, geschieht das heute meist automatisiert. Mit leistungsstarken Rechnern und entsprechenden Programmen werden alle möglichen Zeichenkombinationen ausprobiert, Inhalte von Wörterbüchern sowie gängige Wort-Zahl-Kombinationen getestet und auch bereits gestohlene und im Internet veröffentlichte Zugangsdaten ausprobiert. Kurze Passwörter oder solche, die aus Wörtern oder beliebten Zeichenkombinationen bestehen, bieten daher keinen bis wenig Schutz bei Angriffen.

Empfehlungen der US-Standardbehörde NIST

Nach den früheren Empfehlungen der US-Technologie-Standardbehörde NIST (National Institute of Standards and Technology) sollte ein sicheres Passwort aus mindestens sechs bis acht Zeichen, kleinen und großen Buchstaben, Zahlen und Sonderzeichen bestehen und alle 90 Tage geändert werden. Das empfohlene regelmäßige Wechseln von Passwörtern führte jedoch nicht zu mehr Sicherheit, sondern eher dazu, dass Nutzerinnen und Nutzer ihr Passwort lediglich geringfügig änderten, um es sich auch nach dem Wechsel noch merken zu können. Sie tauschten allenfalls einzelne Zeichen aus, beispielsweise „e“ durch „3“, „s“ durch „$“ oder „l“ durch „!“. Das Ausgangspasswort bleibt jederzeit auf den ersten Blick erkennbar. Damit können auch neue Varianten ohne Aufwand gehackt werden. Die große Anzahl an benötigten Passwörtern führt auch dazu, dass viele ein einziges Passwort für mehrere Anwendungen verwenden.

Im Jahr 2017 gab es bei den Empfehlungen zur Passwortsicherheit des NIST einen Paradigmenwechsel. Die Devise lautet jetzt: weniger Komplexität, dafür ein längeres Passwort wählen.

Das NIST empfiehlt jetzt, Passwörter möglichst lang zu gestalten und am besten aus mehreren Wörtern zusammenzusetzen – idealerweise mit Leerzeichen dazwischen. Diese Variante nennt man auch Passphrase.

Empfehlungen des Bundesinstituts für Sicherheit in der Informationstechnik

Die Empfehlungen des Bundesinstituts für Sicherheit in der Informationstechnik (BSI) sehen ähnlich aus: je länger, desto besser. Mindestens acht Zeichen sollten Passwörter aber auf jeden Fall haben und sie sollten nicht in Wörterbüchern vorkommen. Das BSI empfiehlt, für ein Passwort „alle verfügbaren Zeichen“ zu nutzen, also Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.[3]

Das BSI weist aber auch darauf hin, dass viele Online-Dienste Vorgaben machen, welche Zeichen bei einem Passwort zu verwenden sind.

[3] https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html;jsessionid=A262FA7CB181058F2F13D5A6DB495A72.2_cid341

Empfehlungen verschiedener Institutionen zur Passwortsicherheit auf einen Blick:

<table>
<tr><th></th><th>BSI</th><th>HPI</th><th>NIST</th><th>Institut für Internet-Sicherheit</th></tr>
<tr><td>Passwortlänge</td><td>mindestens 8 Zeichen</td><td>mindestens 10 bis 15 Zeichen</td><td>mindestens 8 Zeichen;
je länger, desto besser, die Obergrenze sollte nicht unterhalb von 64 Zeichen liegen.</td><td>mindestens 12 Zeichen</td></tr>
<tr><td>Buchstaben</td><td rowspan="3">alle verfügbaren Zeichen können verwendet werden</td><td rowspan="3">Das Passwort sollte verschiedene Zeichentypen einbeziehen</td><td>Passphrasen aus mehreren Wörtern und Leerzeichen</td><td>Groß- und Kleinschreibung</td></tr>
<tr><td>Ziffern</td><td rowspan="2">nicht (mehr) zwingend nötig</td><td>ja</td></tr>
<tr><td>Sonderzeichen</td><td>ja</td></tr>
<tr><td rowspan="4">Sonstiges</td><td colspan="3">sollte nicht in Wörterbüchern stehen</td><td>sinnfreie Zeichenkette</td></tr>
<tr><td colspan="2">keine Namen/persönliche Daten</td><td></td><td></td></tr>
<tr><td colspan="2">keine gängigen / „sinnvollen“ Varianten</td><td></td><td></td></tr>
<tr><td colspan="4">keine Passwörter mehrfach verwenden</td></tr>
<tr><td>Regelmäßiger Passwortwechsel</td><td>ja</td><td>ja, aber keine alten Passwörter/ Variationen</td><td>nein, nur bei Angriffs-verdacht</td><td>maximal 30 Tage Gültigkeit</td></tr>
<tr><td>Link</td><td>https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html</td><td>https://hpi.de/pressemitteilungen/2018/change-your-password-day-hpi-gibt-tipps-fuer-starke-passwoerter.html</td><td>https://pages.nist.gov/800-63-3/</td><td>https://www.internet-sicherheit.de/downloads/infografiken/authentifikationsverfahren/</td></tr>
</table>

Stand 05.02.2018

2. Marktcheck zur Passwortsicherheit

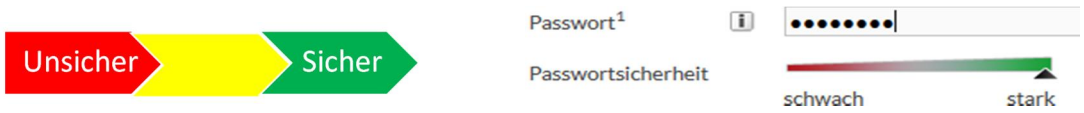
2.1. Umfang und Art der Stichprobe

Die Verbraucherzentrale Rheinland-Pfalz hat stichprobenartig Websites von insgesamt 141 Online-Shops, E-Mail-Diensten und Social-Media-Anbietern untersucht: Grundlage für die Auswahl der Stichprobe waren Recherchen im Internet, beispielsweise die 100 umsatzstärksten Online-Shops.

Die Verbraucherzentrale hat folgende Fragen unter die Lupe genommen:

- Gibt es zwingende Vorgaben zur Passwortlänge?
- Gibt es zwingende Vorgaben zur Verwendung von Ziffern, Sonderzeichen oder Groß-und Kleinbuchstaben?
- Gibt es weitere Hinweise zur Passwortsicherheit?

Manche Anbieter geben darüber hinaus eine Hilfestellung in Form einer Art Ampel. Das Passwort wird überprüft und eine farbliche Skala zeigt die „Sicherheit“ des Passwortes an.



War diese Ampel auf einer Seite vorhanden, hat die Verbraucherzentrale getestet, welche Ergebnisse sie bei den folgenden häufig genutzten Passwörtern anzeigt.

- qwertz (Tastenfolge auf der Tastatur, sechs Zeichen)
- pa$$w0rt (Buchstaben, Sonderzeichen, Ziffer, acht Zeichen, Variation eines gängigen Wortes)

Allerdings ließen die Vorgaben zum Passwort diesen Test nicht immer zu.

2.2. Ergebnisse

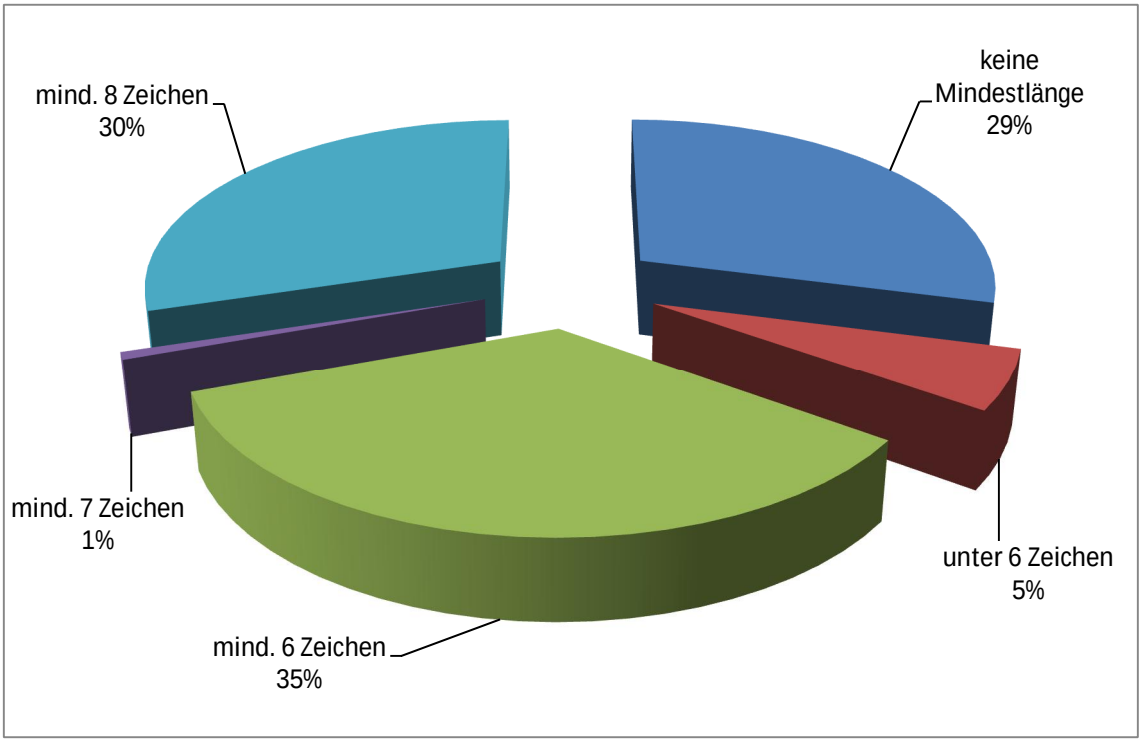
Manche Anbieter machen technische Vorgaben zur Gestaltung eines Passworts, andere nicht. Wird beispielsweise eine Mindestlänge vorgegeben, sind kürzere Eingaben ungültig. Auch wenn bestimmte Zeichensorten technisch gefordert werden, ist eine entsprechende Gestaltung des Passwortes nötig.

Zwingende Vorgaben zur Passwortlänge

Lediglich 30 Prozent der untersuchten Anbieter machen zwingende Vorgaben zur Passwortlänge, die den aktuellen Vorgaben des BSI von mindestens acht Zeichen entsprechen. 29 Prozent machen keinerlei Vorgaben. Bei 41 Prozent sind die Vorgaben aus Sicht der Verbraucherzentrale unzureichend.

Die Ergebnisse im Überblick

n = 141



Bei den Anbietern, die Vorgaben zur Passwortlänge machen, reicht das Spektrum von mindestens vier Zeichen bis maximal 60 Zeichen. 35 Prozent der Anbieter verlangen mindestens sechs Zeichen. Dies entspricht keinesfalls mehr den aktuellen Anforderungen an ein Passwort. Kein Anbieter verlangt zwingend mehr als acht Zeichen, in Einzelfällen sind sogar nur maximal zwölf Zeichen erlaubt. Hier wäre das Benutzen einer Passphrase, wie sie das NIST fordert, nicht sinnvoll möglich.

Wie verlässlich ist die Ampel?

Bei 56 der untersuchten Anbieter findet sich die oben beschriebene Ampel. Sie bietet zwar einen Anhaltspunkt zur Sicherheit des Passworts, ist aber nicht unbedingt verlässlich und häufig sogar äußerst fragwürdig: So wird das Passwort „pa$$w0rt“ fast immer als „sicher“ oder „stark“ eingestuft.

Oft geben die Seitenbetreiber auch nur Tipps, wie ein sicheres Passwort aussehen könnte, kontrollieren aber die Umsetzung nicht.

Beispiele:

Selbst das Passwort „qwertz“ – also die Tastenabfolge von sechs nebeneinanderliegenden Buchstaben auf der Tastatur – wurde in Einzelfällen noch als „mittelsicher“ eingestuft.

Diese Ampeln suggerieren eine Sicherheit, die nicht unbedingt gegeben ist.

Welche weiteren Vorgaben machen die Anbieter?

Wenige Anbieter verlangen über die Mindestanzahl an Zeichen hinaus zwingend die Einhaltung weiterer Regeln, zum Beispiel:

- maximal drei gleiche aufeinanderfolgende Buchstaben oder Zahlen
- wenigstens ein Buchstabe, maximal vier gleiche Buchstaben
- Mischung aus mindestens zwei der folgenden Kriterien: Sonderzeichen, Zahlen, große oder kleine Buchstaben

Immerhin geben etliche Anbieter weitere Tipps zur Gestaltung eines sicheren Passwortes, wie:

- „Wählen Sie ein möglichst langes Passwort.“
- „Es sollte Groß- und Kleinschreibung enthalten.“
- „Es sollte Sonderzeichen (!?$§#...) enthalten.“
- „Es sollte Zahlen enthalten.“

Weitergehende Hinweise von Anbietern:

- „Sie sollten keine existierenden Wörter verwenden.“
- „Login-Name und Passwort sollten nicht identisch sein.“
- „Verwenden Sie nicht dasselbe Passwort, welches Sie für andere Konten online benutzen.“

- „Wir raten von Wörtern aus dem Wörterbuch ab.“

Ein E-Mail-Anbieter gibt sehr konkrete Hinweise:

- „Bitte vermeiden Sie zu Ihrer eigenen Sicherheit Passwörter, die durch einfaches Nachforschen oder simples Ausprobieren erraten werden könnten.
  Vermeiden Sie daher die Verwendung von
  - Personennamen aus Ihrem persönlichen Umfeld wie Kinder, Verwandte, Nachbarn.
  - Daten, die mit Ihrer Person in Zusammenhang stehen wie Kontonummer, Autokennzeichen oder Telefonnummer.
  - Tastaturmuster wie „qwertz“ oder „123456“.
  - Wörtern, die in einem Wörterbuch vorkommen.
  - Mischen Sie Ziffern und Buchstaben in Groß- und Kleinschreibung und verwenden Sie weit mehr als 6 Zeichen / Buchstaben, dann erhalten Sie ein sicheres Passwort.
  - Da sich solche Passwörter nur schwer merken lassen, empfiehlt sich die Verwendung einer Eselsbrücke. Aus einem leicht zu merkenden Satz bilden Sie das Passwort aus den Anfangsbuchstaben der einzelnen Wörter: „Gestern habe ich bei Tante Martha 2 Tassen Tee getrunken“ ergibt das Passwort „GhibTM2TTg“.“

Andere Hinweise von Seitenbetreibern sind jedoch nicht wirklich zielführend. Hier ein paar Beispiele:

- „Damit Ihr Passwort sicher ist, müssen folgende Voraussetzungen erfüllt sein: 1 Zahl, 1 Großbuchstabe, 1 Kleinbuchstabe“
- „6 Zeichen (nur Zahlen und/oder Buchstaben erlaubt in Verbindung mit mindestens 5 Zeichen)“
- „Kombinieren Sie Buchstaben und Ziffern, z.B. erdbeere34“

Handelt es sich allerdings jeweils nicht um Vorgaben, sondern nur um Empfehlungen der Anbieter, ist eine Anmeldung mit einfachen und unsicheren Passwörtern jedoch ohne Probleme möglich.

3. Passwortchecks im Internet

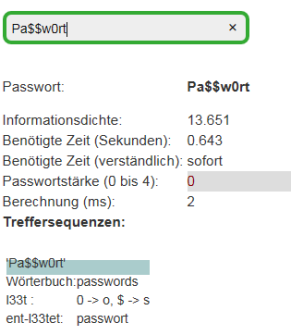
Es gibt Internetseiten, welche die Sicherheit von Passwörtern checken. Auch diese arbeiten unterschiedlich und sind nicht unbedingt immer aussagekräftig.

Hier ein paar Beispiele:

https://wiesicheristmeinpasswort.de/

Test mit qwertz

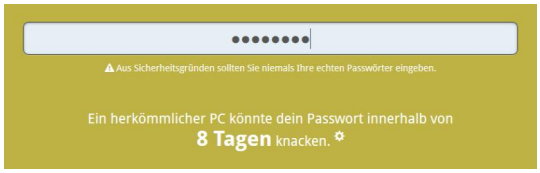
Test mit Pa$$w0rt



https://checkdeinpasswort.de/

Test mit qwertz

Test mit Pa$$w0rt



Passwortcheck des Datenschutzbeauftragten des Kantons Zürich:

https://www.passwortcheck.ch/passwortcheck/passwortcheck

Passwortcheck des Anbieters Microsoft

http://www.sicherheit-macht-schule.de/Hintergruende/Privatsphaere/1232_Passwortpruefer.htm

Alle diese Dienste sind browserbasiert, d.h. man muss sein Passwort in die Maske eines Internetdienstanbieters eingeben. Die meisten dieser Dienste geben an, das eingegebene Passwort nicht zu speichern oder zu übertragen. Dies lässt sich aber nicht kontrollieren. Die Verbraucherzentrale empfiehlt, aus Sicherheitsgründen niemals aktive Passwörter einzugeben.

4. Was tun bei Verdacht auf einen Passwort-Diebstahl?

Die Sicherheitsbehörde NIST empfiehlt beispielsweise, Passwörter nicht mehr zwangsläufig nach einer bestimmten Zeit zu ändern, sondern nur, wenn der Verdacht eines Passwortdiebstahls vorliegt. Hinweise darauf geben Berichte in den Medien. Alternativ kann auch der Dienst „Have I Been Pwned“ (https://haveibeenpwned.com) des unabhängigen Sicherheitsforschers Troy Hunt genutzt werden. Dieser Dienst trägt gestohlene Identitätsdaten aus Leaks[4] zusammen, die Hacker frei verfügbar ins Netz gestellt haben. Dies ermöglicht Nutzerinnen und Nutzern einen Abgleich darüber, ob eine E-Mail-Adresse oder ein Passwort in den Datenbanken mit gestohlenen Einträgen zu finden ist. Tauchen die eigenen Daten dort auf, ist ein Ändern des Passwortes dringend nötig. Anders herum heißt ein Nicht-Auftauchen jedoch nicht zwangsläufig, dass die Daten nicht gestohlen wurden.

Sicherheitstest des BSI

https://www.sicherheitstest.bsi.de/

Der Sicherheitstest des BSI gibt Auskunft darüber, ob eine E-Mail-Adresse und das zugehörige Passwort von einem Hackerangriff betroffen sind.

Identity Leak Checker

https://sec.hpi.de/ilc/search?lang=de

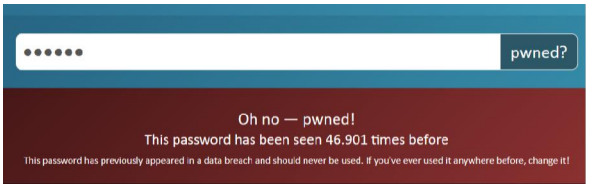
[4] Der Begriff *Leak* (englisch für Leck, Loch, undichte Stelle) bezeichnet im deutschsprachigen Raum die nicht autorisierte Veröffentlichung von Informationen.

Dieses Tool stammt vom Hasso-Plattner-Institut. Es ist in deutscher und englischer Sprache verfügbar und durchsucht Internet-Datenbanken nach gestohlenen Identitätsdaten.

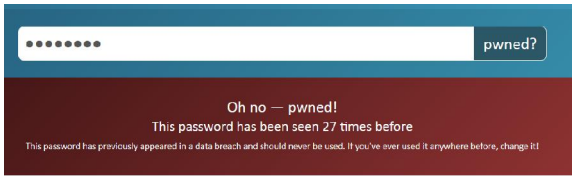
haveibeenpwned

https://haveibeenpwned.com/Passwords

Test mit qwertz



Test mit Pa$$w0rt



Grundsätzliches Problem all dieser Dienste ist, dass sie internetbasiert arbeiten und es daher problematisch ist, aktive Passworte einzugeben. Doch zumindest dem BSI sollte man hier vertrauen können.

5. Auch Anbieter sind in der Pflicht

Die Verbraucherzentrale appelliert an die Anbieter, zumindest im Hinblick auf die Mindestzeichenlänge zwingende Vorgaben für das Passwort zu machen.

Ein Passwort sollte mindestens acht Zeichen lang sein, besser noch zwölf Zeichen. Die maximal mögliche Zeichenlänge sollte nicht unter 64 Zeichen liegen.

Das NIST empfiehlt, häufig genutzte Kennwörter bereits bei der Entwicklung der Software zu blocken. Unsichere häufig genutzte Passwörter wären dann nicht mehr zulässig. Damit könnten Wörterbuch-Attacken entschärft werden, die Kennwortlisten aus größeren Leaks einfach durchprobieren.[5]

6. Tipps der Verbraucherzentrale für ein sicheres Passwort

Die Verbraucherzentrale gibt folgende Tipps für ein sicheres Passwort:

- Das Passwort sollte keinen Sinn ergeben und nicht in Wörterbüchern vorkommen.
- Gängige Varianten wie asdfg oder abcd oder 123456 sind tabu.
- Das Passwort sollte möglichst lang sein und mindestens acht Zeichen umfassen. Eine Länge von zwölf Zeichen ist schon viel sicherer.
- Namen von Familienangehörigen, Haustieren, Lieblingsstars sind ebenfalls tabu.
- Das Passwort sollte nicht an Dritte weitergeben werden und auch weder auf einem Zettel am Computer kleben noch im Browser gespeichert sein.
- Niemals dasselbe Passwort mehrfach verwenden.

[5] https://www.security-insider.de/nist-definiert-neue-passwort-regeln-a-564471/

- Merkhilfe: Man denkt sich einen langen Satz aus und nimmt die Anfangsbuchstaben als Passwort. So kann man auch Sonderzeichen und Zahlen einbauen – und das Passwort lässt sich trotzdem noch merken.

7. Impressum

Verbraucherzentrale Rheinland-Pfalz e.V.
Seppel-Glückert-Passage 10
55116 Mainz
Für den Inhalt verantwortlich:
Ulrike von der Lühe, Vorstand der Verbraucherzentrale Rheinland-Pfalz e.V.

Gefördert durch:

RheinlandPfalz
MINISTERIUM FÜR FAMILIE, FRAUEN, JUGEND, INTEGRATION UND VERBRAUCHERSCHUTZ

Kontakt

Verbraucherzentrale Rheinland-Pfalz e.V.
Team Telekommunikation und digitale Medien
Seppel-Glückert-Passage 10
55116 Mainz
E-Mail: telekommunikation@vz-rlp.de
www.verbraucherzentrale-rlp.de

Titelbild: kalhh | Pixabay.com (CC0)
Tabellen und Abbildungen: Verbraucherzentrale Rheinland-Pfalz e.V.

Mainz, 28. August 2018