

Wozu Passwörter?

Passwörter dienen dazu, die Identität eines Benutzers zu beweisen.

Ein Passwort sollte folgende Eigenschaften haben:


- ausreichende Länge
- nicht leicht erratbar
- leicht merkbar

Dasselbe Passwort mehrfach verwenden?

Soll ich mir ein supersicheres Passwort auswendig merken und dann überall verwenden?

Nein.


Einige News



Hacker überfällt Linuxforums.org und erbeutet Daten von 276.000 Accounts

Ein Unbekannter hat Zugriff auf Interna von Linuxforums.org bekommen und dabei Nutzerdaten inklusive Passwörtern kopiert.

gestern, 11:20 Uhr  4



DNA-Webseite MyHeritage: Hacker kopiert Daten von 92 Millionen Nutzern


Auf der Ahnenforschungs- und DNA-Test-Webseite hat es ein Datenleck gegeben. Dabei wurden auch Passwörter abgezogen. Die Ursachen sind bislang noch unklar.


06. Juni 2018, 10:24 Uhr  34



Hacker kapert Datenbank vom ownCloud-Forum

Das offizielle ownCloud-Forum war Opfer einer Hacker-Attacke. Der Angreifer soll Zugriff auf persönliche Daten von Mitgliedern inklusive Passwörter gehabt haben.

15. Mai 2018, 16:07 Uhr  24



Twitter ruft nach Sicherheitspanne zum Passwortwechsel auf

Durch eine Panne wurden bei Twitter intern Passwörter unverschlüsselt abgespeichert. Das Unternehmen empfiehlt eine sofortige Passwortänderung.

04. Mai 2018, 07:53 Uhr  101  heise online

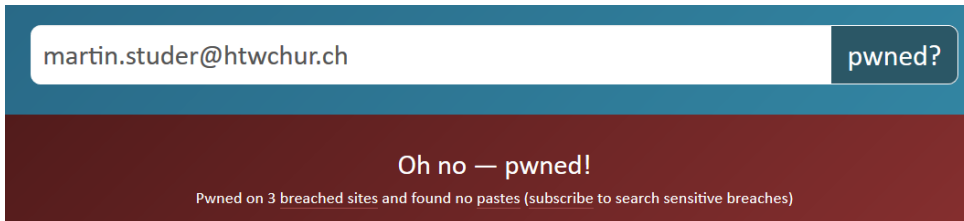
Quelle:

<https://www.heise.de/security>

Wie merke ich, dass ich betroffen bin?


Seiten wie

- <https://haveibeenpwned.com/> oder
 - <https://www.checktool.ch/> (von MELANI = Melde- und Analysestelle Informationssicherung des Bundes)
- geben Auskunft darüber, ob Passwörter/Daten, welche zu einer Mailadresse gehören, veröffentlicht wurden.



Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

- **Adobe:** In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.
Compromised data: Email addresses, Password hints, Passwords, Usernames
- **GeekedIn:** In August 2016, the technology recruitment site GeekedIn left a MongoDB database exposed and over 8M records were extracted by an unknown third party. The breached data was originally scraped from GitHub in violation of their terms of use and contained information exposed in public profiles, including over 1 million members' email addresses. Full details on the incident (including how impacted members can see their leaked data) are covered in the blog post on [8 million GitHub profiles were leaked from GeekedIn's MongoDB - here's how to see yours.](#)
Compromised data: Email addresses, Geographic locations, Names, Professional skills, Usernames, Years of professional experience
- **last.fm:** In March 2012, the music website Last.fm was hacked and 43 million user accounts were exposed. Whilst Last.fm knew of an incident back in 2012, the scale of the hack was not known until the data was released publicly in September 2016. The breach included 37 million unique email addresses, usernames and passwords stored as unsalted MD5 hashes.
Compromised data: Email addresses, Passwords, Usernames, Website activity

Individuelle Passwörter mit System

Soll ich für jeden Dienst ein individuelles Passwort anlegen, das nach einem System aufgebaut ist?

Netflix:

meinsupergeheim**sNetflix**Passwort

HTW:

meinsupergeheim**sHTW**Passwort

Postfinance:

meinsupergeheim**sPostfinance**Passwort

Individuelle Passwörter mit System

Wenn das System für einen Aussenstehenden erkennbar ist, lautet die Antwort klar:

Nein.

Begründung: Wird das Passwort eines Dienstes bekannt, lassen sich die Passwörter für andere Dienste herleiten.

Zufällig generierte Passwörter

Sehr sicher sind Passwörter, welche zufällig generiert sind, z.B.

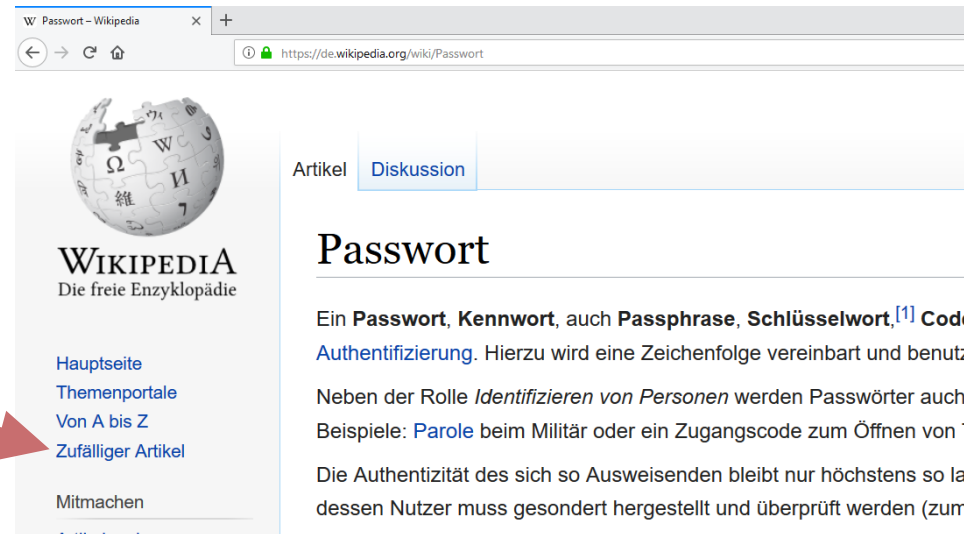
qXj2xyghEVk5p3xu

Leider sind diese auch kaum merkbar.

KeePass ist in der Lage, solche Passwörter zu generieren und zu speichern.

Passwort aus 4 zufälligen Wörtern

Eine Methode um ein sicheres und dennoch merkbares Passwort zu erstellen ist die Aneinanderreihung von 4 zufälligen (kleingeschriebenen) Wörtern. Eine gute Quelle dafür ist ein Duden oder Wikipedia.



Beispiel:

türkeifloorbackkleinkariert

Passwort aus 4 zufälligen Wörtern

Ein so generiertes Passwort hat eine vergleichbare Stärke wie ein zufällig generiertes Passwort mit 12 Stellen.

Allgemeine Regeln im Umgang mit Passwörter

Passwörter sollen nicht

- aufgeschrieben
- unverschlüsselt gespeichert
- gemailt
- weitergegeben

werden.