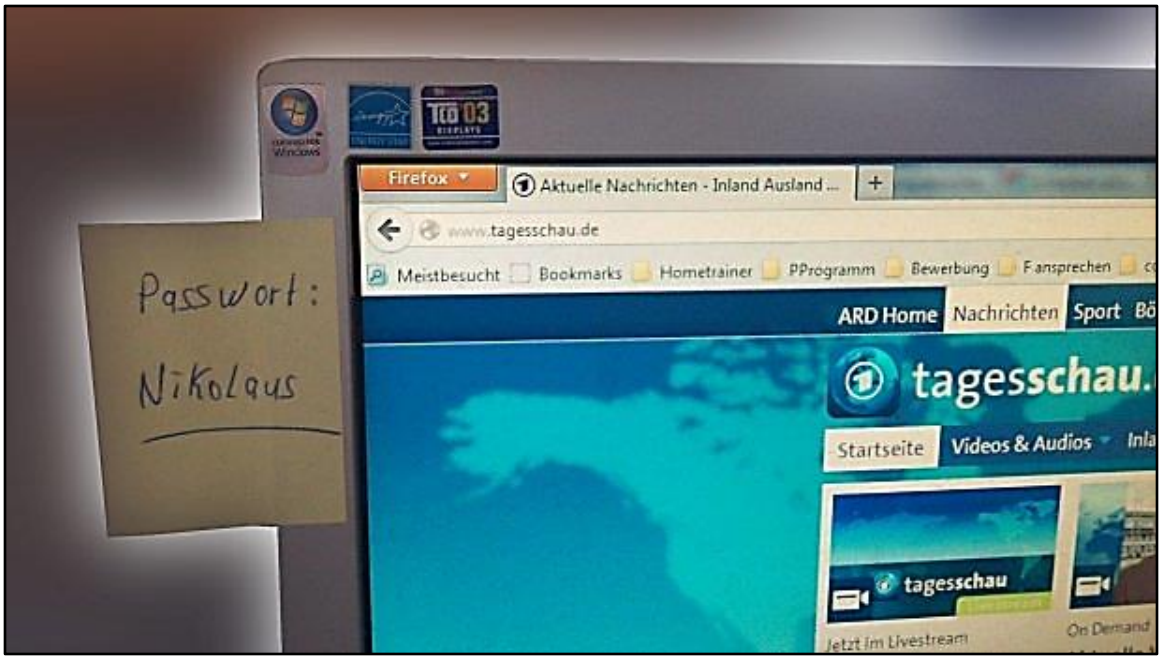
COMPUTERIA SOLOTHURN

Passwörter

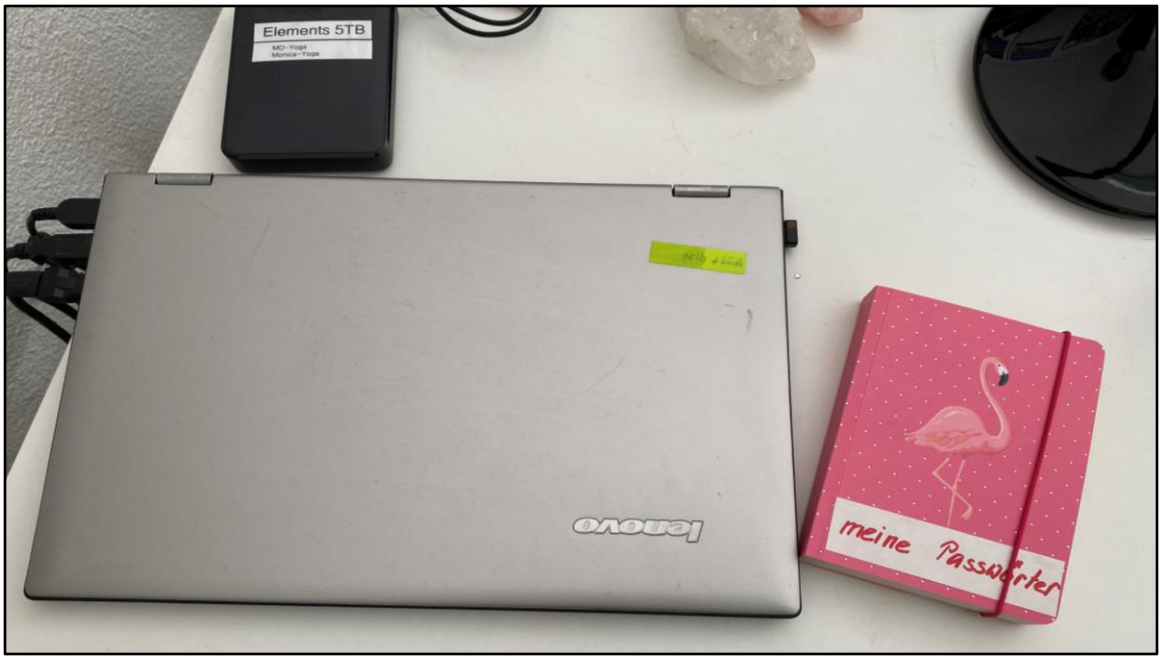
24. November 2022

Martin Dürig



Das beste Passwort nützt wenig, wenn es direkt ersichtlich ist.

… ist aber immer noch häufig der Fall!



Es ist sinnvoll, sich seine Passwörter aufzuschreiben, aber gerade so macht es wenig Sinn…

Es muss nicht unbedingt ein Einbrecher sein, der Interesse daran hat, es gibt auch andere Personen, die daran interessiert sein könnten.

1. Frage

Was ist ein gutes Passwort?

Vor einigen Jahren war ein einfaches Passwort mit 4 Buchstaben noch gebräuchlich.

Heute werden längere und komplexere Passwörter verlangt.

Das Ganze wir auf dem Server gesteuert und der Administrator kann festlegen, wie komplex ein Passwort sein muss.

Der Computer übersetzt ja bekanntlich jedes Zeichen in I und 0.

Man nennt das auch **Binärsystem**

Somit muss der Hacker lediglich sehr viele Kombinationen ausprobieren.

Zahlen ergeben einfache 0 I Kombinationen,
Buchstaben sind etwas länger,
Sonderzeichen noch länger, da es auch sehr viele gibt

Also:
Ein gutes Passwort hat …

- **Gross- und Kleinbuchstaben**
- **Zahlen**
- **Sonderzeichen**
- **Ist mind. 8 Zeichen lang**

Das dürfte wohl in der Zwischenzeit bekannt sein!

Zahlen

Dezimal	Binär/Dual
0	00000000
1	00000001
2	00000010
3	00000011
4	00000100
5	00000101
6	00000110
7	00000111
8	00001000
9	00001001
10	00001010

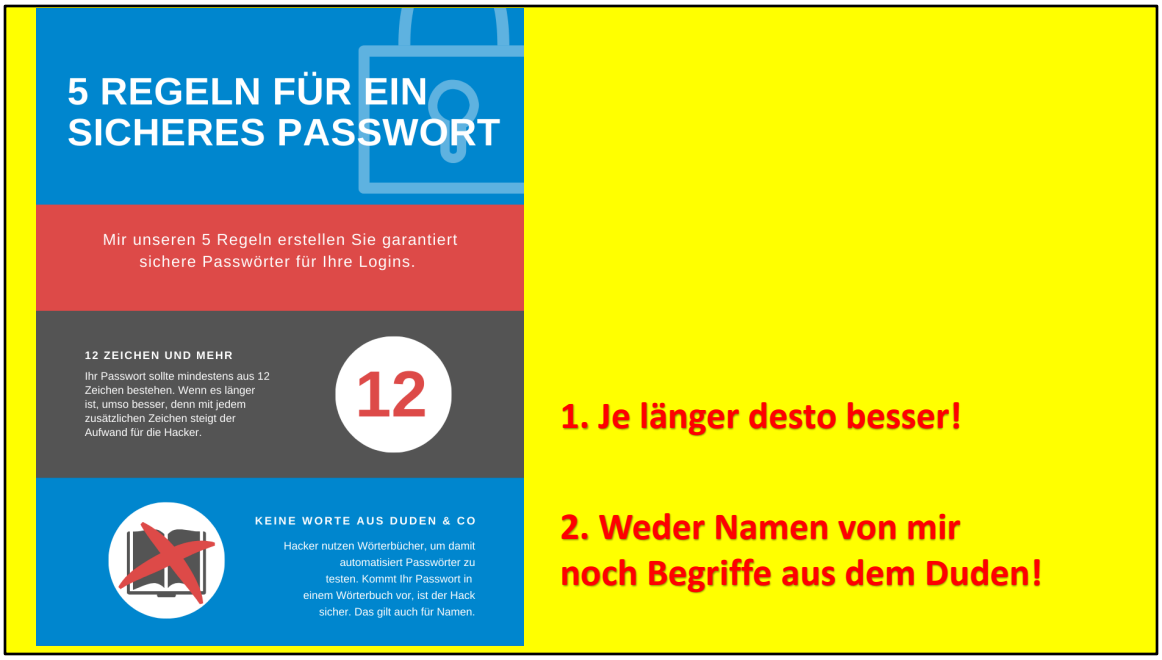
Gross-Buchstaben

	Binär
@	01000000
A	01000001
B	01000010
C	01000011
D	01000100
E	01000101
F	01000110
G	01000111
H	01001000
I	01001001
J	01001010
K	01001011
L	01001100
M	01001101
N	01001110
O	01001111

Ganz kurz:

Im Binärsystem sind Zahlen relativ einfach,

Grossbuchstaben, Kleinbuchstaben und Sonderzeichen komplexer.



1. Heute werden meist 8-stellige Passwörter verlangt

2. Namen, Wohnort, Geburtsdatum von mir und auch Autonummer sind immer schlecht!
   Ebenso Begriffe aus dem Wörterbuch

3. Buchstaben + Zahlen + Sonderzeichen

4. Passworthierarchien erstellen

5. Masterpasswort / Eselsbrücken:
«Ich liebe M&M's und esse täglich 30! »
= IlM&M'suet30!

3. Bedingung: 3 Komponenten!

4. Es empfiehlt sich, mehrere PW zu haben.
   Ideal wäre überall ein anderes.
   Man kann auch eine Hierarchie erstellen nach Wichtigkeit

5. Auch eine Buchstabenfolge aus einer Eselsbrücke,
   kombiniert mit Sonderzeichen ist empfehlenswert

Wenn möglich doppelt schützen «2-Stufen-Authentifizierung»

Wenn möglich immer die 2-Stufen-Authentifizierung einsetzen.

Das heisst: Nach dem Passwort wird mir ein Code auf mein Smartphone zugestellt.

Wenn möglich
Fingerprint Sensor verwenden

FACE ID

Wenn möglich
Face ID verwenden

Für die Anmeldung am Compi gibt es bei Notebooks oft den Fingerprint-Sensor.
Externe Fingerprint Sensoren sind im Handel erhältlich.

Ipads und Iphones sind mit Fingerabdruckerkennung oder mit Face-ID ausgerüstet. Also bitte einsetzen!

ACHTUNG:
Der E-Mail Account sollte unbedingt gut passwortgeschützt sein.

Oft werden Web-Mail Zugänge gehackt und dann darüber Spam verteilt.

Konsequenz:
Der Provider sperrt den E-Mail Account!
Das Entsperren ist dann aufwendig, geht aber!

Wichtig zu wissen:

Hat ein Hacker Zugriff auf meine E-Mails, kann er auch andere Passwörter knacken mit der Funktion „Passwort vergessen“

Oder der Hacker kann auf Seiten von mir zugreifen und dank der Funktion «Passwort vergessen»

… auf meine Kosten einkaufen, denn häufig ist ja ein Zahlungsmittel hinterlegt

Passwort-Hierarchie, je nach Wichtigkeit

Stufe 1 (wenig wichtig):

- **Login Internetseiten, wenig Wichtiges (kein Zahlungsmittel hinterlegt)**

Stufe 2 (wichtig):

- **Login Persönlicheres, Einkaufen**

Stufe 3 (sehr wichtig):

- **E – Banking, E-Mail-Adresse (nicht jede Bank gleiches PW!)**

Auch eine Passwort-Hierarchie ist sinnvoll.

Je nach Wichtigkeit ein komplexeres Passwort verwenden


Passwort verbessern

Martin1952

Mart!n1952

M@rt!n1952

19M@rt!n52

Hier ein Beispiel:

Stufenweise machen wir ein einfaches Passwort sicherer.

Passwort hacken

Hacker sehen nicht unbedingt so aus!

Häufig sind es Maschinen, die Passwörter zu hacken versuchen.

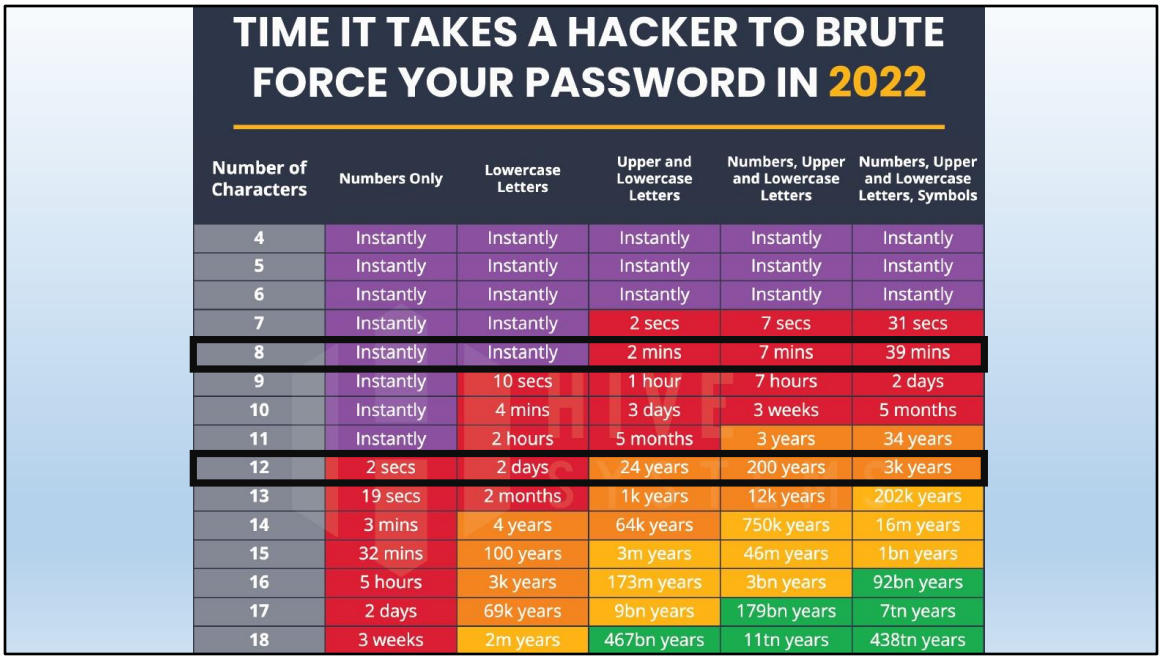
Wie lange dauert es, ein Passwort zu knacken?

Dank immer schnelleren Rechnern dauert es auch immer weniger lang, ein Passwort zu hacken, vorausgesetzt, man versteht etwas davon …

Ein Rechner kann ein 8-stelliges komplexes Passwort in weniger als einer Stunde knacken

Gut zu wissen:

Ein Hacker probiert nicht einfach aus, sondern überlässt das einem Computerprogramm.



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

Man beachte bitte diese aktuelle Aufstellung

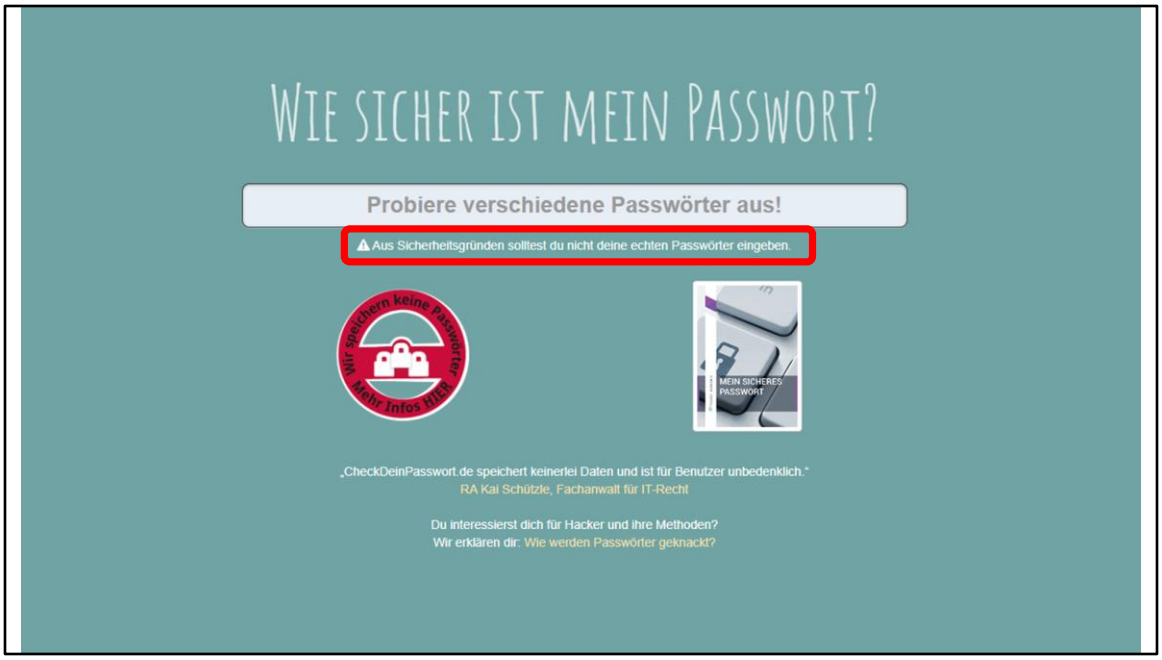
… und wenn die Rechenleistung eines Rechenzentrums benutzt wird, dauert es noch weniger lang.

Übrigens: auch das ist ein Rechenzentrum…

Mein Passwort checken

www.checkdeinpasswort.de

Ein Link, um die Stärke eines Passworts zu testen.



Bitte Hinweis beachten!

Nicht meine eingesetzten Passwörter eingeben, sondern leicht abgeänderte.

Hier ist klar:

- Häufig verwendet
- Zu kurz
- Zu wenig verschiedene Zeichensorten

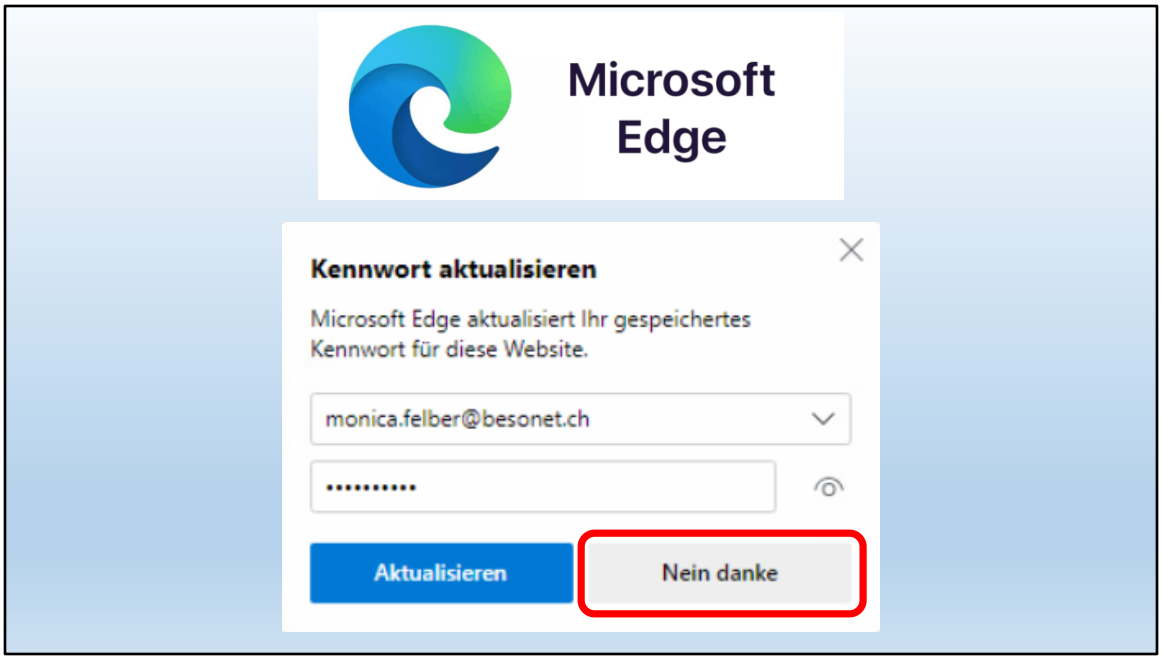
… also nicht verwenden!

Dieses Passwort erfüllt alles perfekt!

Na ja, ob die Zeitdauer stimmt, lassen wir offen…

alle wollen meine Passwörter speichern !!!

Immer wieder treffen wir auf Anwendungen, die mein Passwort speichern wollen.

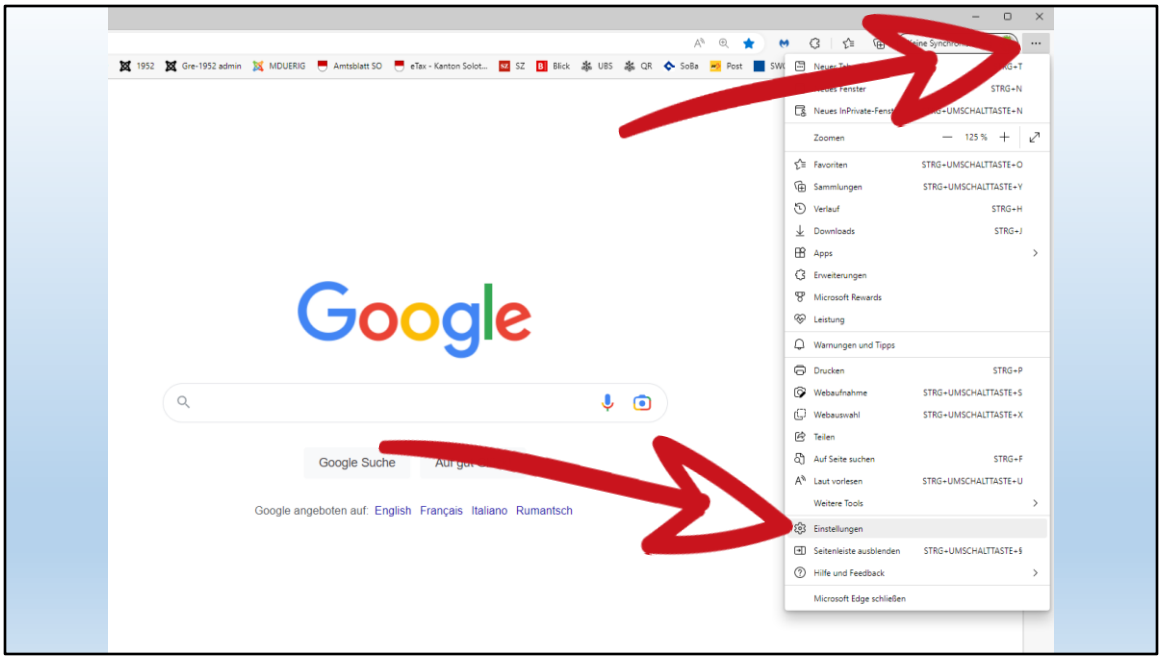


So zB Microsoft Edge!

Ist zwar nett, aber will ich das wirklich?

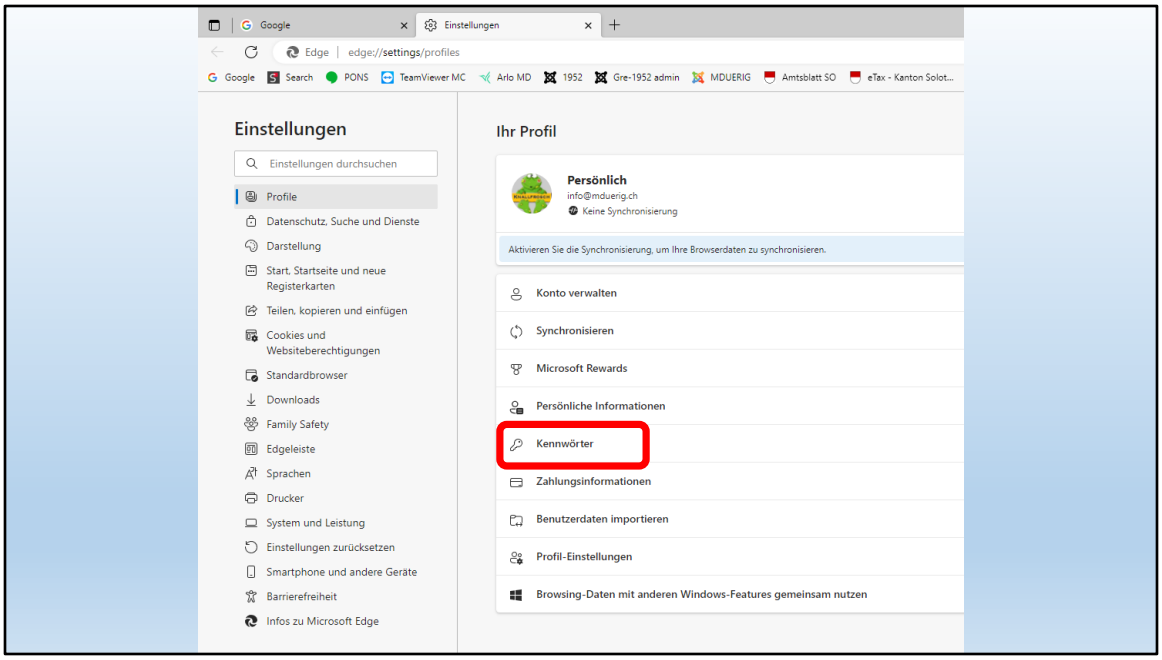
Frage: WO werden meine Passwörter gespeichert?

Antwort: Keine Ahnung!
Bei Edge zB lokal. Aber wirklich nur lokal?????

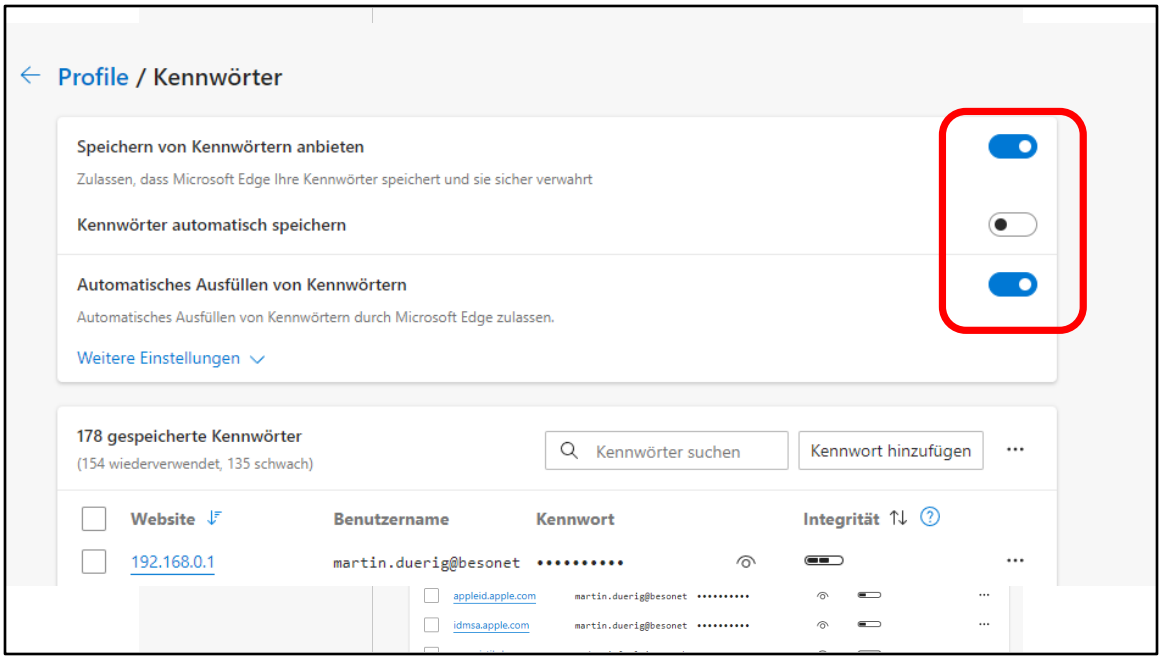


Wenn ich das aber nicht will?

Auf der Startseite bei Edge oben rechts die drei Punkte anklicken «Einstellungen» wählen.



Unter «Profil» erkennt man den Punkt «Kennwörter»



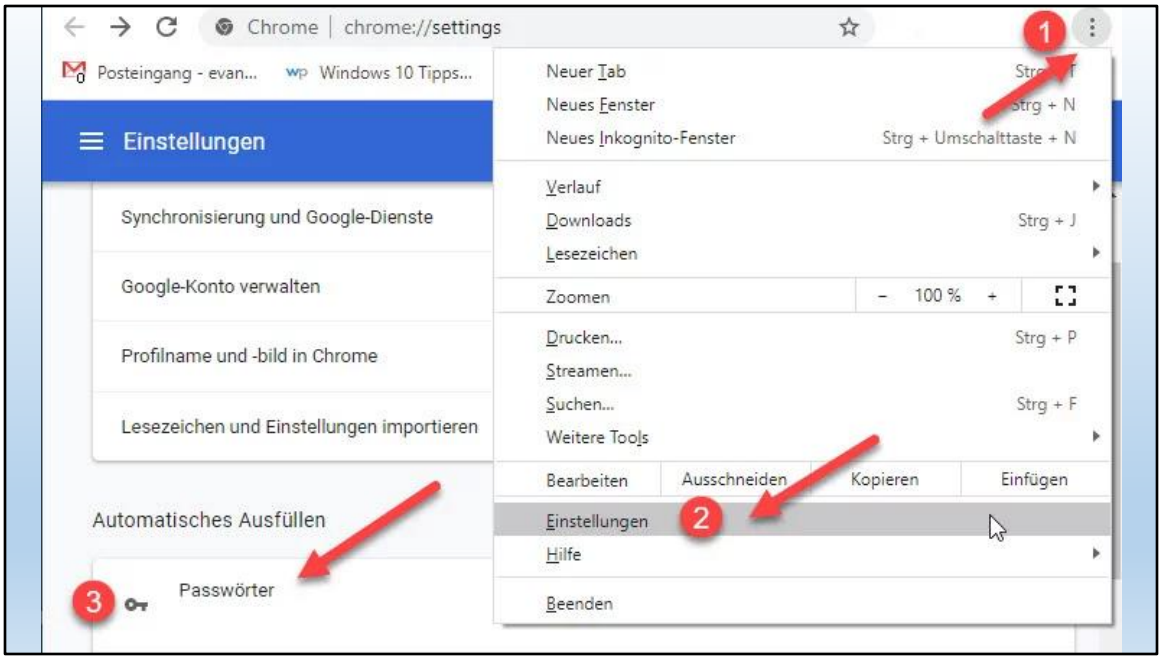
Hier lässt sich einstellen, ob das Speichern von Kennwörtern überhaupt erlaubt sein soll.

Wer auf sicher gehen will, verbietet das!

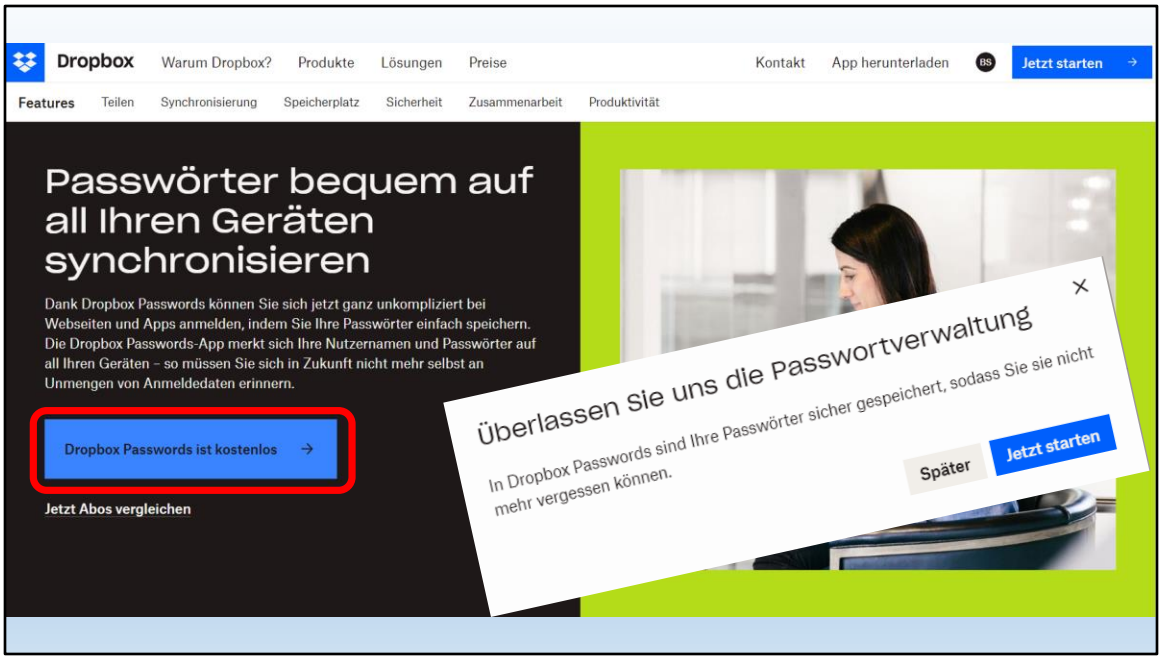
chrome

…auch Google will unsere Passwörter!

Google ist nicht besser als Microsoft!
Google gilt ja als der grosse Datensammler.

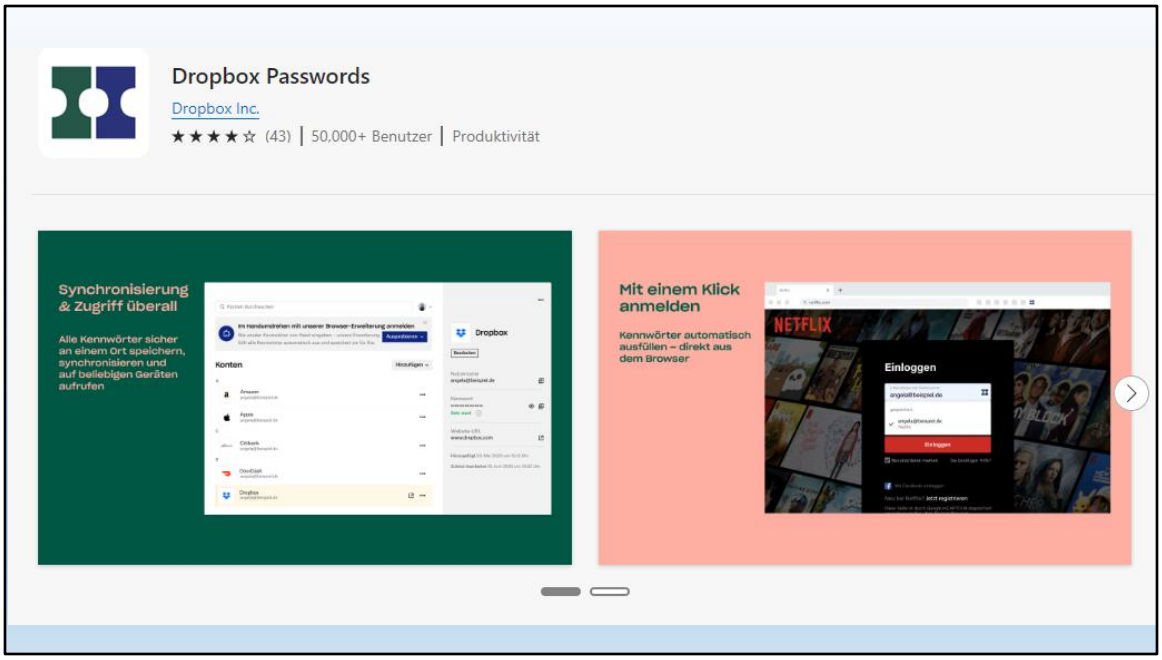


Das Einstellen geht gleich wie bei Edge



Sogar Dropbox bietet sich an!

Allerdings wird auf den eigenen Passwort-Manager verwiesen.



Dropbox hat einen Passwortmanager, der doch interessant aussieht und vieles verspricht.

Weil sich niemand mehrere (sichere) Passwörter merken kann, gibt es…

… gibt es Besseres als Papier, Post-it oder Büchlein:

Passwortmanager!

Passwortmanager können uns das Leben mit Passwörtern erleichtern.

Es gibt viele, sogar sehr viele!

… mehr darüber in einer der nächsten Computerias!

gleicher Ort – gleicher Referent