

Kurzworkshop

Passwortmanager und Generelle IT-Security-Tipps

Zentrum für Lehren und Lernen

HAW Hamburg

Niels Gandraß

2026-01-13

Inhaltsübersicht

- Passwörter und Passwortmanager
- Live-Demo
- Multi-Faktor-Authentisierung
- Sicherheitstipps im Browser
- Was tun wenn doch mal etwas passiert?
- Q&A Session

Passwörter und Passwortmanager

Wie man dem digitalen Zoo an Passwörtern wieder Herr:in wird

Was ist ein sicheres Passwort?

Was ist ein sicheres Passwort?

1. Viel zu lang

Was ist ein sicheres Passwort?

1. Viel zu lang
2. Hat viele tolle Sonderzeichen

Was ist ein sicheres Passwort?

1. Viel zu lang
2. Hat viele tolle Sonderzeichen
 - Bonuspunkt für Umlaute
 - Großes ß zählt doppelt!
 - Schonmal ein Emoji im Passwort probiert? 😎

Was ist ein sicheres Passwort?

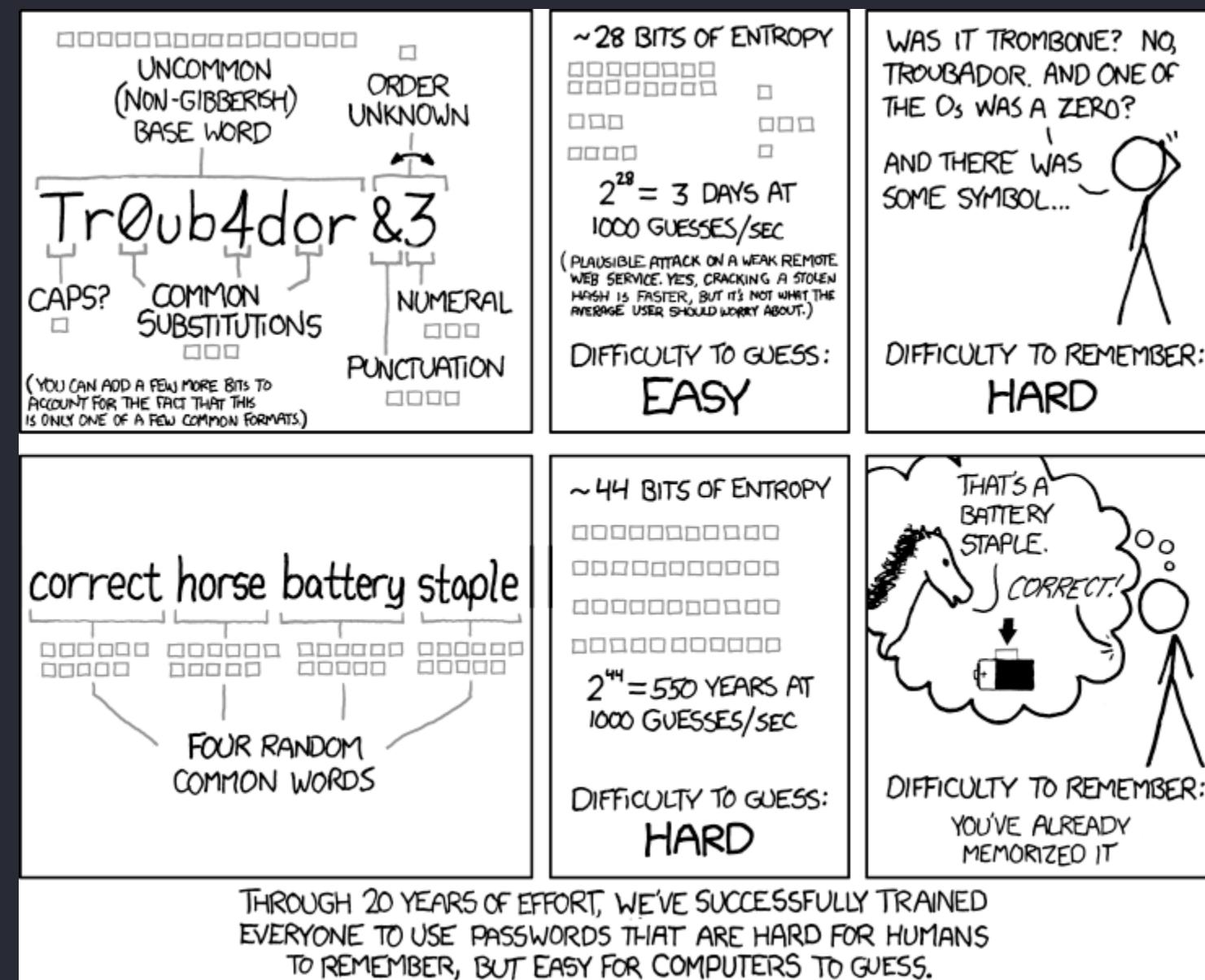
1. Viel zu lang
2. Hat viele tolle Sonderzeichen
 - Bonuspunkt für Umlaute
 - Großes ß zählt doppelt!
 - Schonmal ein Emoji im Passwort probiert? 😎
3. Besitzt mehr Ziffern als π

Was ist ein sicheres Passwort?

1. Viel zu lang
2. Hat viele tolle Sonderzeichen
 - Bonuspunkt für Umlaute
 - Großes ß zählt doppelt!
 - Schonmal ein Emoji im Passwort probiert? 😎
3. Besitzt mehr Ziffern als π
4. Ist absolut unmöglich zu merken ...

Aber es gibt doch Abhilfe!

... schwer zu erratende aber leicht zu merkende Passwörter sind möglich ...



xkcd #936

Perfekt - Wir haben eine Lösung für sichere und leicht zu merkende Passwörter!

Perfekt - Wir haben eine Lösung für sichere und leicht zu merkende Passwörter!

Nun benötigen wir nur noch für jede Website ein
eigenes sicheres Passwort :)

Perfekt - Wir haben eine Lösung für sichere und leicht zu merkende Passwörter!

für jede Website ein eigenes sicheres
Passwort

Perfekt - Wir haben eine Lösung für sichere und leicht zu merkende Passwörter!

FÜR JEDE WEBSITE?!

Perfekt - Wir haben eine Lösung für sichere und leicht zu merkende Passwörter!

FÜR JEDE WEBSITE?!

... und bitte alle im Kopf behalten ;)

Passwortmanager

Passwortmanager

- Lösen das Problem sich viele sicherer Passwörter korrekt zu merken
 - ... und generieren einem auch direkt welche!

Passwortmanager

- Lösen das Problem sich viele sicherer Passwörter korrekt zu merken
 - ... und generieren einem auch direkt welche!
- Ermöglichen einen Überblick wo man überall Nutzerkonten hat

Passwortmanager

- Lösen das Problem sich viele sicherer Passwörter korrekt zu merken
 - ... und generieren einem auch direkt welche!
- Ermöglichen einen Überblick wo man überall Nutzerkonten hat
- Bieten viele Erleichterungen im Alltag (z.B. Auto-Fill)

Passwortmanager

- Lösen das Problem sich viele sicherer Passwörter korrekt zu merken
 - ... und generieren einem auch direkt welche!
- Ermöglichen einen Überblick wo man überall Nutzerkonten hat
- Bieten viele Erleichterungen im Alltag (z.B. Auto-Fill)
- Sind kryptographisch hervorragend abgesichert

Passwortmanager

- Lösen das Problem sich viele sicherer Passwörter korrekt zu merken
 - ... und generieren einem auch direkt welche!
- Ermöglichen einen Überblick wo man überall Nutzerkonten hat
- Bieten viele Erleichterungen im Alltag (z.B. Auto-Fill)
- Sind kryptographisch hervorragend abgesichert
- Solide OpenSource-Lösungen halten problemlos mit kommerziellen Anbietern mit
 - ... und das ganz ohne Tracking und Kosten :)

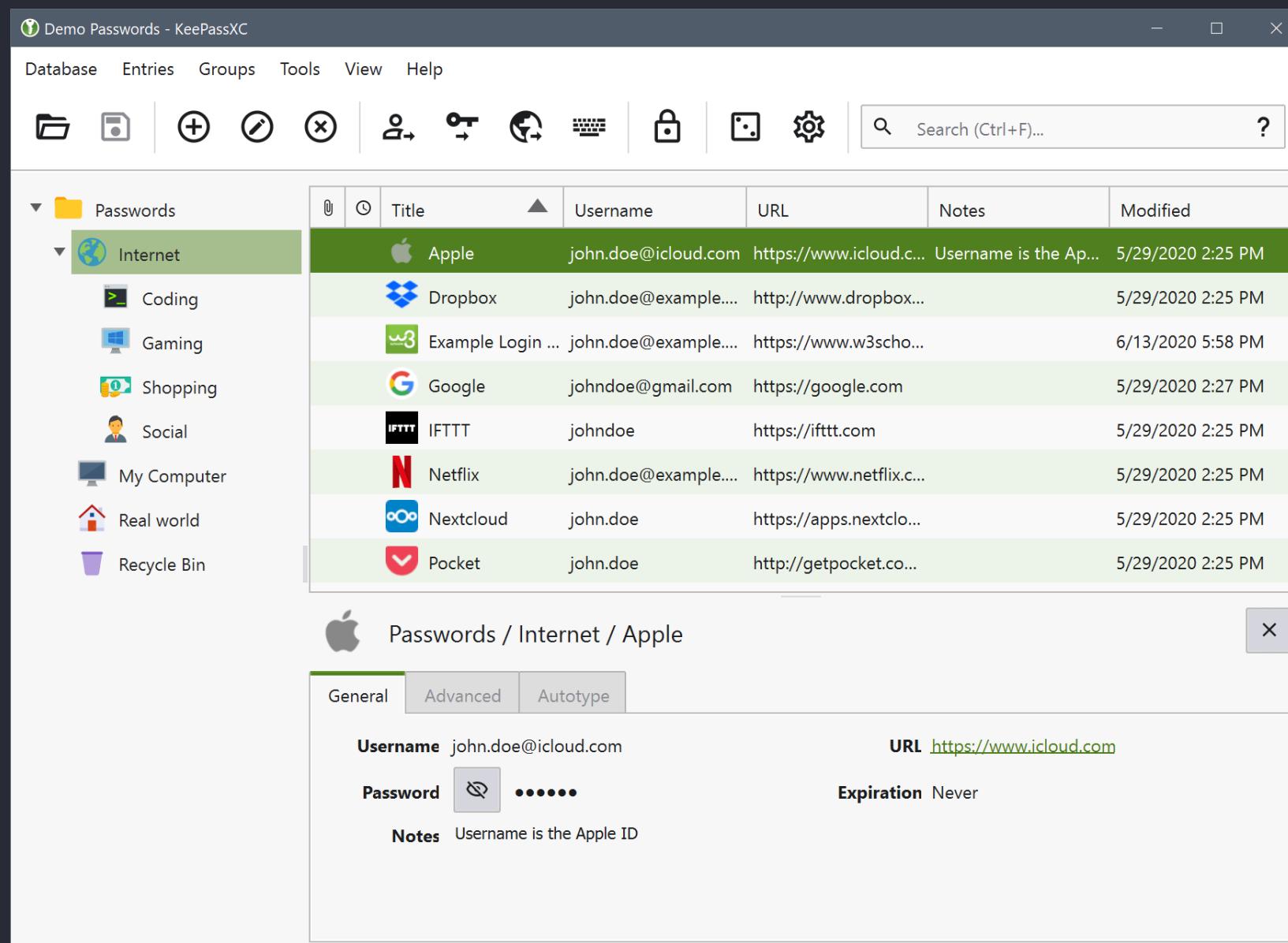
Passwortmanager

- Lösen das Problem sich viele sicherer Passwörter korrekt zu merken
 - ... und generieren einem auch direkt welche!
- Ermöglichen einen Überblick wo man überall Nutzerkonten hat
- Bieten viele Erleichterungen im Alltag (z.B. Auto-Fill)
- Sind kryptographisch hervorragend abgesichert
- Solide OpenSource-Lösungen halten problemlos mit kommerziellen Anbietern mit
 - ... und das ganz ohne Tracking und Kosten :)

Vergleich von Passwort-Managern vom BSI (Stand: 09.12.2025):
Passwortmanager im Test: IT-Sicherheit und Datenschutz im Fokus

KeePassXC

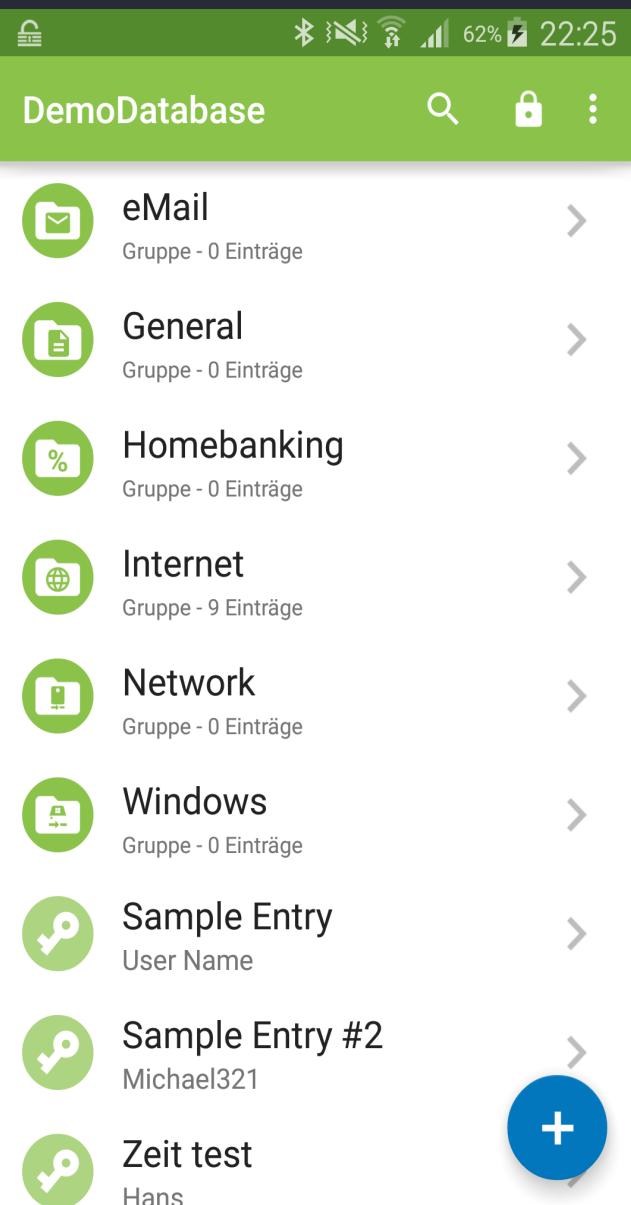
Nutzerfreundlicher Open-Source Passwortmanager (Win, Mac, Linux)



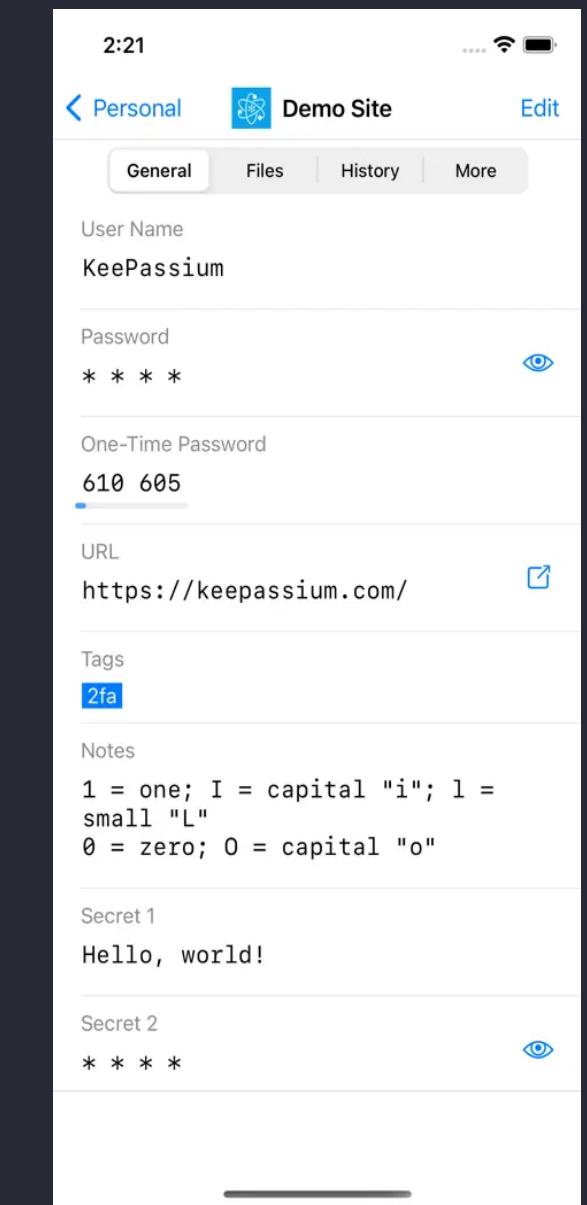
Web: <https://keepassxc.org/>

KeePass auf dem Smartphone

Es gibt ebenfalls Apps für Android und iOS



Keepass2Android



KeePassium

Live-Demo

Features und Integration von KeePassXC im Alltag

Multi-Faktor-Authentisierung

Der unverzichtbare Usability-Feind

MFA: Warum tun wir uns das eigentlich an?

Passwörter können erraten werden oder "verloren" gehen.

Weitere Faktoren schützen uns vor Missbrauch durch externe Dritte!

MFA, 2FA, OTP, TOTP, HOTP, HSM, ... wie bitte?

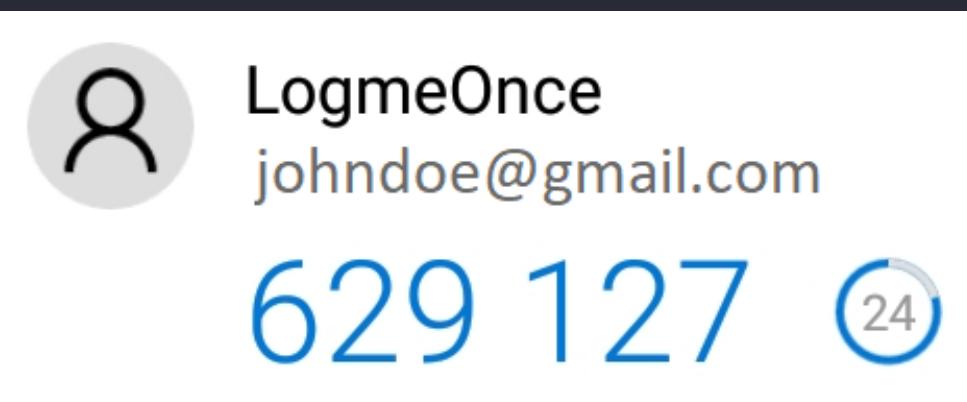
MFA, 2FA, OTP, TOTP, HOTP, HSM, ... wie bitte?

Multi-Faktor-Authentisierung (MFA) bedeutet, dass weitere Faktoren für eine erfolgreiche Authentifizierung notwendig sind. Die **Zwei-Faktor-Authentisierung (2FA)** beschränkt sich auf einen zweiten Faktor.

MFA, 2FA, OTP, TOTP, HOTP, HSM, ... wie bitte?

Multi-Faktor-Authentisierung (MFA) bedeutet, dass weitere Faktoren für eine erfolgreiche Authentifizierung notwendig sind. Die **Zwei-Faktor-Authentisierung (2FA)** beschränkt sich auf einen zweiten Faktor.

In unseren Fällen geht es fast immer um **2FA mit rotierende Zahlencodes (TOTP)**. Diese basieren auf einem geteilten Geheimnisses ("Secret Key") der häufig einmalig als QR-Code eingelesen wird.



Welche Möglichkeiten gibt es für 2FA per TOTP?

Welche Möglichkeiten gibt es für 2FA per TOTP?

Hinterlegung im Passwortmanager

Das TOTP Geheimnis wird direkt im Passwortmanager hinterlegt

Vorteile

Nachteile

Welche Möglichkeiten gibt es für 2FA per TOTP?

Hinterlegung im Passwortmanager

Das TOTP Geheimnis wird direkt im Passwortmanager hinterlegt

Vorteile

- Alles gesammelt an einem Ort
- Beste Usability
- Native Integration (Auto-Fill)
- Schützt effektiv vor externen Angreifern und bei Passwort-Leaks

Nachteile

Welche Möglichkeiten gibt es für 2FA per TOTP?

Hinterlegung im Passwortmanager

Das TOTP Geheimnis wird direkt im Passwortmanager hinterlegt

Vorteile

- Alles gesammelt an einem Ort
- Beste Usability
- Native Integration (Auto-Fill)
- Schützt effektiv vor externen Angreifern und bei Passwort-Leaks

Nachteile

- Alles gesammelt an einem Ort
- Wird effektiv zu "1 $\frac{1}{2}$ Faktoren"
- Schützt nicht bei kompromittierten Endgeräten

Welche Möglichkeiten gibt es für 2FA per TOTP?

Nutzung einer Authenticator App

Zum Beispiel: Aegis (FOSS), Google Authenticator oder Microsoft Authenticator

Vorteile

Nachteile

Welche Möglichkeiten gibt es für 2FA per TOTP?

Nutzung einer Authenticator App

Zum Beispiel: Aegis (FOSS), Google Authenticator oder Microsoft Authenticator

Vorteile

- Zweiter Faktor nicht mehr direkt neben Passwörtern abgelegt
- Echte 2FA durch unabhängiges Gerät
 - Solange nur ein Gerät kompromittiert wird ist kein Zugriff auf die Konten möglich
- Die **beste Lösung** für **alltägliche Anwendungsfälle**

Nachteile

Welche Möglichkeiten gibt es für 2FA per TOTP?

Nutzung einer Authenticator App

Zum Beispiel: Aegis (FOSS), Google Authenticator oder Microsoft Authenticator

Vorteile

- Zweiter Faktor nicht mehr direkt neben Passwörtern abgelegt
- Echte 2FA durch unabhängiges Gerät
 - Solange nur ein Gerät kompromittiert wird ist kein Zugriff auf die Konten möglich
- Die **beste Lösung** für **alltägliche Anwendungsfälle**

Nachteile

- Weicht zu "1 $\frac{3}{4}$ Faktoren" auf, sobald die Passwort-Datenbank auf dem Smartphone verwendet wird
 - Willkommen in der Hölle der Banking-Apps 🔥
- Authenticator App muss zusätzlich gegen Datenverlust gesichert werden (Backup)

Welche Möglichkeiten gibt es für 2FA per TOTP?

Externes Gerät / Hardware Token

Für besonders wichtige / zentrale Zugänge (z.B. wenn Studierendendaten betroffen sind)

Vorteile

Nachteile

Welche Möglichkeiten gibt es für 2FA per TOTP?

Externes Gerät / Hardware Token

Für besonders wichtige / zentrale Zugänge (z.B. wenn Studierendendaten betroffen sind)

Vorteile

- Extern unerreichbarer zweiter Faktor
 - Kann nicht über Internet kompromittiert werden ❤️
- Prüft nicht nur "Wissen" sondern auch "Besitz"
- Die **einige Lösung** für **besonders
sicherheitsrelevante Anwendungsfälle**

Nachteile

Welche Möglichkeiten gibt es für 2FA per TOTP?

Externes Gerät / Hardware Token

Für besonders wichtige / zentrale Zugänge (z.B. wenn Studierendendaten betroffen sind)

Vorteile

- Extern unerreichbarer zweiter Faktor
 - Kann nicht über Internet kompromittiert werden ❤️
- Prüft nicht nur "Wissen" sondern auch "Besitz"
- Die **einige Lösung** für **besonders sicherheitsrelevante Anwendungsfälle**

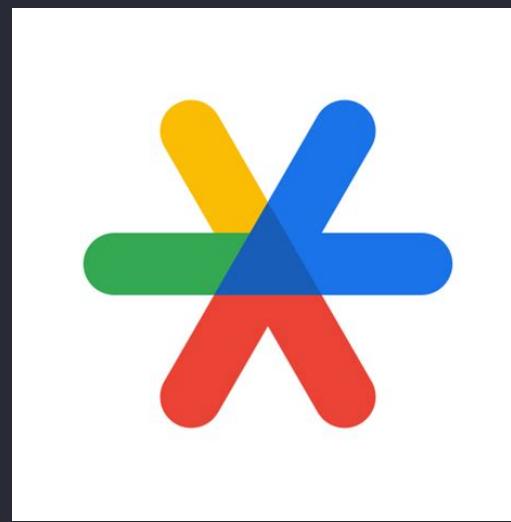
Nachteile

- Extra Gerät notwendig
- Usability eher bescheiden
- Teilweise kompliziert zu konfigurieren
- Backup nur über zweites Gerät möglich

Die Allround-Empfehlung: Zwei-Faktor-Authentisierung (2FA) per Authenticator App



Aegis (FOSS)



Google Authenticator



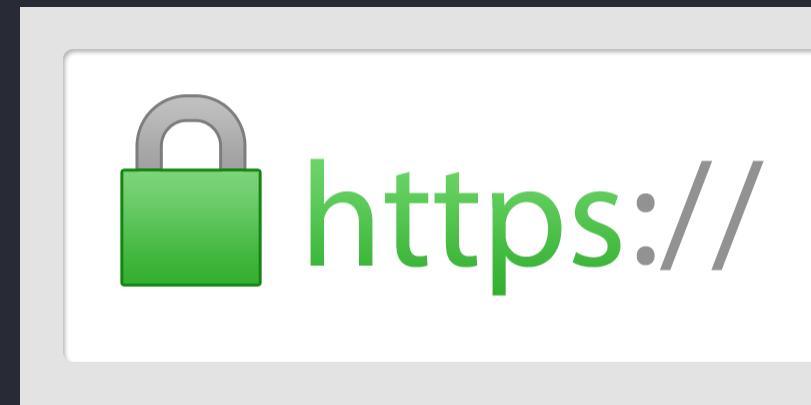
Microsoft Authenticator

Die genannten Apps unterstützen die Hinterlegung mehrerer Dienste.
Bitte installiert euch nicht für jeden Anbieter eine eigene App!

Sicherheitstipps im Browser

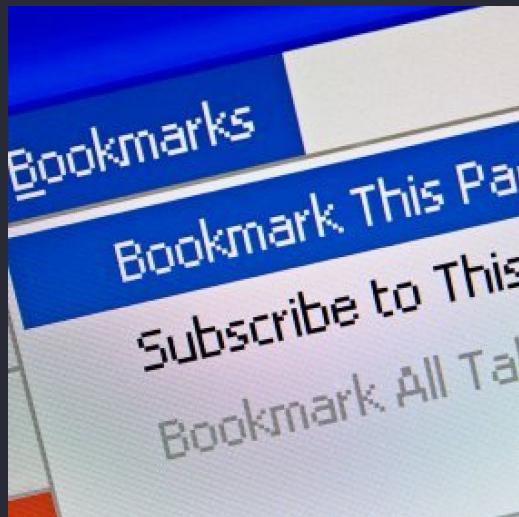
Einfache aber effektive Maßnahmen für mehr Sicherheit im Browser

Auf sicherer HTTPS-Verbindung achten



Schützt vor "Mithörern" zwischen eurem Computer und dem Server.
Ohne diese Verschlüsselung können eure Daten im Klartext auf dem Transportweg (z.B. im selben WLAN)
mitgelesen werden!

Lesezeichen für wichtige Websites anlegen statt verdächtige Links klicken



Verhindert die Nutzung gefälschter URLs. Niemals Links aus verdächtigen Mails öffnen. Stattdessen über den Browser direkt auf die Website navigieren und dort den Sachstand prüfen!

Auch von Suchmaschinen gelistete Links sollten dank Positionierungsmöglichkeiten (z.B. Google Ad-Sense) kritisch geprüft werden!

Beispiel: Maleware-Werbung über die Google Suche

A screenshot of a Google search results page for the query "7zip". The search bar at the top shows "7zip". Below the search bar, there are filters for "All", "Images", "Videos", "News", "Books", and "More". The results section starts with a "Sponsored" result from [benjaminmooretc.com](http://www.benjaminmooretc.com), which links to "Download Archiver for Windows - Best File Archiver". A red arrow points to the three-dot menu icon next to the link. Below this is a standard search result for "7-Zip" from [7-zip.org](https://www.7-zip.org), which links to "7-Zip". The right side of the screen displays the official 7-Zip software page, featuring the 7-ZIP logo, a brief description, and various technical details like release date, author, developer, size, operating systems supported, and programming languages used.

7zip - Google Search

https://www.google.com/search?q=7zip&biw=1280&bih=609&ei=MafFY_zhK7CwqtsPl-aeqAs&ved=0ahUKEwi8vrmT68z8AhUwmGoFHRezB7U4ChDh1...

Google

7zip

All Images Videos News Books More Tools

About 28,100,000 results (0.52 seconds)

Sponsored

[benjaminmooretc.com](http://www.benjaminmooretc.com) · http://www.benjaminmooretc.com

Download Archiver for Windows - Best File Archiver

Archiver Best File Archiver for Windows PC.

[7-Zip](https://www.7-zip.org) · https://www.7-zip.org

7-Zip

7-Zip is a file archiver with a high compression ratio. Download **7-Zip 22.01 (2022-07-15)** for Windows: Link, Type, Windows, Size. Download ...

[Download](#)

p7zip is the command line version of 7-Zip for Linux / Unix, ...

[7z Format](#)

is the new archive format, providing high compression ...

[FAQs](#)

You must run 7-Zip File Manager in administrator mode. Right

7-ZIP 7-Zip Software

7-Zip is a free and open-source file archiver, a utility used to place groups of files within compressed containers known as "archives". It is developed by Igor Pavlov and was first released in 1999. 7-Zip has its own archive format called 7z, but can read and write several others. [Wikipedia](#)

Initial release date: July 18, 1999

Original author: Igor Pavlov

Developer: Igor Pavlov

Size: 1.1–1.7 MB

Operating system: Windows/ReactOS, BSD, macOS, Linux,

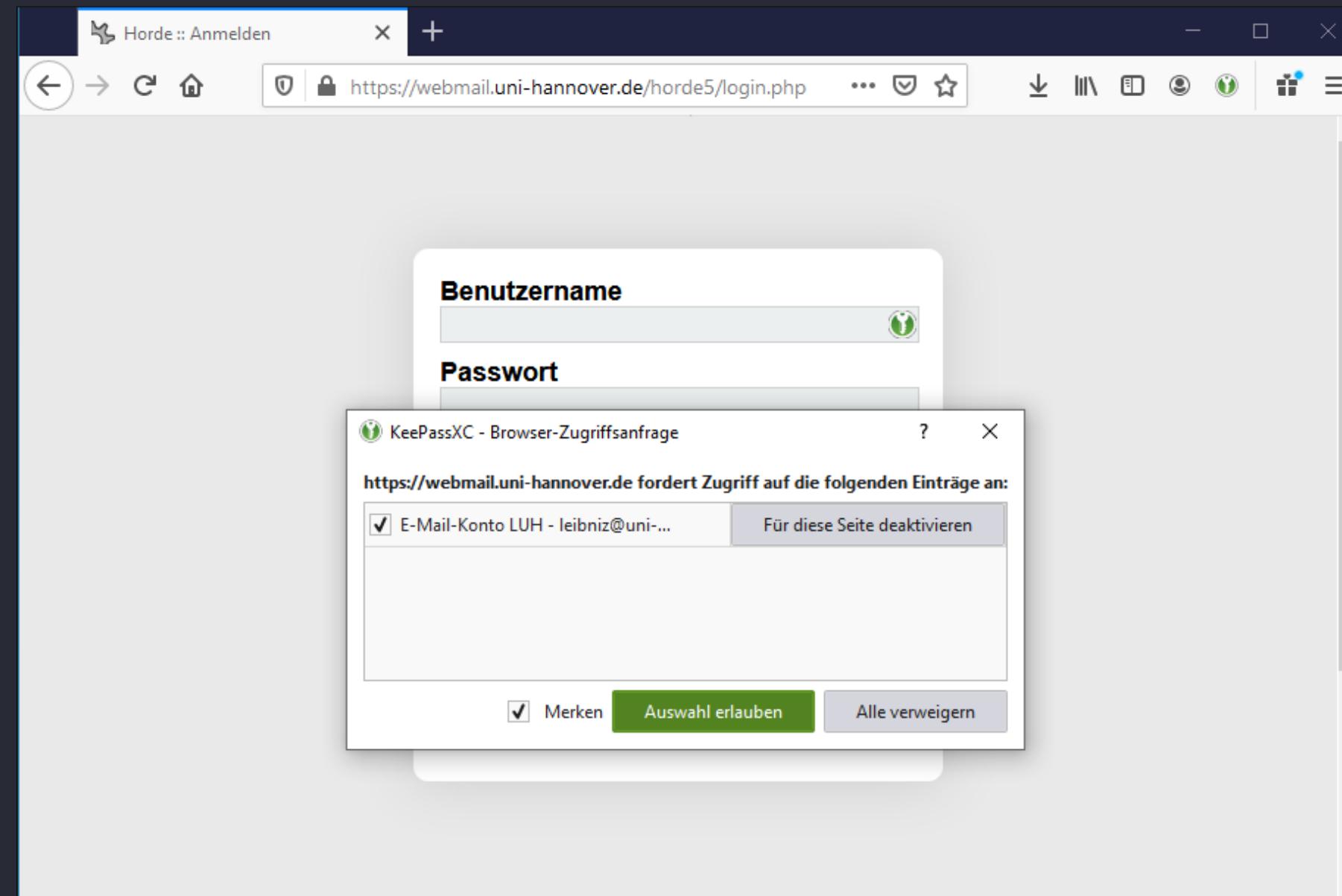
Stable release: 22.01 (15 July 2022; 5 months ago)

Programming languages: C, C++, Assembly language

Verwendung des KeePassXC Browser Addons

Bietet nicht nur praktisches Auto-Fill sondern auch prüft direkt die URL der Website!

Verhindert die versehentliche Eingabe von Zugangsdaten auf betrügerischen Website-Kopien



Für Firefox, Chrome, Edge: <https://keepassxc.org/download/#browser>

Ad-Blocker nutzen!

Diese Browser-Addons sorgen nicht nur für ein angenehmeres Internet-Erlebnis sondern schützen auch vor betrügerischen Anzeigen ("Malvertising")



Für Firefox, Chrome, Edge, Opera: <https://ublockorigin.com/>

Ad-Blocker nutzen!

Diese Browser-Addons sorgen nicht nur für ein angenehmeres Internet-Erlebnis sondern schützen auch vor betrügerischen Anzeigen ("Malvertising")



Für Firefox, Chrome, Edge, Opera: <https://ublockorigin.com/>

Bonustip Javascript-Blocker: Super effektiv aber echt anstrengend zu benutzen ...

Beispiel: Jetzt ein Tiramisu 😊

CHEFKOCH

z.B. Pfannkuchen, Lasagne, Low Carb

Wochenplaner Kochbuch Anmelden

PLUS Rezepte Magazin Videos Community

flaschenpost 20% AUF ALLES*

DEINEN EINKAUF LIEFERN LASSEN.

Jetzt neu bei dir

*Exklusiv in den neuen Liefergebieten.
Alle Infos: flaschenpost.de/erweitertes-liefergebiet

SPAZIERENGEHEN ZUM ABNEHMEN: WIE VIEL DU IN JEDEM ALTER GEHEN MUSST UM 20 KG ZU VERLIEREN

Alter Zielgewicht (kg)

45	62
55	65
65	70

BERECHNEN

PLUS Nutze Chefkoch ohne Banner!

Tiramisu

So gut wie beim Italiener

4,8 (622) 430 Kommentare

CK_Print Magazin/Tobias Pankratz/Blueberry Food Studios

Speichern Planen Drucken

30 Min. Arbeitszeit Normal Schwierigkeit 9.12.2004 Erstellt am

Viele Menschen wissen das nicht!
sicherclip.org

Weitere Rezepte - genauso gut!

Spaghetti-Eis-Dessert 4,8/5 (1099)
30 Min. normal simpel

Crème brûlée 4,8/5 (1132)
20 Min. normal simpel

Tiramisu 4,8/5 (1082)
30 Min. normal simpel

Mascarpone-Himbeerquark 4,8/5 (1062)
15 Min. normal simpel

Anzeige

SPAZIERENGEHEN ZUM ABNEHMEN: WIE VIEL DU IN JEDEM ALTER GEHEN MUSST UM 20 KG ZU VERLIEREN

Alter

45

Jetzt neu bei dir

*Exklusiv in den neuen Liefergebieten.
Alle Infos: flaschenpost.de/erweitertes-liefergebiet

Beispiel: Jetzt ein Tiramisu 😊

The screenshot shows the CHEFKOCH website interface with several promotional banners overlaid on the content:

- Banner 1 (Top Left):** A red banner for "flaschenpost" offering "20% AUF ALLES*" on purchases. It includes the text "DEINEN EINKAUF LIEFERN LASSEN." and a green button "Jetzt neu bei dir".
- Banner 2 (Top Center):** An advertisement for "SPAZIERENGEHEN ZUM ABNEHMEN: WIE VIEL DU IN JEDEM ALTER GEHEN MUSST UM 20 KG ZU VERLIEREN". It features a colorful illustration of a woman walking and includes a weight loss calculator table.
- Banner 3 (Top Right):** Another "flaschenpost" banner with the same "20% AUF ALLES*" offer and "DEINEN EINKAUF LIEFERN LASSEN." message.
- Banner 4 (Bottom Left):** An advertisement for "Viele Menschen wissen das nicht!" featuring a person driving a car. The text reads: "Anzeige", "Viele Menschen wissen das nicht!", "sicherclip.org", and "Weiterlesen".
- Banner 5 (Bottom Center):** A second "SPAZIERENGEHEN ZUM ABNEHMEN" banner with the same text as Banner 2.

The main content on the page is a recipe for "Tiramisu". The recipe card includes:

- Rating: ★★★★☆ (4.2)
- Comments: 430 Kommentare
- Image: A photograph of a slice of tiramisu on a plate.
- Summary: "So gut wie beim Italiener"
- Preparation time: 30 Min.
- Difficulty: Normal
- Created: 9.12.2004
- Action buttons: Speichern, Planen, Drucken, and a share icon.

Below the recipe, there is a section titled "Weitere Rezepte - genauso gut!" with links to other dessert recipes:

- Spaghetti-Eis-Dessert (4.8/5, 1099 reviews)
- Crème brûlée (4.8/5, 1132 reviews)
- Tiramisu (4.8/5, 1082 reviews)
- Mascarpone-Himbeerquark (4.8/5, 1062 reviews)

Beispiel: Jetzt ein Tiramisu 😊

 CHEFKOCH

PLUS Rezepte Magazin Videos Community

Wochenplaner Kochbuch Anmelden

Tiramisu

So gut wie beim Italiener
★ 4,8/5 (622)



CK_Print-Magazin/Tobias Pankrath/Blueberry Food Studios

30 Min. Arbeitszeit Normal Schwierigkeit 9.12.2004 Erstellt am

Zutaten

Für 4 Portionen (-) 4 (+)

500 g Mascarpone	Italien	Europa	Dessert
100 g Puderzucker	Creme		
200 g Löffelbiskuits			
4 Eigelb			
2 Eiweiß			
3 Tasse/n Kaffee, gekochter abgekühlt			
2 EL Amaretto evtl. auch 3			
Kakaopulver, ungesüßtes zum Bestreuen			

Weitere Rezepte - genauso gut!

 ★ 4,8/5 (1099) Spaghetti-Eis-Dessert 30 Min. simpel	 ★ 4,8/5 (1132) Crème brûlée 20 Min. normal
 ★ 4,8/5 (1082) Tiramisu 30 Min. simpel	 ★ 4,8/5 (1062) Mascarpone-Himbeerquark 15 Min. simpel

Ähnliche Rezepte entdecken

Italien Europa Dessert

Creme

Beispiel: Jetzt ein Tiramisu 😊



CHEFKOCH

Wochenplaner Kochbuch Anmelden

PLUS Rezepte Magazin Videos Community

Tiramisu

So gut wie beim Italiener
★ 4,8/5 (622)

CK Print-Magazin/Tobias Pankratz/Blueberry Food Studios

🕒 30 Min. Arbeitszeit 🌐 Normal Schwierigkeit 📅 9.12.2004 Erstellt am

Zutaten

Für 4 Portionen (-) 4 (+)

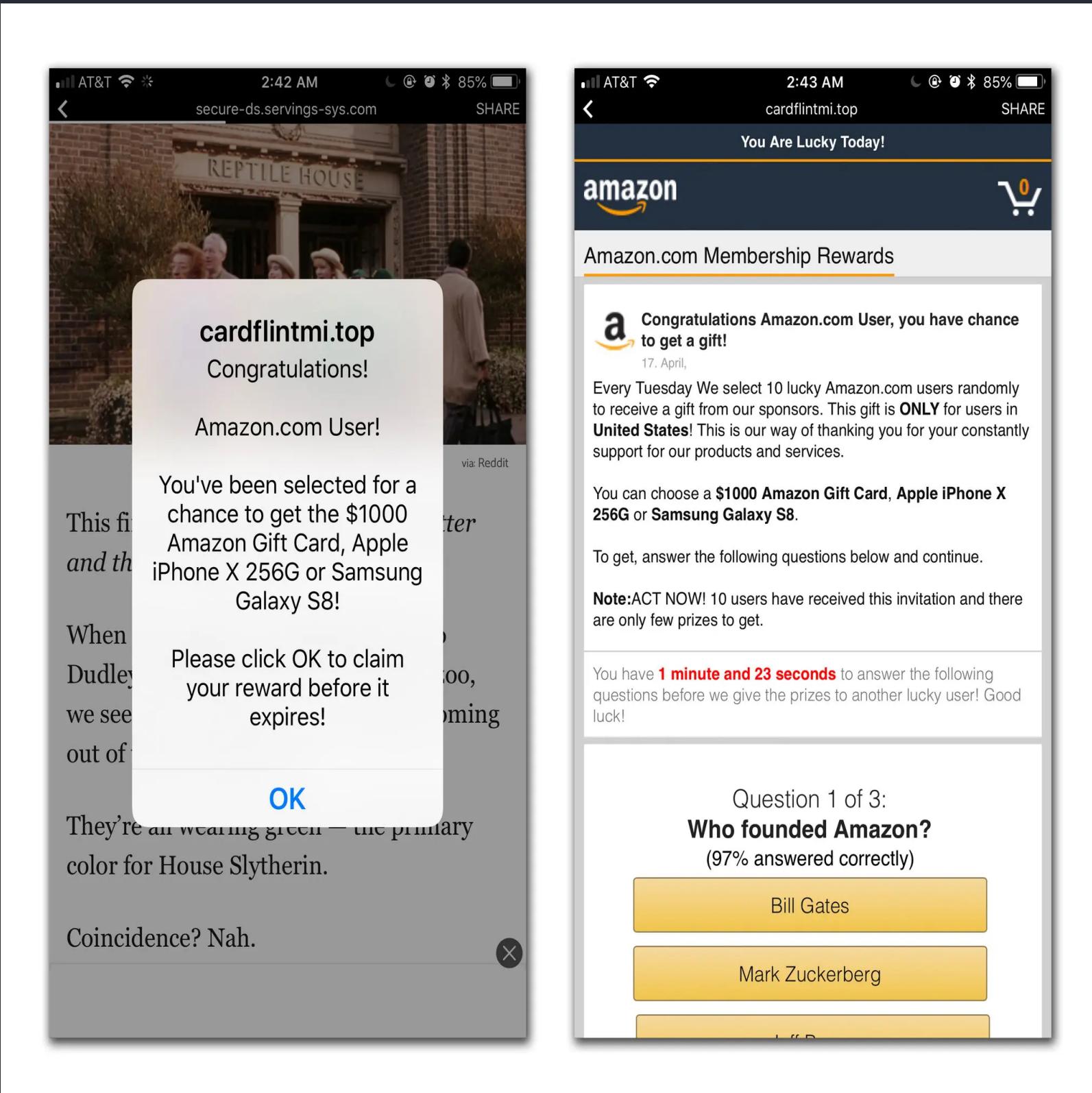
500 g Mascarpone
100 g Puderzucker
200 g Löffelbiskuits
4 Eigelb
2 Eiweiß
3 Tasse/n Kaffee, gekochter abgekühlt
2 EL Amaretto evtl. auch 3
Kakaopulver, ungesüßtes zum Bestreuen

Ähnliche Rezepte entdecken: Italien, Europa, Dessert, Creme

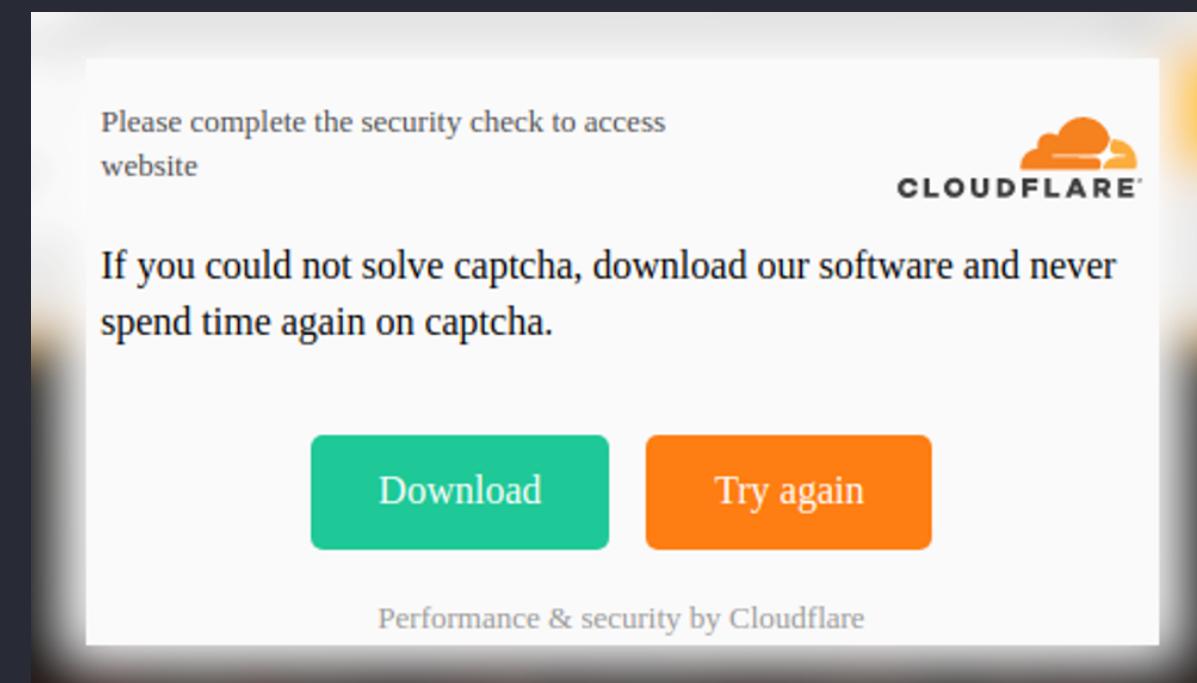
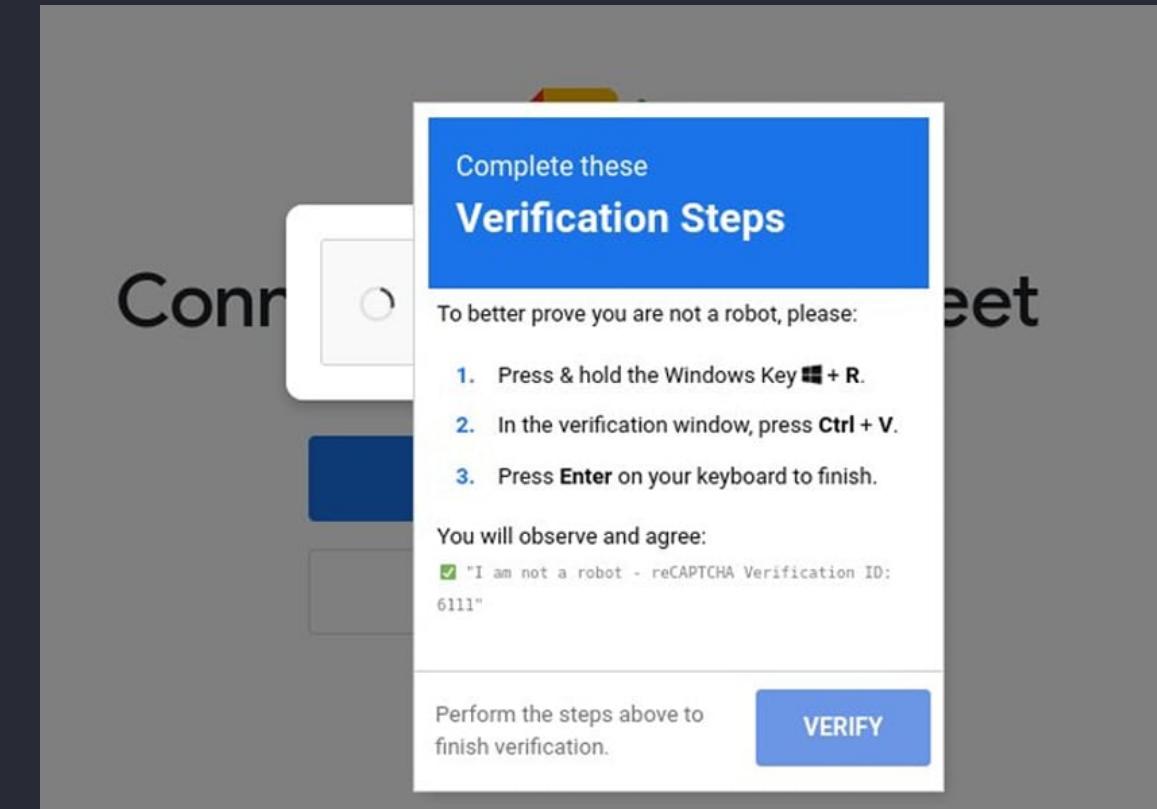
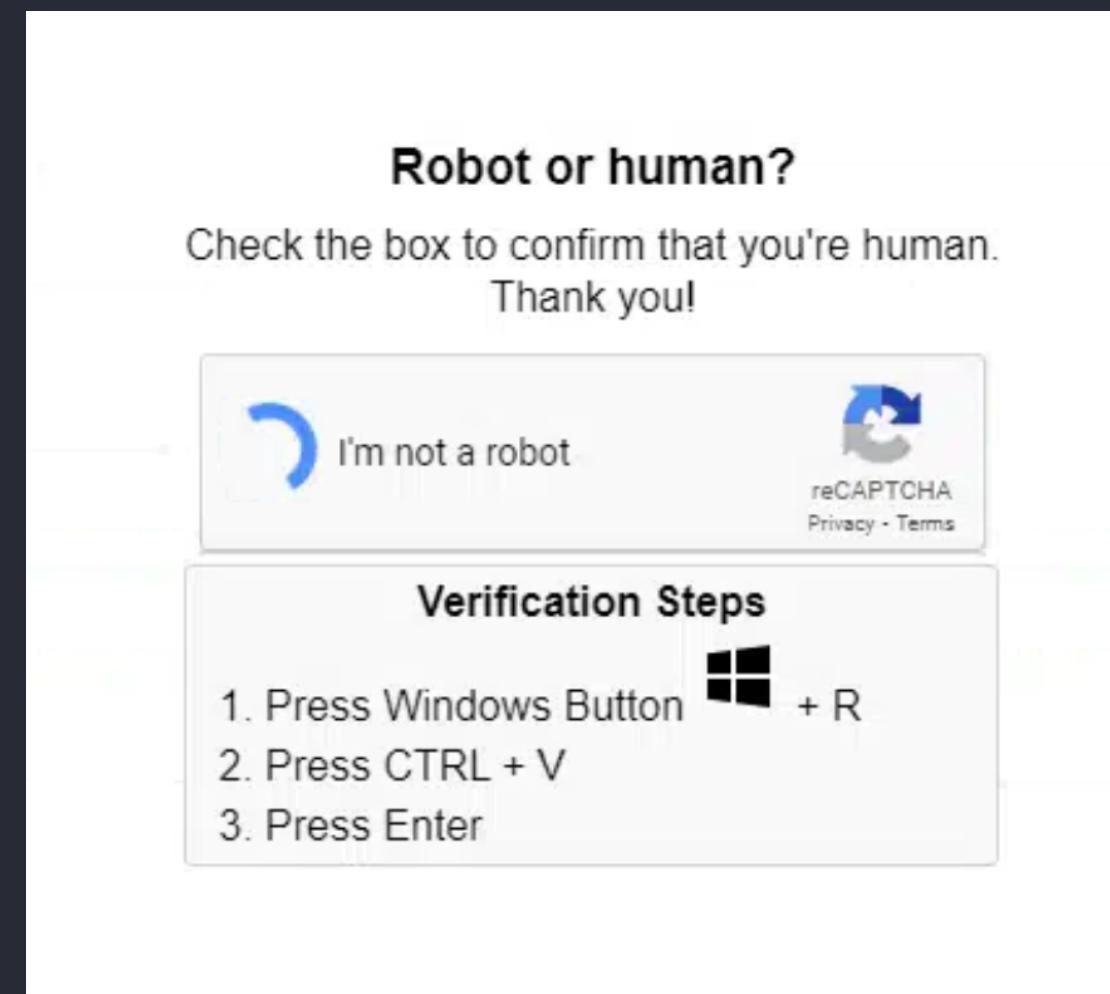
Weitere Rezepte - genauso gut!

- ★ 4,8/5 (1099) Spaghetti-Eis-Dessert 30 Min. 🌐 simpel
- ★ 4,8/5 (1132) Crème brûlée 20 Min. 🌐 normal
- ★ 4,8/5 (1082) Tiramisu 30 Min. 🌐 simpel
- ★ 4,8/5 (1062) Mascarpone-Himbeerquark 15 Min. 🌐 simpel

Werbung ist nicht nur nervig sondern kann auch gefährlich sein!



Beispiel: Fake-Captchas



Browser-Empfehlung

Welchen Browser soll ich denn nun nutzen?



Mozilla Firefox

Für den alltäglichen Gebrauch



LibreWolf

Für die besonders engagierten

Bonustip: Tracking verringern für mehr Privatsphäre im Browser

Stellt euren Browser so ein, dass **beim Start sämtliche Cookies gelöscht werden**. Damit die Usability nicht zu sehr leidet können Cookies **einzelner Websites behalten** werden (z.B. E-Mail Login, SSO / IDM, ...)

Bonustip: Tracking verringern für mehr Privatsphäre im Browser

Stellt euren Browser so ein, dass **beim Start sämtliche Cookies gelöscht werden**. Damit die Usability nicht zu sehr leidet können Cookies **einzelner Websites behalten** werden (z.B. E-Mail Login, SSO / IDM, ...)



Das Browser-Addon "Privacy Badger" von der EFF blockiert bekannte Tracker ganz automatisch
<https://privacybadger.org/>

Was tun wenn doch mal etwas passiert?

Falschen Link geklickt, komischen E-Mail Anhang geöffnet oder "Mein Computer tut komische Dinge"?

1. Fehler eingestehen und Probleme anerkennen

Jedem Menschen passieren Fehler. Ob bewusst oder unbewusst. Selbst den Profis :)

Es ist nichts schlimmer als sich in Problemfällen dafür zu **schämen** den falschen Link geklickt oder den falschen Anhang geöffnet zu haben. Gerade in der IT sorgt das **Ignorieren solcher Probleme** häufig für eine **Verschlimmerung!**

2. Sofortmaßnahmen ergreifen

Ein paar Dinge helfen stets den Schaden **einzudämmen** und **weitere Probleme** zu **verhindern**.

2. Sofortmaßnahmen ergreifen

Ein paar Dinge helfen stets den Schaden **einzudämmen** und **weitere Probleme** zu **verhindern**.

1. Verdächtige E-Mails und Co. nicht löschen (Nachvollziehbarkeit / "Gutprüfung")
 - Wenn ein Anhang geöffnet oder ein Programm ausgeführt wurde ist es eh zu spät

2. Sofortmaßnahmen ergreifen

Ein paar Dinge helfen stets den Schaden **einzudämmen** und **weitere Probleme** zu **verhindern**.

1. Verdächtige E-Mails und Co. nicht löschen (Nachvollziehbarkeit / "Gutprüfung")
 - Wenn ein Anhang geöffnet oder ein Programm ausgeführt wurde ist es eh zu spät
2. Verdächtige Fenster und Programme schließen

2. Sofortmaßnahmen ergreifen

Ein paar Dinge helfen stets den Schaden **einzudämmen** und **weitere Probleme** zu **verhindern**.

1. Verdächtige E-Mails und Co. nicht löschen (Nachvollziehbarkeit / "Gutprüfung")
 - Wenn ein Anhang geöffnet oder ein Programm ausgeführt wurde ist es eh zu spät
2. Verdächtige Fenster und Programme schließen
3. Auf dem Gerät nicht mehr in neue Dienste einloggen

2. Sofortmaßnahmen ergreifen

Ein paar Dinge helfen stets den Schaden **einzudämmen** und **weitere Probleme** zu **verhindern**.

1. Verdächtige E-Mails und Co. nicht löschen (Nachvollziehbarkeit / "Gutprüfung")
 - Wenn ein Anhang geöffnet oder ein Programm ausgeführt wurde ist es eh zu spät
2. Verdächtige Fenster und Programme schließen
3. Auf dem Gerät nicht mehr in neue Dienste einloggen
4. Gerät vom Netzwerk trennen

2. Sofortmaßnahmen ergreifen

Ein paar Dinge helfen stets den Schaden **einzudämmen** und **weitere Probleme** zu **verhindern**.

1. Verdächtige E-Mails und Co. nicht löschen (Nachvollziehbarkeit / "Gutprüfung")
 - Wenn ein Anhang geöffnet oder ein Programm ausgeführt wurde ist es eh zu spät
2. Verdächtige Fenster und Programme schließen
3. Auf dem Gerät nicht mehr in neue Dienste einloggen
4. Gerät vom Netzwerk trennen
5. Gerät herunterfahren

2. Sofortmaßnahmen ergreifen

Ein paar Dinge helfen stets den Schaden **einzudämmen** und **weitere Probleme** zu **verhindern**.

1. Verdächtige E-Mails und Co. nicht löschen (Nachvollziehbarkeit / "Gutprüfung")
 - Wenn ein Anhang geöffnet oder ein Programm ausgeführt wurde ist es eh zu spät
2. Verdächtige Fenster und Programme schließen
3. Auf dem Gerät nicht mehr in neue Dienste einloggen
4. Gerät vom Netzwerk trennen
5. Gerät herunterfahren
6. Wenn betroffen: Kritische Zugänge direkt sperren lassen (z.B. Online-Banking)

3. Hilfe suchen

Fragt den IT-Menschen in eurem Umfeld um Rat

Im Normalfall sind IT-Menschen sehr **dankbar** wenn Nutzende aktiv zu solchen Problemen und Sicherheitsbedenken **nachfragen**! Seid ihr euch bei einer E-Mail unsicher fragt euren IT-Menschen gerne **im Vorfeld**.

4. Nachbereitung

Gemeinsam mit der IT prüfen

4. Nachbereitung

Gemeinsam mit der IT prüfen

- Lag überhaupt eine Kompromittierung vor?
 - Falls ja: Wechsel aller prinzipiell betroffenen Passwörter und Zugänge

4. Nachbereitung

Gemeinsam mit der IT prüfen

- Lag überhaupt eine Kompromittierung vor?
 - Falls ja: Wechsel aller prinzipiell betroffenen Passwörter und Zugänge
- Welche Daten sind betroffen?
 - Bei dem **Verdacht des Datenabflusses** ist eine **Meldung** beim IT-Sicherheitsbeauftragten und Datenschutzbeauftragten der Hochschule notwendig. Das ist nicht schlimm aber **zwingend notwendig!**

4. Nachbereitung

Gemeinsam mit der IT prüfen

- Lag überhaupt eine Kompromittierung vor?
 - Falls ja: Wechsel aller prinzipiell betroffenen Passwörter und Zugänge
- Welche Daten sind betroffen?
 - Bei dem **Verdacht des Datenabflusses** ist eine **Meldung** beim IT-Sicherheitsbeauftragten und Datenschutzbeauftragten der Hochschule notwendig. Das ist nicht schlimm aber **zwingend notwendig!**

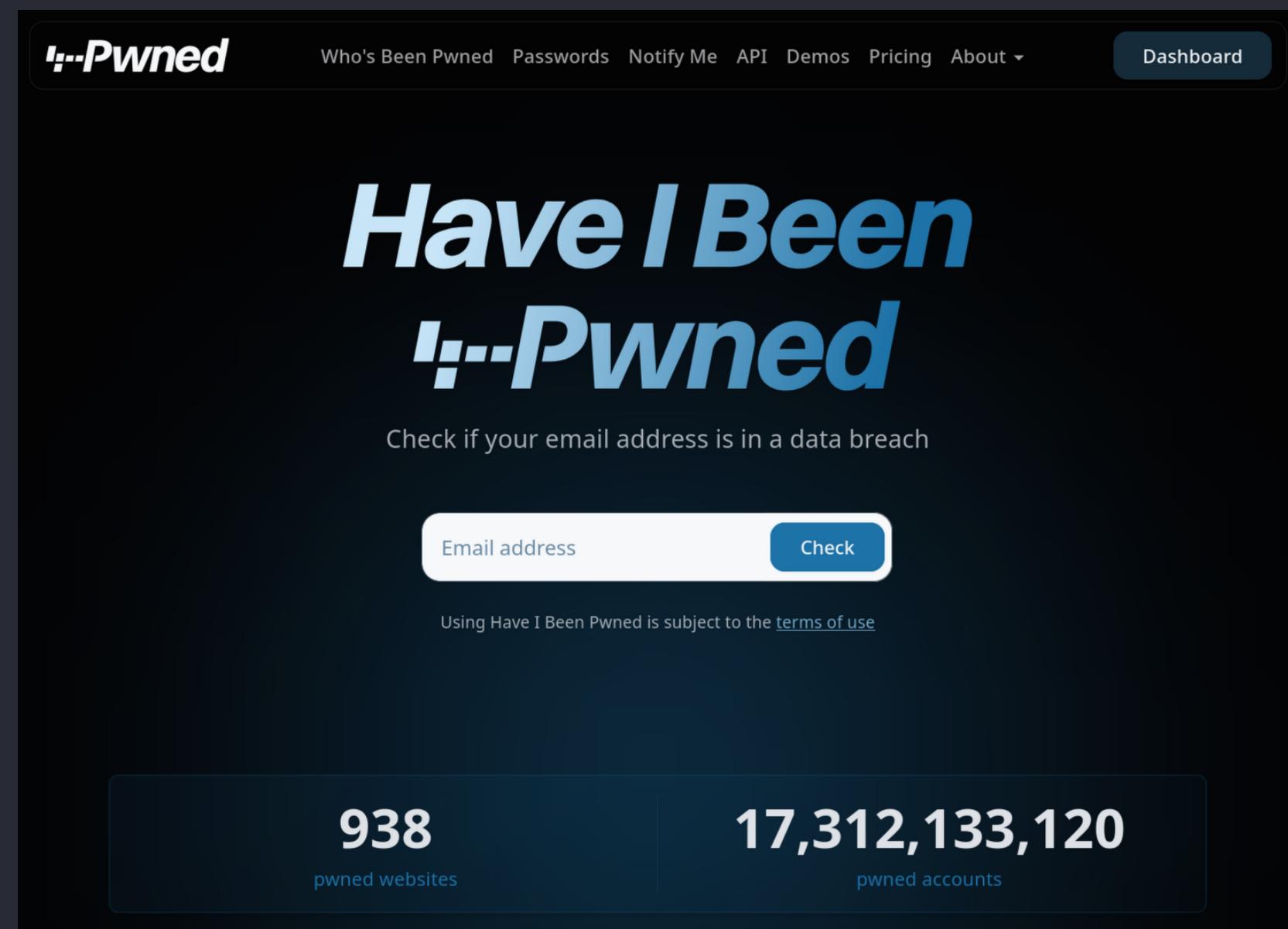
Wenn vorhanden: Rücksetzung auf vorheriges Backup zum Ausschluss weiterer Kompromittierung

-> **Backups gerne in einem weiteren Termin**

Ihr habt ja hoffentlich alle welche ... ;)

Bonustip: Herausfinden wenn man von Daten- / Passwort-Leaks betroffen ist

Sammlung von öffentlichen Daten-Leaks mit Prüf- und Benachrichtigungsfunktion



<https://haveibeenpwned.com/>

Bonustip: Herausfinden wenn man von Daten- / Passwort-Leaks betroffen ist

Email Breach History
Timeline of data breaches affecting your email address

13 Data Breaches

Oh no — pwned! This email address has been found in multiple data breaches. Review the details below to see where your data was exposed.

Stay Protected
Get notified when your email appears in future data breaches [Notify Me](#)

The timeline shows three data breach entries:

- Oct 2013: 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[View Details](#)
- Jul 2012: Dropbox**
In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).
Compromised data:
 - Email addresses
 - Passwords[View Details](#)
- Mar 2012: 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...
[View Details](#)

Q&A Session

Noch nicht erschlagen? Dann gerne fragen!