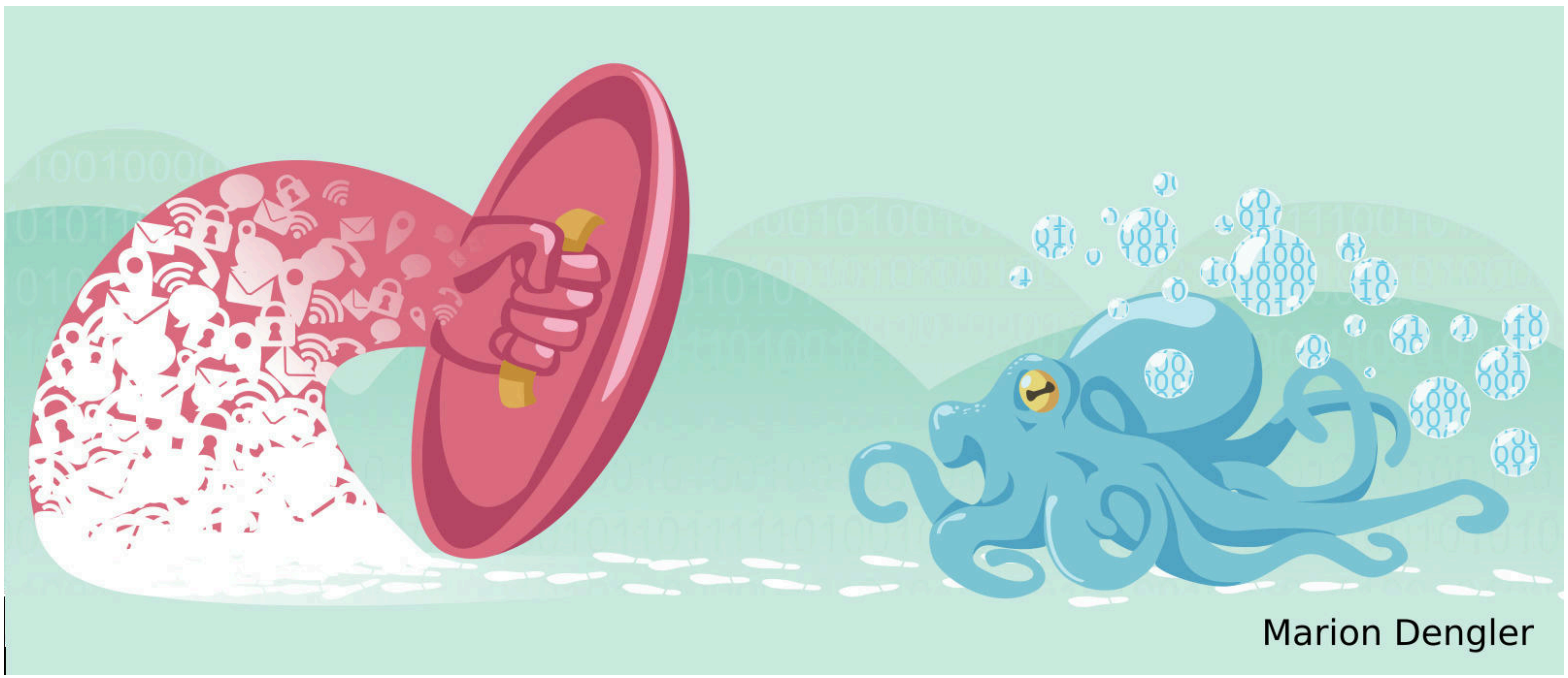
Digitale Selbstverteidigung



2025-05-25

Wer sind wir?

- Gemeinnütziger Verein, zum Austausch über Technik und ihrer gesellschaftlicher Auswirkungen
- Treffen finden regelmäßig jede Woche statt
- Veranstaltungen/Workshops zur Volks- & Berufsbildung
- Offen für alle interssierten Wesen

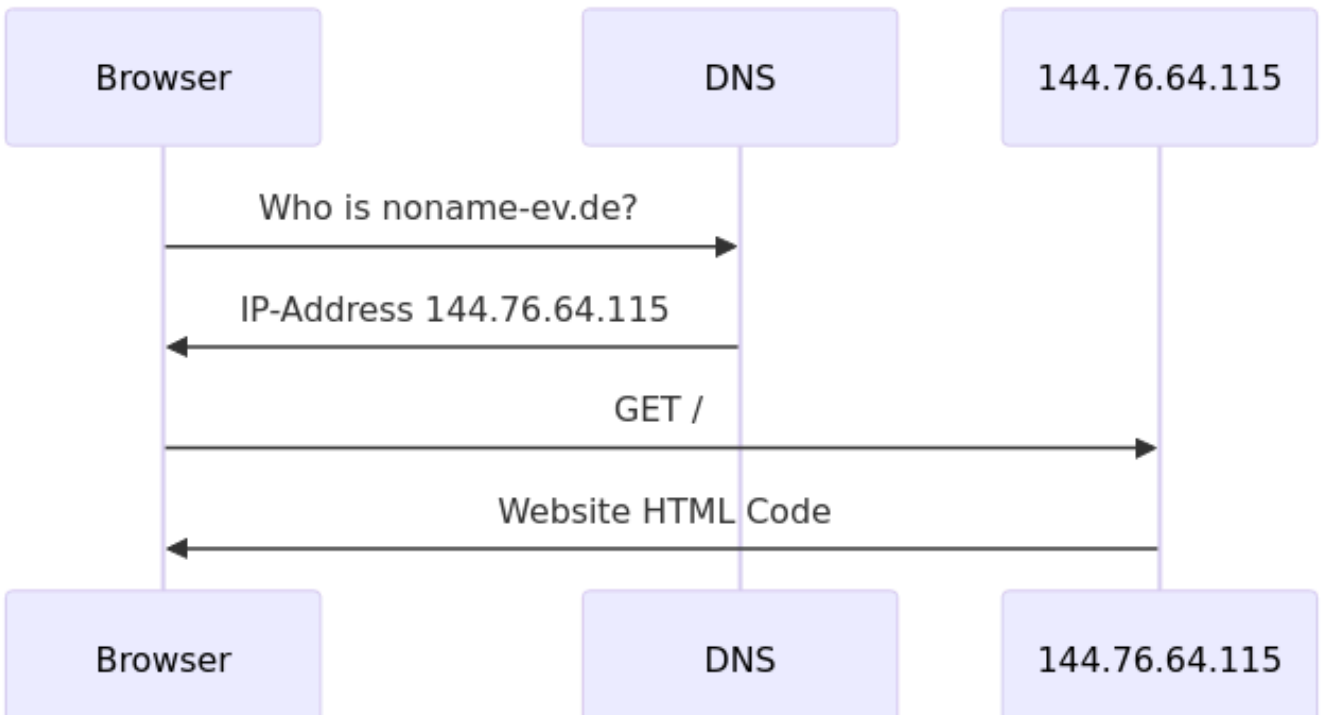
NoNAME
www.noname-ev.de

Roter Faden

- Wie werden Benutzer im Internet verfolgt?
  - Wie funktioniert das eigentlich überhaupt?
  - Was passiert mit den Daten?
- Was für Konsequenzen hat das für den einzelnen und die Gesellschaft?
- Gibt es Alternativen?
- Praxis Tip: Sichere Zugänge

Wie funktioniert das Internet?

Wie funktioniert das Internet?



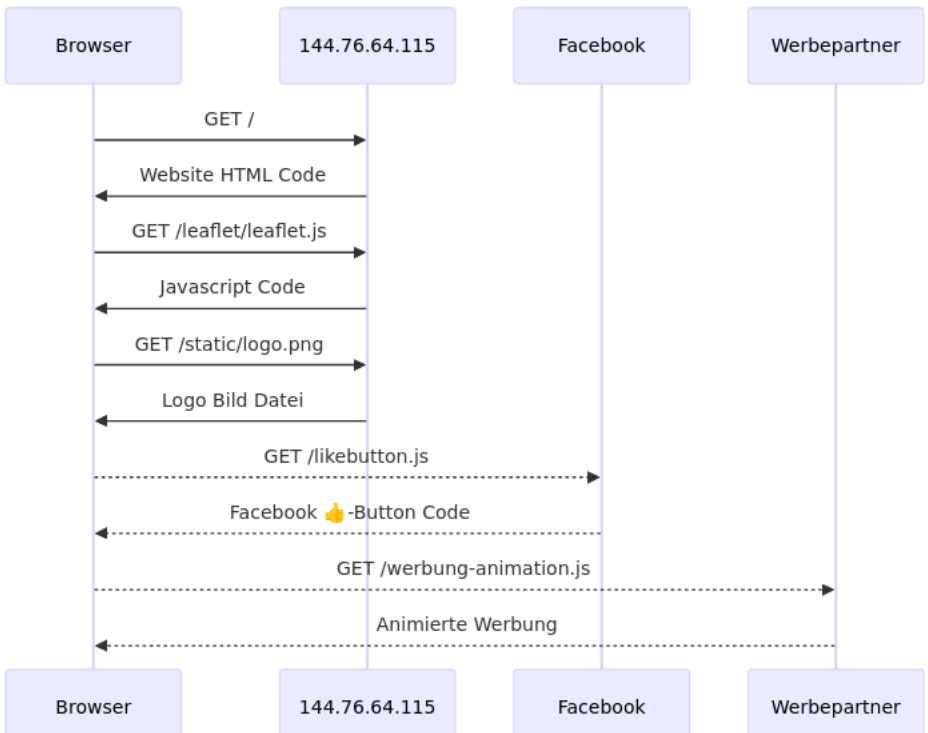
Wie funktioniert das Internet?

HTML - Hyper Text Markup Language

```
<!DOCTYPE html>
<html lang="de">
    <head>
        ...
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <link rel="stylesheet" href="/css/main.css">
        <script src="/leaflet/leaflet.js"></script>
        ..
    </head>
    <body lang="de">
        ...
    <h1 id="digitale-selbstverteidigung">Digitale Selbstverteidigung</h1>
    <div class="main_right">
        <img src="/img/logo.jpg"/>
    </div>
    ...
    </body>
</html>
```

- Strukturierter Text
- Enthält Referenzen auf weitere Resourcen die geladen werden müssen
  - Bilder
  - Styling
  - Code
- Diese können auch von ganz anderen Server stammen!

Wie funktioniert das Internet?



Wo fallen Daten an?


```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:136.0)
Gecko/20100101 Firefox/136.0
Accept: text/html, application/xhtml+xml, application/xml
Accept-Language: en-US,en;q=0.5
Referer: https://www.noname-ev.de/cryptoparty.html
Cookies: RGFzIGlzdCBlaW4gYmVpc3BpZWwgQ29va2llCg==
...
```

Grundsätzliche Daten

Fallen durch die Kommunikation an sich an

- Zeitpunkt
- IP-Addresse
  - grobe Geoposition
  - Internet Anbieter

Anfrage Daten

Werden vom Browser in Anfrage übermittelt

- Browser Daten
  - Version
  - Betriebsystem
- Referer
  - Von welcher Seite bin ich gekommen?
- Cookies 🍪
  - Wiedererkennung bei erneutem Aufruf

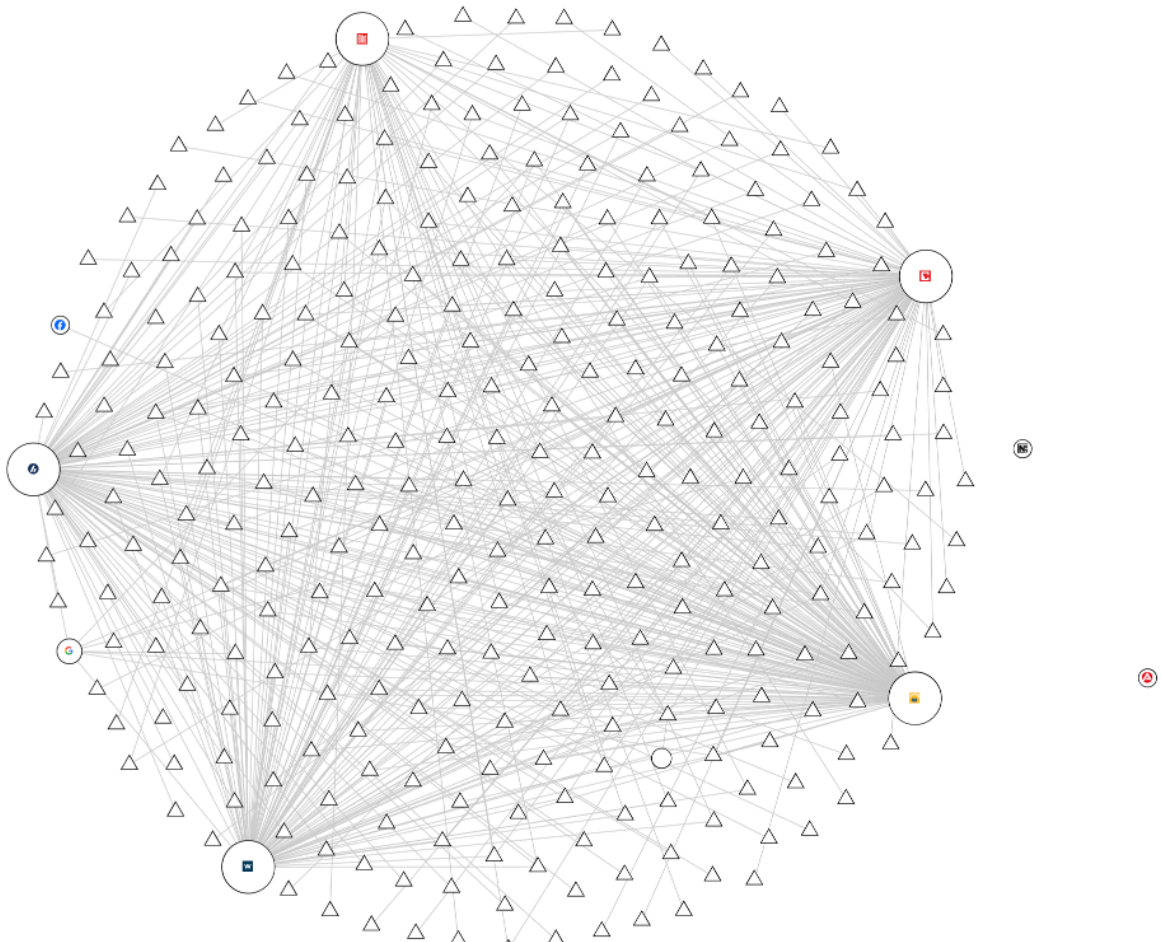
Was bedeuted Tracking im Netz?

1. Es ist grundsätzlich möglich über das Sammeln von Metadaten zu erhalten Anfragen den einzelnen Nutzer wieder zu erkennen.
2. Das ist auch für 3te-Parteien möglich, auf deren Seite man nicht direkt gegangen ist, sondern von denen nur einzelnen Inhalte bezogen werden. Beispiele für extern bezogenen Inhalte: Bilder, Funktionalität (Code) und insbesondere Werbung!
3. Über den Referer Header ist es 3ten-Parteien sogar möglich nachzuvollziehen auf welcher Seite man tatsächlich unterwegs ist.

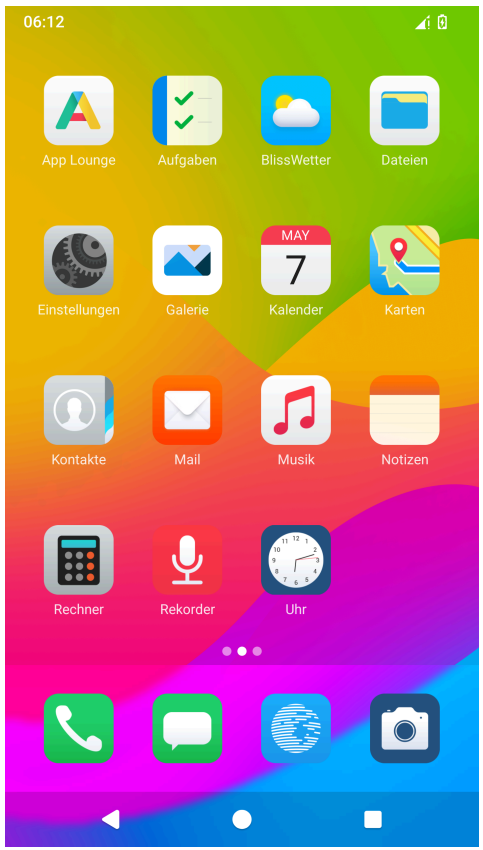
Was bedeuted Tracking im Netz?

1. Es ist grundsätzlich möglich über das Sammeln von Metadaten zu erhalten Anfragen den einzelnen Nutzer wieder zu erkennen.
2. Das ist auch für 3te-Parteien möglich, auf deren Seite man nicht direkt gegangen ist, sondern von denen nur einzelnen Inhalte bezogen werden. Beispiele für extern bezogenen Inhalte: Bilder, Funktionalität (Code) und insbesondere Werbung!
3. Über den Referer Header ist es 3ten-Parteien sogar möglich nachzuvollziehen auf welcher Seite man tatsächlich unterwegs ist.

DEMO



Mobile Apps sammeln auch Daten



- Mobile Apps ermöglichen Datensammelei über die gleichen Mechanismen
- Viele Apps speichern keine Daten auf dem Gerät -> permanente Kommunikation mit Online Diensten
- Potenziell Zugriff auf viel genauere Informationen
  - genauere Standort Daten
  - eindeutige Gerätekennung (Mobile Advertising IDs)
- Billig produzierte Apps nutzen Entwicklungsframeworks
  - Frameworks sind Aufwendig zu in der Entwicklung
  - Monetarisierung durch implizites Nutzer-Tracking
  - In-App Werbung
- Liste Bekannter Apps mit Tracking [1]

Was passiert mit den Daten?

Aufbereitung [2]

- Gesammelte Daten nach Nutzer Gruppiert
- Zuweisung von Kategorien (Annahmen über den Nutzer basieren auf den gesammelten Daten)
  - Frau/Mann/…
  - verheiratet/single/…
  - Fußballfan/Autoliebhaber/
  - Schwanger
  - Religiöse Zugehörigkeit

Verwertung

- Verkauf durch an/durch Databroker [3]
- Nutzung für geziehlte Werbung in Echtzeit
- Auswertung durch Käufer

Anonyme Daten?

Verkaufte Daten sind in der Regel “anonymisiert”.

Nur weil ein Datensatz nicht direkt den Namen, Telefonnummer und Wohnort einer Person enthält sind die Daten nicht automatisch anonym!

- Nur wenige eindeutige Signale in den Daten können dazu führen Rückschlüsse auf die Person hinter den Daten zu ziehen [4]
- Sobald genaue Standortdaten mit dabei sind ist es ein leichtes herauszufinden zu wem der Datensatz gehört
- Anhand der Browsing Historie lassen sich viel Informationen über eine Person erschließen:
  - Intressen
  - Lebensituation
- Potentiell Interessant für geziehltes Phishing -> Identitätsdiebstahl

Soziale Medien

Die großen Internet Konzerne haben es perfektioniert aus gesammelten Daten Geld zu machen

- Facebook, Youtube, Instagram, Ticktock

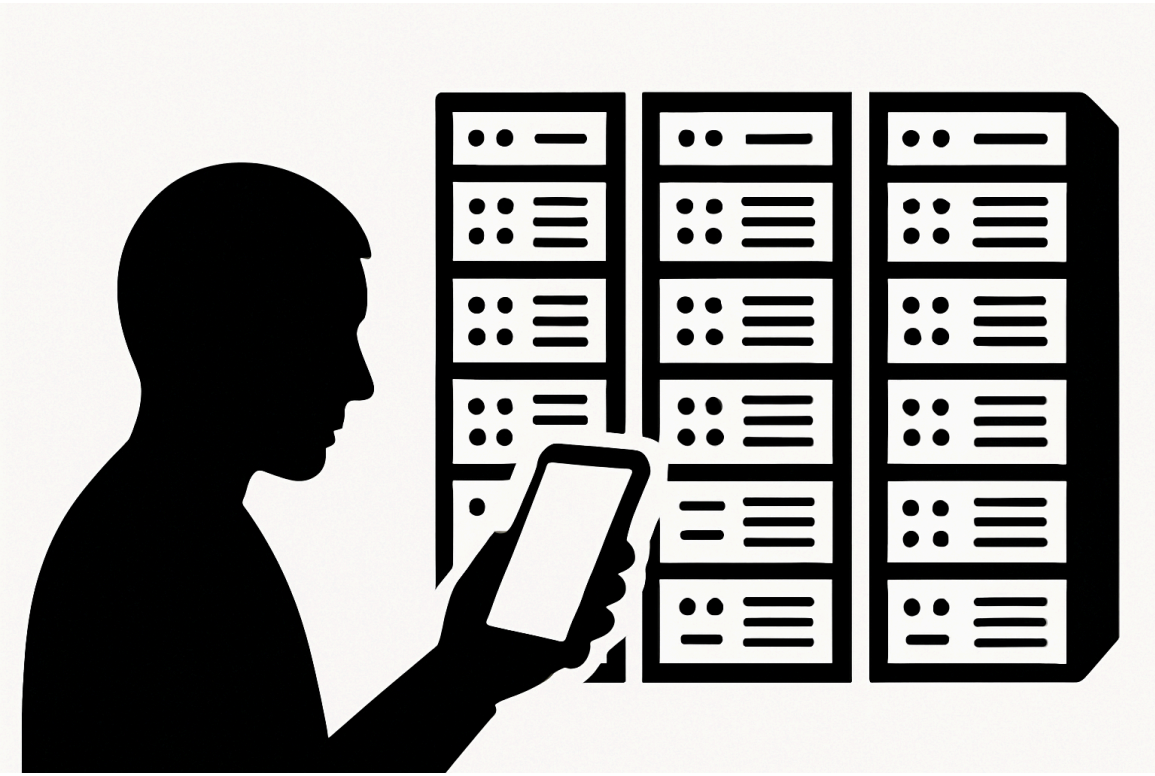
In Echtzeit finden Auktionen statt in denen Teilnehmer im Austausch für Geld dem Nutzer der Platform ihre Nachricht anzeigen dürfen (in der Regel Werbung)

- Stichwort: Aufmerksamkeitsökönomie, Attention-Economie [5], [6]

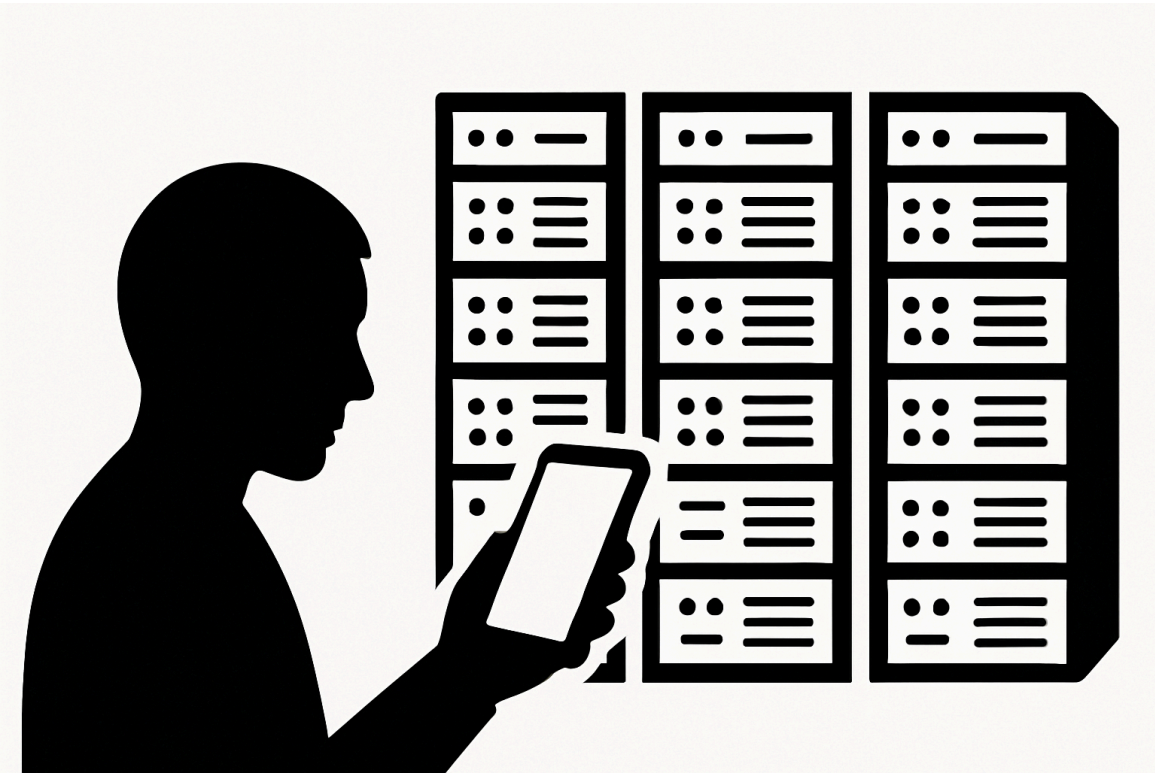
Ein Algorithmus entscheidet also was dem Nutzer als nächstes angezeigt wird

- je länger ein Nutzer auf einer Platform Zeit verbringt desto mehr Auktionen können stattfinden
- je mehr Auktionen passieren, desto mehr Geld verdient die Platform mit dem Nutzer
- Algorithmus entscheidet basierend auf Informationen über den Nutzer was gezeigt wird um den Nutzer möglichst lange auf der Platform zu halten

Wie gut kennt die Maschine euch?

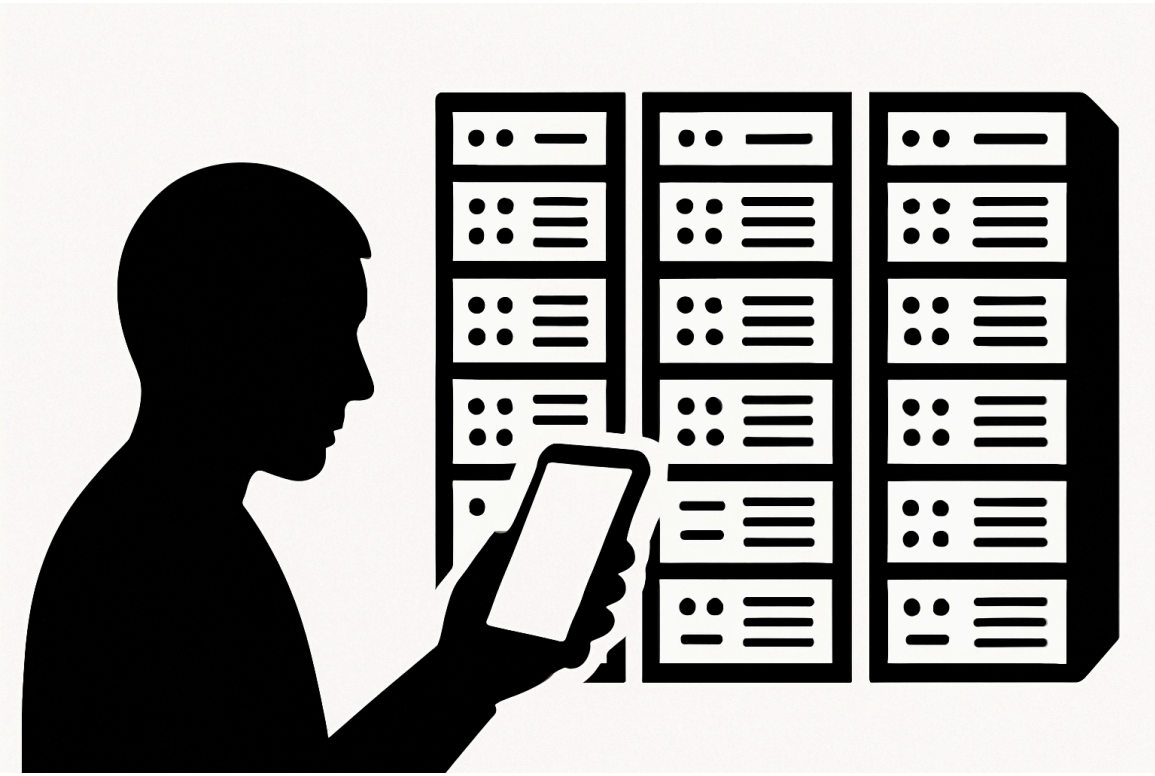


Wie gut kennt die Maschine euch?



Wer ist schon mal in ein “Youtube Rabithole” gefallen?

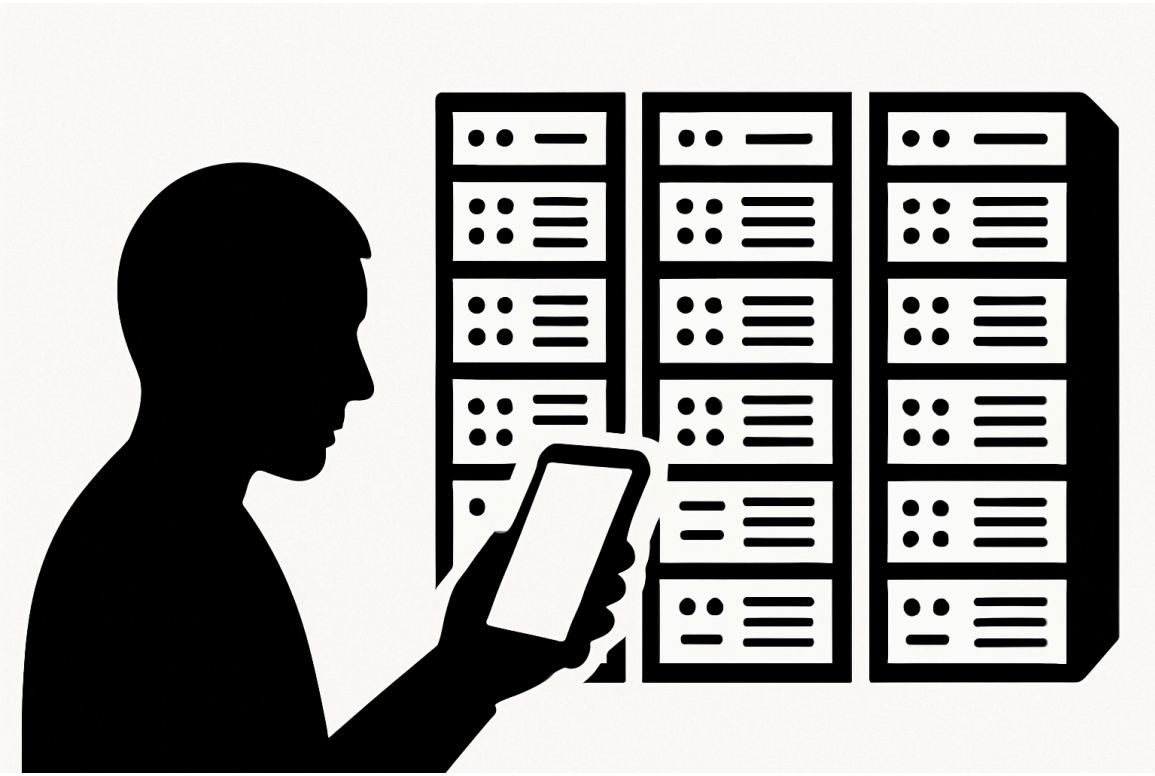
Wie gut kennt die Maschine euch?



Wer ist schon mal in ein “Youtube Rabithole” gefallen?

Wer hat schon mal die Zeit vergessen beim scrollen auf Social Media (Doomscrolling)?

Wie gut kennt die Maschine euch?

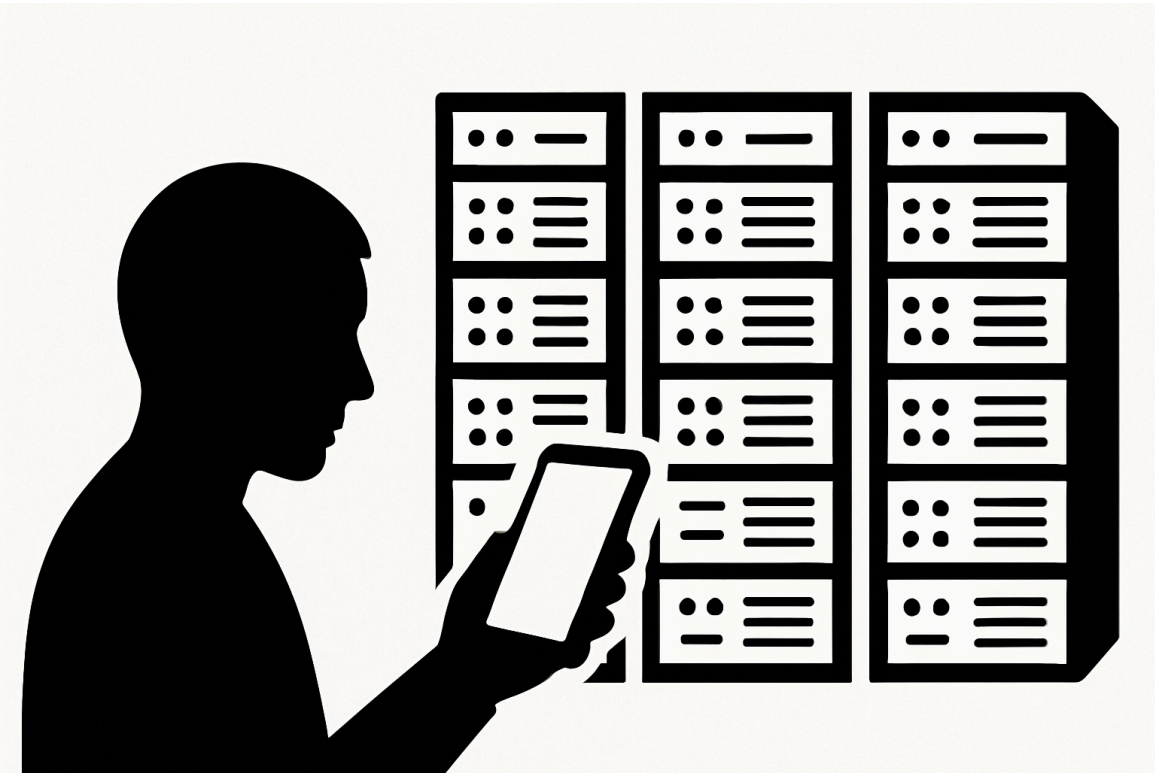


Wer ist schon mal in ein “Youtube Rabithole” gefallen?

Wer hat schon mal die Zeit vergessen beim scrollen auf Social Media (Doomscrolling)?

Je mehr Zeit ihr auf einer Social Media Platform verbringt desto mehr Geld verdient die Platform

Wie gut kennt die Maschine euch?



Wer ist schon mal in ein “Youtube Rabithole” gefallen?

Wer hat schon mal die Zeit vergessen beim scrollen auf Social Media (Doomscrolling)?

Je mehr Zeit ihr auf einer Social Media Platform verbringt desto mehr Geld verdient die Platform

Das Produkt ist eure Aufmerksamkeit und damit ist was verkauft wird eure Zeit!!!

Versteckte gesellschaftliche Kosten

- Entwicklung der nächsten Generationen
  - Zuviel Bildschirmzeit verzögert und behindert die Entwicklung von Kindern
- Die Welt verstehen
  - Fakenews verbreiten sich 6x schneller als Fakten

https://ledger.humanetech.com/

- Aufmerksamkeit und Kognitive Leistung
- Physikalische und Mentale Gesundheit
- Soziale Beziehungen
  - Soziale Medien lenken uns davon ab mit den Menschen die direkt vor uns sind zu interagieren
    $\rightarrow$ Man fühlt sich verbunden und doch sozial isoliert

- Politik und Wahlen
  - Microtargeting von Werbung ermöglicht geziehte Desinformation für den der am meisten zahlt
- Systemische Unterdrückung

Versteckte gesellschaftliche Kosten

- Entwicklung der nächsten Generationen
  - Zuviel Bildschirmzeit verzögert und behindert die Entwicklung von Kindern
- Die Welt verstehen
  - Fakenews verbreiten sich 6x schneller als Fakten

https://ledger.humanetech.com/

- Aufmerksamkeit und Kognitive Leistung
- Physikalische und Mentale Gesundheit
- Soziale Beziehungen
  - Soziale Medien lenken uns davon ab mit den Menschen die direkt vor uns sind zu interagieren
    → Man fühlt sich verbunden und doch sozial isoliert

- Politik und Wahlen
  - Microtargeting von Werbung ermöglicht geziehte Desinformation für den der am meisten zahlt
- Systemische Unterdrückung

Was ist euch eure Zeit Wert?

Alternative Dienste

Motivation1: Datenschutz

Wenn ihr nix zahlt seit ihr das Produkt

- Wenn ihr nicht versteht wie eine Firma Geld verdient, verkauftt sie meistens eure Daten
- Warum ist das problematisch
  - rechtliche Situationen können sich ändern
  - Diskriminierung
  - Verfolgung

Motivation2: Abhängikeit

- Was wäre es wenn Office 365 für 1 Woche abgeschaltet ist
- a) Cloud als zentraler Schwachpunkt (nicht der Fokus hier)
- b) Abhängigkeit von ausländischen Regierungen (z.B Amerika)
  - Aktuelles Beispiel USA Sanktionen gegen ICC [7]
- Software als Waffe - Spionage - Abschaltungen

Pilotprojekte

- https://european-alternatives.eu/
- Limux München (durchwachsen)

Vergleich China

- https://www.itsec.gov.cn/aqkkcp/cpgg/202312/t20231226_162074.html
  - Ziel unabhängige IT
  - Empfehlungen um von Amerikanischer Hardware wechzukommen
  - Alternative Software Empfehlungen

Disclaimer / Datenschutz / Unabhängigkeit / Lebenskomfort

- Jeder muss für sich selber entscheiden
  - Wo ist man bereit Kompromisse zu treffen?
  - Welche Daten sind einem wirklich wichtig
  - Was ist mein Bedrohungsscenario
- Unternehmen und Behörden sollten nicht für euch entscheiden dürfen
  - hilft hier: DSGVO

OpenSource

- Sourcecode ist frei verfügbar
- Kann normalerweise umsonst benutzt werden
  - Kosten sind der eigene Betrieb/Personal
- jeder kann sich anschauen was das Programm macht
- unabhängige Prüfungen ohne Behinderung durch Unternehmen
- Globales Kollektivgut
  - zu verstehen wie Forschungsergebnisse & mathematische Formeln
- OpenSource ist überall drinnen
  - Beispiel Sqlite in jedem Browser, auch Chrome

Email

- Selberhosten möglich, aber nur empfohlen wenn Hobby

Beispielhafte Anbieter:

- Wirtschaftsmodel ist der Kunde zahlt pro Monat x €
- posteo.de
  - Z.b. bekannt aus Verweigerung der Vorratsdatenspeicherung
- mailbox.org
  - Setzt sich generell auf mehreren Ebenen für Datenschutz ein
  - Transparents-Reports wie viele behördliche Anfragen es pro Jahr gibt (und wieviele ungültig sind)

Desktop/Android:

- Thunderbird statt Outlook oder GMail
- Applemail wirkt erstmal ok und ist mit multiplen Providern kompatibel

CloudDienste

- Nextcloud
  - Gibt es auch gehostet (monatliche Gebühr), z.B. bei Hetzner
  - Dateinsychronisation (vgl. Dropbox)
  - Editor (multiplayer Office)
  - Kalendar & Kontakte
- Empfehlung auch für Vereine
- viele Mailprovider können Kalendar und Kontaktbuch synchronization
  - funktioniert unter iOS nativ, Android benötigt App

Messenger

- End to End
  - Zwischen den Enden ist es technisch nicht möglich die Daten zu entschlüsseln
  - Perfect Forward Privacy (auch in Zukunft)
- Whatsapp (du bist das Produkt)
  - Darf laut Nutzungsbedingungen extrem viel
  - Laut Hersteller allerdings End to End
- Signal
  - Betrieben durch Spenden
  - Schützt nicht vor menschlichen Versagen

- Matrix (Element)
  - Opensource, Federation
  - “umsonst” (weil von Vereinen/Universitäten gehostet)
  - Universität Heidelberg -> HeiChat
  - Uni Account ist login

- Threema
  - App kostet Geld
  - Firma mit Sitz in der Schweiz

Langfristig:

- EU fordert Interoperabilität (Digital Markets Act)
  - Wie gut das technisch machbar ist, mal schauen

Browser

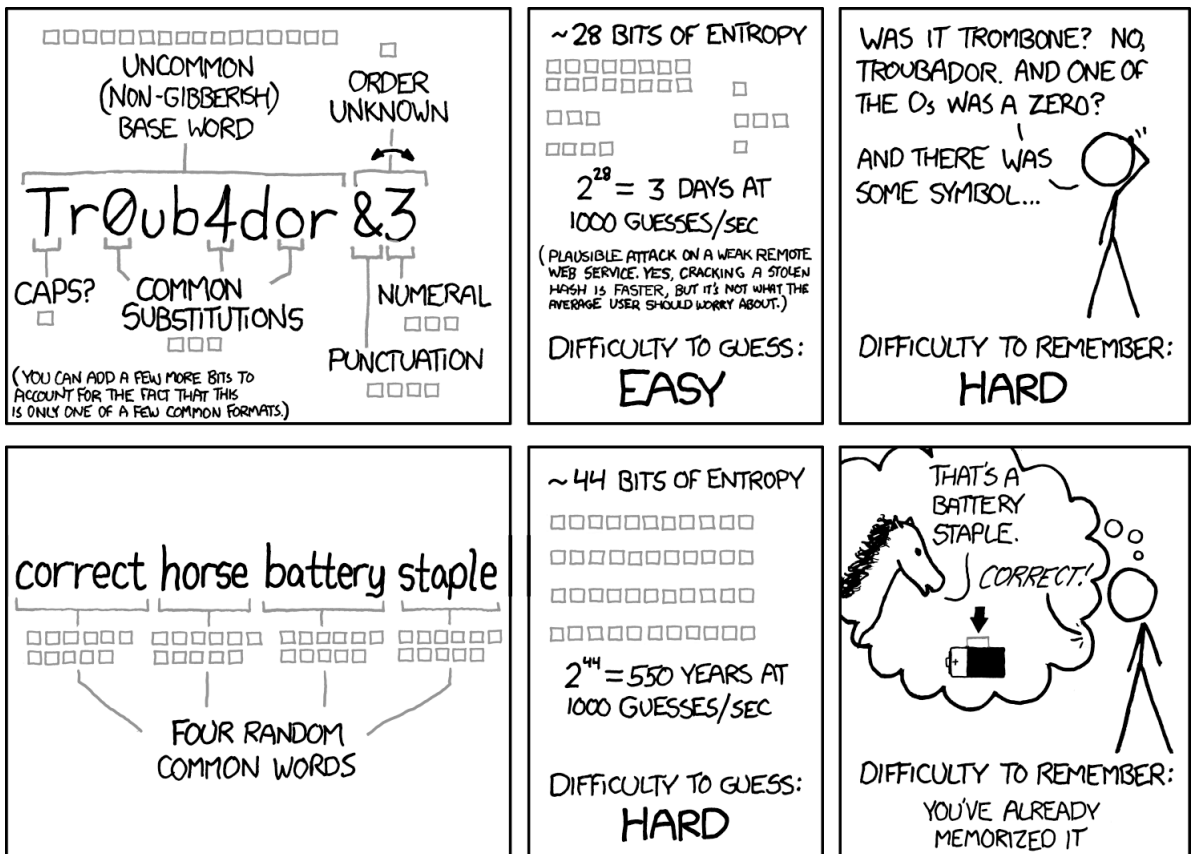
Egal welchen Browser ihr gut findet

- Installiert einen Adblocker
- Sowohl wegen Privacy als auch wegen Angriffen
  - Personalisierte Werbung ermöglicht auch gezielt unsichere Benutzer anzugreifen
- Chrome vs Firefox
  - Firefox als Empfehlung
  - Allerdings hat Google in Chrome Adblock apis reduziert (erst for kurzem)
- Leider momentan kein perfekter Browser verfügbar

- Browser sind sehr komplex
  - Video playback
  - Bildschirmaufnahme
  - Audio übertragung
  - 3d Grafiken ect.

  z.B Chrome hat > 32Million Zielen Sourcecode
- Teuer / Aufwendig zu programmieren
- Daher wenige Alternativen
  - natürliche Monpolbildung
  - regulatische Eingriffen sinnvoll

Sichere Passwörter / Sichere Zugänge



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Hive Systems Super Password Calculator

Password	correcthorsebatterystaple	25	characters long	
Lowercase	TRUE	26	abcdefghijkl	
Uppercase	FALSE	0	ABCDEFGHIJ	
Numbers	FALSE	0	0123456789	
Symbols 1	FALSE	0	^*%$!&@#	
Symbols 2	FALSE	0	-()=+_	
Symbols 3	FALSE	0	?/.>, <`~|;:]}[{	
		26	characters possible	
Combinations	236,773,830,007,968,000,000,000,000,000,000,000	236	dec	passwords
Hash	H/s (bcrypt)			
GPU	A100			
GPU quantity	8			
Crackspeed	1,045,197	1	m	H/s
Max Time Req.	226,535,165,442,496,000,000,000,000,000	226	oct	Seconds
	62,926,434,845,137,800,000,000,000	62	spt	Hours
	2,621,934,785,214,080,000,000,000	2	spt	Days
	374,562,112,173,440,000,000,000	374	sx	Weeks
	86,247,854,776,778,800,000,000	86	sx	Months
	7,183,382,973,189,250,000,000	7	sx	Years

HIVE SYSTEMS

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	7 secs	14 secs	23 secs
5	Instantly	11 secs	6 mins	15 mins	27 mins
6	1 sec	5 mins	5 hours	15 hours	1 day
7	10 secs	2 hours	2 weeks	1 month	3 months
8	2 mins	2 days	2 years	7 years	17 years
9	16 mins	2 months	84 years	411 years	1k years
10	3 hours	4 years	4k years	25k years	85k years
11	1 day	111 years	228k years	1m years	5m years
12	2 weeks	2k years	11m years	97m years	419m years
13	4 months	75k years	616m years	6bn years	29bn years
14	3 years	1m years	32bn years	376bn years	2tn years
15	30 years	50m years	1tn years	23tn years	144tn years
16	303 years	1bn years	86tn years	1qd years	10qd years
17	3k years	34bn years	4qd years	89qd years	705qd years
18	30k years	894bn years	234qd years	5qn years	49qn years
19	303k years	23tn years	12qn years	344qn years	3sx years
20	3m years	604tn years	633qn years	21sx years	242sx years
21	30m years	15qd years	32sx years	1spt years	16spt years
22	303m years	408qd years	1spt years	82spt years	1oct years
23	3bn years	10qn years	89spt years	5oct years	83oct years
24	30bn years	276qn years	4oct years	315oct years	5non years
25	303bn years	7sx years	241oct years	19non years	406non years

H/s (bcrypt) A100 with 8 GPUs

Stand 2025

Lasst uns ein Spiel spielen

Bitte die Hand heben, wenn ihr jemanden kennt auf den die folgenden Fragen zutreffen.

1. Ich habe bei (fast) allen Diensten das gleiche Passwort
2.
3.
4.

Lasst uns ein Spiel spielen

Bitte die Hand heben, wenn ihr jemanden kennt auf den die folgenden Fragen zutreffen.

1. Ich habe bei (fast) allen Diensten das gleiche Passwort
2. Mein Passwort enthällt öffentlich bekannte Informationen. Z.B. meinen Namen / Geburtstag / den Namen meines Hundes / Autos?
3.
4.

Lasst uns ein Spiel spielen

Bitte die Hand heben, wenn ihr jemanden kennt auf den die folgenden Fragen zutreffen.

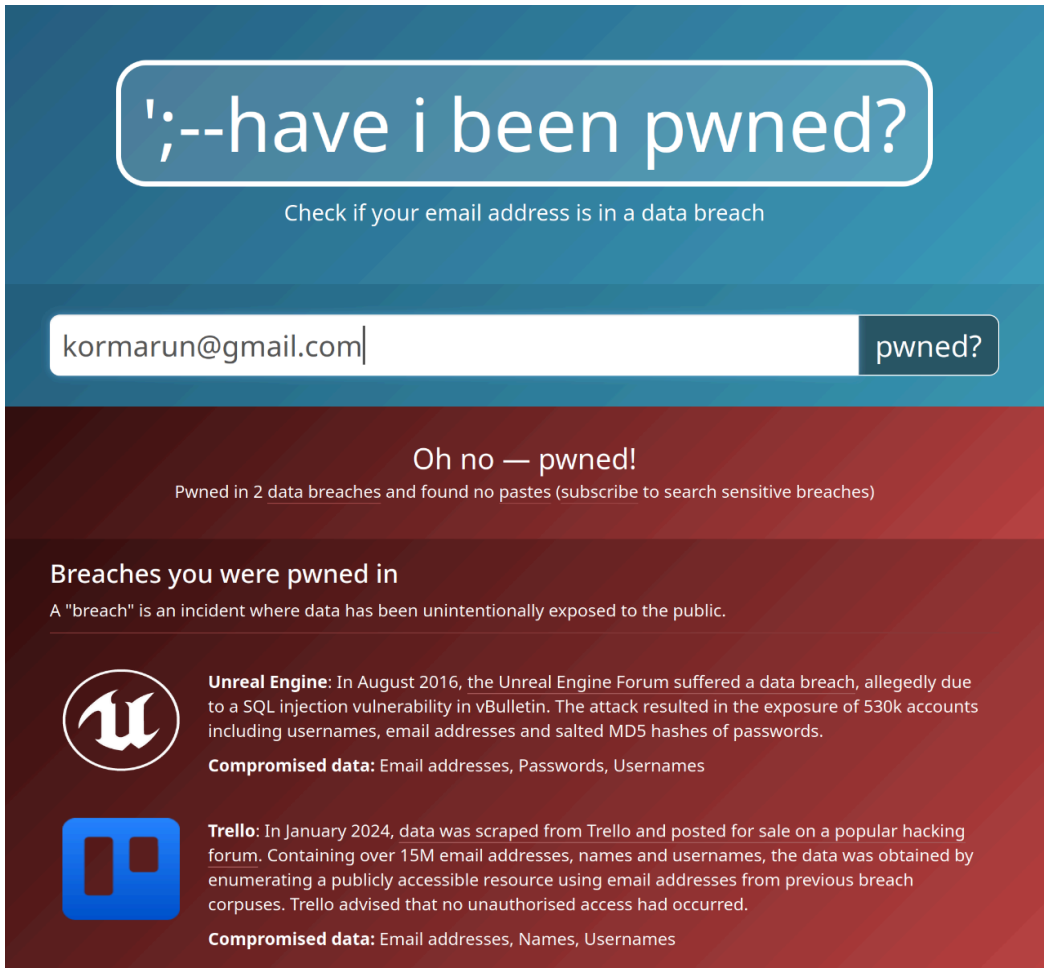
1. Ich habe bei (fast) allen Diensten das gleiche Passwort
2. Mein Passwort enthällt öffentlich bekannte Informationen. Z.B. meinen Namen / Geburtstag / den Namen meines Hundes / Autos?
3. Ich habe ein Passwort in den letzten 5 Jahren geändert?
4.

Lasst uns ein Spiel spielen

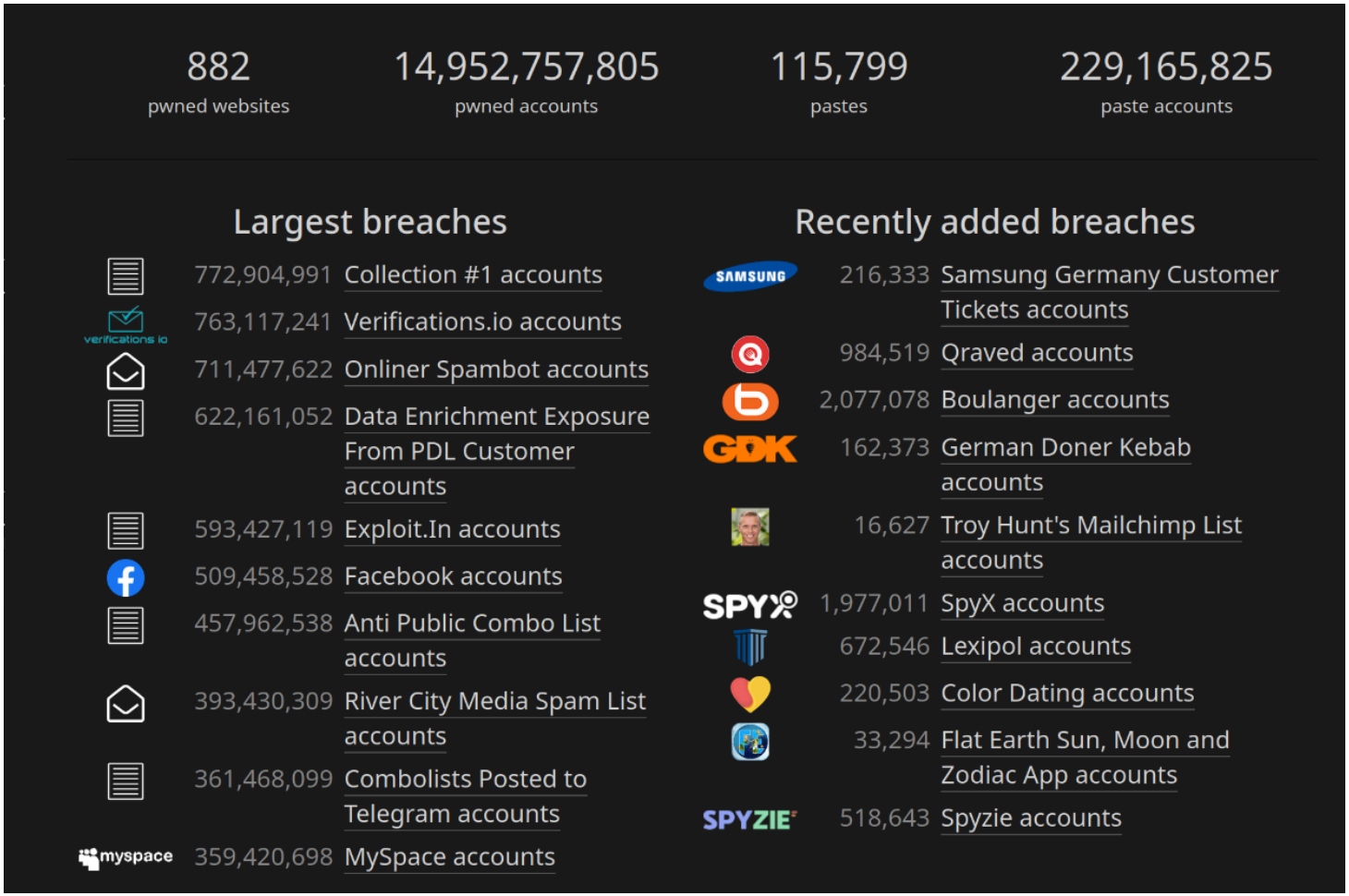
Bitte die Hand heben, wenn ihr jemanden kennt auf den die folgenden Fragen zutreffen.

1. Ich habe bei (fast) allen Diensten das gleiche Passwort
2. Mein Passwort enthällt öffentlich bekannte Informationen. Z.B. meinen Namen / Geburtstag / den Namen meines Hundes / Autos?
3. Ich habe ein Passwort in den letzten 5 Jahren geändert?
4. Ich habe von einem Dienst eine Email bekommen, dass Zugangsdaten entwendet wurden.

Demo HaveIBeenPwned



Früher oder später trifft es jeden



Früher oder später trifft es jeden

Deshalb: Risiko-Minimierung

- Nicht überall gleiches Passwort
  - Wenn einem Dienst Daten abhanden kommen, bleibt der Rest verschont
  - Gilt auch für Nutzernamen
- Hin und wieder prüfen ob es Lecks gab
  - Viele Passwort-Manager haben das eingebaut
- 2-Faktor Authentifizierung aktivieren
- Passwort-Manager

Zwei sind besser als eins

2-Faktor/Mehrfakor Authentifizierung

Zugang zu einem Dienst/Webseite wird nur gewährt wenn sich Nutzer durch eine Kombination an Merkmalen ausweist.

- Etwas das man weiß: Passwort
- Etwas das man besitzt: Hardware-Token / Handy / Karte
- Etwas das man ist: Fingerabdruck / Retinascan
  - Hochqualitative Bilder können schon ausreichen um Lesegeräte zu überlisten
  - Kann man nicht ändern

Beispiel: Password + Hardwaretoken: Erraten des Passwortes reicht nicht aus - Muss mich auch noch beklauen

Zwei sind besser als eins

In absteigender Reihenfolge der Sicherheit

- Hardwaretokens (FIDO, YubiKey, Bankkarte)
- TOTP / Authenticator-App auf dem Handy
- SMS 2FA

Zwei sind besser als eins

- Beim Online-Banking: TAN-Generator in den man die Bank-Karte einschieben kann und Flickercode/QR-Code scannen kann, hat zusätzlichen Vorteil, dann man Menge und Empfänger die authorisiert werden prüfen kann.
- Wer eine Banking-App und TAN-App auf dem gleichen Handy hat, hat keinen 2FA mehr

Passwort-Manager

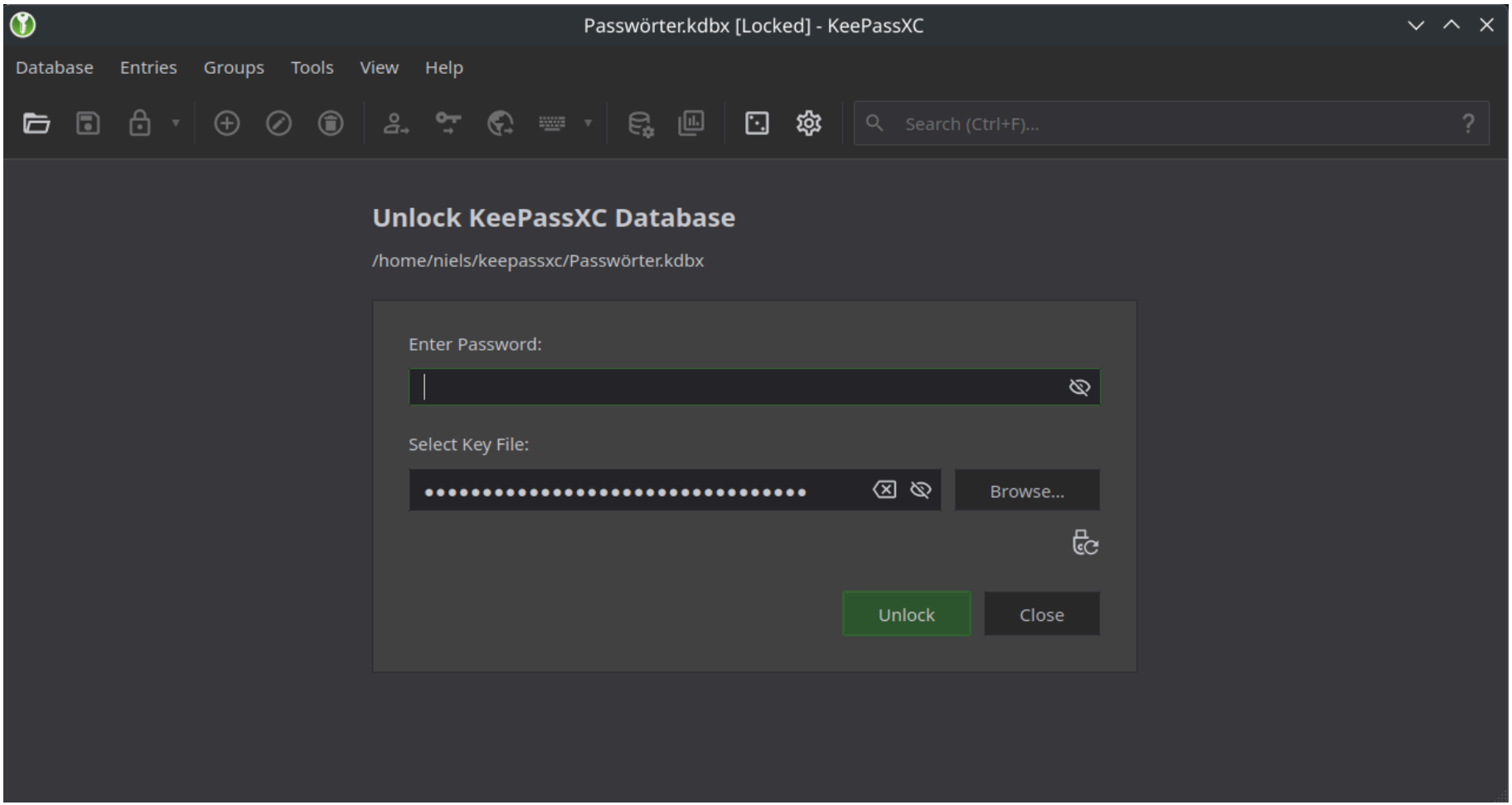
- Verwaltung von Nutzernamen, Passwörtern, Recovery-Phrasen für verschiedene Dienste
- Viele können automatisch gegen HaveIBeenPwned prüfen
- Können automatisch Login-Seiten befüllen

Passwort-Manager

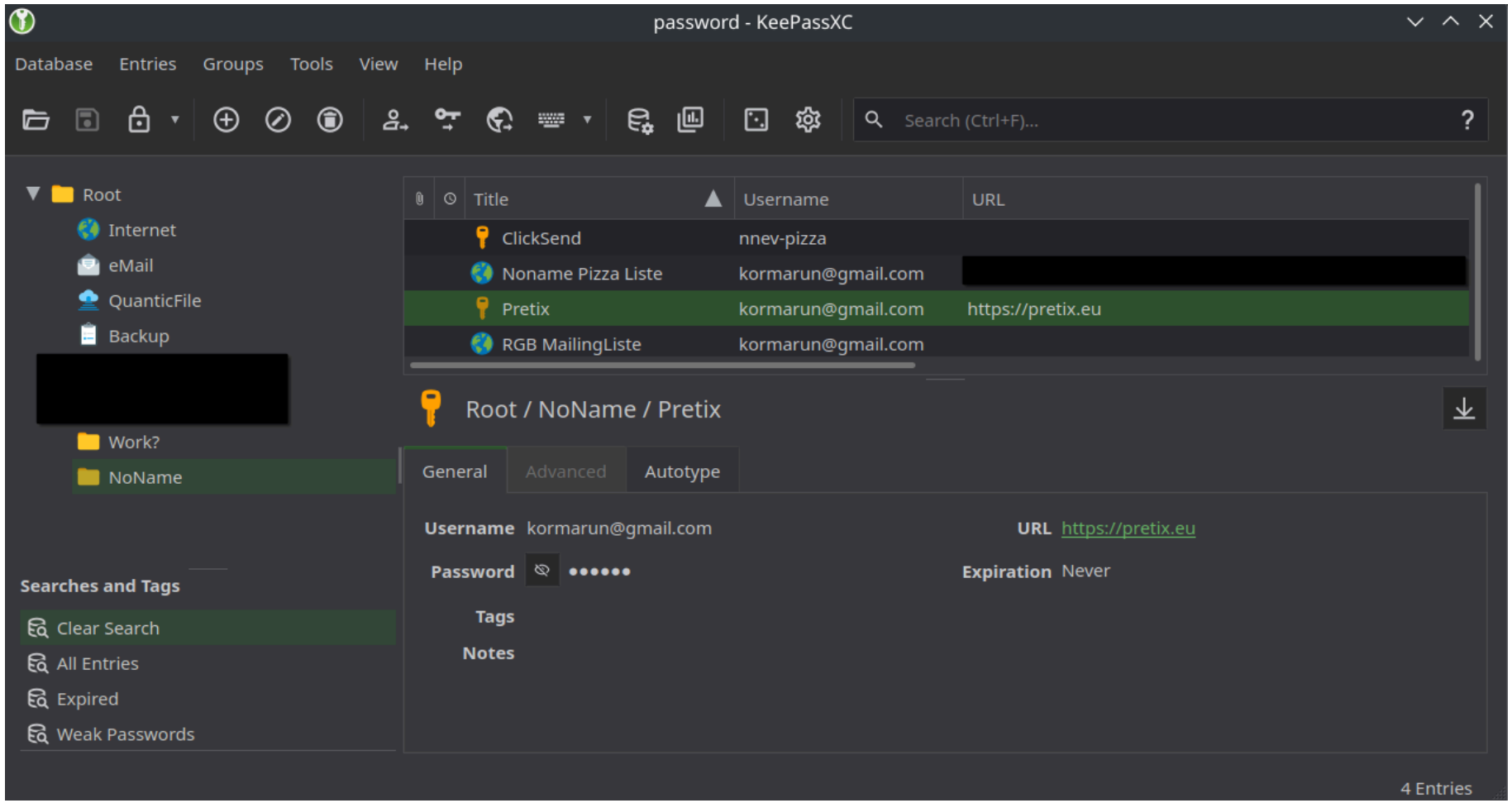
Beispiele für geeignete Software:

- MacOS kommt von Haus aus mit Passwort-Manager
- KeePass: OpenSource, Lokale Anwendung, Starke Verschlüsselung, nicht so portabel
- Bitwarden: Online-Dienst, kann selber betrieben werden
- Passwortsammlung auf Zetteln ist im privaten Kontext sicher genug
  - Firmen haben etwas dagegen wenn die Passwortsammlung offen auf dem Scheibtisch liegt

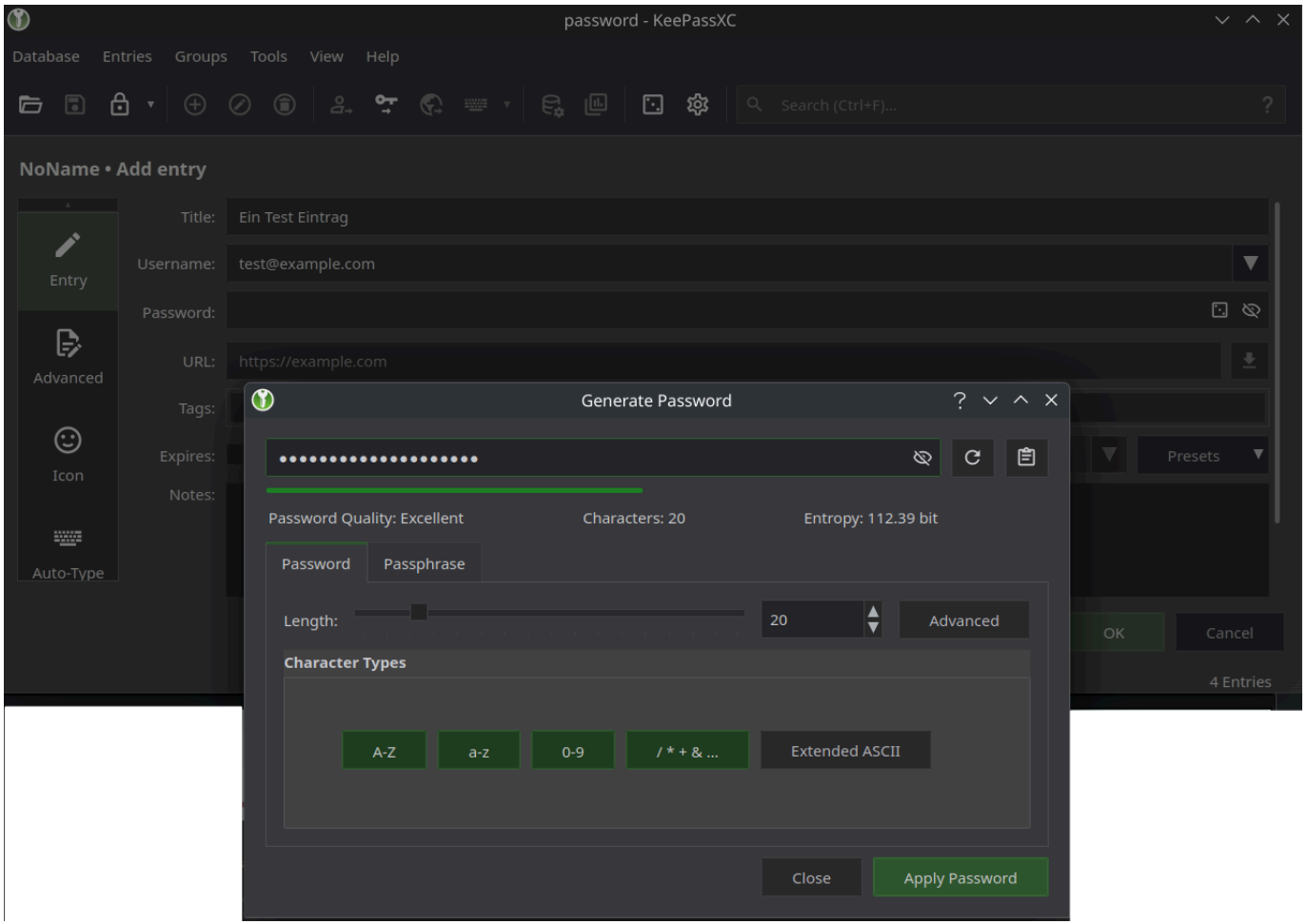
Passwort-Manager



Passwort-Manager



Passwort-Manager



Quellen

[1] S. Meineck and I. Dachwitz, “Databroker Files: Neuer Datensatz enthüllt 40.000 Apps hinter Standort-Tracking.” Accessed: Mar. 25, 2025. [Online]. Available: https://netzpolitik.org/2025/databroker-files-neuer-datensatz-enthuellt-40-000-apps-hinter-standort-tracking/

[2] admin, “Immaterial Labour and Data Harvesting.” Accessed: Apr. 25, 2025. [Online]. Available: https://labs.rs/en/facebook-algorithmic-factory-immaterial-labour-and-data-harvesting/

[3] S. Meineck and I. Dachwitz, “Databroker Files: Firma verschleudert 3,6 Milliarden Standorte von Menschen in Deutschland.” Accessed: Mar. 25, 2025. [Online]. Available: https://netzpolitik.org/2024/databroker-files-firma-verschleudert-36-milliarden-standorte-von-menschen-in-deutschland/

[4] M. Henning, “Weitere Studie belegt Lüge „anonymer“ Daten.” Accessed: Apr. 02, 2025. [Online]. Available: https://netzpolitik.org/2019/weitere-studie-belegt-luege-anonymer-daten/

[5] “The Social Dilemma - A Netflix Original documentary.” Accessed: Mar. 24, 2025. [Online]. Available: https://thesocialdilemma.com/

[6] “Im Sog der Sucht-Maschine - Die ganze Doku.” Accessed: Apr. 02, 2025. [Online]. Available: https://www.arte.tv/de/videos/109029-000-A/im-sog-der-sucht-maschine/

[7] h. online, “Criminal Court: Microsoft's email block a wake-up call for digital sovereignty.” Accessed: May 25, 2025. [Online]. Available: https://www.heise.de/en/news/Criminal-Court-Microsoft-s-email-block-a-wake-up-call-for-digital-sovereignty-10387383.html

Bonus Emailverschlüsselung

Verschlüsselung ist nur mit erheblichen Aufwand möglich

- Bereits kleine Fehler unterwandern Sicherheit
  - Metadaten sind trotzdem noch sichtbar
- Zertifizierung funktioniert deutlich besser
  - Nachweis bzgl. Webbrowser mit Zertifikat wer der Absender ist
  - Inhalt in diesem Fall allerdings im Klartext
- De-Mail hätte vernünftig sein können, leider juristische statt technische Sicherheit
  - Technisch unsichere Verfahren wurden einfach als sicher definiert….
  - Hätte Problem, woher initial zuverlässig die notwendigen Informationen für Verschlüsselung zu einer anderen Person bekommen lösen können

Fazit: Heutzutage sind Messenger hier schon weiter

Suchmaschinen

Es gibt einige Alternativen zu Google

- Kompromiss zwischen Qualität, Werbefinanzierung, Tracking
- Infrastrukturbedingt nur begrenzt sinnvoll selber hostbar
  - Googles Index ist laut Google größer als 100 Terabytes
  - benötigt kontinuierliches Crawlen / Verarbeitung / Stromverbrauch
  - Meine Meinung: Staatliche Regulierung sinnvoller, momentan bester Ansatz

- DuckDuckGo
  - Werbefinanziert aber versprechen kein Tracking zu betreiben
    - Werbung quasi nur über Suchbegriff
- Ecosia
  - Not For Profit
  - Werbefinanziert, Überschuss wird investiert in Aufforstung
- Yacy
  - https://yacy.net/
  - OpenSource dezentrale Peer to Peer Suchmaschine
  - Auch nur lokal verwendbar, z.B. als private Suchmaschine für das FirmenNetzwerk