

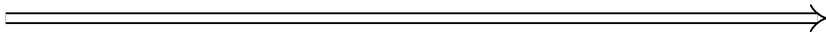
Account Sicherheit & Passwort-Manager

19. September 2026

Hauke Teten

✉ info@teten.org | m @hauke:teten.org

Ablauf



Passwort-Manager

Passwort Sicherheit
und 2FA

Praxis Vorstellung

Passwort-Manager

Zugriff auf mehreren Geräten

Verschlüsselte Aufbewahrung

Speichern von zusätzlichen Dateien

Einfache Suche

Android / iOS Auto-Fill

Automatisches Ausfüllen im Browser

Jedem Account kann ein einzigartiges Passwort zugewiesen werden

Synchronisation

Verwalten von großen Mengen

Übersichtlich

Passwort-Manager

Online Anbieter

- Bitwarden
- NordPass
- 1Password
- Proton Pass
- Dashlane
- LastPass
- ...

Lokal / Self-Hosted

- KeePass und Derivate
z.B. KeePassXC, KeePassDX
- Bitwarden-Server / Vaultwarden
- Padloc
- Passbolt
- ...

Passwort Sicherheit

Was macht ein Passwort „sicher“?

Sicherheit ist proportional zu den möglichen Kombinationen.

$$Kombinationen = (Anzahl\ Zeichen)^{Länge}$$

$$K = N^L \tag{1}$$

$$S \propto N^L \tag{1}$$

$$\propto c \cdot N^L \quad \text{mit } c = Faktor$$

Passwort Sicherheit

Länge oder Anzahl Zeichen?

$$S \propto c \cdot N^L \quad (2)$$
$$\implies L \succ N$$

Länge überwiegt die Zeichenvielfalt!

Passwort Sicherheit

Kombinationen N^L beschreiben

Entropie H

Die durchschnittliche Anzahl von Entscheidungen (Bits), die benötigt werden, um ein Zeichen aus einer Zeichenmenge zu identifizieren oder zu isolieren.

Quelle: Wikipedia.org

$$H = \log_2(N^L) = L \cdot \log_2(N) \quad | \quad 2^x \quad (3)$$
$$2^H = N^L$$

$$\implies S \propto c \cdot 2^H \quad (2)$$

Passwort Sicherheit

Rechenbeispiel

Passwort 1

x9*5rgt+q=c2x

$$N_1 = 43 \quad L_1 = 13$$

mit $N_1 \in \{ 0 - 9, a - z, <, >, *, +, !, ?, = \}$

$$H_1 = 13 \cdot \log_2(43) \approx 70.5 \text{ Bit}$$

Passwort 2

htgdufscbwdoobjkxymzf

$$N_2 = 26 \quad L_2 = 21$$

mit $N_2 \in \{ a - z \}$

$$H_2 = 21 \cdot \log_2(26) \approx 98.7 \text{ Bit}$$

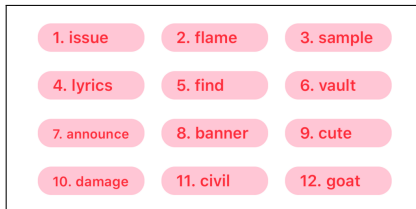
Passwort Sicherheit

Passwort Auswahl

Diceware-Prinzip

Für die Erzeugung einer Passphrase werden mehrere Wörter aus einer Wortliste durch Würfeln ausgewählt und aneinandergehängt.

Quelle: Wikipedia.org



Passwort Sicherheit

Persönliche Empfehlung für ein Master-Passwort

Fünf bis sieben zufällig generierte Wörter.

Bsp. EN: joyous - gradually - swooned - crumpet - motion - resubmit
→ joyousgraduallyswoonedcrumpetmotionresubmit $\implies L = 43$

Bsp. DE: frau - schild - fahrzeug - hamburger - rasenmäher - einliefern
→ frauschildfahrzeughamburgerrasenmähereinliefern $\implies L = 47$

Passwort Sicherheit

Persönliche Empfehlung für Passwörter generell

Auto-Fill / Kopieren

Anzahl Zeichen

$N \in \{ 0 - 9, a - z, \dots \}$

Länge

Maximal möglich
oder ca. $L = 100$

Abtippen / Kopieren

Anzahl Zeichen

Diceware-Prinzip

Länge

Maximal möglich
oder ca. $L = 11$ Wörter

L und N anpassen an Passwortanforderungen

Zwei-Faktor-Authentifizierung

Was ist 2FA?

Account Login

- | | |
|----------------|--------------|
| - Benutzername | → Faktor 0 |
| - Passwort | → Faktor 1 |
| - 2FA | → Faktor 2 |
| <hr/> | |
| - 3FA | → Faktor 3 |
| - x FA | → Faktor x |

⇒ Multi-Faktor-Authentifizierung

Multi-Faktor-Authentifizierung

MFA-Arten

- One-time password (OTP)
z.B. SMS, E-mail, ...
- Time-based one-time password (TOTP)
z.B. Authenticator-Apps, ...
- Biometrisch
z.B. Fingerabdruck, Iris, ...
- Kryptografische Authentifizierung
z.B. FIDO2 / Passkey, Challenge-Response, ...

Multi-Faktor-Authentifizierung

Hardware-Security-Module (HSM)

- TPM (Trusted Platform Module)
- Hardware-Token

Protokolle

- OTP
- OpenPGP
- U2F
- Challenge-Response
- ...
- FIDO2 / Passkey
- Smart card / PIV
- WebAuthn
- OATH-TOTP/-HOTP

Hardware-Token

Anbieter

- YubiKey
- NitroKey
- OnlyKey

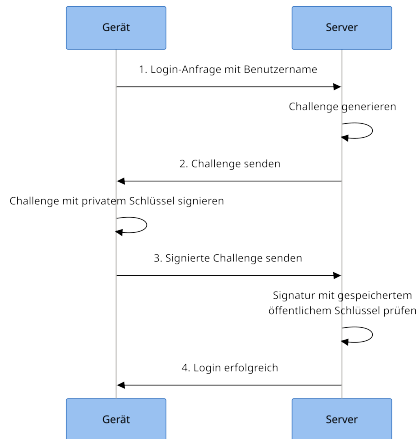


Passkey

Passkey als Auth.-Faktor

- Erweiterung des FIDO2-Standards
- Asymmetrische Kryptografie
 - Schlüsselpaar: Public-key/Private-key
 - Private-key verlässt nie das Gerät
- Authentifizierung durch Signierung
 - Wie bei einem OpenPGP Schlüsselpaar

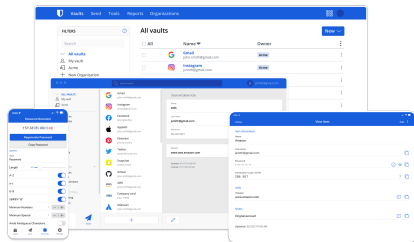
⇒ **Phishing resistenter Login**



Anwendung: Als 2FA oder direkter Passwortersatz

Bitwarden

- Open-Source
 - Server
 - Clients
 - Android
 - iOS
- Cross-Platform-Kompatibilität
- Optionales Self-Hosting
 - Bitwarden-Server / Vaultwarden
- Browser-Integration
- Android / iOS Auto-Fill



 **bitwarden**

Eigenes Setup

Laptop und Desktop	→	KeePassXC
Smartphone (Android)	→	KeePassDX
Synchronisation	→	Syncthing-Server

Vorteile

- Open-Source
- Lokal (offline)
- Browser Integration / Android Auto-Fill
- 2FA mit YubiKey Challenge-Response



Zusammenfassung

Wie sichere ich meine Online-Accounts / Passwort-Manager?

Passwort-Manager wählen

z.B. KeePass oder Bitwarden

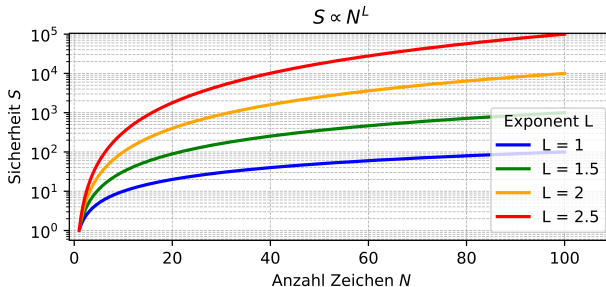
Sicheres Master-Passwort

z.B. [joyousgraduallyswoonedcrumpetmotionresubmit](#)

Multi-Faktor-Authentifizierung

- z.B.
- Hardware-Token (OTP, Challenge-Response, TOTP)
 - Authenticator-App (TOTP)
 - Passkey

Fragen oder Feedback?



Hauke Teten



info@teten.org



@hauke:teten.org