



Sicher mit Passwörtern im Alltag – einfach & praxistauglich

Praktische Strategien für mehr Sicherheit im digitalen Alltag Ihres Betriebs

– Christian von zur Gathen, IT Koordination



Wie sicher sind Ihre Passwörter?

- Wer von Ihnen nutzt dasselbe Passwort für mehrere Online-Konten?
- Wer hat schon mal Passwörter auf Zettel geschrieben oder im Smartphone gespeichert?
- Wer hat sich schon gedacht: „So wichtig bin ich doch gar nicht, dass jemand daran interessiert ist“?

Wer kennt es ? "Ein Tablet im Betrieb mit dem Passwort '1234'..."

 **Bequem kann gefährlich werden – heute sehen wir, wie man's besser macht.**



Warum einfache Passwörter keine Option mehr sind

Passwörter sind das wichtigste Schloss unserer digitalen Türen.



Datenlecks

Millionen Passwörter werden jährlich gestohlen



Phishing-Mails

Gefälschte E-Mails täuschen echte Logins vor



Wiederverwendung

Ein gehacktes Konto gefährdet alle anderen

 **Bekannte Phishing Mails kommen vermeintlich von:** Microsoft, Google, Amazon, DHL/Deutsche Post, PayPal, Sparkasse/Deutsche Bank, eBay, Apple, Booking.com, Airbnb, Ionos uvm.

 **Schwach**

T%3k\$8

Kurz und komplex

 **Stark**

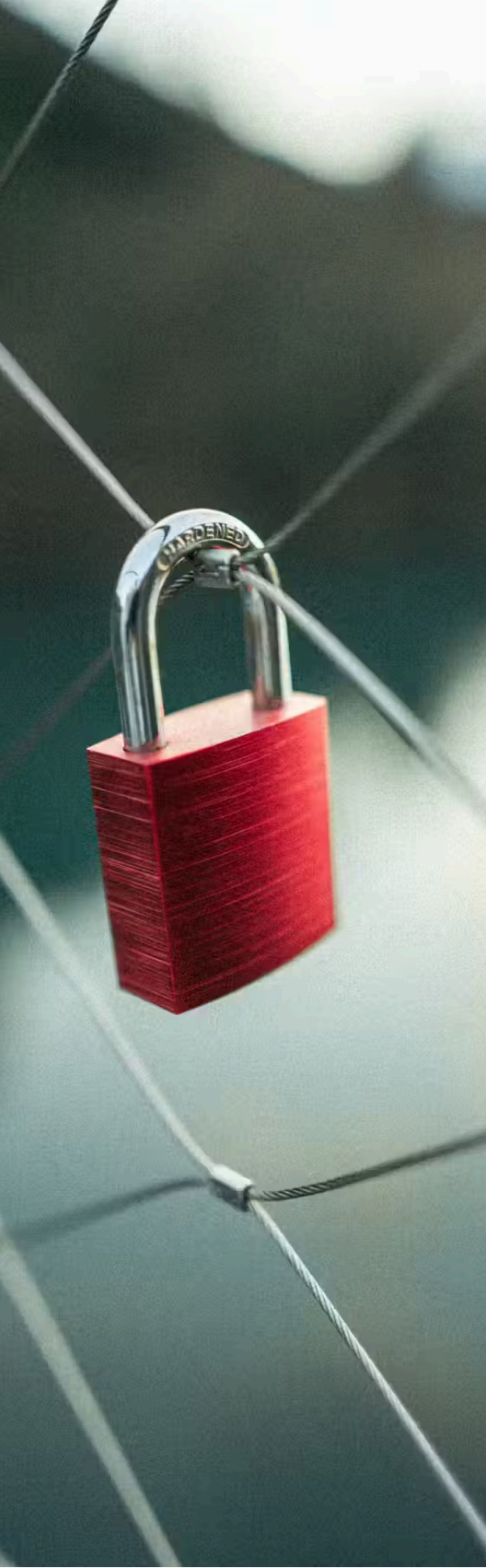
MeinHundMagKeineWurst2024!

Grundregel: Länge > Komplexität

 **Sehr Stark**

cjb_k!zt_tex0GE%m!1Qq8QDU!"

Noch besser: Lang & Komplex



Strategien für sichere & einfache Passwörter

01

Ein Passwort pro Account

Jeder Zugang erhält sein eigenes, einzigartiges Passwort

02

Regel: Die Länge ist das, was zählt!

mindestens 12 Zeichen - darunter Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen

03

2-Faktor-Authentifizierung

Zusätzliche Sicherheitsebene durch zweiten Bestätigungsschritt

04

Der Satztrick:

Heute Nachmittag um 16:30 Uhr gehe ich ins Fußballtraining! = **HNu16:30giiF!**

Typische Fehler vermeiden

Ein Passwort für alles

Viele nutzen dasselbe Passwort für E-Mail, Online-Banking, Shops, Portale oder Streaming Anbieter.

Versand per WhatsApp / E-Mail

Keine sensiblen Zugangsdaten über Messenger oder Mail teilen

Gemeinsame Team-Logins

Ohne Kontrolle weiß niemand, wer Zugriff hat

Zettel oder Fotos

Passwörter niemals physisch notieren oder fotografieren

Worst-Case-Szenarien

Fall 1) Gefälschte Rechnungen / Business Email Compromise (BEC) → direkte Geldverluste

Fall 2) Ransomware verschlüsselt IT-Systeme → Betrieb lahmgelegt, Auftragsverlust, Kosten

Fall 3) Kundendatenabfluss → Datenschutz-Folgen (Reputation & DSGVO-Bußen)

Fall 4) Missbrauch von Lieferanten- oder Bankzugängen → Fehlbestellungen, Warenverlust, Liquiditätsengpässe

 Die HDI-Cyberstudie zeigt: **Ein erfolgreicher Angriff kostet deutsche KMU im Schnitt 95.000 Euro** – genug, um bei vielen kleinen Betrieben **die wirtschaftliche Existenz ernsthaft zu bedrohen**.

Rund **35 %** der deutschen Unternehmen waren in den letzten zwei Jahren Opfer eines Cyberangriffs.

 Und jeder Cyberangriff beginnt mit einer Schwachstelle! **Gehören Sie nicht dazu!**

Passwortkultur im Betrieb

Verantwortung festlegen: Wer hat in Sachen Passwörtern den Hut auf ? Der Chef, das Büro oder ein einzelner Mitarbeiter?

1. Keine Zettel oder Fotos

Physischer Verlust oder Diebstahl,
Soziale Risiken, Keine
Verschlüsselung

2. Keine Sammeldateien wie Excel, Word verwenden.

Fehlende Verschlüsselung, i.d.R.
einfache Passwörter

3. Ein Passwort pro Konto

Jeder Account erhält einzigartige
Zugangsdaten => Begrenzung d.
Schadens, Transparenz & Kontrolle

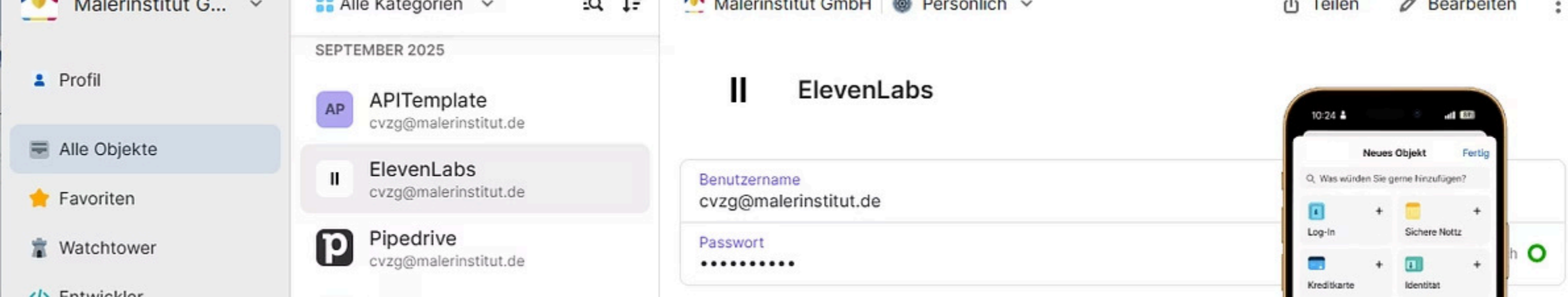
4. Passwortverwaltung nutzen

Zentrale Verwaltung inkl. aller Team-Accounts

5. 2FA aktivieren

Zwei-Faktor-Authentifizierung für doppelte Sicherheit

Sicherheit ohne Stress



Was macht ein Passwortmanager?

Ihr digitaler Tresor für maximale Sicherheit und Komfort



Digitaler Tresor

Sichere Speicherung von
Passwörtern, Kreditkarten,
Dokumenten und Software-
Logins



Zugriff von überall

Synchronisation auf PC, Tablet
und Smartphone – immer
verfügbar

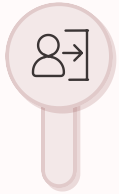


Automatisches Ausfüllen

Passwörter werden automatisch
gespeichert und eingefügt

⚠ Browserbasierte Passwort-Manager sind bequem, aber riskant: Sie bieten keine echte Ende-zu-Ende-Verschlüsselung, schwächeren Datenschutz, höhere Angriffsflächen und kaum Kontrolle über Speicherung, Freigabe und Wiederherstellung sensibler Daten.

Live-Demo – 1Password in Aktion



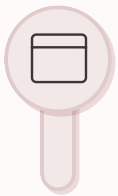
Anmeldung

Zugriff auf 1Password Web oder App



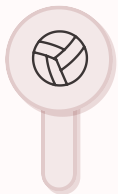
Passwort generieren

Neues, starkes Passwort erstellen und speichern



Automatisches Login

Nahtlose Anmeldung auf Websites



Gemeinsamer Tresor

Sichere Teamzugänge verwalten



Mobile Nutzung

1Password auf dem Smartphone



Highlight: Starkes Passwort wird automatisch erstellt und eingefügt – ohne Aufwand!

Fragerunde / Diskussion

Typische Fragen

Masterpasswort vergessen?

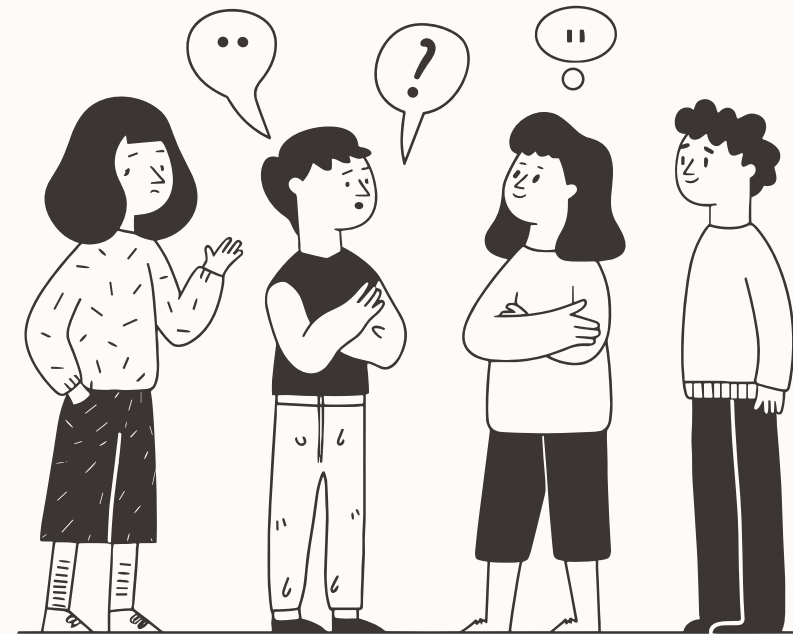
Wiederherstellungsoptionen und Notfallzugriff verfügbar

Ist 1Password sicher?

Verschlüsselung nach Militärstandard, Zero-Knowledge-Architektur, SOC 2 Typ 2-zertifiziert, End-to-End-Verschlüsselung.

Was kostet das?

Flexible Tarife für Einzelpersonen, Familien und Teams



"Welchen Ihrer Zugänge würden Sie als Erstes sichern wollen?"

Abschluss & Mitnahme



Starke Passwörter

Bedeuteten einen starken, geschützten Betrieb



Passwortmanager sparen ...

Zeit, Nerven und erhöhen die Sicherheit



Sofort starten

Erste Schritte zur digitalen Sicherheit erhalten Sie in unserem Handout

Ihre nächsten Schritte

Scannen Sie den QR-Code für unser [Handout](#)



INSTITUT FÜR UNTERNEHMENSFÜHRUNG



Kommentar hinzufügen

Passwortmanager- Handout

Ihr digitaler Schlüsselbund für den Arbeitsalltag – einfach und sicher.

🕒 Erste Schritte vor der Nutzung eines Passwortmanagers

Kurzfassung:

- ✓ Entfernen Sie alte Passwort-Zettel, Notizen und Fotos
- ✓ Prüfen und ordnen Sie Ihre bestehenden Passwörter
- ✓ Tragen Sie alle Logins in den Passwortmanager ein
- ✓ Löschen Sie unsichere oder doppelt gespeicherte Listen
- ✓ Organisieren Sie gemeinsame Zugänge über Team-Tresore
- ✓ Notieren Sie Ihr Master-Passwort sicher im Notfall-Kit

► Ausführlichere Anleitung



Vielen Dank!