

CAW Januar 2026

- *Offene Plätze für Kurse*
- So werden Sie (wahrscheinlich) niemals „gehackt“
- Cloud-Dienste für private Anwender (Sinn / Zweck / Nutzen / Kosten)
- Alternativen zu Skype (Einstellung im Mai 2025)
- Passkeys
- 10 Tipps für mehr Android Sicherheit
- Ihre Fragen

Kursangebote

Workshop KI - Lutz Harjes am 03.02.2026, 15.30 - 17.00 Uhr - 6 freie Plätze

PC Windows Anfänger - Lutz Harjes ab 10.02.2026, 15.30 - 17.00 Uhr - noch 2 freie Plätze

Fahrradnavigation - Bernd Batke am 18. + 25.02.2026, 09.00 - 12.00 Uhr - noch 2 - 3 freie Plätze

PC Windows - Folgekurs - Harald Meyer - ab 26.02.2026, 09.00 - 10.30 Uhr - noch 1 - 2 freie Plätze

So werden Sie *niemals* gehackt

Siehe Word Datei

- **Passwortsicherheit und Schwachstellen**
- **Merkmale sicherer Passwörter**
- **Zweifaktor-Authentifizierung (2FA)**
- **Passkeys als Alternative**
- **Praktische Tipps**

Tabelle: Zeitaufwand zum Knacken von Passwörtern (Brute-Force)

Passwortlänge	Nur Zahlen (0–9)	Kleinbuchstaben (a–z)	Buchstaben (a–Z)	Buchstaben + Zahlen	Alle Zeichen (a–Z, 0–9, Symbole)
4 Zeichen	< 1 Sekunde	< 1 Sekunde	< 1 Sekunde	< 1 Sekunde	< 1 Sekunde
6 Zeichen	< 1 Sekunde	< 1 Sekunde	< 1 Sekunde	< 1 Sekunde	Sekunden bis Minuten
8 Zeichen	Sekunden	Minuten	Stunden	Stunden bis Tage	Tage bis Wochen
10 Zeichen	Minuten	Stunden	Tage	Wochen	Jahre
12 Zeichen	Stunden	Tage	Wochen	Jahre	Jahrzehnte
14 Zeichen	Tage	Wochen	Jahre	Jahrzehnte	Jahrhunderte oder länger
16 Zeichen	Wochen	Monate	Jahrzehnte	Jahrhundert	Praktisch nicht knackbar

Passwörter absichern in 3 Schritten

Individualisieren: Für jedes Konto ein eigenes Passwort

Zusatzschutz: falls möglich, durch 2FA absichern

Passkeys nutzen: Alternative zu Passwörtern, sind sicherer und nutzen Verschlüsselung

Hallo liebes CAW-Team,
zunächst wünsche ich euch ein frohes Neues Jahr und hoffe, dass ihr die Feiertage gut überstanden habt.

Eine Frage nur zum nächsten Programm am 21.1.

Ich hatte mir den Termin in meinem neuen Kalender notiert mit dem Hinweis auf "Passkey". Aber ist weiß nicht mehr, wo ich die Info her habe. Hattet ihr das Thema evtl. beim letzten Mal angekündigt? Auf der Themenliste finde ich es nicht.

Das Thema interessiert mich, da ich täglich die Meldung beim Öffnen von T-online-Email erhalte. Es könnte wahrscheinlich auch viele Andere interessieren, die mit T-Online arbeiten, oder? Vielleicht ein Thema für zukünftige CAW's?

Bitte mal prüfen.

Vielen Dank im Voraus.

Gruß Manfred

Passkeys – Anmeldung ohne Passwort

Was sind Passkeys?

Eine sichere Alternative zu Passwörtern, die dein Gerät nutzt.

So meldest du dich an:

- Fingerabdruck
- Gesichtserkennung
- Geräte-PIN

Vorteile:

- ✓ Kein Passwort merken
- ✓ Schutz vor Phishing
- ✓ Schneller & sicherer Login

Wie erstellt man Passkeys?

1. Konto öffnen oder anmelden

Auf einer Website oder App, die Passkeys unterstützt (z. B. Google, Apple, Microsoft).

<https://Passkeys.directory>

2. „Passkey erstellen“ auswählen

Oft unter *Sicherheit* oder *Anmeldeoptionen*.

3. Identität bestätigen

Mit Fingerabdruck, Gesichtserkennung oder Geräte-PIN.

4. Fertig

Der Passkey wird **automatisch auf deinem Gerät gespeichert**.

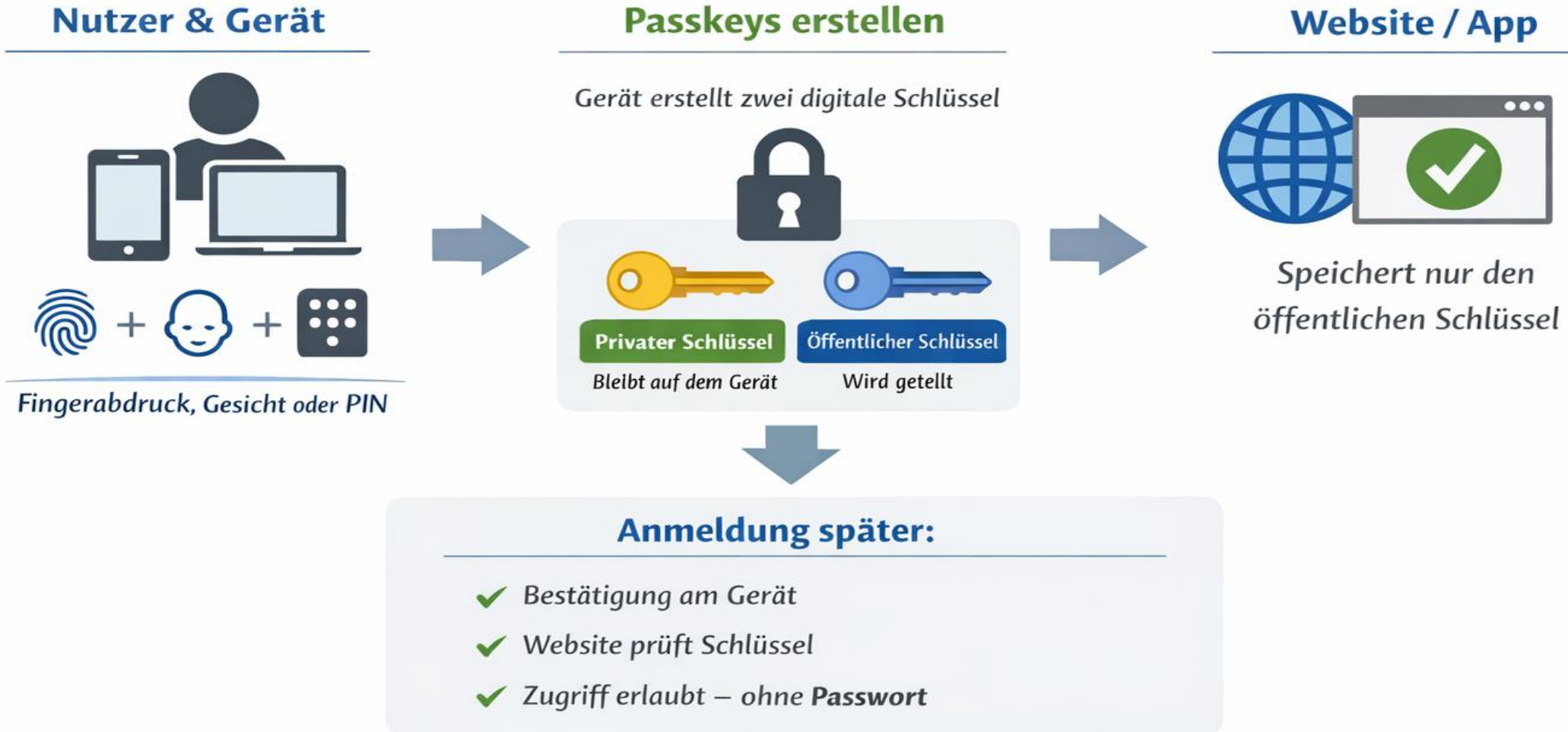
Was passiert im Hintergrund?

- Dein Gerät erzeugt ein **Schlüsselpaar**
- Der **private Schlüssel bleibt auf deinem Gerät**
- er **öffentliche Schlüssel** wird beim Anbieter gespeichert
- Kein Passwort wird übertragen oder gespeichert

Wichtig zu wissen

- Ein Passkey ist **gerätegebunden**
- Über Cloud-Dienste kann er auf **neue Geräte synchronisiert** werden
- **Mehrere Passkeys** pro Konto sind möglich

Passkeys erstellen – so funktioniert's



Passkeys = sichere Anmeldung ohne Passwort. 🗝️

Sehr geehrtes Team,

Verbrauchertipp: Mehr Privatsphäre bei Paypal.

Rückschlüsse zur Person, also sensible Daten werden preisgegeben.

Um dieses zu vermeiden sollten bei Paypal Einstellungen vorgenommen werden.

So wie beschrieben funktioniert es nicht.

Bitte um Erklärung.😊

**Mit freundlichem Gruß
Sabine Haberkamp**

Aktuelle Infos

„Entfernen Sie alte Computer jetzt aus Windows 11, bevor Sie an Ihre Grenzen stoßen.“

Gemeint ist damit in der Regel, dass in einem **Microsoft-Konto oder in Windows 11 noch alte, nicht mehr genutzte Geräte (PCs/Laptops)** registriert sind. Diese können Probleme verursachen, z. B.:

- Erreichen des **Gerätelimits** im Microsoft-Konto (10)
- Verwirrung bei **OneDrive-Sync**, Microsoft Store oder Lizenzaktivierungen
- Sicherheitsrisiken durch **veraltete oder verlorene Geräte**

So entfernen Sie alte Computer aus Windows 11 / Ihrem Microsoft-Konto

Über das Microsoft-Konto

- 1.Öffnen Sie: **account.microsoft.com/devices**
- 2.Melden Sie sich mit Ihrem Microsoft-Konto an
- 3.Wählen Sie den **alten oder nicht mehr genutzten PC**
- 4.Klicken Sie auf „**Gerät entfernen**“
- 5.Bestätigen Sie den Vorgang

Wann sollten Sie alte Geräte entfernen?

- PC verkauft, verschenkt oder entsorgt
- Neuinstallation mit anderem Microsoft-Konto
- Gerät seit Monaten/Jahren nicht mehr genutzt
- Probleme mit Lizenzen, OneDrive oder Windows-Aktivierung

10 Tipps für mehr Android-Sicherheit

1. Updates regelmäßig installieren
2. Google Konto absichern
3. App-Berechtigungen prüfen
4. Standort clever nutzen (Nur während der Nutzung)
5. Werbung & Tracking deaktivieren
6. Browser & Suche wechseln (Brave oder Firefox)
7. Android Sicherheitsfunktionen aktivieren
8. Vorsicht in offenen WLANs
9. Nur Apps aus dem Play Store installieren
10. Vorsicht vor Phishing & Malware

Für die Aktivierung erweiterter Sicherheits-Updates ist ein Microsoftkonto Pflicht. Laut Microsoft muss man mit dem Konto auch mindestens alle 60 Tage aktiv sein.

-