

EDV Stammtisch Donnerstag, 29. Jänner

Themen:

- **WLAN als Sicherheitsgefahr** – worauf sollte man achten?
- **VPN** – was ist das und warum ist es eine sichere Verbindung?
- **Was ist WERO?**
- **Was ist der digitale Euro?**
- Tipps und Hinweise – **egal ob Android oder iOS**

Diese Funktion am Handy birgt unerwartete Gefahren

Fast jeder besitzt heutzutage ein Smartphone.

Eine Funktion sollte man aber nicht durchgehend eingeschaltet lassen.

WLAN als Sicherheitsgefahr

Dazu zählt auch die Nutzung der WLAN-Funktion.
In einem Bericht für Cybersicherheit, wird vor Schwachstellen gewarnt, die sich in allen modernen Smartphones befinden.
Besonders WLAN und mobile Netzwerke sollen unerwartete Gefahren bergen.

Das ist der Grund

Smartphone-Nutzer, die öffentliche WLAN-Netzwerke verwenden, sind besonders gefährdet für sogenannte Man-in-the-Middle-Angriffe (MitM). Bei dieser Art von Angriff befinden sich Hacker unbemerkt zwischen der WLAN-Quelle (z.B. dem Router) und dem Gerät des Nutzers. Dadurch können sie heimlich den gesamten Datenverkehr abfangen und mitlesen, ohne dass es der Nutzer oder die WLAN-Quelle bemerkt.

Man-in-the-Middle-Angriffe (MitM)



Dies geschieht vor allem in ungesicherten oder offenen Netzwerken, wie sie oft in Cafés, Flughäfen oder anderen öffentlichen Bereichen angeboten werden.

Um das Risiko von Datenklau und Angriffen über WLAN zu minimieren, solltest du folgende einfache Regeln beachten:

WLAN abschalten, wenn du es nicht brauchst:

Deaktiviere die WLAN-Funktion deines Smartphones immer komplett, wenn du dich nicht aktiv mit einem vertrauenswürdigen Netzwerk verbinden willst.

Das verhindert, dass dein Handy ständig nach Netzwerken sucht und dabei Informationen sendet und dadurch auch mehr Strom verbraucht.

- **Automatische Verbindung deaktivieren:**
Stelle sicher, dass dein Gerät sich nicht automatisch mit bekannten oder offenen WLAN-Netzwerken verbindet.
- **Vorsicht bei öffentlichen Hotspots:** Nutze öffentliche und ungesicherte WLANs (wie in Cafés, Bahnhöfen oder Hotels) nur im Notfall und erledige dort keine wichtigen Dinge.
- Banking und Passwörter meiden: Führe über öffentliche WLANs **niemals Online-Banking durch oder gib Passwörter ein.**

- **Updates installieren:** Halte das Betriebssystem und alle Apps auf deinem Smartphone immer auf dem neuesten Stand, um bekannte Sicherheitslücken zu schließen.

Sehr sichere Verbindung!

- **VPN nutzen:** Verwende immer eine VPN-Verbindung (Virtuelles Privates Netzwerk), wenn du öffentliche WLANs nutzen musst.



Ein VPN verschlüsselt deinen gesamten Datenverkehr und schützt ihn so vor Man-in-the-Middle-Angriffen.

Was macht ein VPN ganz einfach gesagt?

Ein VPN ist wie **ein geschützter Tunnel** im Internet. Alles, was dein PC oder Handy ins Internet schickt, wird **verschlüsselt** und kommt von außen **anonymisiert** an.

Warum ist ein VPN am PC sinnvoll?

1. Schutz in öffentlichen WLANs

Café, Hotel, Bahnhof, Arztpraxis, Gasthaus – diese WLANs sind oft **offen oder schlecht gesichert**.

Ohne VPN können andere im selben Netz theoretisch mitlesen:

- Passwörter
- E-Mails
- Online-Banking
- Vereins- oder private Daten

 Mit VPN: **niemand kann hineinschauen**

2. Weniger Überwachung & Nachverfolgung

Ohne VPN können:

- Internetanbieter
 - Webseiten
 - Werbenetzwerke
- sehen, **welche Seiten du besuchst**

 Mit VPN:

- deine **IP-Adresse wird verborgen**
 - dein Surfverhalten wird **nicht eindeutig zuordenbar**
-

3. Zusätzliche Sicherheit bei sensiblen Dingen

Besonders wichtig bei:

- Online-Banking
- E-Mails
- Vereinsarbeit
- Cloud-Diensten
- Behördenportalen

Ein VPN ersetzt **kein Antivirus**, ist aber eine **wichtige Zusatzschicht**.

Warum auch am Mobiltelefon?

Viele unterschätzen das Handy – dabei ist es **ständiger online als der PC**.

1. Automatische WLAN-Verbindungen

Handys verbinden sich oft automatisch mit:

- fremden WLANs
- bekannten, aber unsicheren Netzen

👉 VPN schützt im Hintergrund, ohne dass du ständig daran denken musst.

2. Schutz vor Standort- & Profilbildung

Apps sammeln:

- Standortdaten
- Nutzungszeiten
- Surfverhalten

Ein VPN:

- erschwert Profilbildung
- schützt vor übermäßiger Datensammlung

3. Sicherheit für Messenger & E-Mail

Gerade bei:

- E-Mail
- Fotos
- Cloud-Backups

Ein VPN verhindert, dass Daten unterwegs abgefangen werden.

Typische Fragen, die ich oft höre „Ist das nicht nur etwas für Kriminelle?“

Nein. Genauso wie:

- Vorhänge
- Haustüren
- Briefumschläge

→ **Privatsphäre ist kein Verbrechen**

„Macht das alles langsamer?“

Ein wenig – aber bei guten Anbietern **kaum spürbar**.

Für normales Surfen, Mailen, Videos absolut unproblematisch.

Kurz zusammengefasst

Ein VPN ist sinnvoll, weil es:

-  deine Daten schützt
-  deine Privatsphäre wahrt
-  dich im öffentlichen WLAN absichert
-  auch am Handy im Hintergrund schützt

Hier sind **einige empfehlenswerte VPN-Anbieter für PC und Mobiltelefon**, mit einer erklärenden, persönlichen Einordnung, damit du leichter entscheiden kannst 

☀️ 1. Surfshark – Top Allround-Wahl (Preis & Leistung)

Warum ist Surfshark so beliebt?

- Sehr *günstig* bei längeren Abos und mit **unbegrenzten Geräten** – du kannst PC, Handy, Tablet, Router etc. gleichzeitig schützen.
- Gute **Geschwindigkeit** (perfekt für Videos, Streaming & Surfen).
- Viele praktische Extras wie Werbeblocker & Schutz vor Trackern.
- 7-Tage-Test oder 30-Tage-Geld-zurück-Garantie oft verfügbar.

👉 Super Wahl, wenn du viele Geräte schützen willst und ein **gutes Preis-Leistungs-Verhältnis** suchst.

🔒 2. NordVPN – Sicherheit & Geschwindigkeit

Stärken:

- Sehr große Server-Auswahl & **starke Verschlüsselung**.
- Besonders gut für Streaming, Gaming und Inhalte aus anderen Ländern.
- Apps für Windows, macOS, Android, iOS, Router etc.

👉 Etwas teurer als Surfshark, aber **mehr Premium-Features und höchste Sicherheit**.

3. Proton VPN – Fokus auf Datenschutz (auch kostenlos)

Besonderheiten:

- Sehr **starker Datenschutz**, gehört zu Proton Mail, sehr transparent.
- Es gibt eine **kostenlose Version**, wenn du nur Grundschatz brauchst.
- Paid-Pläne bringen höhere Geschwindigkeit und mehr Server.

👉 Ideal, wenn dir **Anonymität & Privatsphäre** noch wichtiger sind als Streaming-Funktionen.

4. ExpressVPN – Premium-Option

Gute Gründe dafür:

- Ausgezeichnete **Zuverlässigkeit und Stabilität**, besonders für Streaming.
- Einfach zu bedienen, sehr gute Apps.

👉 Perfekt, wenn du bereit bist, für **Top-Performance** etwas mehr zu zahlen.



Kurze Zusatzhinweise

- Viele VPN-Dienste bieten heute **30-Tage-Geld-zurück-Garantie** oder kostenlose Testphasen an – du kannst also erst probieren, bevor du dich langfristig bindest.
 - Achte darauf, dass der Anbieter eine **No-Logs-Politik** hat (also keine Aktivitäten speichert) und eine **Kill-Switch-Funktion**, falls die Verbindung mal abreißt.
-



Welche Option passt zu dir?

- **Budget & viele Geräte** → Surfshark
- **Maximale Sicherheit & Features** → NordVPN
- **Starker Datenschutz + kostenlose Basisversion** → Proton VPN
- **Top-Streaming & einfache Bedienung** → ExpressVPN

Beste VPN-Dienste Januar 2026

Surfen Sie sicher und anonym im Internet mit einem Top-VPN aus unserer Liste der empfohlenen Marken.

- ✓ 100% Privatsphäre und Anonymität
- ✓ Schnelle Server für Nutzer weltweit
- ✓ Getestet mit beliebten Geräten & Dienstleistungen
- ✓ Beste Angebote & Geld-zurück-Garantien



📅 Zuletzt aktualisiert: 24 Januar 2026

1 SCHNELLSTES VPN



Super-sicherer und vertrauenswürdiger VPN-Dienst, der starke Verschlüsselung, eine No-Logs-Richtlinie und ein globales Servernetzwerk bietet.

Kompatibilität: iOS Apple Android Windows Fire TV PlayStation Xbox IPTV Kodi

🏆 60-Tage Geld-zurück-Garantie

- ✓ Schnellster VPN-Dienst
- ✓ Schnelles und zuverlässiges Servernetzwerk
- ✓ Strikte Keine-Protokolle-Richtlinie
- ✓ Unterstützung für bis zu 10 Geräte
- ✓ Starke AES 256-Bit-Verschlüsselung
- ✓ Blockiert Werbung und Tracker

9.9

Website besuchen ➔

norton.com

2



Sichere VPN-Dienste, die sich auf Datenschutz und Geschwindigkeit konzentrieren, bieten fortschrittliche Sicherheitsfunktionen und uneingeschränkten Zugang weltweit.

Kompatibilität: iOS Apple Android Windows Fire TV PlayStation Xbox IPTV Kodi

🏆 30-Tage Geld-zurück-Garantie

- ✓ Unabhängig geprüfte strikte No-Logs-Richtlinie
- ✓ Open-Source-Apps, die unabhängig geprüft werden
- ✓ Sichere Core-Multi-Hop-Server
- ✓ Integrierte Werbung- und Tracker-Blockierung
- ✓ Unterstützt OpenVPN, WireGuard und Stealth

9.5

Website besuchen ➔

protonvpn.com

3



Schneller & robuster VPN-Dienst für anonymen Online-Zugang mit zusätzlichen kostenlosen Sicherheitsfunktionen.

Kompatibilität: iOS Apple Android Windows Fire TV PlayStation Xbox IPTV Kodi

🏆 30-Tage Geld-zurück-Garantie

- ✓ Fortgeschrittene Verschlüsselungstechnologie
- ✓ Zusätzlicher Schutz für öffentliches Wi-Fi
- ✓ Unterstützt alle beliebten Plattformen
- ✓ Weltweite Abdeckung
- ✓ Kostenloses Antivirus & Ad Blocker enthalten
- ✓ Kundensupport rund um die Uhr

9.4

Website besuchen ➔

totalvpn.com

1 Gerät
Norton VPN Standard

1 Jahr

60% RABATT*

49,99 € 19,99 € im 1. J.

Entspricht

1,67 €

/Monat

Ersparnis im Vergleich zum Verlängerungspreis
von 49,99 €/Jahr.

[Siehe Abonnementdetails unten.*](#)

Jetzt abonnieren

- ✓ Maskierung der IP-Adresse, sodass Ihre Online-Aktivitäten verborgen bleiben
- ✓ Grenzübergreifender Zugriff auf Ihre Lieblingsinhalte
- ✓ Werbeblocker zum Surfen ohne lästige Werbung¹⁴
- ✓ Verzicht auf Protokollierung zugunsten des Datenschutzes
- ✓ Notausschalter zum Schutz vor Offenlegung privater Daten
- ✓ IP-Rotation und Doppel-VPN zur Stärkung der Privatsphäre

Bis zu 5 Geräte
Norton VPN Plus

1 Jahr

68% RABATT*

94,99 € 29,99 € im 1. J.

Entspricht

2,50 €

/Monat

Ersparnis im Vergleich zum Verlängerungspreis
von 94,99 €/Jahr.

[Siehe Abonnementdetails unten.*](#)

Jetzt abonnieren

- ✓ Maskierung der IP-Adresse, sodass Ihre Online-Aktivitäten verborgen bleiben
- ✓ Grenzübergreifender Zugriff auf Ihre Lieblingsinhalte
- ✓ Werbeblocker zum Surfen ohne lästige Werbung¹⁴
- ✓ Verzicht auf Protokollierung zugunsten des Datenschutzes
- ✓ Notausschalter zum Schutz vor Offenlegung privater Daten
- ✓ IP-Rotation und Doppel-VPN zur Stärkung der Privatsphäre
- ✓ KI-gestützter Schutz vor Betrug, Phishing und Malware
- ✓ Überwachung des Darknets auf Ihre Daten⁸
- ✓ Passwort-Manager zur Verwendung starker Passwörter
- ✓ 10 GB Cloud-Backup⁴ zur Sicherung wichtiger Dateien

Bis zu 10 Geräte
Norton VPN Ultimate

1 Jahr

61% RABATT*

104,99 € 39,99 € im 1. J.

Entspricht

3,33 €

/Monat

Ersparnis im Vergleich zum Verlängerungspreis
von 104,99 €/Jahr.

[Siehe Abonnementdetails unten.*](#)

Jetzt abonnieren

- ✓ Maskierung der IP-Adresse, sodass Ihre Online-Aktivitäten verborgen bleiben
- ✓ Grenzübergreifender Zugriff auf Ihre Lieblingsinhalte
- ✓ Werbeblocker zum Surfen ohne lästige Werbung¹⁴
- ✓ Verzicht auf Protokollierung zugunsten des Datenschutzes
- ✓ Notausschalter zum Schutz vor Offenlegung privater Daten
- ✓ IP-Rotation und Doppel-VPN zur Stärkung der Privatsphäre
- ✓ KI-gestützter Schutz vor Betrug, Phishing und Malware
- ✓ Überwachung des Darknets auf Ihre Daten⁸
- ✓ Passwort-Manager zur Verwendung starker Passwörter
- ✓ 50 GB Cloud-Backup⁴ zur Sicherung wichtiger Dateien
- ✓ Kindersicherung zum Schutz Ihrer Kinder³

€ 7,91 /Monat

Abschluss mit Augenzwinkern 🤗

„Wer heute kein VPN nutzt, surft ein bissl so,
als würde er seine Postkarten
ohne Kuvert verschicken.“

Kennt ihr diese neuen Zahlungsarten?

Von Wero bis zum digitalen Euro - die OÖN haben sich das näher angesehen.

PayPal, Google Pay und Apple Pay als Dienstleister, Visa, Mastercard und American Express als Kreditkartenanbieter:

Den Markt für Zahlungsabwicklung dominieren US-Anbieter.

In Europa regt sich dagegen Widerstand, es formieren sich Initiativen wie **Wero** oder der **digitale Euro**.

Wie unterscheiden sich Wero und der digitale Euro?

Der **digitale Euro** ist ein von der Europäischen Zentralbank (EZB) geplantes Projekt. Geplant sind eine gesetzliche Akzeptanzpflicht bei Händlern und eine Verfügbarkeit im ganzen Euroraum.

Laut EZB soll es ab 2029 so weit sein.

Bei **Wero** handelt es sich um eine Partnerschaft großer europäischer Banken. Verfügbar ist Wero also nur bei den teilnehmenden Banken, und die Händlerakzeptanz ist wie bei anderen Bezahlverfahren freiwillig.

Was ist Wero?

Wero ist ein vom europäischen Bankenverbund gestarteter Bezahldienst. Verfügbar ist Wero bisher in Frankreich, Deutschland, den Niederlanden, Luxemburg und Belgien, es gibt 46 Millionen Nutzer.

Diese können Wero nun auch beim Online-Einkauf verwenden. An der Kassa in Geschäften soll man ab 2026 und 2027 bezahlen können.

Die Idee dahinter ist, eine **eigene europäische Alternative** zu Visa, Mastercard, PayPal & Co. zu schaffen.

Was Wero kann (bzw. können soll):

-  **Geld in Echtzeit senden** – direkt von Konto zu Konto
-  Nutzung über die **Bank-App**, keine separate Wallet nötig
-  Start mit **P2P-Zahlungen** (Person zu Person), später auch **Online- und Ladenzahlungen**
- **EU** Fokus auf **Europa**, mit hohen Datenschutz- und Sicherheitsstandard

Kommt Wero auch in Österreich?

"Wenn Wero einfach, sicher und alltagstauglich ist, kann es zu einer starken europäischen Alternative zu den US-Diensten werden", sagt Martin Seiter, Spartenobfrau-Stellvertreter der Sparte Banken und Versicherungen in der Wirtschaftskammer Oberösterreich und Vorstandsdirektor bei der Oberbank

Der **digitale Euro** ist im Grunde eine **elektronische Form des Euro**,
herausgegeben von der **Europäischen Zentralbank (EZB)**.

Man kann ihn sich vorstellen wie **Bargeld fürs Smartphone** –
staatlich, sicher und direkt von der Zentralbank, nicht von einer
Geschäftsbank.

Was ist der Unterschied zum „normalen“ Euro?

1. Bargeld (Scheine & Münzen)

- Physisch, anonym
- Direkt von der EZB
- Funktioniert auch ohne Technik
- Wird weniger genutzt

2. Heutiger Euro auf dem Konto

- Digital, **aber**: Das Geld liegt bei **deiner Bank**
- Banken schaffen dieses Geld größtenteils selbst (Giralgeld)
- Abhängig von Bankensystem, Öffnungszeiten, Gebühren

3. Digitaler Euro (geplant)

- Digital **und** direkt von der EZB
- So sicher wie Bargeld
- Könnte auch offline funktionieren (z. B. per Handy-zu-Handy)
- Gedacht für den Alltag: Einkaufen, Überweisen, Rechnungen zahlen

Warum will man den digitalen Euro?

Ein paar wichtige Gründe:

- Bargeld verschwindet langsam, man will eine staatliche Alternative
- **Unabhängigkeit von großen Tech-Konzernen und ausländischen Bezahlssystemen**
- Schutz vor rein privaten Digitalwährungen
- Sicherstellen, dass jeder Zugang zu staatlichem Geld hat

Häufige Sorgen

- **Überwachung?**

Die EZB betont, dass der digitale Euro **so wenig Daten wie möglich** erfassen soll – näher am Bargeld als an heutigen Kartenzahlungen.

- **Abschaffung von Bargeld?**

Offiziell ganz klar: **Nein**. Bargeld soll bleiben.

👉 **Der digitale Euro ist kein neues Geld**, sondern eine **neue Art, den Euro zu nutzen** – modern, staatlich abgesichert und als Ergänzung zu Bargeld und Bankkonten.

Ich erkläre dir, so wie es nach den bisherigen Plänen der EZB aussehen soll.

1. „Brieftasche“ (Wallet) bekommen

Du würdest einen **digitalen Euro** in einer **Wallet** haben, etwa:

- als **App auf dem Smartphone**
- oder über eine **Bank / Sparkasse**
- eventuell auch über eine **separate EZB-App**

Diese Wallet funktioniert wie eine **digitale Geldbörse**, nicht wie ein klassisches Bankkonto.

2. Geld hineinladen

Du tauschst ganz normal:

- Euro vom Girokonto **in digitalen Euro**
- oder später vielleicht Bargeld → digitaler Euro

Das ist **1:1**, ohne Kurs oder Gebühren.

3. Bezahlen im Alltag

a) Im Geschäft

- Handy an das Kassenterminal halten (ähnlich wie NFC)
- Betrag bestätigen
- Fertig – **kein Kartenanbieter**, keine Kreditkarte dazwischen

b) Online

- „Mit digitalem Euro bezahlen“ anklicken
- Wallet bestätigt die Zahlung
- Geld ist sofort beim Händler

4. Geld an andere Menschen senden

Wie Bargeld weitergeben – nur digital:

- Geld direkt von **Wallet zu Wallet**
- ohne Banklaufzeiten
- auch **kleine Beträge**, z. B. 2 oder 5 Euro

5. Offline bezahlen (besonders interessant)

Geplant ist:

- Bezahlen **ohne Internet**
- z. B. Handy zu Handy oder Karte zu Terminal
- späterer Abgleich, wenn wieder Verbindung besteht

Das kommt dem **Bargeld-Gefühl** sehr nahe.

6. Grenzen und Schutz

Damit Banken nicht destabilisiert werden, ist vorgesehen:

- **Höchstbetrag pro Person** (z. B. einige tausend Euro)
- nicht zum Sparen gedacht, sondern zum **Bezahlen**

7. Was du nicht damit machst

- Keine Kredite
- Keine Zinsen
- Kein Spekulationsobjekt

Der digitale Euro ist eher wie **Scheine im Portemonnaie**, nur eben digital.

Ein kleines Alltagsbeispiel

Du gehst zum Bäcker:

- Kaffee + Brötchen: 3,40 €
 - Handy kurz ans Terminal
 - Zahlung durch – **ohne Karte, ohne Bank, ohne Gebühren**
-

Ob **Rentner oder technikferne Menschen** damit zurechtkommen

Das ist eine **sehr berechtigte Sorge** – und genau darüber wird in der EU intensiv diskutiert.

Kurz gesagt:

 **Ja, sie sollen damit zurechtkommen können – aber nur, wenn es richtig umgesetzt wird.**

1. Nicht nur Smartphone – mehrere Wege

Der digitale Euro soll **nicht nur übers Handy** funktionieren. Geplant sind auch:

- **Plastikkarte** (ähnlich einer Bankkarte, aber ohne Konto)
- **Einfache Geräte** mit wenigen Tasten
- Nutzung über **Bank, Sparkasse oder Postfiliale**

Man soll ihn also auch nutzen können, **ohne App-Gewusel**.

2. Bedienung wie beim Bargeld

Das Ziel ist:

- Betrag sehen
- „Ja“ drücken
- fertig

Kein Login-Marathon, keine versteckten Menüs.

Für viele Rentner wäre das **nicht komplizierter als eine EC-Karte**.

3. Hilfe vor Ort

Ganz wichtig:

- Einrichtung und Erklärung bei **Banken & Sparkassen**
- Persönliche Hilfe, nicht nur Online-Tutorials
- Möglichkeit, alles **klassisch erklären zu lassen**

Ohne so eine Betreuung würde das Projekt scheitern – das ist auch den Verantwortlichen klar.

Österreich ist traditionell ein Land mit sehr hoher Bargeld-Affinität.

Im Vorjahr erfolgten in Österreich laut OeNB 62 Prozent aller Zahlungen mit Bargeld. Das sei einer der Höchststände im Euroraum.

Wero und der digitale Euro seien kein Ersatz für Bargeld, sondern eine Ergänzung. "Bargeld bleibt Teil unserer Kultur, digitale Zahlungen sind Teil unserer Zukunft". Beides zusammen garantiert Freiheit und Wahlmöglichkeit beim Bezahlen."

Egal, ob Android oder iOS

Sowohl Android- als auch iOS-Nutzerinnen und -Nutzer sind einer aktuellen Untersuchung zufolge durch gleich mehrere Applikationen gefährdet. Die folgenden **Apps zu löschen**, wenn du sie verwendest, kann sich entsprechend lohnen.



Betroffene Android-Apps - Identifizierte Android-Apps:

Pic Stitch: 5 Millionen+ Downloads

Meru Cabs: 5 Millionen+ Downloads

Sulekha Business: 500.000+ Downloads

ReSound Tinnitus Relief: 500.000+ Downloads

Saludsa: 100.000+ Downloads

Chola Ms Break In: 100.000+ Downloads

EatSleepRIDE Motorcycle GPS: 100.000+ Downloads

Beltone Tinnitus Calmer: 100.000+ Downloads

Betroffene iPhone-Apps - Identifizierte iOS-Apps:

Crumbl: 3,9 Millionen+ Bewertungen

Eureka: Verdienne Geld für Umfragen – 402.100+ Bewertungen

Videoshop – Video Editor – 357.900+ Bewertungen

Solitaire Clash: Gewinne echtes Geld – 244.800+ Bewertungen

Zap Surveys – Verdienne leicht Geld – 235.000+ Bewertungen

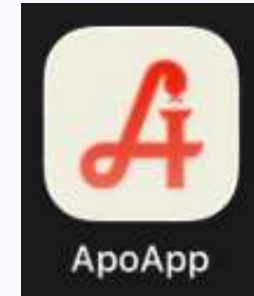
Zwar bedeutet das Vorhandensein einer der oben genannten Exemplare auf deinem Handy oder Tablet noch nicht, dass deine persönlichen Daten gestohlen wurden. Sie sind darüber allerdings zugänglich für Kriminelle. Die Apps zu löschen, ist also die beste Option, sich kurzfristig zu schützen.

Neue "ApoApp":

Beipackzettel nun digital abrufbar

Ob ein Medikament in der Apotheke verfügbar ist, kann man ab sofort über eine neue App abfragen.

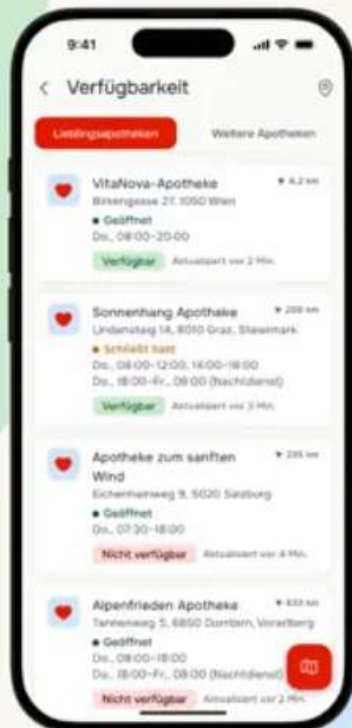
Die "ApoApp" der Apothekerkammer bietet zudem digitale **Beipackzettel**, eine Suche nach **geöffneten Apotheken** in der Nähe und die Möglichkeit, einen **Einnahmeplan** mit **Erinnerungsfunktion** zu erstellen.



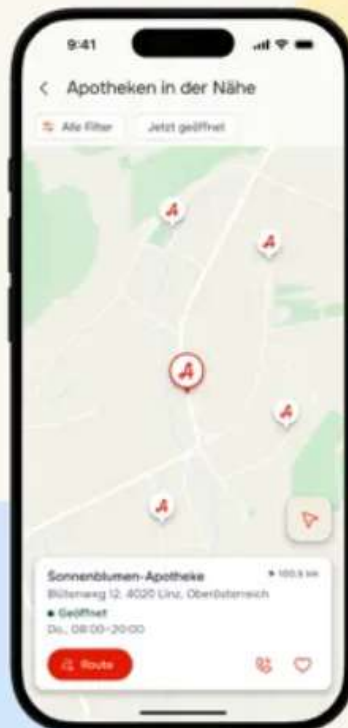
Apotheken finden & Medikation planen



Im Blick haben, wo Medikamente lagernd sind



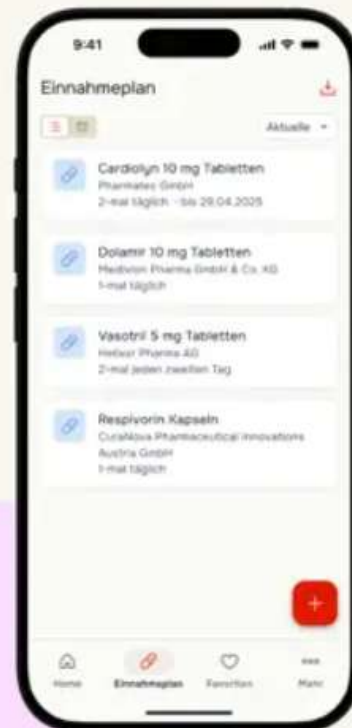
Einfach Apotheken in der Nähe finden



Nie wieder vergessen Medikamente einzunehmen



Individuellen Medikationsplan erstellen

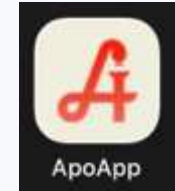


Weitere Services sollen integriert werden und nach und nach mehr Apotheken an Bord kommen. Bisher seien fast 1000 der mehr als 1400 Apotheken in Österreich an die App angeschlossen.

Die Medikamentenverfügbarkeit am jeweiligen Standort werde automatisch alle **zehn Minuten aktualisiert**.

Angezeigt wird die Verfügbarkeit einer Arznei in Apotheken in der Nähe der Position des Handys und in zuvor als Favoriten gespeicherten "Lieblingsapotheken".

Die "ApoApp" sei "nur ein erster kleiner Schritt, auf den viele folgen werden", sagte Ulrike Mursch-Edlmayr, Präsidentin der Österreichischen Apothekerkammer.



Die **Gesundheits-Hotline 1450** bietet ab Februar für jene, die mit Apps nicht so vertraut sind, auch telefonisch Auskunft über die nächstgelegene Apotheke und die Medikamentenverfügbarkeit.

Und zum Abschluss noch ein kleines Stück unnützes Wissen:

In der EDV gibt es kein „funktioniert nicht“ – nur ein
„funktioniert noch nicht“.

In diesem Sinne danke ich euch fürs Dabeisein!

Der nächste EDV-Stammtisch kommt bestimmt – und bis dahin gilt:

Bleibt neugierig, bleibt kritisch und vergesst nicht:

Der Computer ist immer schuld. 🤔