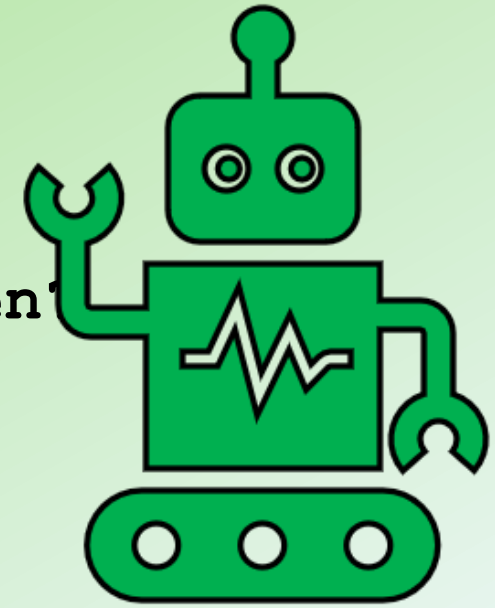
CAW November 2026

- Aktuelle Informationen
- „Senioren mit Smartphone“ App
- 5 Mythen zu Android
- KFZ- Versicherung / Wie kann ich vergleichen
- Fragen / Antworten



Fragen

Hallo liebes CAW-Team,
vielleicht könnt ihr bei einem der nächsten Termine mal was zu Sicherheitslücken in Systemen vortragen und wie Hacker diese finden.

Aktuelles Beispiel wäre das Thema in der letzten Woche mit den gehackten Kühltruhen in den Supermärkten. Wie passiert sowas?
Vielen Dank im Voraus.

Gruß

Manfred Bischoff

Liebes Computertreff Team,

Ich möchte morgen gerne an dem Treffen teilnehmen.
Ich habe im Moment dringende Fragen zum Umgang mit meinem Smartphone.
Wichtig ist mir die Verwaltung meiner Speicher und Übertragung von Smartphone auf meinen Laptop.
Ich mache seit einiger Zeit online Banking und möchte bei der Verwaltung der Unterlagen meiner Mutter und bei Abrechnungen Krankenkasse und Pflegekasse mehr digital machen.
Für mich sind es immer nur ganz kleine Schritte weil sich kaum etwas "von selbst" erklärt.

Deshalb wäre es für mich sehr wichtig, wenn ich bei Ihnen Unterstützung bekomme,
Mit freundlichen Grüßen
Christine Brungs

Aktuelles

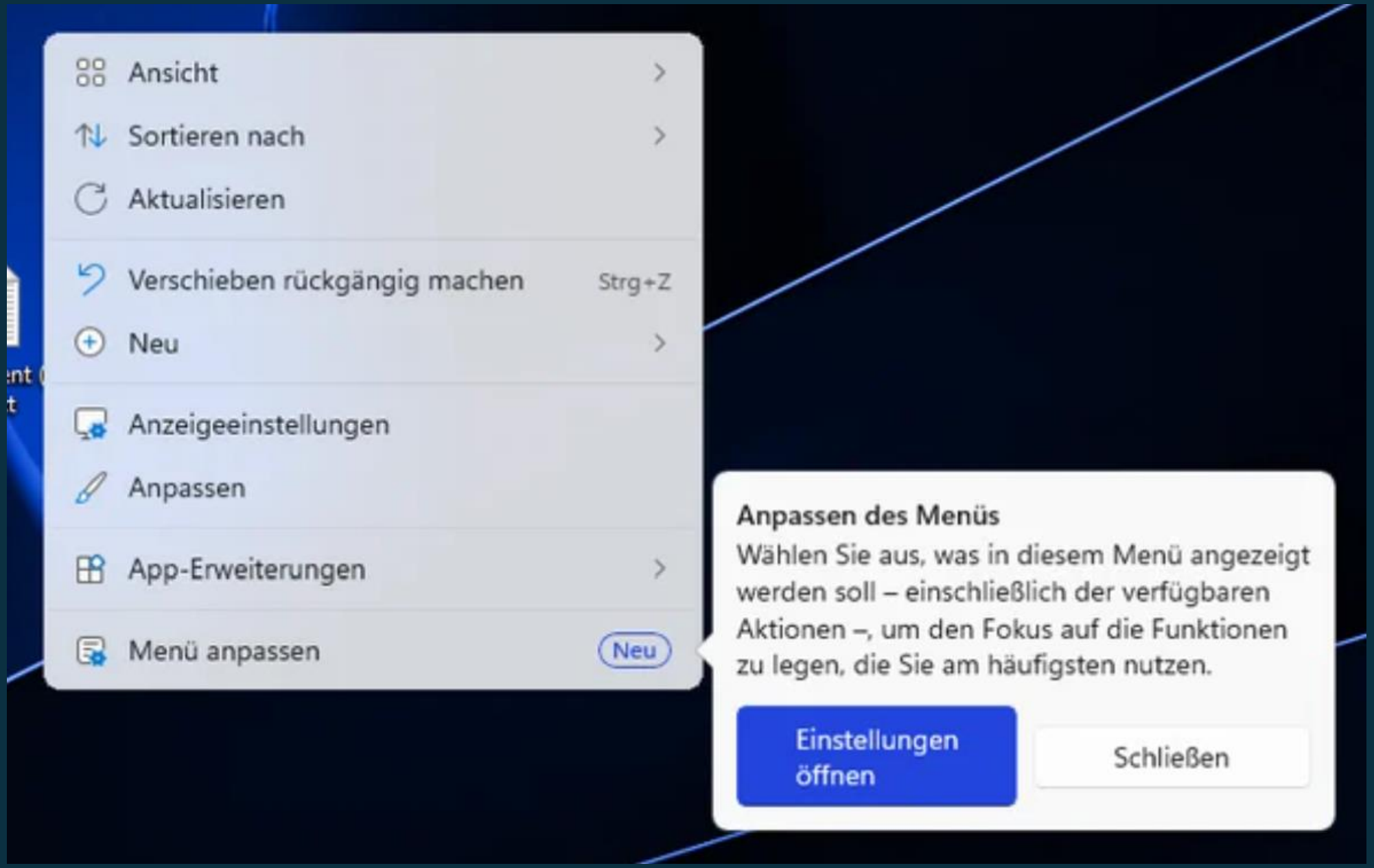
Microsoft hat einen Klickpfad beim installieren der Home-Edition blockiert; Microsoft Konto muss angelegt werden; lokale Konten bleiben per Befehl möglich; Hardwaregrenzen bestehen weiter.

Aktuellen Berichten zufolge plant Microsoft für das nächste Jahr kein Windows 12, sondern konzentriert sich stattdessen auf ein umfangreiches Update in Form von Windows 11 27H2. Bis es so weit ist, erhält die aktuelle Variante des Betriebssystems 26H2 jeden Monat neue Funktionen.

Rettung ohne USB-Laufwerk

Für den Fall eines Systemfehlers integriert Microsoft eine Funktion namens **Cloud Rebuild**. Anwender sollen Windows 11 damit direkt aus der Cloud neu installieren können, selbst wenn das Gerät nicht mehr bootet. Der Prozess lädt das Installationsabbild sowie die passenden Treiber über Windows Update herunter. Ein manuell erstelltes USB-Rettungsmedium ist dann nicht länger erforderlich. Bei Nutzung dieser Funktion werden alle persönlichen Dateien, Programme, Benutzerkonten und Einstellungen gelöscht

System – Wiederherstellung – Diesen PC neu erstellen


Ansicht
Sortieren nach
Aktualisieren
Verschieben rückgängig machen
Strg+Z
Neu
Anzeigeeinstellungen
Anpassen
App-Erweiterungen
Menü anpassen
Neu
Anpassen des Menüs
Wählen Sie aus, was in diesem Menü angezeigt werden soll – einschließlich der verfügbaren Aktionen –, um den Fokus auf die Funktionen zu legen, die Sie am häufigsten nutzen.
Einstellungen öffnen
Schließen

Opera

- Kostenlos und ohne Anmeldung.
- Unbegrenztes Datenvolumen.
- VPN direkt im Browser integriert.
- Auswahl zwischen Europa, Amerika und Asien.
- Für Windows und Android verfügbar.



VPN-Erweiterungen für andere Browser

Auch für Chrome, Firefox und Edge gibt es kostenlose VPN-Erweiterungen:

- Proton VPN – kostenlos, unbegrenztes Datenvolumen.
- hide.me – kostenlose Variante.
- Windscribe – kostenlos mit Datenlimit.

Mein ELSTER: Benachrichtigung zur Datensynchronisierung
Ausstellende Stelle: ELSTER – Ihr Online-Finanzamt , USt-Identifikationsnummer DE 813 297 313
Ihr ELSTER-Konto: **info@seniorenzentrum-weyhe.de**
Kennnummer: **2656870563345**
Frist: **18.11.2026**
Betreff: **Verwaltungsmitteilung**
Bitten wir Sie, die Daten Ihres IMAP-Kontos zu synchronisieren.

IMAP jetzt synchronisieren

Mit freundlichen Grüßen
ELSTER – Ihr Online-Finanzamt2026-11-13 18:40:43 || iYhNDkVvgyoIhlc1

Quelldaten:

```
Return-Path: <elster25@www.fujii-shoji.jp>
Authentication-Results: kundenserver.de; dkim=none; spf=pass
 smtp.mailfrom=elster25@www.fujii-shoji.jp; dmarc=none
 header.from=www.fujii-shoji.jp; iprev=pass policy.iprev=112.78.125.84
```

https://www.abuseipdb.com/check

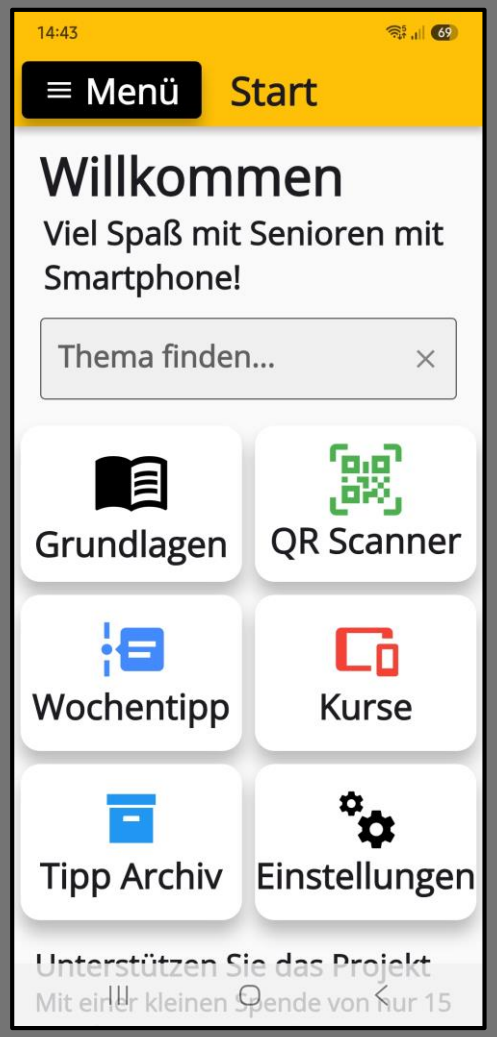
Missbrauch einer IP Adresse

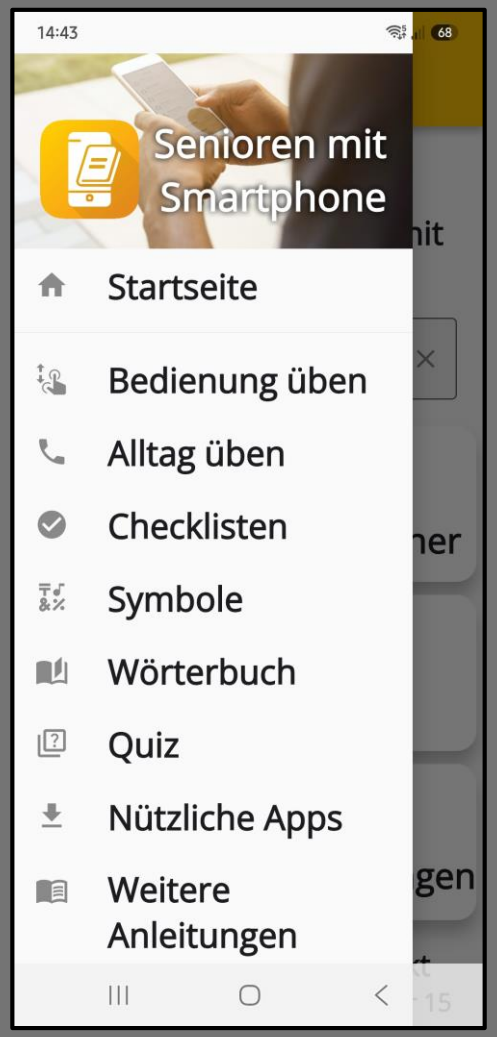
Die Umsatzsteuer-Identifikationsnummer **DE 813 297 313** gehört dem **Bayerischen Landesamt für Steuern (Dienststelle München)**, unter anderem im Zusammenhang mit dem Online-Finanzamt ELSTER.

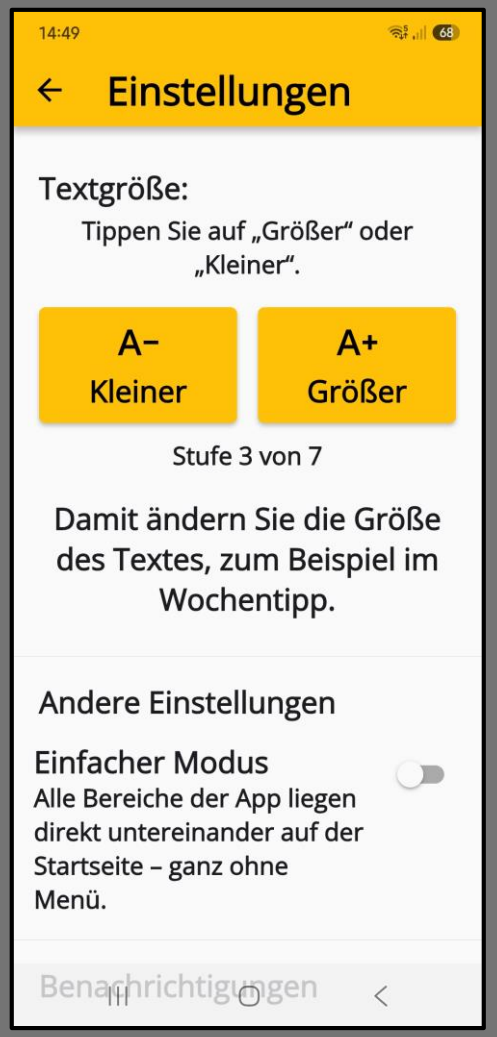
Sicherheitshinweis

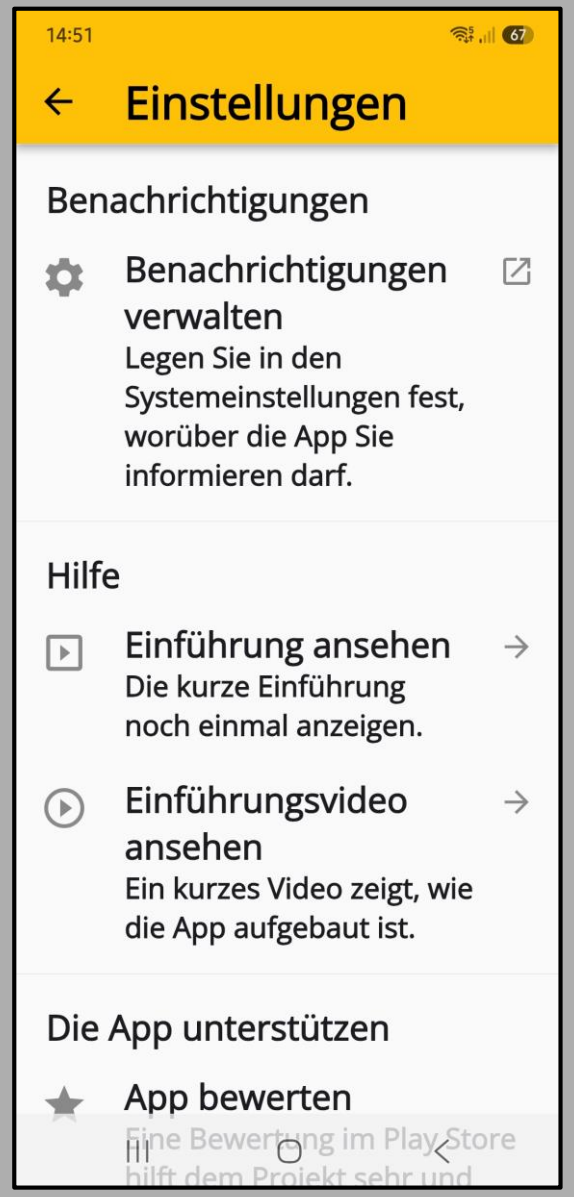
Falls Sie eine E-Mail oder Nachricht erhalten haben, die sich auf ELSTER oder die Steuerverwaltung bezieht, loggen Sie sich niemals über Links aus der Nachricht ein. Rufen Sie ELSTER direkt im Browser auf und beachten Sie Warnungen vor Phishing, etwa vom **Landesamt für Steuern Niedersachsen**

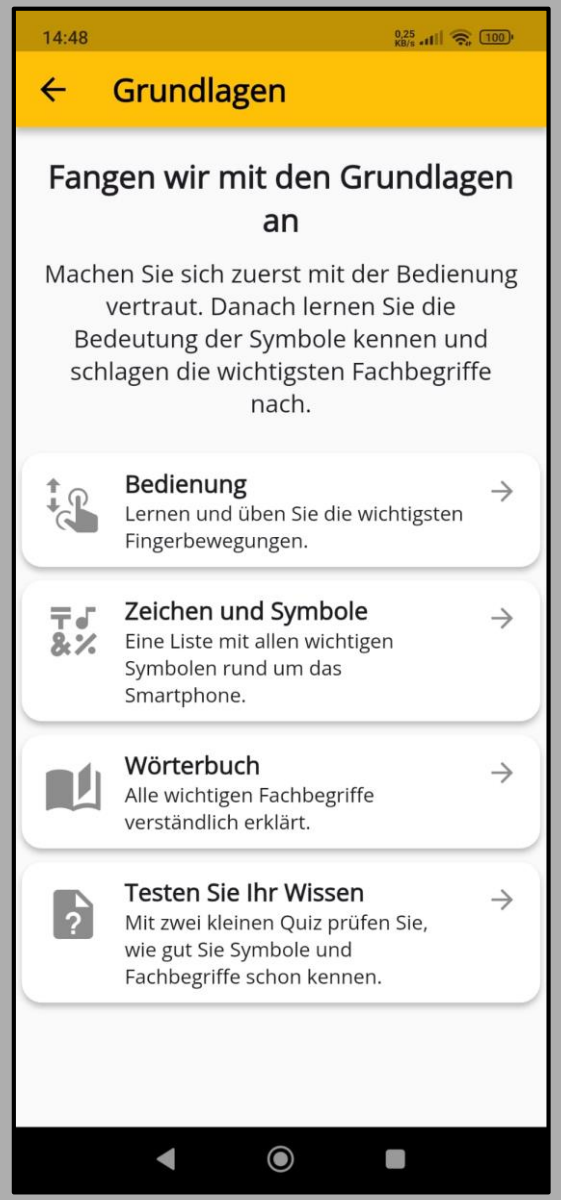
Senioren mit Smartphone App



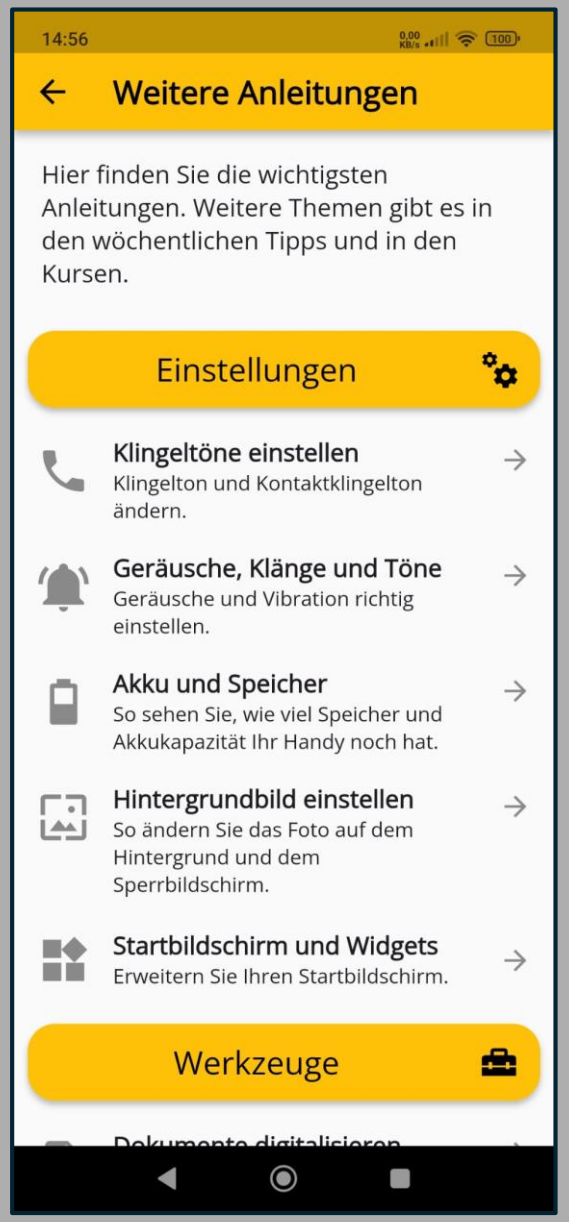


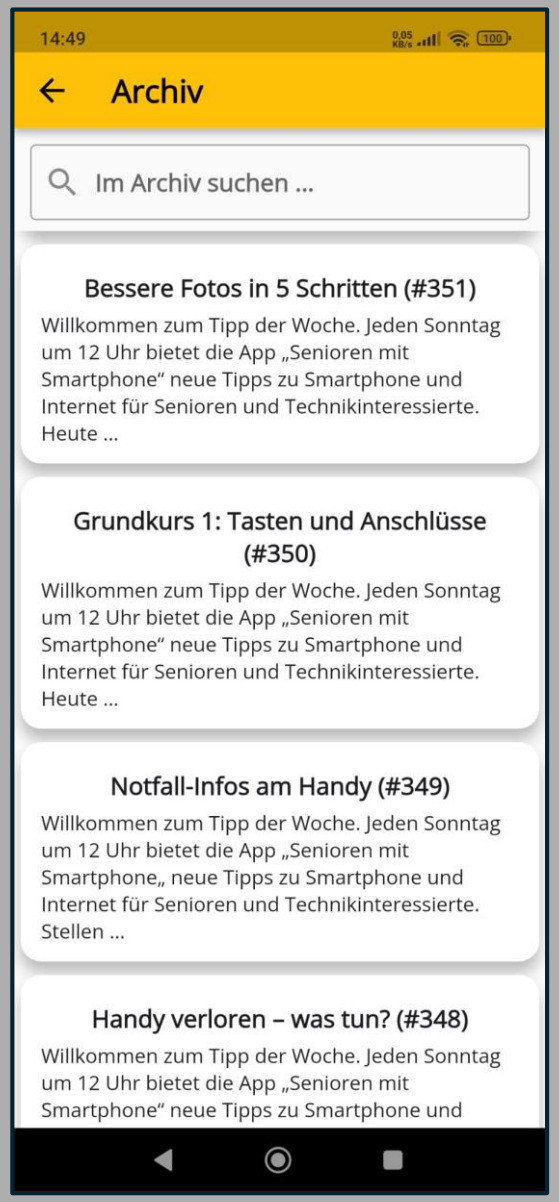



14:51
Einstellungen
Benachrichtigungen
Benachrichtigungen verwalten
Legen Sie in den Systemeinstellungen fest, worüber die App Sie informieren darf.
Hilfe
Einführung ansehen
Die kurze Einführung noch einmal anzeigen.
Einführungsvideo ansehen
Ein kurzes Video zeigt, wie die App aufgebaut ist.
Die App unterstützen
App bewerten
Eine Bewertung im Play Store hilft dem Projekt sehr und


14:48
Grundlagen
Fangen wir mit den Grundlagen an
Machen Sie sich zuerst mit der Bedienung vertraut. Danach lernen Sie die Bedeutung der Symbole kennen und schlagen die wichtigsten Fachbegriffe nach.
Bedienung
Lernen und üben Sie die wichtigsten Fingerbewegungen.
Zeichen und Symbole
Eine Liste mit allen wichtigen Symbolen rund um das Smartphone.
Wörterbuch
Alle wichtigen Fachbegriffe verständlich erklärt.
Testen Sie Ihr Wissen
Mit zwei kleinen Quiz prüfen Sie, wie gut Sie Symbole und Fachbegriffe schon kennen.


14:55
Symbole
Nach einem Symbol suchen ...
Grundlagen
Home/Startseite
Das Symbol bringt Sie immer zum Startbildschirm
Einstellungen (Ein Zahnrad)
Das Symbol führt Sie zu den Einstellungen des Telefons. Hier können Sie die Helligkeit und andere Dinge einstellen.
Aktualisieren
Das Symbol bedeutet, dass Sie etwas aktualisieren können
Menü (drei Striche)
Verwenden Sie diese Schaltfläche, um das Menü zu öffnen, wie in dieser App
Menü (drei Punkte)
Verwenden Sie diese Schaltfläche, um weitere Möglichkeiten zu öffnen, genau wie bei WhatsApp
Lupe
Hier können Sie etwas suchen oder


14:56
Weitere Anleitungen
Hier finden Sie die wichtigsten Anleitungen. Weitere Themen gibt es in den wöchentlichen Tipps und in den Kursen.
Einstellungen
Klingeltöne einstellen
Klingelton und Kontaktklingelton ändern.
Geräusche, Klänge und Töne
Geräusche und Vibration richtig einstellen.
Akku und Speicher
So sehen Sie, wie viel Speicher und Akkukapazität Ihr Handy noch hat.
Hintergrundbild einstellen
So ändern Sie das Foto auf dem Hintergrund und dem Sperrbildschirm.
Startbildschirm und Widgets
Erweitern Sie Ihren Startbildschirm.
Werkzeuge


14:49
Archiv
Im Archiv suchen ...
Bessere Fotos in 5 Schritten (#351)
Willkommen zum Tipp der Woche. Jeden Sonntag um 12 Uhr bietet die App „Senioren mit Smartphone“ neue Tipps zu Smartphone und Internet für Senioren und Technikinteressierte. Heute ...
Grundkurs 1: Tasten und Anschlüsse (#350)
Willkommen zum Tipp der Woche. Jeden Sonntag um 12 Uhr bietet die App „Senioren mit Smartphone“ neue Tipps zu Smartphone und Internet für Senioren und Technikinteressierte. Heute ...
Notfall-Infos am Handy (#349)
Willkommen zum Tipp der Woche. Jeden Sonntag um 12 Uhr bietet die App „Senioren mit Smartphone„ neue Tipps zu Smartphone und Internet für Senioren und Technikinteressierte. Stellen ...
Handy verloren – was tun? (#348)
Willkommen zum Tipp der Woche. Jeden Sonntag um 12 Uhr bietet die App „Senioren mit Smartphone“ neue Tipps zu Smartphone und


14:49
Wochentipp
Wochentipp merken
Bessere Fotos in 5 Schritten (#351)
vom 18.10.2026
Willkommen zum Tipp der Woche. Jeden Sonntag um 12 Uhr bietet die App „Senioren mit Smartphone“ neue Tipps zu Smartphone und Internet für Senioren und Technikinteressierte.
Heute startet eine neue Reihe: „Fotos & Erinnerungen“. In sechs Teilen zeige ich Ihnen, wie Sie schöne Fotos machen, sie gut aufbewahren und mit Ihrer Familie teilen. Die Teile erscheinen immer am dritten Sonntag im Monat, im Wechsel mit Tipps zu nützlichen Alltags-Apps.
Wir fangen ganz vorne an: bei der Kamera selbst. Vielleicht kennen Sie das: Auf dem Bildschirm sah das Enkelkind noch wunderbar aus, und hinterher ist das Foto unscharf, zu dunkel oder schief. Das liegt fast nie an Ihnen und auch nicht am Handy. Meist fehlen nur ein paar kleine Handgriffe. Heute zeige ich Ihnen fünf davon. Sie brauchen dafür keine neue App, nur die Kamera, die schon auf Ihrem

14:49

Kursauswahl

Suchen Sie sich einen Kurs aus:

Lektion 3 von 8
WhatsApp Kurs
Lernen Sie alles über WhatsApp in diesem großartigen Kurs. Werden Sie ein WhatsApp-Experte.

Lektion 2 von 3
Internet Grundlagen
In diesem Kurs werden Sie die wichtigsten Begriffe rund um das Internet lernen.

Abgeschlossen
Google Play Store
Erkunden Sie den Marktplatz auf Ihrem Mobiltelefon und laden Sie aufregende Apps herunter, ohne Abofalle.

Abgeschlossen
Google Maps
Auf diese Weise wird die nächste Reise noch besser werden. Ob mit dem Auto, dem Zug oder einfach mit dem Fahrrad.

Die App entsteht in meiner Freizeit. Über eine kleine Spende für Server und Strom freue ich mich sehr – tippen Sie dafür einfach hier. Vielen Dank!

14:57

YouTube

So benutzen Sie YouTube

YouTube ist ein Videoportal, auf dem Sie kostenlos Videos ansehen können. Dort finden Sie alle Arten von Videos: Ausschnitte aus Film und Fernsehen, Musikvideos, Anleitungen und vieles mehr.

Auch für Sie ist die Plattform praktisch – zum Beispiel, um Musik zu hören oder die Tagesschau noch einmal anzusehen.

So funktioniert es

Sie brauchen die App „YouTube“. Sie ist auf den meisten Smartphones bereits installiert. Suchen Sie nach diesem Symbol – oft ist es im Ordner „Google“ zu finden:

Haben Sie die App geöffnet, tippen Sie oben rechts auf die Lupe und geben Sie

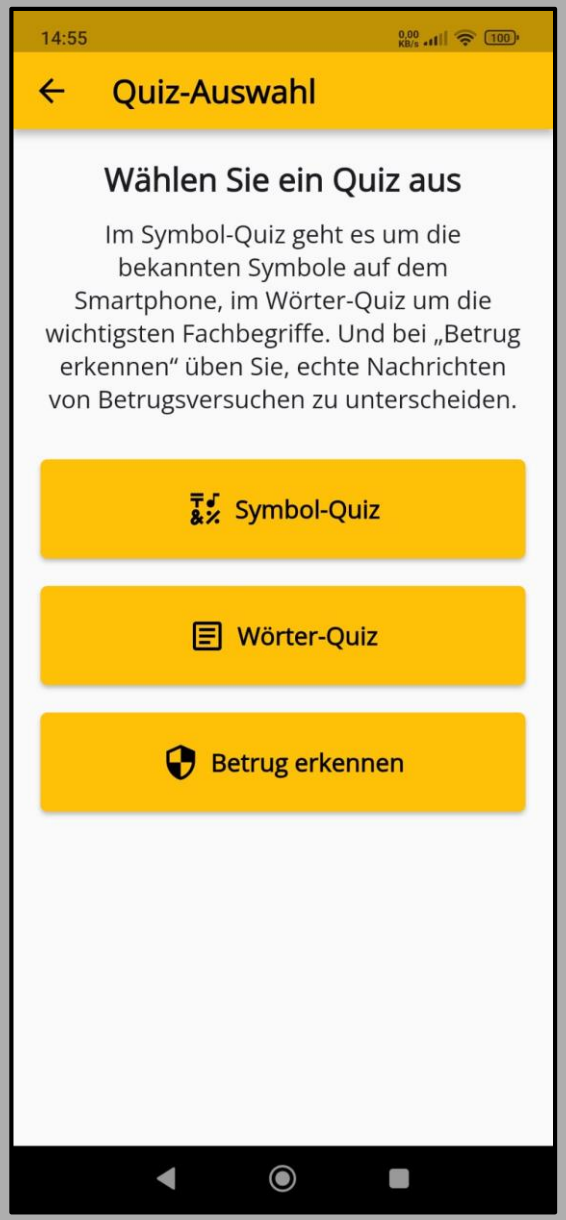
14:57

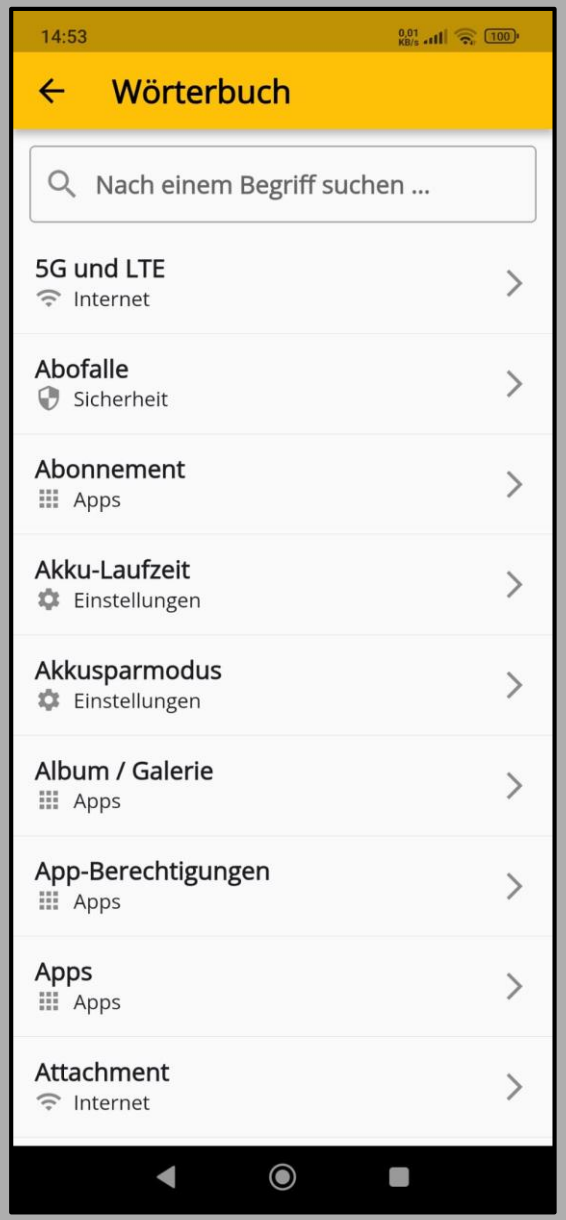
WhatsApp

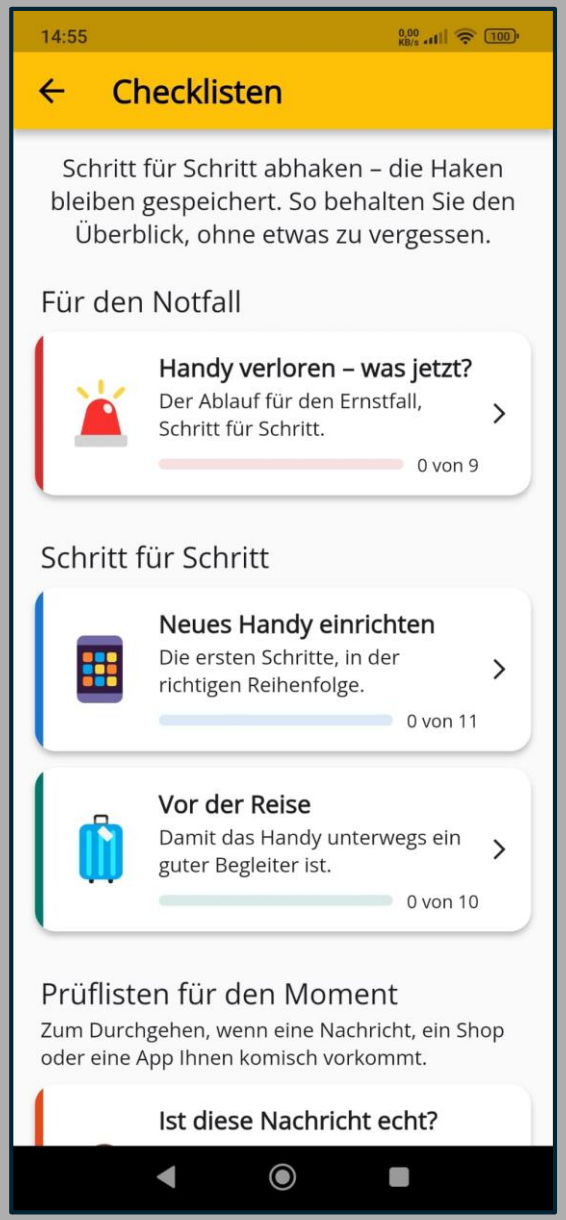
WhatsApp besser verstehen

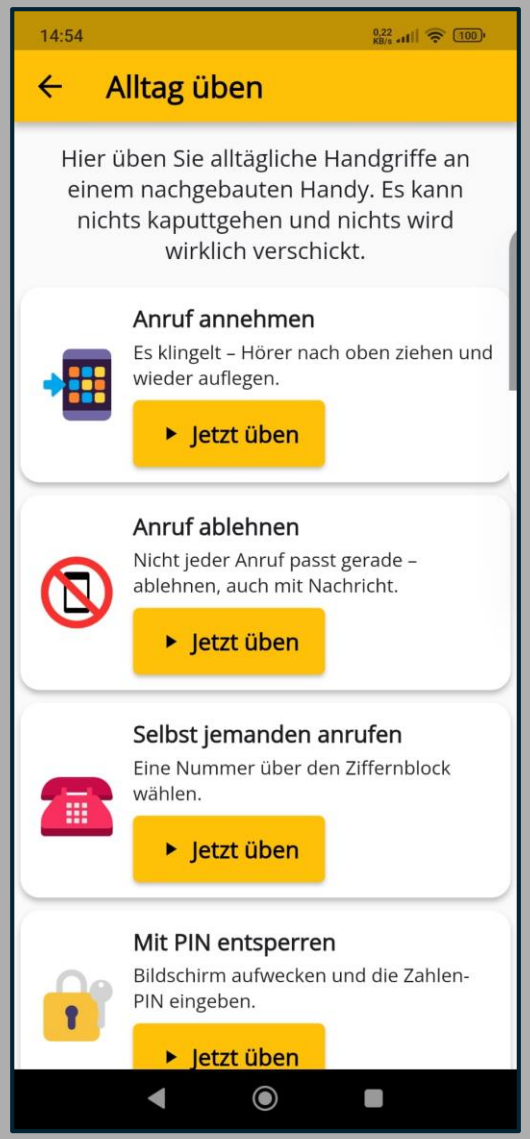
Tippen Sie ein Thema an, um die Erklärung zu lesen.

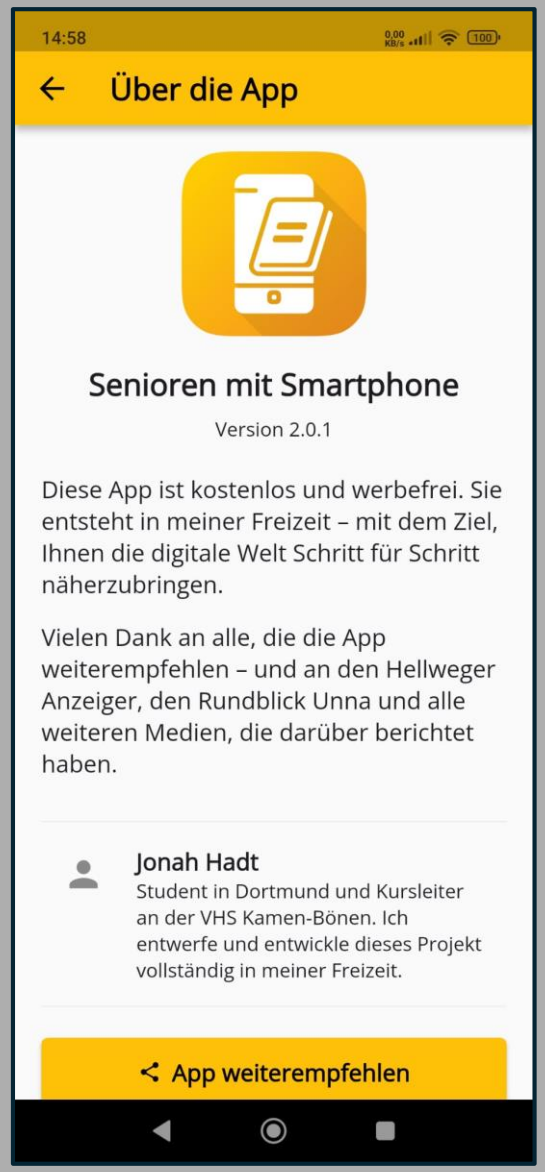
- Nachrichten
- Status
- Textarten
- Anrufe


14:55
Quiz-Auswahl
Wählen Sie ein Quiz aus
Im Symbol-Quiz geht es um die bekannten Symbole auf dem Smartphone, im Wörter-Quiz um die wichtigsten Fachbegriffe. Und bei „Betrug erkennen“ üben Sie, echte Nachrichten von Betrugsversuchen zu unterscheiden.
Symbol-Quiz
Wörter-Quiz
Betrug erkennen


14:53
Wörterbuch
Nach einem Begriff suchen ...
5G und LTE
Internet
Abofalle
Sicherheit
Abonnement
Apps
Akku-Laufzeit
Einstellungen
Akkusparmodus
Einstellungen
Album / Galerie
Apps
App-Berechtigungen
Apps
Apps
Apps
Attachment
Internet


14:55
Checklisten
Schritt für Schritt abhaken – die Haken bleiben gespeichert. So behalten Sie den Überblick, ohne etwas zu vergessen.
Für den Notfall
Handy verloren – was jetzt?
Der Ablauf für den Ernstfall, Schritt für Schritt.
0 von 9
Schritt für Schritt
Neues Handy einrichten
Die ersten Schritte, in der richtigen Reihenfolge.
0 von 11
Vor der Reise
Damit das Handy unterwegs ein guter Begleiter ist.
0 von 10
Prüflisten für den Moment
Zum Durchgehen, wenn eine Nachricht, ein Shop oder eine App Ihnen komisch vorkommt.
Ist diese Nachricht echt?





Diese App ist verfügbar sowohl im Google als auch im Apple Store

Smartphone Mythen

1. Drittanbieter Appstores enthalten immer Viren

2. WLAN und Bluetooth sind Einfallstore für Hacker

3. Öffentliche Hotspots sind gefährlich

4. Veraltete Android-Versionen sind unsicher

5. Ständige Spionage durch Kamera und Mikrofon

1a. Drittanbieter AppStores

Jeder Store hat eine eigene App, die als APK Datei heruntergeladen werden kann.

(einschalten: *Installieren unbekannter Apps*)

Diese Einstellung bietet ein Einfallstor für Hacker, also sollte gegebenenfalls nach Installation die Einstellung wieder zurückgesetzt werden.

Drittanbieter-Appstores enthalten nicht grundsätzlich Viren. Das Risiko ist aber je nach Anbieter deutlich unterschiedlich. Einige sind seriös, andere verteilen manipulierte Apps oder Schadsoftware.

1b. Drittanbieter

Appstore	Einschätzung	Besonderheiten
Google Play Store	Relativ sicher	Automatische Sicherheitsprüfungen durch Google Play Protect; Schadsoftware kann trotzdem durchrutschen.
Samsung Galaxy Store	Relativ sicher	Offizieller Store für Samsung-Geräte; ebenfalls keine absolute Garantie.
F-Droid	Für Open-Source-Apps eine interessante Alternative	Apps sind quelloffen; F-Droid baut viele Pakete selbst. Das schließt Sicherheitslücken oder schädliche Apps nicht grundsätzlich aus.
Amazon Appstore	Etablierter Anbieter	Ein weiterer offizieller Appstore; auch hier ist keine absolute Sicherheit garantiert.
APKPure	Vorsicht geboten	APK-Dateien stammen nicht direkt aus dem offiziellen Google Play Store; Herkunft und Integrität sollten geprüft werden.
Beliebige APK-Websites	Erhöhtes Risiko	Dateien können manipuliert sein oder Schadsoftware enthalten.
Unbekannte oder unseriöse Appstores	Hohes Risiko	Mögliche Verbreitung manipulierter Apps, Spionageprogramme und anderer Schadsoftware.

2a. WLAN und Bluetooth

Das permanente Aussenden der MAC-Adresse kostet Akku, automatischen Verbindungsaufbau deaktivieren.

Liste der gespeicherten WLAN-Netzwerke regelmäßig löschen (reduzieren), kann Hinweis auf Standort geben, Gerät kann dann auch ohne GPS geortet werden.

Nehmen sie keine Verbindungsanforderung von Bluetooth Geräten an, die sie nicht kennen, löschen Sie regelmäßig alte Verbindungen, seien Sie vorsichtig wenn sie einen WLAN- oder Bluetooth Hotspot zur Verfügung stellen, lassen Sie den Netznamen nicht öffentlich anzeigen, schalten sie ihn aus wenn er nicht mehr gebraucht wird.

2b. WLAN und Bluetooth

In Cafés, Hotels, Flughäfen oder Bahnhöfen gibt es häufig öffentliche WLANs.

Mögliche Gefahren:

- **Ein Angreifer betreibt einen gefälschten WLAN-Hotspot mit einem vertrauenswürdig klingenden Namen. (z.B.: Hotel_Gast)**
- **Er versucht, die Kommunikation zwischen Smartphone und Internet zu manipulieren.**
- **Er kann versuchen, unverschlüsselte Daten abzufangen.**
- **Er kann Nutzer auf gefälschte Anmeldeseiten locken.**

HTTPS und moderne App-Verschlüsselung schützen viele Daten. Ein Angreifer kann deshalb nicht einfach sämtliche Nachrichten, Passwörter oder Bankdaten mitlesen, nur weil er im gleichen WLAN ist.

2c. WLAN und Bluetooth

Maßnahme	Empfehlung
Öffentliche WLANs	Nur vertrauenswürdige Netzwerke verwenden
Automatische Verbindung	Bei unbekannten WLANs deaktivieren
Heimrouter	WPA2-AES oder WPA3 verwenden
Android-Updates	Regelmäßig installieren
VPN nutzen	Bei Bedarf, besonders in nicht vertrauenswürdigen Netzwerken
Unbekannte Anmeldeseiten	Keine Passwörter eingeben, wenn die Echtheit zweifelhaft ist

2d. WLAN und Bluetooth

Situation	Risikoeinschätzung
Aktuelles Android, Heim-WLAN mit WPA2-AES oder WPA3	Eher gering
Aktuelles Android, Bluetooth für Kopfhörer aktiviert	Im Normalfall gering
Öffentliches WLAN ohne zusätzliche Vorsichtsmaßnahmen	Erhöhtes Risiko
Veraltetes Android ohne Sicherheitsupdates	Erhöhtes Risiko
Unbekannte APK-Dateien installiert und weitreichende Berechtigungen erteilt	Deutlich erhöhtes Risiko
Gezielter Angriff durch einen professionellen Angreifer	Abhängig von Gerät, Software und Angriffsmethode

3. Öffentliche Hotspots

Tätigkeit	Empfehlung
Nachrichten lesen	Normalerweise unproblematisch
Nachrichten über WhatsApp versenden	Bei aktuellem Gerät und offizieller App normalerweise sicher
Webseiten mit HTTPS besuchen	In der Regel sicher
Onlinebanking	Möglichst über die offizielle Banking-App oder die korrekt aufgerufene Bank-Webseite
Einkäufe mit Kreditkarte	Nur auf vertrauenswürdigen Webseiten und bei verschlüsselter Verbindung
Unbekannte Zertifikate installieren	Nein
Unbekannte Apps oder APK-Dateien herunterladen	Vermeiden
Zugangsdaten auf unbekannten Anmeldeseiten eingeben	Nein
Vertrauliche berufliche Daten übertragen	Nur über dafür vorgesehene, abgesicherte Verbindungen

4. Veraltete Android Versionen

Noch im Mai26 waren mehr als 50% aller Android-Mobilgeräte mit Android 14 oder älter unterwegs. Grundsätzlich kein Problem, da Herstellerabhängig die Sicherheitsupdates unabhängig der Android Version erfolgen. Prüfen Sie also unter Einstellungen, ob die Sicherheitsupdates aktuell sind. Sollten für ihr Gerät allerdings schon seit längerem (+6M) keine Updates (Android und/oder Sicherheit) eingespielt sein, sollten Sie über ein neues Gerät nachdenken.😒

Endoflife.date

5. Ständige Spionage durch K / M

Ja, ein gewisses Risiko besteht. Eine ständige heimliche Überwachung durch die Kamera und das Mikrofon ist bei einem normalen, aktuellen Android-Smartphone jedoch nicht der Regelfall. Es lohnt sich, die Einstellungen zu überprüfen und zu wissen, welche Daten Apps sammeln können.

Dabei muss man drei Dinge unterscheiden:

1. **Zugriff auf Kamera und Mikrofon:** Apps können unter bestimmten Voraussetzungen Bilder, Videos und Ton aufnehmen.
2. **Datensammlung durch Apps:** Apps können beispielsweise Nutzungsverhalten, Standortdaten und Interessen erfassen.
3. **Gezielte Spionage:** Schadsoftware oder ein kompromittiertes Smartphone können eine tatsächliche Überwachung ermöglichen.