CAW 19.06.2024

Aktuelles zu Windows

Aktuelles zu Android

Sicherheit im WLAN

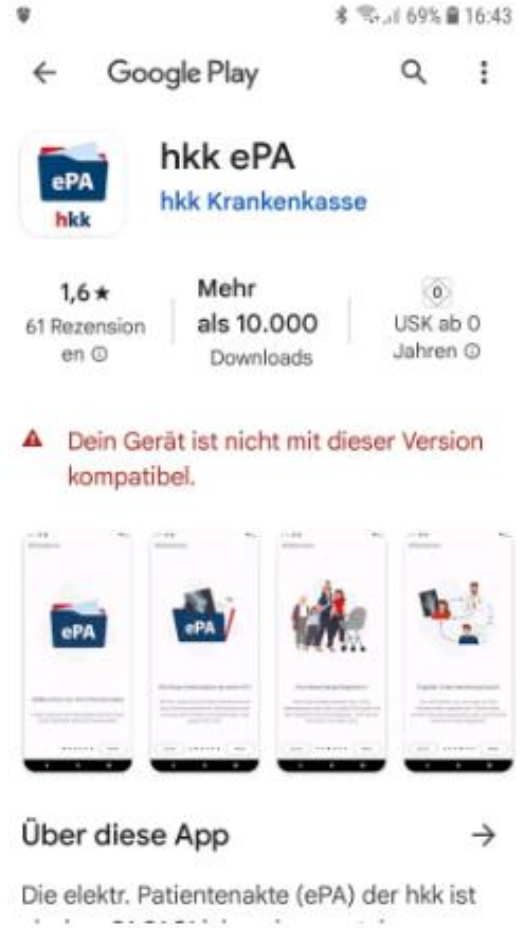
Aktuelles zum E-Rezept

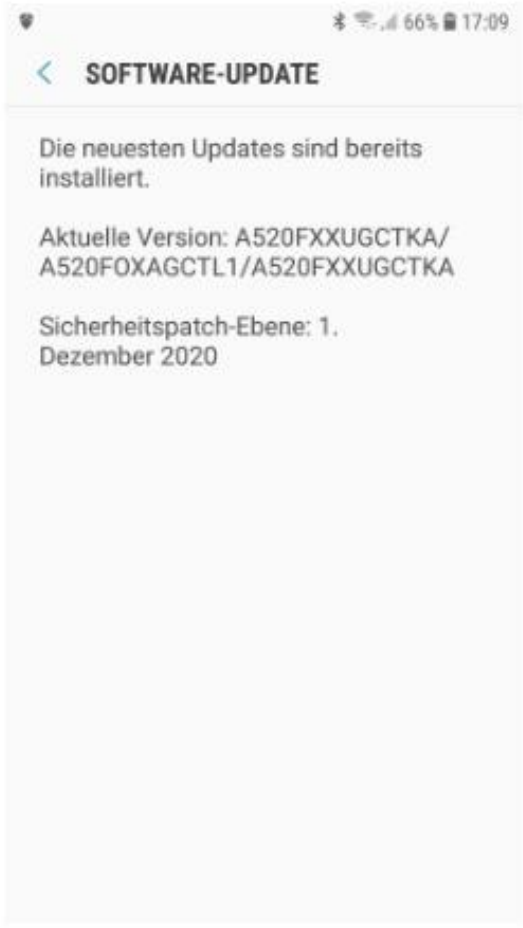
Nutzung der Tastaturkürzel

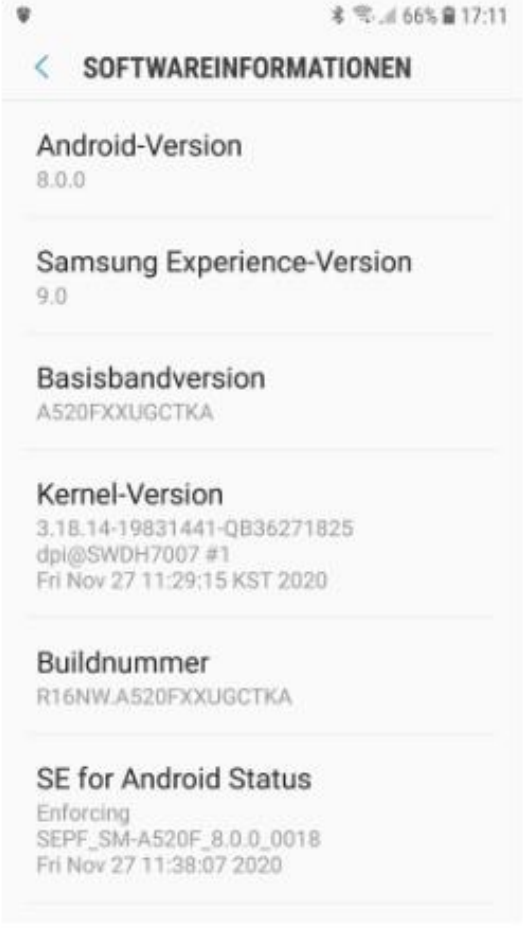
Am wichtigsten sind aber Ihre Fragen, die wir gerne beantworten wollen

Fragen

Ich kann die eRezept App nicht installieren. Mein Gerät ist nicht kompatibel. Was tun? LG Heinfried.







Windows aktuell

NICHTS

https://www.computerbild.de/artikel/cb-News-Finanzen-Vorsicht-bei-dieser-E-Mail-Commerzbank-38568459.html

https://www.computerbild.de/artikel/cb-News-Sicherheit-Diese-gefaehrliche-Mail-sollten-Prime-Kunden-nicht-beantworten-38556661.html

Android aktuell

Android 11	Red Velvet Cake	11	30	8. September 2020	Februar 2024 (41 Monate)
Android 12	Snow Cone	12	31	4. Oktober 2021	März 2024 (29+ Monate)
Android 12L	Snow Cone v2	12.1[A 1]	32	7. März 2022	
Android 13	Tiramisu	13	33	15. August 2022	
Android 14	Upside Down Cake	**14**	34	4. Oktober 2023	
Android 15	Vanilla Ice Cream	15 DP2	35	21. März 2024	März 2024

Legende: Ältere Version; nicht mehr unterstützt | Ältere Version; noch unterstützt | **Aktuelle Version** | Aktuelle Vorabversion

Android aktuell (Software)

Android Smartphone regelmäßig neu starten um zu verhindern, dass es langsamer wird oder hängt.

Außerdem regelmäßig prüfen, ob ein Softwareupdate zur Verfügung steht:

- **Einstellungen - Software-Update**
- **Herunterladen und installieren**
- **Befolgen der Anweisungen auf dem Bildschirm (z.B. zu wenig AKKU)**

Android aktuell (Apps)

Play Store

Konto

Apps und Geräte verwalten

Verwalten

Nach Updates suchen

Alle installieren

(Unter Benachrichtigungseinstellungen kann „Updates verfügbar“ angestellt werden)

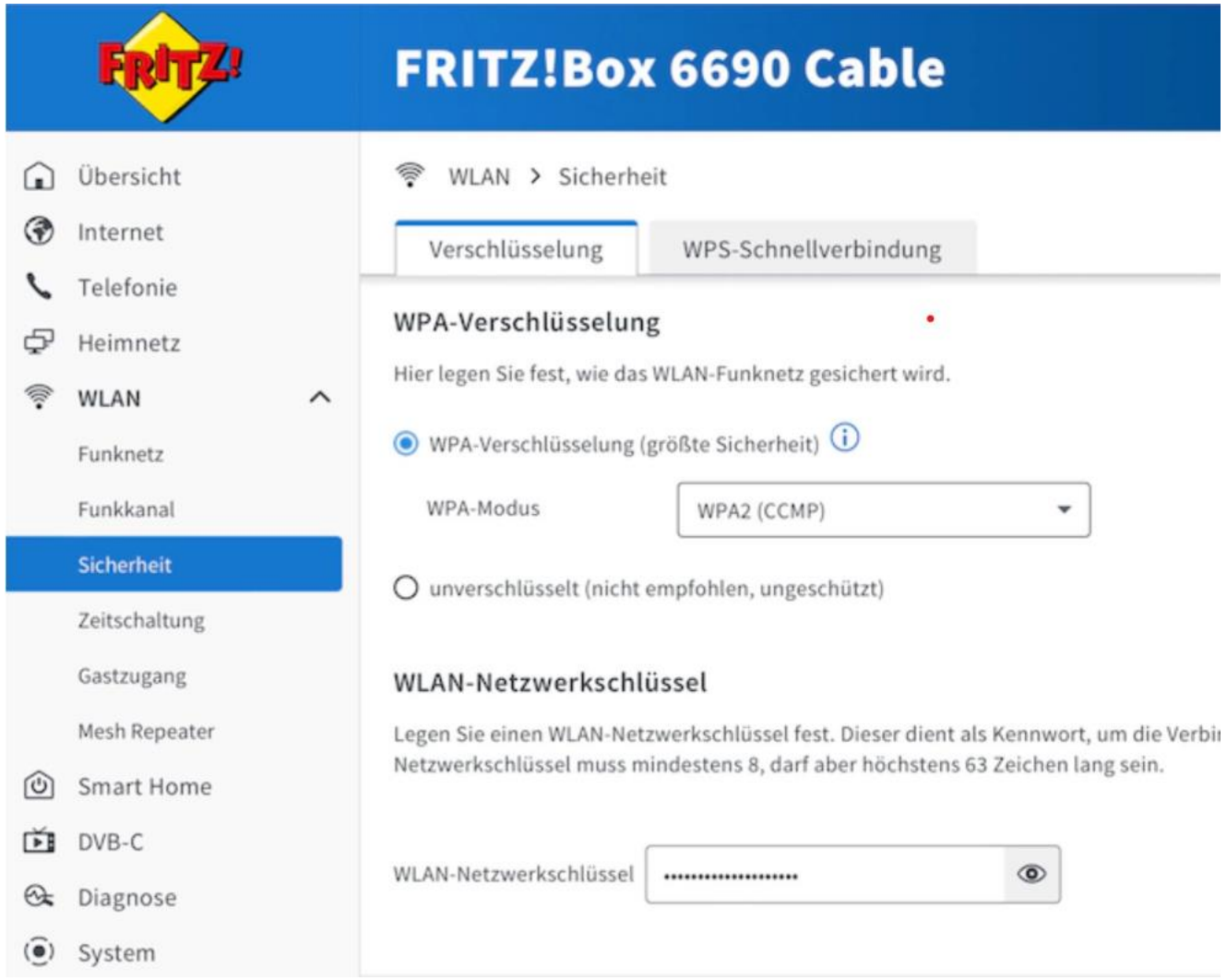
https://www.inside-digital.de/ratgeber/handy-neu-starten

WLAN Sicherheit

Heutzutage hängen in der Regel nur noch sehr leistungshungrige Geräte an störenden Netzwerkkabeln – dank Wireless Local Area Network (WLAN).
Denn ob Notebook, Smartphone oder Fernseher: Der Router bringt mittlerweile nahezu alle Geräte per WLAN ins Internet.
Die Verwendung des kabellosen Netzwerks ist aber mit gewissen Risiken verbunden, denn sobald ein Angreifer oder eine Angreiferin das WLAN geknackt hat, ist der Zugriff auf viele Gerätetypen möglich, die teilweise kein ausreichendes Maß an Schutz besitzen.
Daher sollten Sie Eindringlingen den Zugang erschweren und das drahtlose Heimnetz ausreichend absichern.

Hier erfahren Sie, wie Sie die WLAN-Sicherheit erhöhen und die Tipps bei der weitverbreiteten FritzBox anwenden.

Sicheres Passwort



WLAN-Verschlüsselung

Wenn das WLAN-Verschlüsselungsverfahren nichts taugt, schützt auch das beste Passwort Ihr Netzwerk nicht. Netzwerkgeräte verwenden als Verfahren für gewöhnlich WPA, WPA2 und WPA3. Damit die Verschlüsselung zustande kommt, müssen sowohl Netzwerk- als auch Endgerät dasselbe Verfahren beherrschen. (abwärtskompatibel)

WPA = WI-FI Protected Access (256-Bit-Schlüssel)

WPA2 = WPA incl. AES (Advanced Encryption System)

WPA 3 = WPA incl. PFS (Perfect Forward Secrecy)

Besuchern verschaffen Sie am besten per Gastzugang Zugriff zum Internet, das ist vom regulären Netzwerk getrennt.

Aktuelle Firmware

WPS nur bei Bedarf

Beim WPS-PIN-Verfahren erstellt der Router einen Code, den der User auf dem Endgerät eingeben muss. Liest der Angreifer oder die Angreiferin ihn aus, gelangt er oder sie ins Netzwerk.

Besser ist die WPS-Push-Button-Konfiguration (WPS-PBC): Wie der Name verrät, muss man hier eine physische Taste am Router und am zu verbindenden Gerät drücken. Manchmal verwendet das Endgerät auch eine Software-Taste.

Wenn Sie wirklich sichergehen möchten, dass keine Angreifer über das WPS-Verfahren ins Heimnetz kommen, sollten Sie WPS im Router-Menü ganz ausschalten und es nur für einen kurzen Moment aktivieren, wenn Sie ein neues Gerät per WPS verbinden wollen.

So ändern Sie die WPS-Einstellungen Ihrer FritzBox: Klicken Sie im FritzBox-Menü auf *WLAN*, *Sicherheit* und *WPS-Schnellverbindung*. Hier lässt sich bei *Push-Button-Methode aktiv* der Haken setzen oder entfernen. Bestätigen Sie anschließend mit *Übernehmen*.

Wi-Fi Protected Setup (**WPS**)

WLAN > Sicherheit

Verschlüsselung | WPS-Schnellverbindung

WLAN-Geräte, die das WPS-Verfahren (Wi-Fi Protected Setup) unterstützen, können Sie per Knopfdruck an Ihrer FRITZ!Box mit Ihrem WLAN verbinden.

Schnellverbindung mittels Push-Button-Methode (WPS)

Hier können Sie die Push-Button-Methode (WPS) aktivieren. Dabei werden die Verschlüsselungseinstellungen von der FRITZ!Box sicher zum WLAN-Gerät übertragen und von diesem dauerhaft gespeichert.

☑ Push-Button-Methode aktiv

WLAN-Geräte mittels Push-Button-Methode (WPS-PBC oder DPP)* mit der FRITZ!Box verbinden

1. Informieren Sie sich, wie am WLAN-Gerät die Push-Button-Methode gestartet wird. Abhängig vom WLAN-Gerät erfolgt dies über eine Taste oder über die Benutzeroberfläche des Gerätes.
2. Klicken Sie auf "Push-Button-Methode" starten.
3. Aktivieren Sie innerhalb von 2 Minuten am WLAN-Gerät die Push-Button-Methode (WPS).

Die FRITZ!Box und das WLAN-Gerät verbinden sich nun automatisch miteinander. Dabei werden die Sicherheitseinstellungen der FRITZ!Box automatisch auf das WLAN-Gerät übertragen.

WPS starten

WLAN-Zeitschaltung

Wenn das WLAN nicht eingeschaltet ist, kann es auch niemand angreifen – logisch. Viele Router bieten eine WLAN-Zeitschaltung, mit der sich das Netzwerk zu geplanten Zeiten automatisch abschaltet. Das bietet sich in Zeiträumen an, in denen Sie kein WLAN benötigen, etwa nachts.

So aktivieren Sie die WLAN-Zeitschaltung Ihrer FritzBox: Klicken Sie im FritzBox-Menü auf *WLAN*, *Zeitschaltung* und *Zeitschaltung für das WLAN-Funknetz verwenden*.

Nun lässt sich auswählen, ob sich das WLAN jeden Tag um die gleiche Zeit abschalten soll oder ob Sie einen detaillierten Zeitplan erstellen wollen. Bestätigen Sie anschließend mit *Übernehmen*.

MAC-Adressenfilter

Jedem Gerät ist eine einmalige MAC-Adresse zugeordnet, die sich nicht verändern lässt. Mit einem entsprechenden Filter gewähren Sie Ihren PCs, Handys & Co. den Zugang zum Netzwerk, während Sie alle unbekannten Geräte aussperren. Für geschulte Angreifer ist ein solcher Filter kein großes Hindernis, der Nachbar oder die Nachbarin dürfte sich daran aber die Zähne ausbeißen.

•So aktivieren Sie den MAC-Adressenfilter Ihrer FritzBox:

•Klicken Sie im FritzBox-Menü auf *WLAN*, *Sicherheit, WLAN-Zugang beschränken* und *WLAN-Zugang auf die bekannten WLAN-Geräte beschränken*.

•Die Liste zeigt alle bekannten Geräte an, die Zugang zum Netzwerk haben. Möchten Sie eines der bekannten Geräte aussperren, klicken Sie in der Zeile des Geräts auf das Mülltonnensymbol.

•Per Klick auf *WLAN-Gerät hinzufügen* und Eingabe der MAC-Adresse erlauben Sie einem Gerät den Zugang. Bestätigen Sie anschließend mit *Übernehmen*.

WLAN Sicherheit

- **Passwort und Name des Routers ändern**
- **WLAN-Passwort möglichst komplex halten**
- **Aktuelle Verschlüsselungsstandards nutzen**
- **Die Firewall regelmäßig überprüfen**
- **Den Router mit Updates aktuell halten**
- **Fernzugriff deaktivieren**
- **Ein Gastnetzwerk für Gäste**

https://t3n.de/news/wlan-sicherheit-heimnetzwerk-schuetzen-1625501/

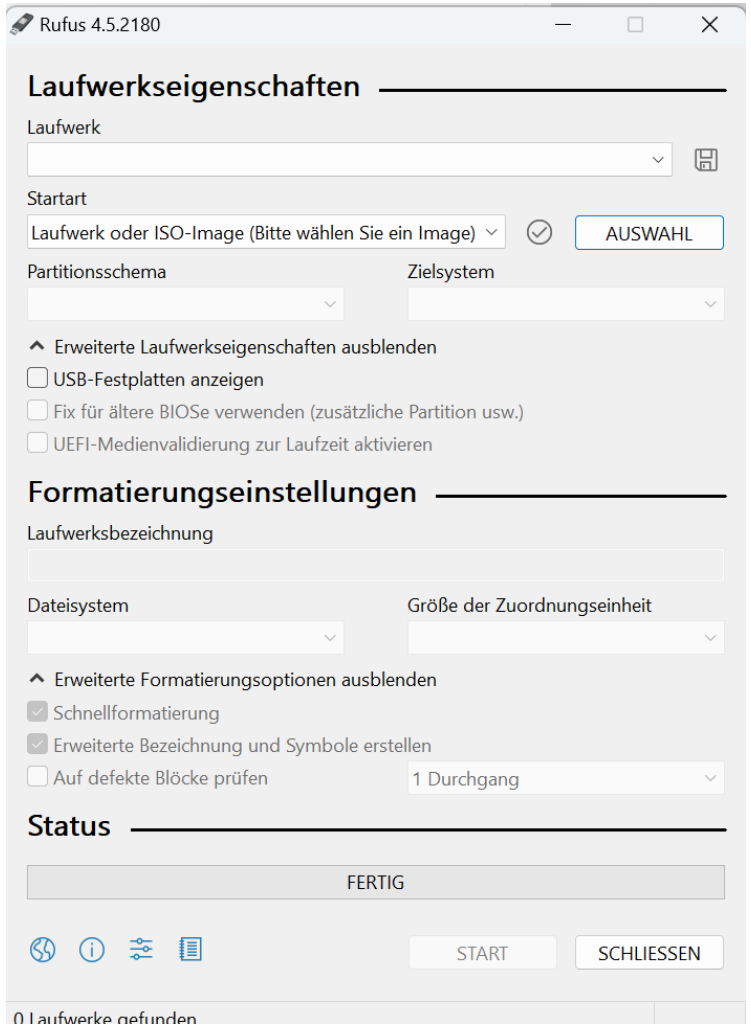
Einfach mal zehn Minuten kein WLAN mehr, und das scheinbar ohne Grund. Manche Router machen das aber völlig absichtlich.

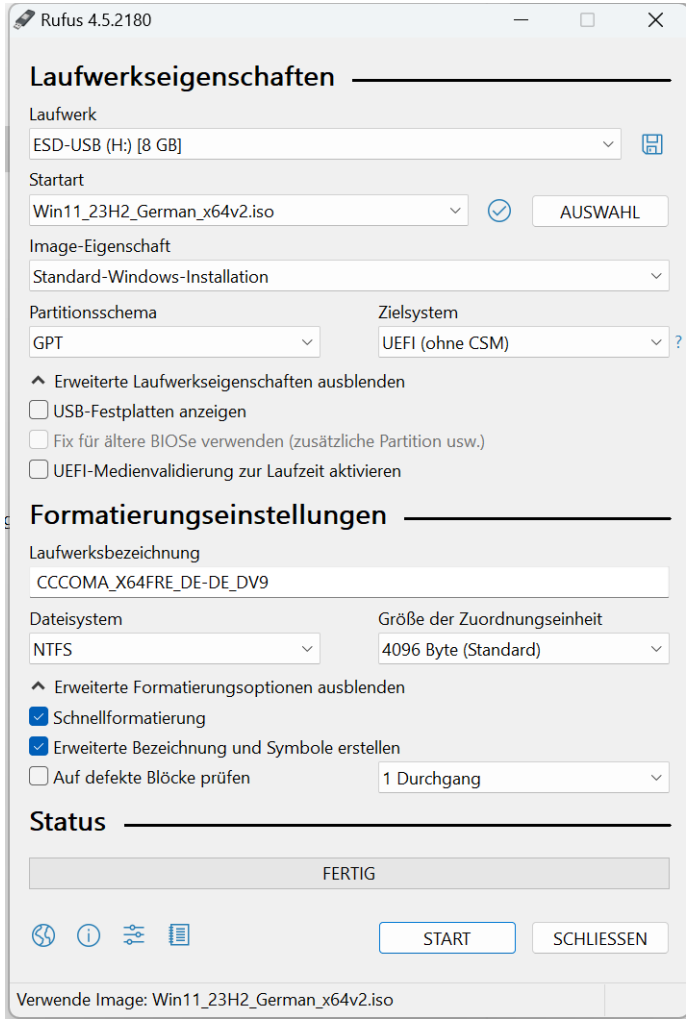
WLANs funken in verschiedenen Frequenzbereichen, gängig sind 2,4 und 5 GHz, in Wi-Fi 6E und Wi-Fi 7 wird sogar ein Bereich um 6 GHz erschlossen. Was die gängigen 5-GHz-Netze betrifft, gibt es aber ein Problem: Viele Radaranlagen, etwa von Flugsicherung, Militär oder Wetterdienst nutzen diese Frequenzen auch und haben Vorrang.
Die FritzBox und auch Router anderer Hersteller dürfen diese bevorrechtigten Nutzer nicht stören. Deshalb prüfen WLAN-Router, ob die entsprechenden Frequenzen frei sind. Bei Doppelbelegungen muss sich die FritzBox zurücknehmen.

Betroffen sind Frequenzen von 5,25 bis 5,35 GHz sowie 5,47 bis 5,725 GHz, was bei WLAN den Kanälen 52 bis 64 und 100 bis 140 entspricht.

https://www.chip.de/news/WLAN-einfach-weg-Darum-kappt-der-Router-absichtlich-die-Verbindung_184451733.html

WIN 11 (Rufus)

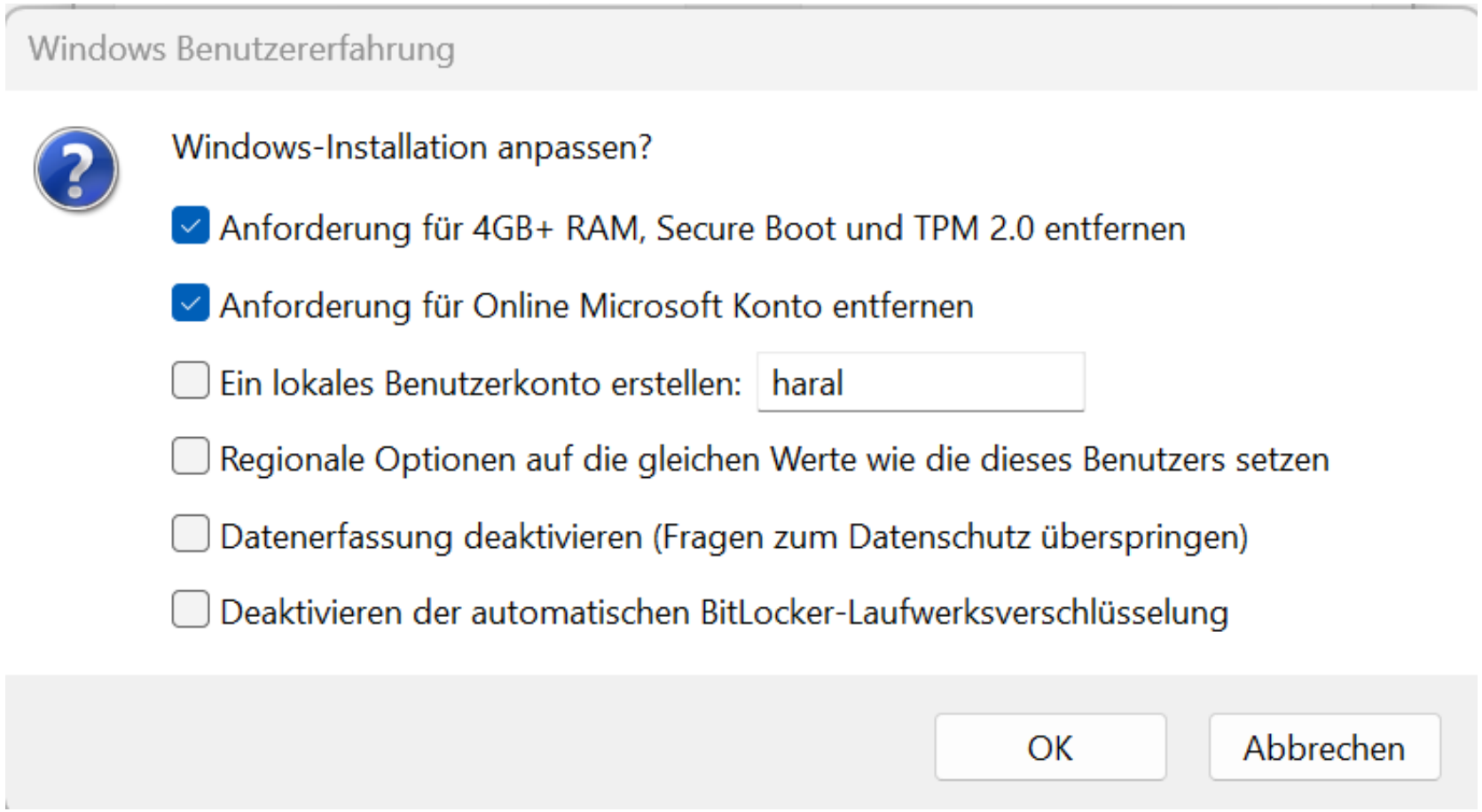




Anmerkung:

Download ISO

WIN 11 (Rufus)


Windows Benutzererfahrung
Windows-Installation anpassen?
Anforderung für 4GB+ RAM, Secure Boot und TPM 2.0 entfernen
Anforderung für Online Microsoft Konto entfernen
Ein lokales Benutzerkonto erstellen:
haral
Regionale Optionen auf die gleichen Werte wie die dieses Benutzers setzen
Datenerfassung deaktivieren (Fragen zum Datenschutz überspringen)
Deaktivieren der automatischen BitLocker-Laufwerksverschlüsselung
OK
Abbrechen

Künstliche Intelligenz

https://www.computerbild.de/artikel/cb-Tipps-Software-Microsoft-Copilot-Windows-11-36084709.html