Stammtisch im März 2026 19.03.2026

Stammtisch im Seniorenbüro und über ZOOM

Übersicht Stammtisch

Schutz an Ihrem PC			
Notruf-Nummern	Termine	Zugänge und Magenta Cloud	

Themenvorschau:
-

Kurz, klar, sicher:

10 Schritte zu mehr Schutz am PC und online

Praktische Schutzmaßnahmen für PC, Netzwerk und E-Mail — sofort umsetzbar.

Senioren für Andere e.V.
Träger des Seniorenbüros Heilbronn

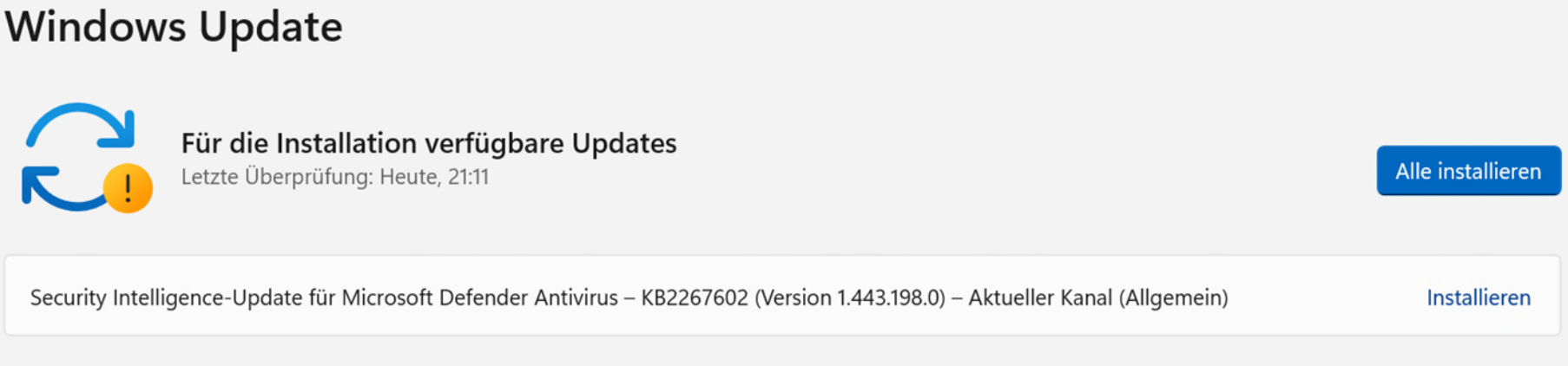
Digital Kompass VOR ORT

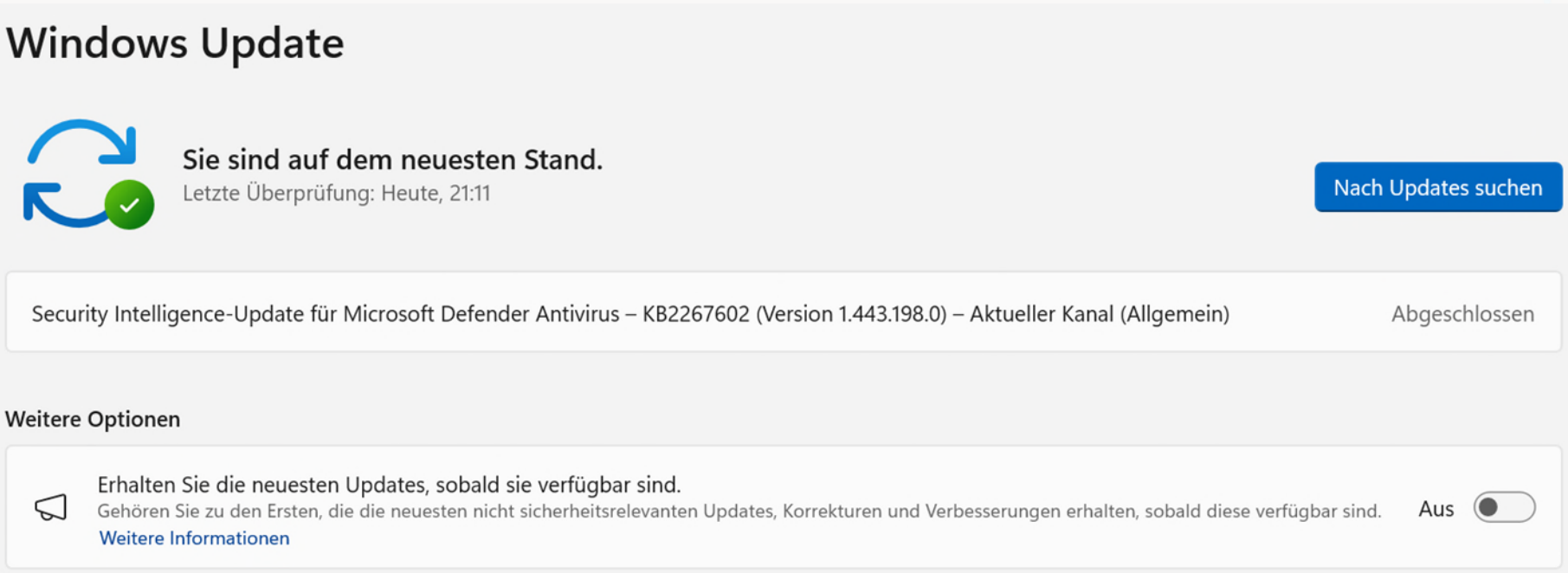
Themenübersicht

1. Windows Update: automatische Updates aktivieren
2. Konto: kein dauerhafter Admin-Account für den Alltag
3. Defender: Echtzeit- & Ransomware-Schutz aktivieren
4. BitLocker: Gerät verschlüsseln; Recovery-Key sicher speichern
5. Backup: 3-2-1-Regel anwenden (wöchentliche Sicherung?)
6. Router: Admin-Passwort ändern, Firmware prüfen, WPS deaktivieren
7. WLAN: WPA2/WPA3 verwenden; Gast-Netz für Besucher
8. Browser: Updates, wenige vertrauenswürdige Erweiterungen, HTTPS prüfen
9. Passwörter: Passwortmanager verwenden + 2FA aktivieren
10. E-Mails: keine Links/Anhänge anklicken ohne Prüfung; Phishing-Muster merken

1. Windows Update: automatische Updates aktivieren

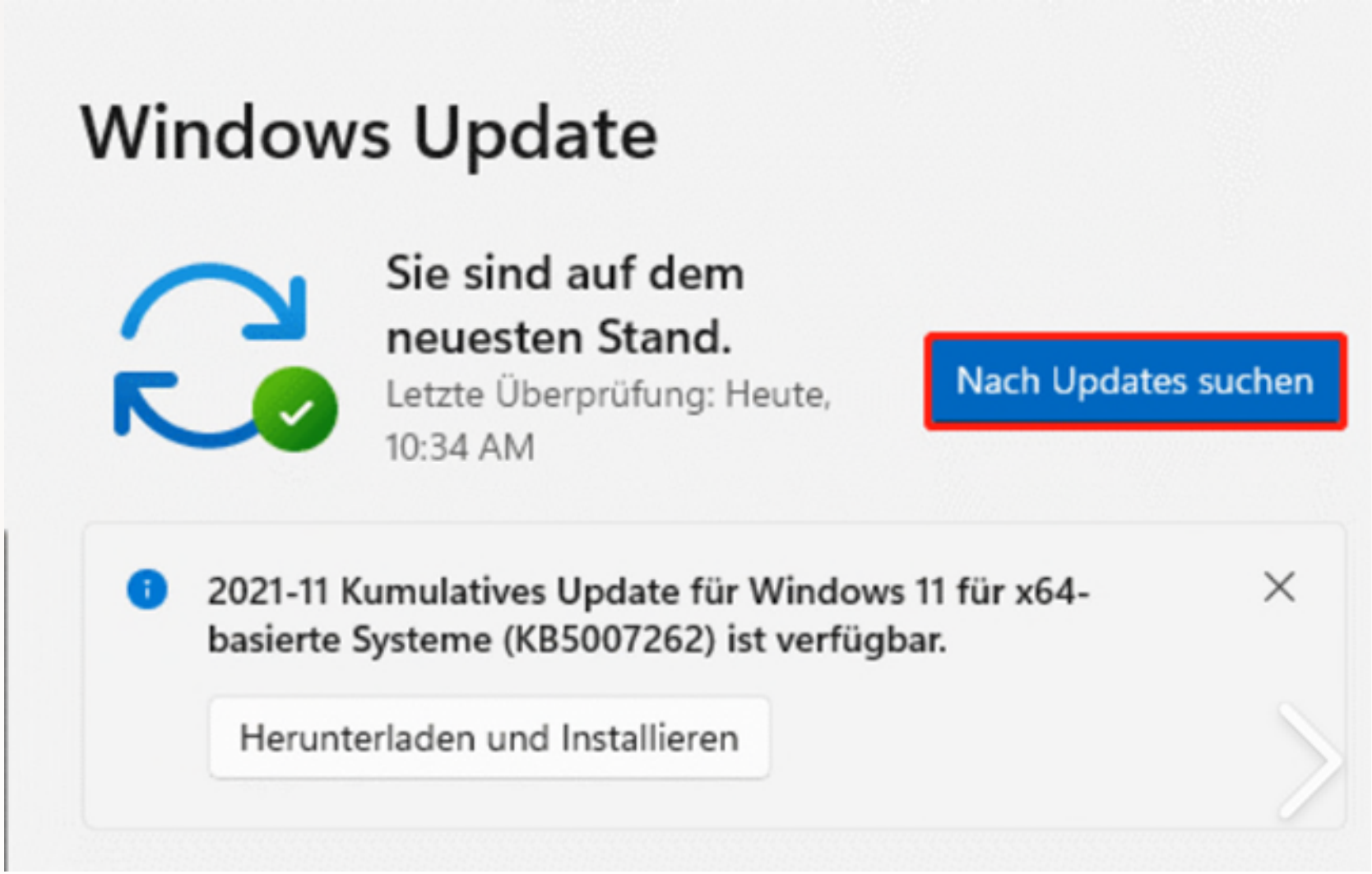
a. Schalte die automatische Installation für Sicherheits- und Qualitätsupdates ein, damit wichtige Korrekturen automatisch aufgespielt werden.
b. Kontrolliere in den Energie- und Update-Einstellungen, dass das Gerät nicht dauerhaft von Updatefenstern ausgeschlossen ist (z. B. durch Energiesparpläne oder aktive Nutzungszeiten).
c. Setze bei Bedarf ruhige Wartungsfenster oder aktive Stunden, in denen ein Neustart erlaubt ist.
d. Plane große Funktions-Updates (Feature-Updates) gezielt für Zeiten mit geringem Arbeitsaufwand.

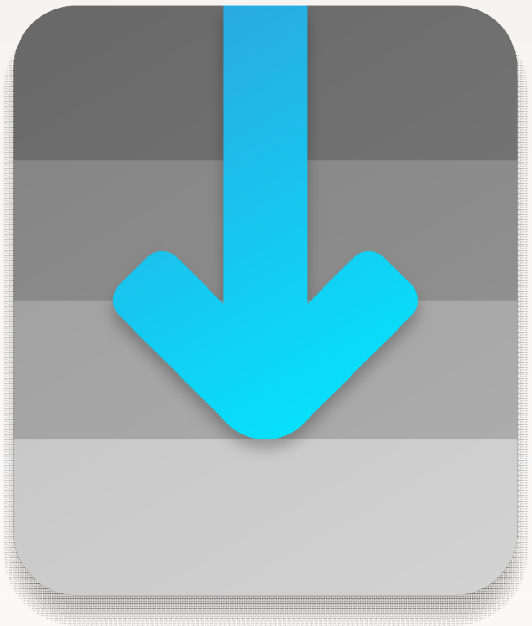




<u>Standardweg</u>
Klicken Sie auf **Start** (Windows-Symbol).
Öffnen Sie **Einstellungen** (Zahnrad).
Wählen Sie **Windows Update**

- bei **Windows 11**: direkt „Windows Update“
- bei **Windows 10**: „Update und Sicherheit“ → „Windows Update“


Windows Update
Sie sind auf dem neuesten Stand.
Letzte Überprüfung: Heute, 10:34 AM
Nach Updates suchen
2021-11 Kumulatives Update für Windows 11 für x64-basierte Systeme (KB5007262) ist verfügbar.
Herunterladen und Installieren



UniGetUI

ist ein Programm für Windows, mit dem man andere Programme **einfach verwalten** kann.

Es zeigt übersichtlich an:

- welche Programme installiert sind
- welche Updates verfügbar sind
- welche neuen Programme man installieren kann

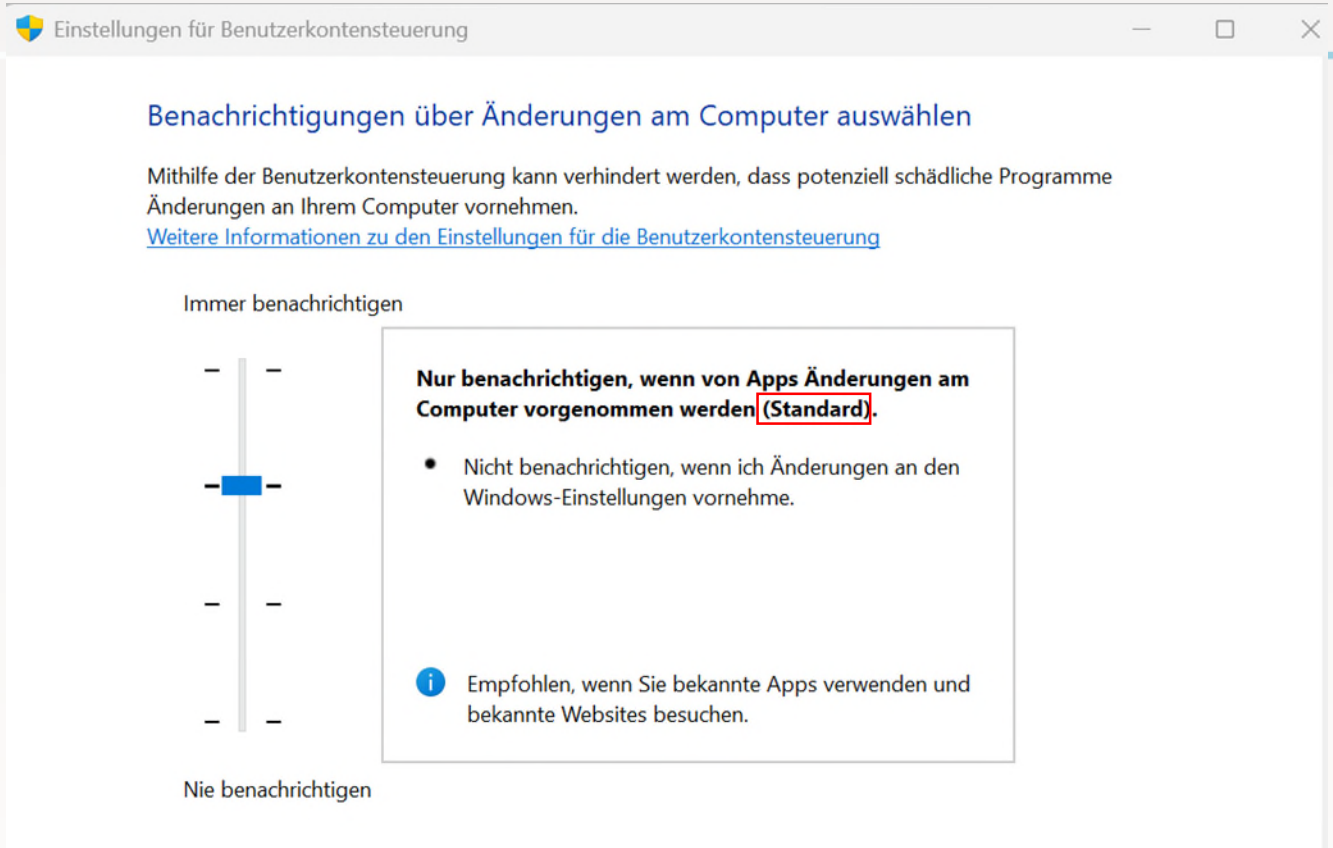
Statt komplizierte Textbefehle einzugeben, klickt man alles bequem mit der Maus. UniGetUI nutzt dabei bekannte Windows-Paketmanager im Hintergrund, macht sie aber **leicht verständlich und benutzerfreundlich**.

2. Konto: kein dauerhafter Admin-Account für den Alltag

1. **Tägliche Arbeit:** Melden Sie sich mit Ihrem Standardkonto an (Surfen, E-Mail, Dokumente).

2. **Wenn Admin-Aufgaben anstehen:** Melden Sie sich kurz mit dem Admin-Konto an **oder** verwenden Sie bei Bedarf die Funktion **„Als Administrator ausführen“** bzw. die Abfrage zur erhöhten Berechtigung (UAC).
   UAC = **User Account Control** = **Benutzerkontensteuerung**.

3. **Admin-Konto sicher halten:** Verwenden Sie ein starkes, einzigartiges Passwort und schalten Sie automatische Anmeldung für dieses Konto aus.



Standardweg

1. Drücken Sie die **Windows-Taste** oder klicken Sie auf **Start**.
2. Tippen Sie **Benutzerkontensteuerung**.
3. Klicken Sie auf **„Einstellungen der Benutzerkontensteuerung ändern“**.

Es öffnet sich ein Fenster mit einem **Schieberegler**. Stellen Sie die gewünschte Benachrichtigungsstufe ein und bestätigen Sie mit **OK** (bei Aufforderung bestätigen Sie als Admin).

Was der Schieberegler bedeutet (in einem Satz):
Ob und wie oft Windows Sie fragt, bevor Programme Änderungen am System durchführen dürfen — von „immer fragen“ (höchste Sicherheit) bis „nie“ (ausgeschaltet, unsicher).

Kurze Sicherheits-Tipps

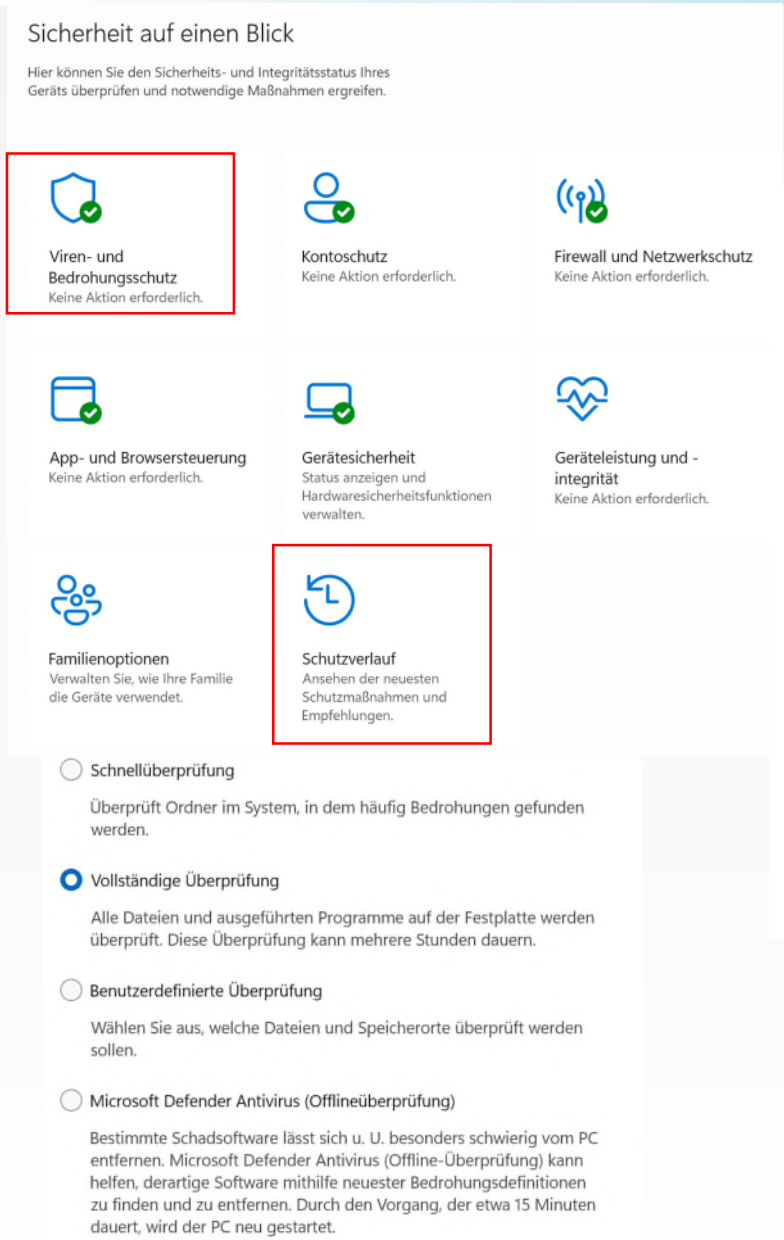
- Geben Sie Admin-Passwörter niemals in unsicheren Dialogen ein.
- Machen Sie wichtige Änderungen nur, wenn Sie sicher sind, warum sie nötig sind.
- Halten Sie das System und die Antivirensoftware aktuell.
- Notieren Sie sich Admin-Zugangsdaten sicher (z. B. Passwortmanager).

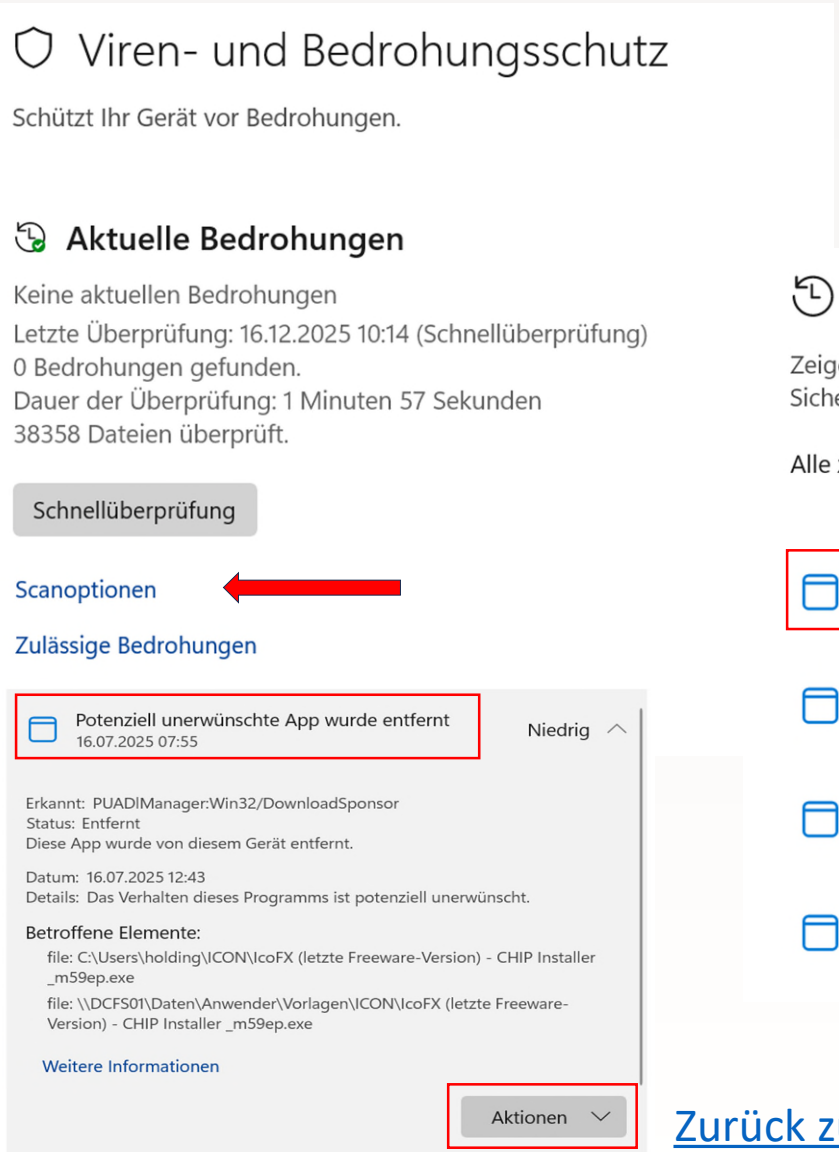
3. Defender: Echtzeit- & Ransomware-Schutz aktivieren

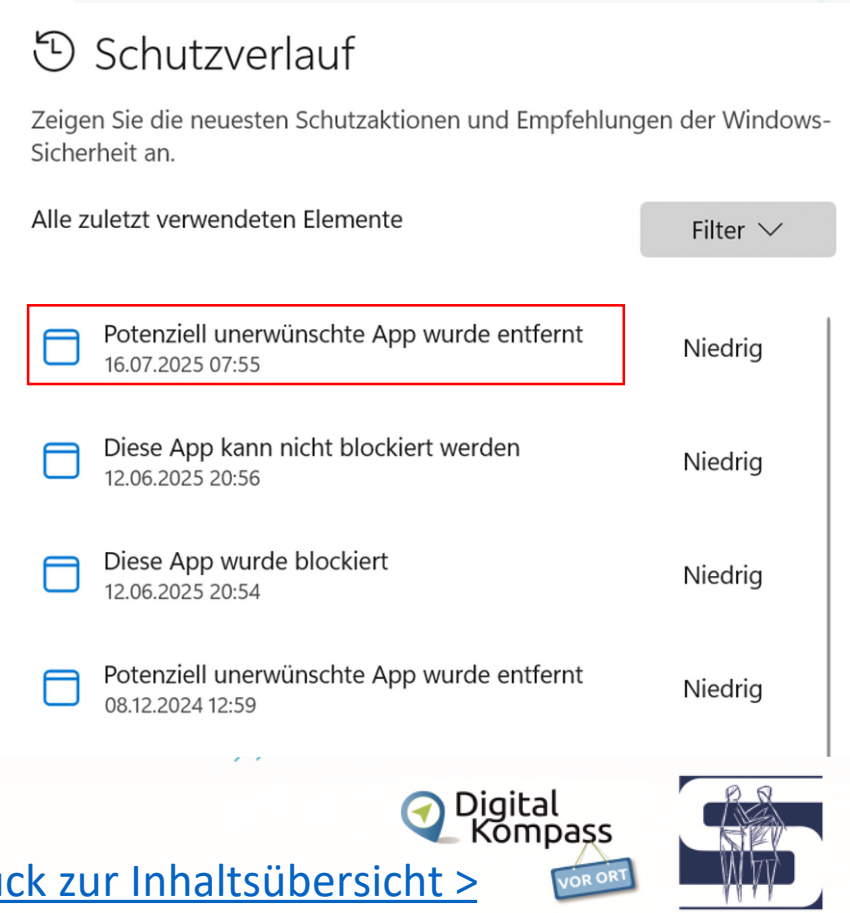
- Windows Defender (oder ein vertrauensbarer AV) sollte Echtzeitscans und autom. Signatur-Updates laufen lassen, damit bekannte Malware früh erkannt wird.
- Aktivieren Sie zusätzlich den Ransomware-Schutz/Controlled Folder Access, um unbefugten Programmen den Zugriff auf wichtige Ordner zu verweigern.
- Prüfen Sie regelmäßig die Quarantäne und führen Sie gelegentliche Vollscans durch.

Praktische Häufigkeiten / Empfohlene Intervalle

- **Echtzeitschutz & Update:** permanent / automatisch
- **Quarantäne prüfen:** wöchentlich
- **Vollständiger Scan:** monatlich (bei hohem Risiko häufiger)
- **Backups:** wöchentlich, monatlich, jährlich, je nach Datenänderungsrate; mindestens einmal im Monat Wiederherstellungstest







Seniorenbüro Heilbronn
Senioren für Andere e.V.
Träger des Seniorenbüros Heilbronn

Zurück zur Inhaltsübersicht >

Digital Kompass VOR ORT

4. BitLocker: verschlüsseln; Recovery-Key sicher speichern

- BitLocker verschlüsselt die Festplatte Ihres Computers. Das bedeutet: Geht das Gerät verloren oder wird gestohlen, kann niemand ohne den Schlüssel auf Ihre Daten zugreifen.
- Aktivieren Sie BitLocker für das Systemlaufwerk und – wenn vorhanden – auch für weitere Datenlaufwerke. Voraussetzung ist in der Regel ein **TPM-Chip**, der den Schlüssel sicher verwahrt.
- Sehr wichtig ist der **Recovery-Key** (Wiederherstellungsschlüssel). Speichern Sie ihn **außerhalb des Geräts**, zum Beispiel auf einem separaten USB-Stick, ausgedruckt oder in einem vertrauenswürdigen Cloud-Speicher. Bewahren Sie ihn nicht nur auf dem verschlüsselten Rechner auf.
- Prüfen Sie vor Reisen oder der Weitergabe des Geräts, ob der Schlüssel tatsächlich auffindbar ist.
- **Ohne Recovery-Key sind die Daten dauerhaft verloren.**

Kurz gesagt:
Sobald ein Gerät den Arbeitsplatz verlässt und/oder sensible Daten enthält, ist Verschlüsselung dringend zu empfehlen, ansonsten bitte keine Verschlüsselung.

5. Backup: 3-2-1-Regel anwenden (montl. Sicherung)

- **3 fach** — Original + 2 Backups.
- **2 Medientypen** — z. B. ext. Festplatte **und** Cloud oder NAS.
- **1 externe Kopie** — an anderem physischem Standort.

- **Automatisieren** — mindestens wöchentlich; zusätzlich regelmäßiges Voll-Image (z. B. halbjährlich).
- **Prüfen & sichern** — Wiederherstellungen testen; Backups verschlüsseln, bei sensiblen Daten

6. Router: Passwort, Firmware, WPS.

- **Admin-Passwort ändern:**
  Ersetze das Standardpasswort durch ein starkes, einmaliges Passwort.
- **Fernzugriff sperren:**
  Deaktiviere Remote-/Cloud-Admin, wenn du es nicht brauchst.
- **Firmware prüfen:**
  Regelmäßig im Router-Menü nach Updates schauen und installieren.
- **WPS deaktivieren:**
  WPS aus — es ist unsicher.
- **Sichere Verwaltung:**
  Admin-Zugang per HTTPS und nur aus dem lokalen Netzwerk erlauben.
- **Sicher aufbewahren:** Passwörter in einem Passwort-Manager speichern.

7. Sicheres WLAN & Gastnetz

WPA2 / WPA3 nutzen
→ Sicher verschlüsseln

Starkes Passwort
→ Mind. 12 Zeichen

SSID/Passwort ändern
→ Bei Verdächt wechseln

Gastnetz einrichten
→ Netz für Gäste trennen

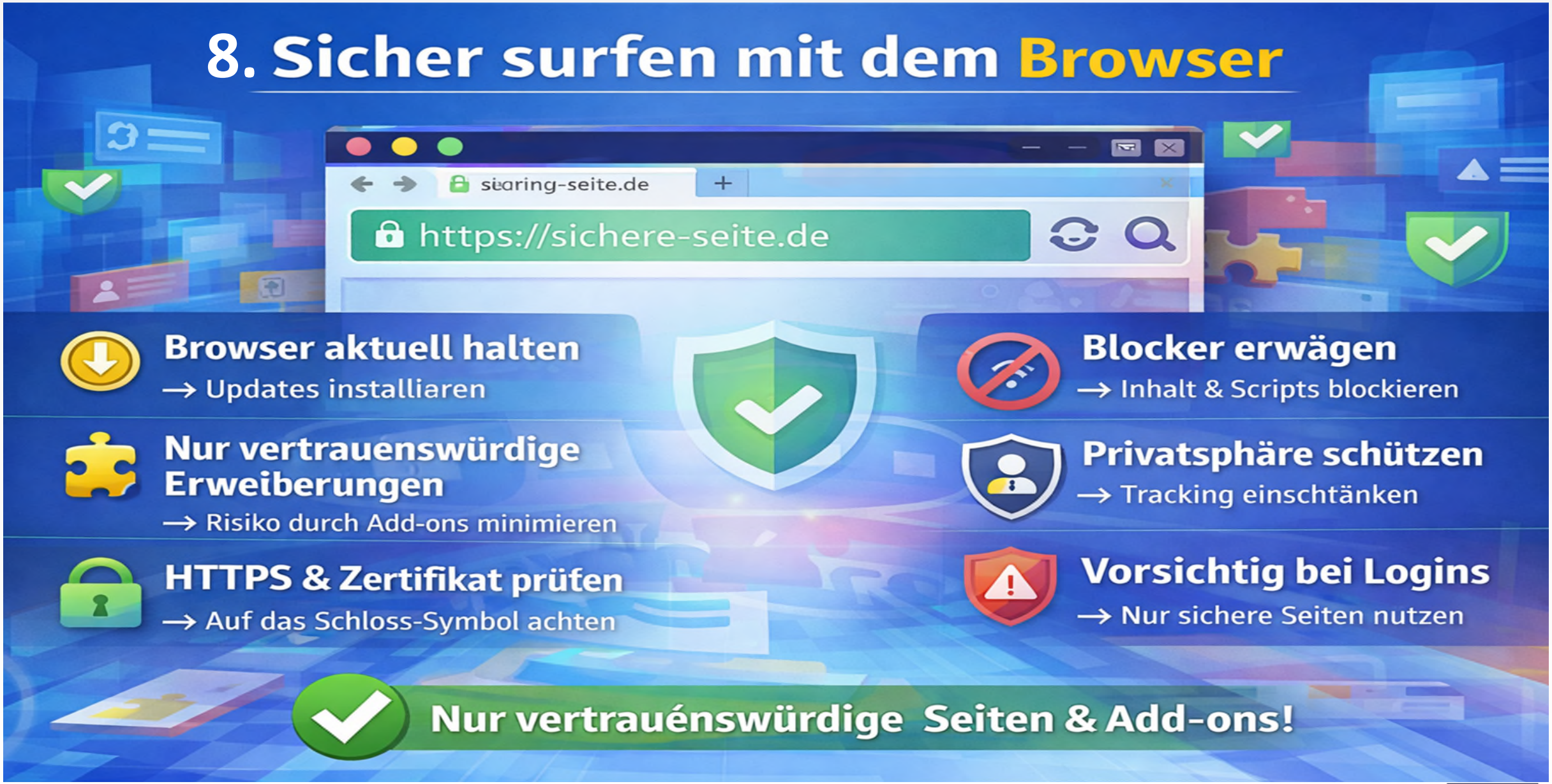
Nur Internetzugang
→ Kein Zugriff aufs Heimnetz

Privates Heimnetz

Gastnetz für Besucher

Privat & Gast getrennt, WLAN sicher!

8. Sicher surfen mit dem Browser



9. Passwörter: Passwortmanager + 2FA aktivieren

- **Passwortmanager benutzen**
  Ein Programm macht und speichert starke, je unterschiedliche Passwörter für jede Seite.
- **Für jedes Konto ein eigenes Passwort**
  Niemals dasselbe Passwort mehrfach verwenden.
- **2FA einschalten**
  Nutze eine Authenticator-App o. einen Hardware-Token.
  SMS nur, wenn nichts anderes geht.
- **Master-Daten sichern**
  Schreibe das Hauptpasswort / die Wiederherstellungs-Phrase auf und bewahre es getrennt und sicher auf (z. B. auf Papier).
- **Bei Diebstahl sofort handeln**
  Passwort ändern und 2FA prüfen, wenn ein Konto ungewöhnlich aussieht.

Kurzcheck: Passwortmanager vorhanden? 2FA aktiv? Master-Daten sicher abgelegt?

9. E-Mails: keine Links/Anhänge anklicken ohne Prüfung; Phishing-Muster merken

- Nicht sofort klicken. Öffne keine Links oder Anhänge ohne Prüfung.

- Absender prüfen. Schau die vollständige E-Mail-Adresse an (nicht nur den Namen).

- Auf Fehler achten. Viele Rechtschreib- oder Grammatikfehler, sowie große Dringlichkeit sind Warnzeichen.
- Links prüfen. Maus darüber halten oder „Link kopieren“ → URL ansehen; bei seltsamen Domains nicht klicken.
- Anhänge nur bei Bedarf öffnen. Nur wenn du sie erwartest; am besten in Vorschau oder sicherer Umgebung (Sandbox).

10. E-Mails: keine Links/Anhänge anklicken ohne Prüfung; Phishing-Muster merken

- Filter nutzen. Spam- und Phishing-Filter im Mail-Programm aktivieren und verdächtige Mails markieren.
- Melden. Betrügerische Mails an den Mail-Provider oder die IT melden.

- Bei Erpressung/Konto-Meldung. Nie Links in der Mail verwenden — die Institution über offizielle Webseite oder Telefon kontaktieren.
- Bei Zweifel handeln. Passwörter ändern und 2FA prüfen, wenn ein Konto betroffen sein könnte.

Themenvorschläge

- **Sicherheit am PC:**
  Aktuelle Bedrohungen wie Viren, Ransomware und Malware
  Praktische Maßnahmen: Firewall, Antivirenprogramme und regelmäßige Systemupdates
  Tipps zur sicheren Nutzung von Passwörtern und Zwei-Faktor-Authentifizierung
- Was bringt mir ein VPN an Sicherheit?
- **Datenschutz im Alltag:**
  Grundlagen des Datenschutzes und warum er wichtig ist
  Sicherer Umgang mit persönlichen Daten im Internet (E-Mail, Social Media, Online-Banking)
  Einstellungen und Tools, um die Privatsphäre zu schützen.
  Sicherheitseinstellungen Google Chrome Browser
- **Betriebssysteme und ihre Besonderheiten:**
  Wichtige Updates und deren Bedeutung für Sicherheit und Stabilität
  Praktische Tipps zur Systemwartung und Datensicherung
  Vergleich verschiedener Betriebssysteme (z. B. Windows, macOS, Linux) im Hinblick auf Benutzerfreundlichkeit und Sicherheitsfeatures

Notrufnummern

Notruf 110

Notruf zur Polizei, ohne Vorwahl. Bei Straftaten, Unfällen ohne Personenschaden, Meldung verdächtiger Beobachtungen

Notruf 112

Notruf zu Feuerwehr und Rettungsdiensten, ohne Vorwahl. Bei lebensbedrohlichen medizinischen Notfällen, Brand, Unwetterschäden.

Notruf 116 117

Kassenärztlicher Bereitschaftsdienst. Bei dringenden, nicht lebensbedrohlichen medizinischen Notfällen, wenn der eigene Arzt nicht erreichbar ist.

Notruf 19 222

Anforderung Krankentransport im Krankenwagen und bei medizinischen Fragen, die kein Notfall sind. Im Hohenlohekreis über Festnetz und Handy mit Vorwahl 07940. In Stadt- und Landkreis Heilbronn ohne Vorwahl, per Handy mit Vorwahl 07131.

Notruf 0761 192 40

Giftnotruf Uniklinik Freiburg (Kinder)

Notruf 089 192 40

Giftnotruf Uniklinik München (Erwachsene)

Notruf 116 116

Sperrnotruf bei gestohlenen oder verlorenen Kredit- und Bankkarten, Online-, Banking, Zugängen und Handykarten.

Telefonseelsorge 0800 111 0 111

Ratsuchenden haben viele Themen, die sie gerne in einem Gespräch äußern möchten, denn Krisen können uns in jeder Lebensphase treffen.

Pflegestützpunkt 07131 64 93 950

Der Pflegestützpunkt ist eine neutrale Beratungsstelle für Menschen, die Informationen aus einer Hand rund um das Thema Pflege benötigen

Selbsthilfebüro 07131 64 93 950

Sozialen mobilen Dienst versorgt Sie zu Hause mit Essen, unterstützen Sie bei der Hausarbeit, erledigen Ihren Einkauf.

Termine im aktuellen Monat

Außerdem finden Sie auf unserer Internetseite
alle Termine und Veranstaltungen des Seniorenbüros.

Zugänge und Magenta-Cloud

Alle Unterlagen unserer Stammtische zu Ihrem persönlichen Gebrauch
finden Sie in unserer Magenta Cloud

PC u. Internet: https://magentacloud.de/s/ct8AjXGHpQe89ES Passwort: tKgPFM6DCL
Smartphone: https://magentacloud.de/s/JzJi4SKdTtpwngn Passwort: wQceWfWFfg

Sie finden die Unterlagen des jeweils letzten Stammtisches auf unsere Internetseite unter:
https://www.senioren-fuer-andere.de/sites/Stammtische.htm

Zugang über Zoom: https://us02web.zoom.us/j/82371658679?pwd=L3gxZFBnMjBodW91RnlaVGFIRzZ1dz09
Meeting-ID: 823 7165 8679; Kenncode: 311 431

Wir freuen uns auf Ihre Teilnahme
Bis dahin – bleiben Sie gesund.
Ihre Senioren-Internet-Helfer