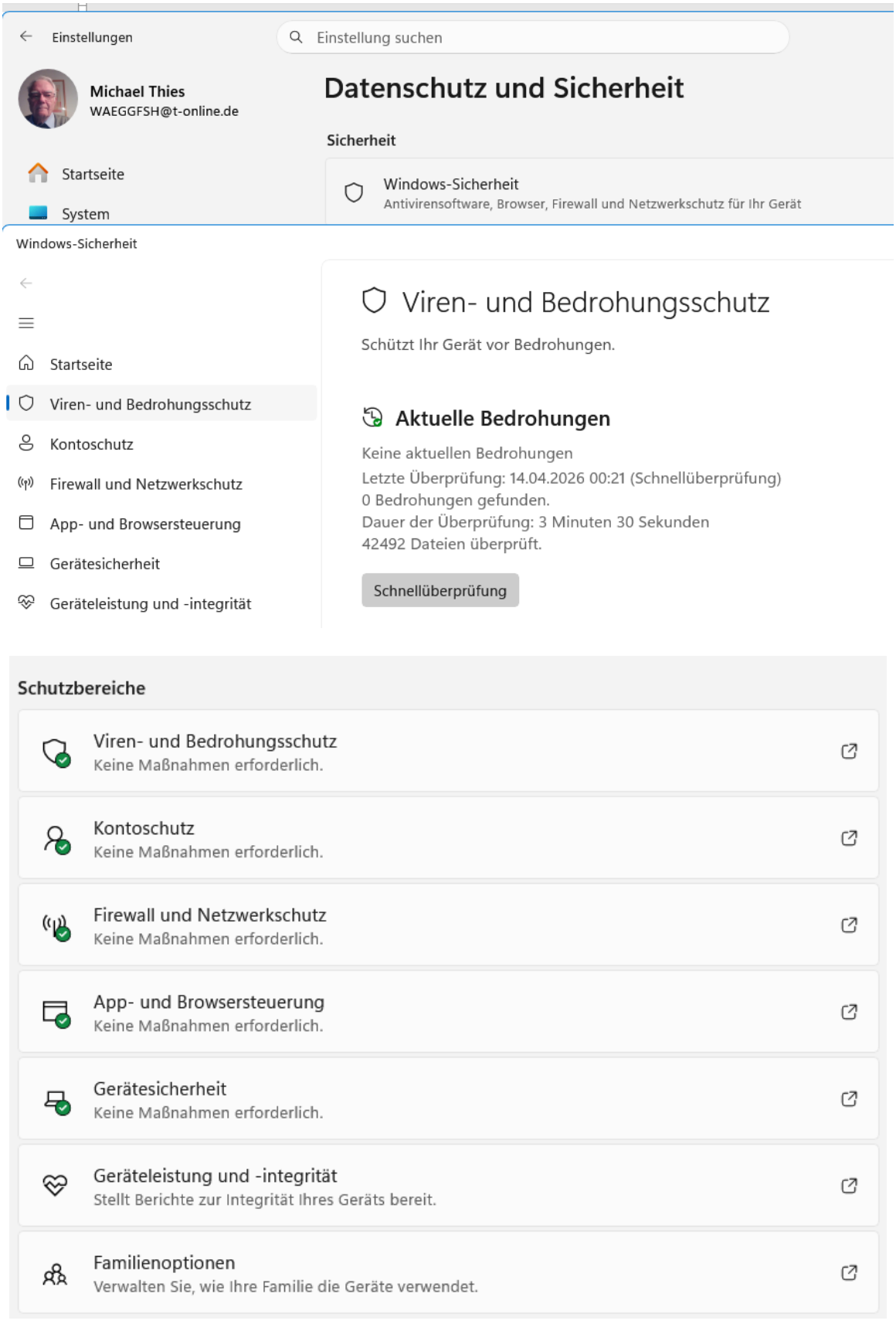
Seniorentreff Grafrath 2026

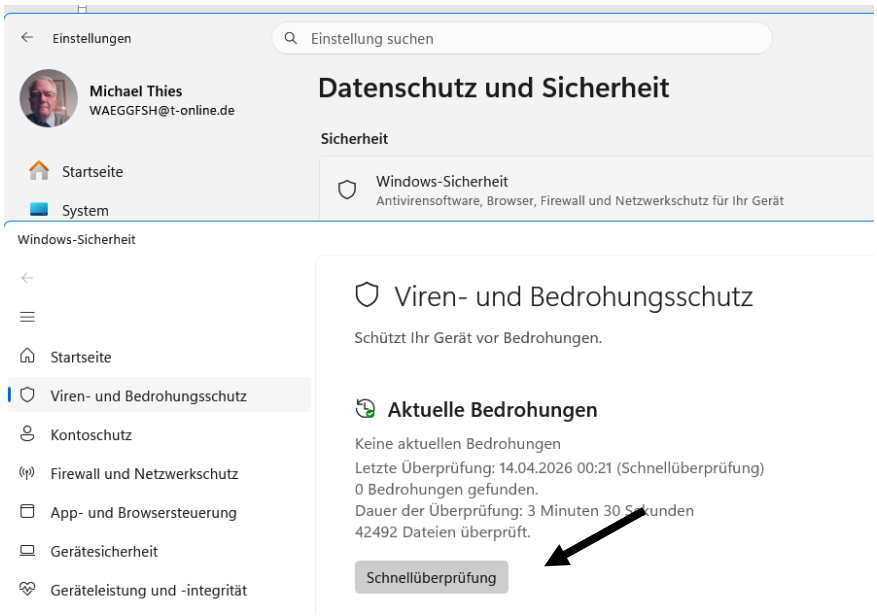


Virenmeldungen in Internet-Browsern

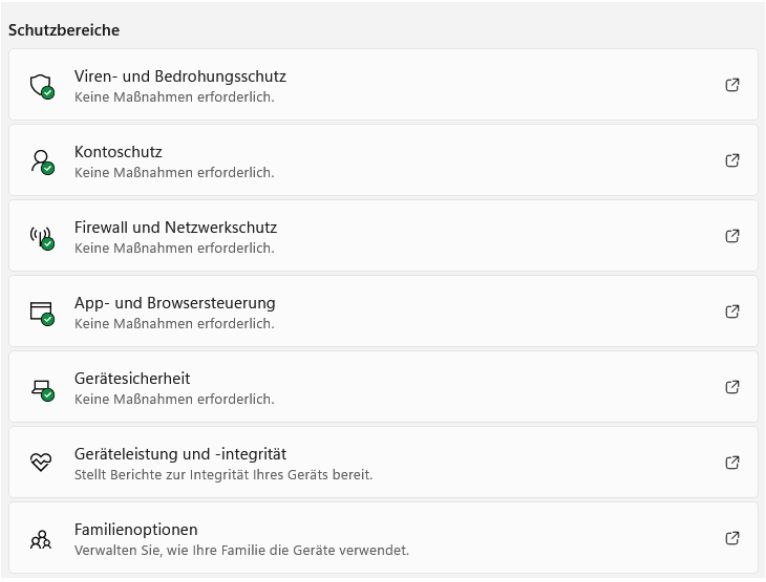
Virenmeldungen z.B. unter Mozilla Firefox können durch verschiedene Faktoren verursacht werden, darunter unseriöse Webseiten, Adware oder Malware. Um diese Meldungen zu beheben, sollten Sie folgende Schritte unternehmen:

Windows 11 führt ein eigenes Antivirenprogramm

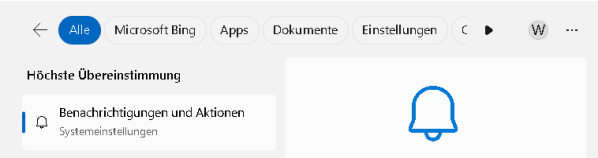
Unter Einstellungen –Datenschutz und Sicherheit – Windows Sicherheit starten Sie das windows-eigene Antivirenprogramm **DEFENDER**. Klicken Sie auf **Schnellüberprüfung**



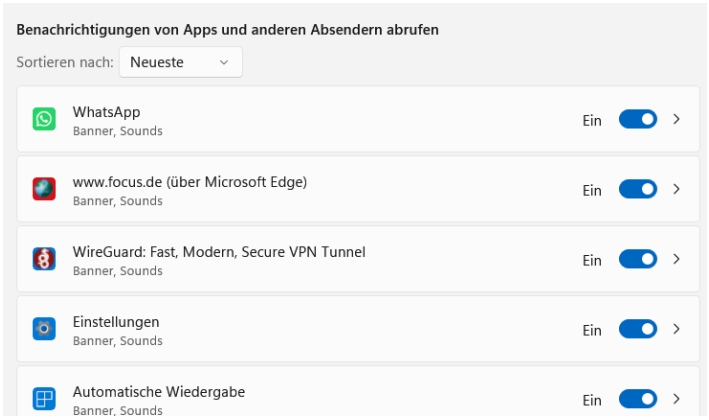
Werden Ihnen nach Abschluss der Virenprüfung keine Unregelmäßigkeiten gemeldet, kann es sich nur um **eine getürkte „Fehlermeldung“** handeln – mit dem Hintergrund, dass Sie sich doch ein passendes aber kostenpflichtiges Virenprogramm herunterladen sollen.



Nachdem feststeht, dass **kein Virenbefall** vorliegt, schreiben Sie in das **SUCHEN**-Feld – links in der Taskleiste -**Benachrichtigungen** ein und öffnen anschließend das Feld Benachrichtigungen und Aktionen.



Im unteren Teil dieser neu geöffneten Seite finden Sie das Feld **Benachrichtigungen von Apps und anderen Absendern**. Hier suchen Sie jetzt das Programm, das Ihnen die getürkten Virenmeldungen anzeigt, heraus und deaktivieren den Eintrag. Das war es, der ganze Schrecken ist verflogen. Deaktivieren Sie aber bitte nicht alle Optionen, da Sie ansonsten keine echten Fehlermeldungen erhalten können



Diese Schritte helfen Ihnen, die Virenmeldungen zu identifizieren und zu entfernen, und sorgen dafür, dass Ihr Browser sicher bleibt.

Eine „Virenmeldung“ kann z.B. wie w.u. angezeigt, aussehen: Achten Sie unbedingt einmal auf grammatikalische und auf Rechtschreibe-Fehler, die Meldungen meist eigen sind. **Kein Schreck!**

Das ist kein Virus – nein, aber Vorsicht. Einfach aussteigen. Vielmehr sollen Sie in Panik die angezeigte Rufnummer anwählen. Man wird dort „versuchen“ Ihnen irgendetwas – angefangen von Antivirenprogrammen – bis hin zu unnötigem Ramsch anzudrehen, viel gefährlicher aber ist die Ausforschung Ihrer Person, Telefon-Nr. eMail-Adresse, Namen ggf. noch Bankverbindung sowie das Ausflöhen Ihres PC nach weiteren interessanten Daten. Die dabei gewonnenen Informationen können anschließend unmittelbar gegen Sie eingesetzt werden. **Also nichts wie weg damit**

Computerviren, Trojaner und Würmer

Viren und Trojaner

Ein **Virus oder Trojaner benötigt immer ein Wirtsprogramm** und verbreitet sich, indem es sich selbst in noch nicht infizierte Dateien kopiert und diese so anpasst, dass das Virus mit ausgeführt wird. Zu den infizierbaren Dateien zählen normale Programmdateien (erkennbar an der Erweiterung .exe, .com), Programmbibliotheken (.dll), Skripte (.vbs), sowie Bootsektoren. Diese beiden Typen wollen vorrangig zerstören bzw. das ordnungsgemäße Arbeiten z.B. von einer Erpressung abhängig machen.

Ist die Dateierweiterung – erkennbar an dem Punkt und den nachfolgenden 3-4 Buchstaben – deaktiviert, können Sie eine Gefahr nicht erkennen. Siehe auch unter Punkt 2 der Programmbeschreibungen. Voraussetzung: Sie haben durch Klick auf eine dieser Dateien, diese aktiviert.

Würmer

Würmer sind in Ihrer Wirkung den Viren sehr ähnlich, **benötigen jedoch keinen "Wirt",** z.B. Makros oder den Bootsektor, für Ihre Verbreitung. Im Gegensatz zu Viren warten Würmer nicht passiv darauf, von einem Anwender auf einem neuen System aufgerufen zu werden, sondern versuchen, **aktiv** (also selbständig) in neue Systeme einzudringen. Sie nutzen dazu Sicherheitsprobleme auf dem Zielsystem aus, wie zum Beispiel: mangelhafte Standardpasswörter, fehlerhafte Software (Adobe Flash-Player war lange ein Zielprogramm). Ein Wurm kann sich dann wie ein Virus in eine andere Programmdatei einfügen, da sie sich selbst kopieren und die Kommunikationsplattformen von verschiedenen Computern nutzen um sich wie vor zu verteilen.

Microsoft verrät, ob Sie für Windows 11 einen zusätzlichen Virenscanner benötigen

Praktisch jeder Windows-Nutzer fragt sich: Brauche ich für Windows 11 neben dem eingebauten Defender noch einen weiteren Virenscanner eines Drittanbieters? Oder reicht der Defender? Oder brauche ich eventuell gar keinen Virenschutz? Jetzt hat Microsoft eher beiläufig verraten, dass man keinen zusätzlichen Virenschutz für Windows 11 benötigt, wenn man den Windows Defender eingeschaltet hat.

Diese Einschätzung fand die US-amerikanische IT-Nachrichtenseite Windowslatest in diesem Microsoft-Dokument. Das Dokument datiert vom 9. April 2026.

Microsoft stellt darin wenig überraschend fest, dass Windows 11 das sicherste Windows aller Zeiten sei (wieder einmal…) und bereits einen vollständigen Virenschutz enthalte, nämlich Windows Defender (mehr dazu lesen Sie in Was ist Microsoft Defender und wie gut schützt er vor Viren und anderen Bedrohungen?), der standardmäßig ausgeführt und automatisch aktualisiert wird.

Microsoft erläutert, warum das unternehmenseigene Antivirenprogramm für die meisten Nutzer ein Antivirenprogramm von Drittanbietern überflüssig machen würde. Zudem erklären die Redmonder, in welchen Fällen ein zusätzlicher Virenschutz doch erforderlich sein könnte.

Diese Windows-11-Nutzer benötigen keinen zusätzlichen Virenschutz

Demnach reiche der Windows Defender als Virenschutz für die meisten Nutzer völlig aus: “Für viele Nutzer von Windows 11 deckt Microsoft Defender Antivirus die alltäglichen Risiken ab, ohne dass zusätzliche Software erforderlich ist. Die Entscheidung,

ein Antivirenprogramm eines Drittanbieters zu installieren, hängt davon ab, wie Sie Ihren PC nutzen und welche Funktionen Ihnen wichtig sind".

Dabei geht Microsoft von einer typischen Konfiguration mit regelmäßigen Updates (insbesondere den Updates des Patch Days), Standard-Sicherheitseinstellungen und üblichen Nutzungsmustern aus, wie beispielsweise Downloads nur von sicheren Quellen. Im Antivirus-Test der PC-WELT schneidet Windows Defender gut ab.

Das spräche gegen einen zusätzlichen Virenschutz

Die Installation eines weiteren Antivirenprogramms führt zu zusätzlichen Hintergrundprozessen, erhöht die RAM- und CPU-Auslastung und kann unter Umständen zu Konflikten mit den integrierten Schutzfunktionen führen. Der gleichzeitige Betrieb mehrerer Echtzeit-Scanner kann zudem zu unvorhersehbaren Verhaltensweisen führen. Im Idealfall sollten Sie sich auf ein einziges Echtzeit-Antivirenprogramm beschränken.

Allerdings kann auch der Windows Defender Sicherheitslücken aufweisen, wie dieser Fall zeigte. Dann kann es sinnvoll sein, zusätzliche Schutzmaßnahmen zu ergreifen.