Anonym und sicher Surfen mit Edge

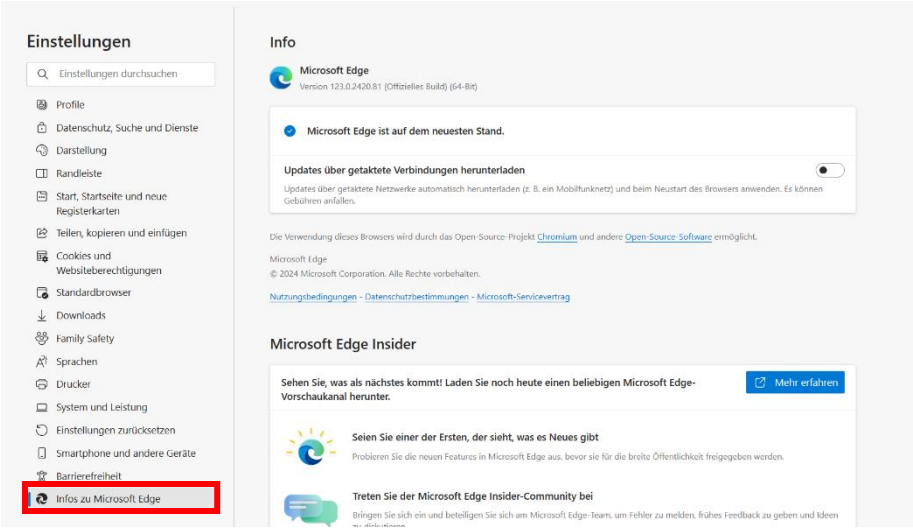
Diese Angaben haben den Stand April/2024 und erheben nicht den Anspruch auf Vollständigkeit!

Es ist wichtig, die Datenschutzeinstellungen in meinem Browser zu kontrollieren und anzupassen, um meine persönlichen Daten und meine Privatsphäre im Internet zu schützen. Durch die Anpassung dieser Einstellungen kann ich bestimmen, welche Informationen über mich gesammelt und geteilt werden, und sicherstellen, dass meine Online-Aktivitäten nicht ungewollt nachverfolgt werden. Aber auch hier muss ich mir im Klaren sein: einen 100 % igen Schutz gibt es nicht!

Es gibt mehrere Funktionen und Schutzmechanismen um Schutz und Anonymität zu gewähren.

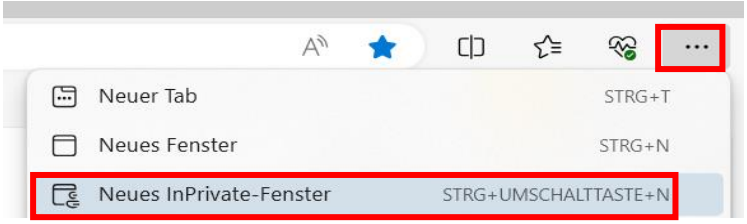
1. Updates aktuell halten

Unter Einstellungen und Info kann man den aktuellen Updatestand herausfinden

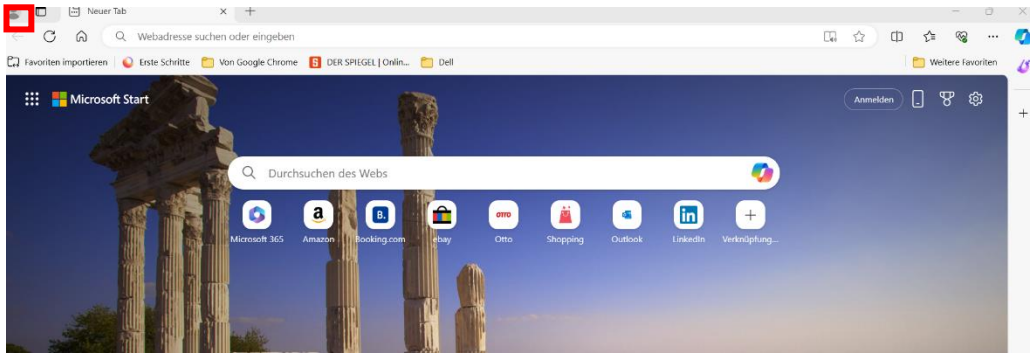


2. InPrivate-Modus

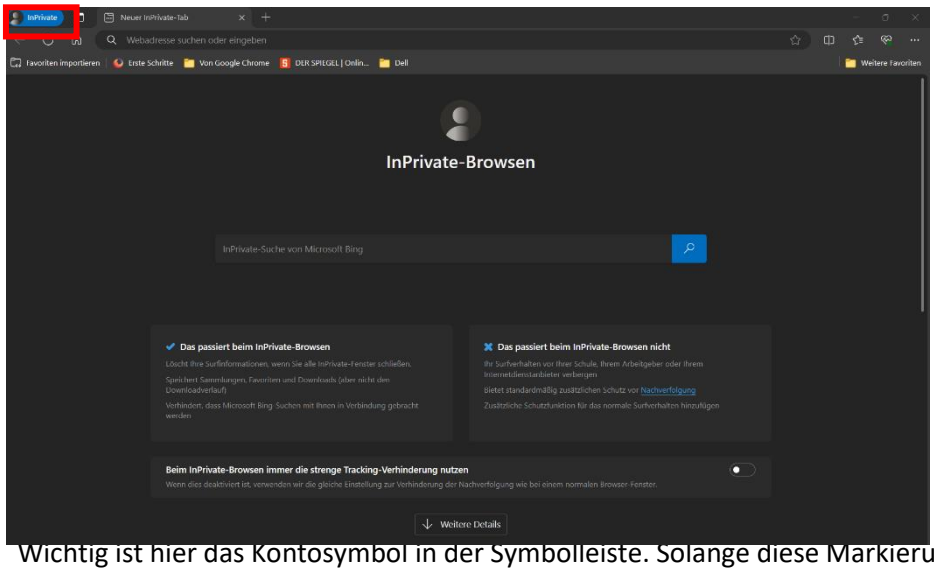
In diesem Modus verzichtet Edge auf das Speichern von Daten, mit denen deine Aktivitäten verfolgt werden könnten. Auch die Cookies werden hier nur für die Surfsitzung aufgehoben und danach wieder gelöscht.
Um den InPrivate-Modus nutzen zu können gehe auf die drei Punkte am rechten Rand deiner Menüleiste.



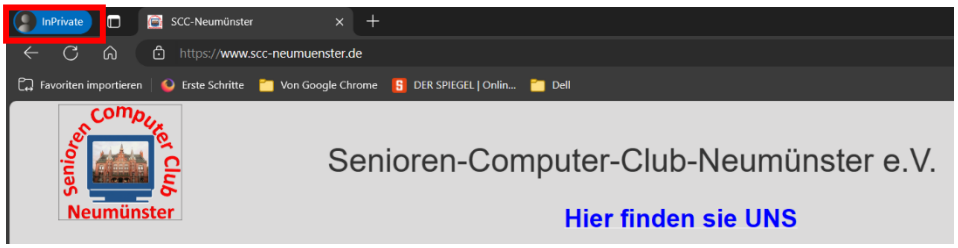
Es öffnet sich ein neues Fenster, das sich von dem normalen Browserfenster deutlich unterscheidet
Normal:



InPrivat-Modus:



Wichtig ist hier das Kontosymbol in der Symbolleiste. Solange diese Markierung sichtbar ist, kannst du dich darauf verlassen, im Datenschutzmodus zu sein.



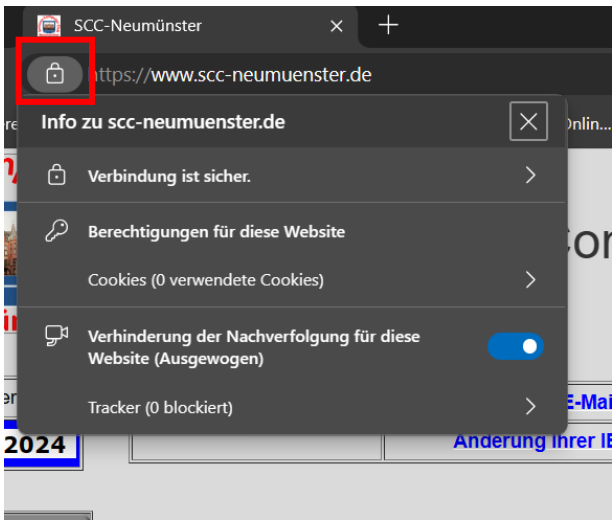
Du kannst wie gewohnt surfen, shoppen usw. Um den InPrivate-Modus zu beenden schließe einfach das Browserfenster.

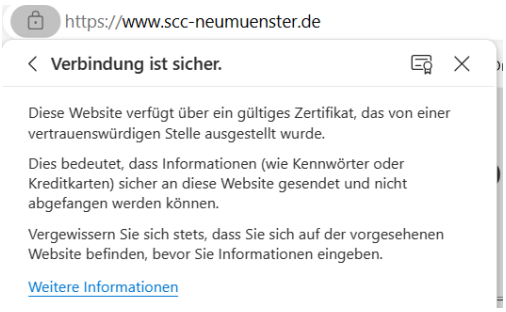
Du kannst den InPrivate-Modus auch nutzen, wenn du zum Beispiel auf einem fremden Rechner surfen möchtest.

3. Tracking

Tracking bezieht sich auf das Verfolgen von Daten über das Verhalten von Personen im Internet, oft durch Cookies oder andere Technologien. Es wird verwendet, um Informationen wie besuchte Websites, Suchanfragen und Klicks zu sammeln, um Profile zu erstellen und personalisierte Werbung oder Inhalte bereitzustellen.

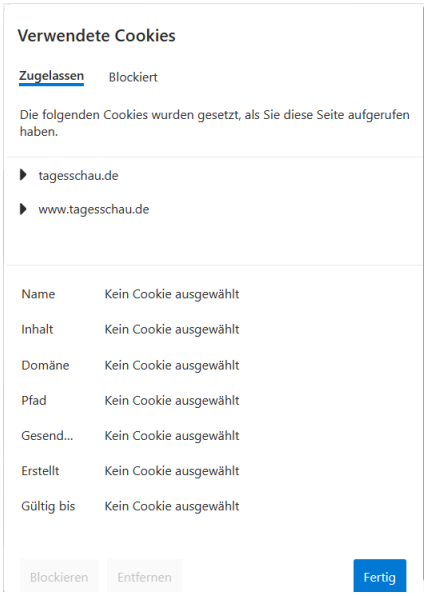
Zu jeder aktuell geöffneten Webseite gibt es Webseiteninformationen die man über das Schlosssymbol aufrufen kann. Ein erstes Indiz für eine sichere Webseite ist das "https"

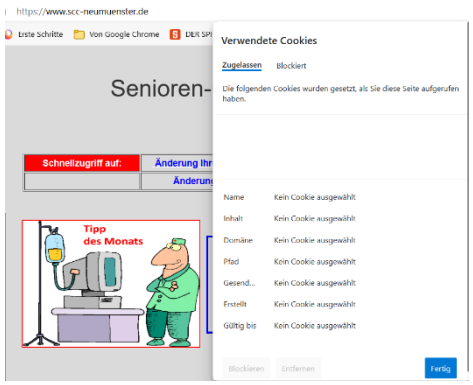




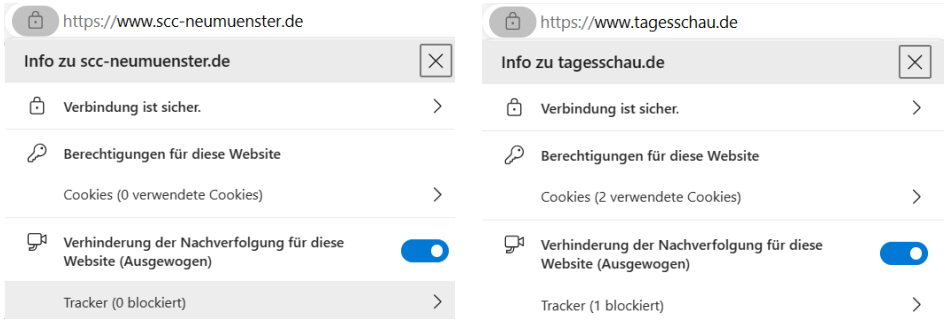
Hier erfährt man einiges über die Webseite:

- Als erstes wird angezeigt, ob die Verbindung sicher ist. Gerade, wenn man vertrauliche Informationen wie Kennwörter oder ähnliches eingeben möchte sollte die Verbindung sicher sein!
- Darunter sieht man Informationen über verwendete Cookies und die Berechtigungen die du für jede Webseite festlegen kannst



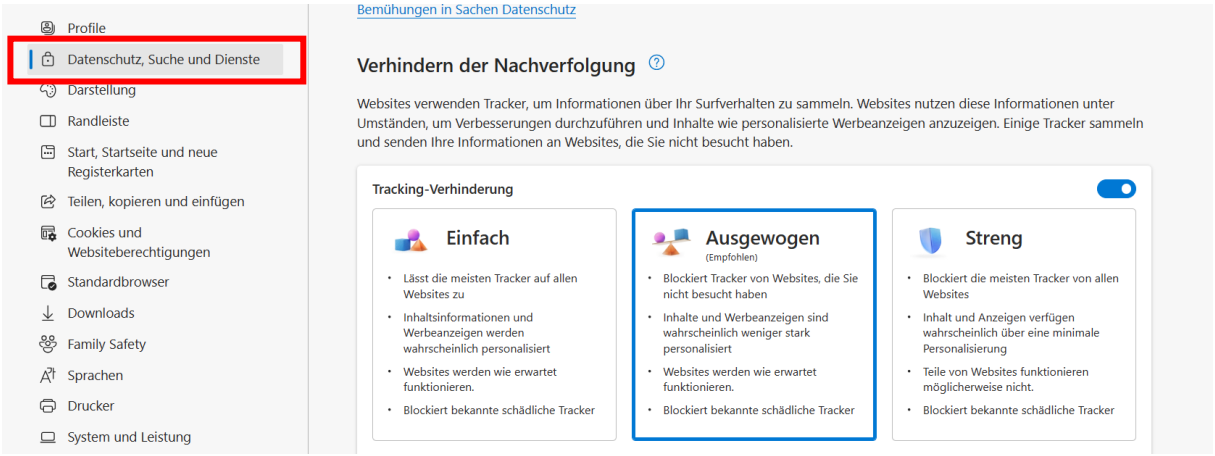


- Danach sieh man die Verhinderung der Nachverfolgung für diese Webseite mit den, auf dieser Webseite vorhandenen Tracking-Elementen



Hier sieht man auf dem rechten Bild, dass ein Tracker blockiert wurde

In den Einstellungen des Browsers kann man seine eigenen Datenschutzeinstellungen auswählen. Dafür rufe die Einstellungen über die drei Punkte im Browser auf und wähle dann links Datenschutz, Suche und Dienste aus

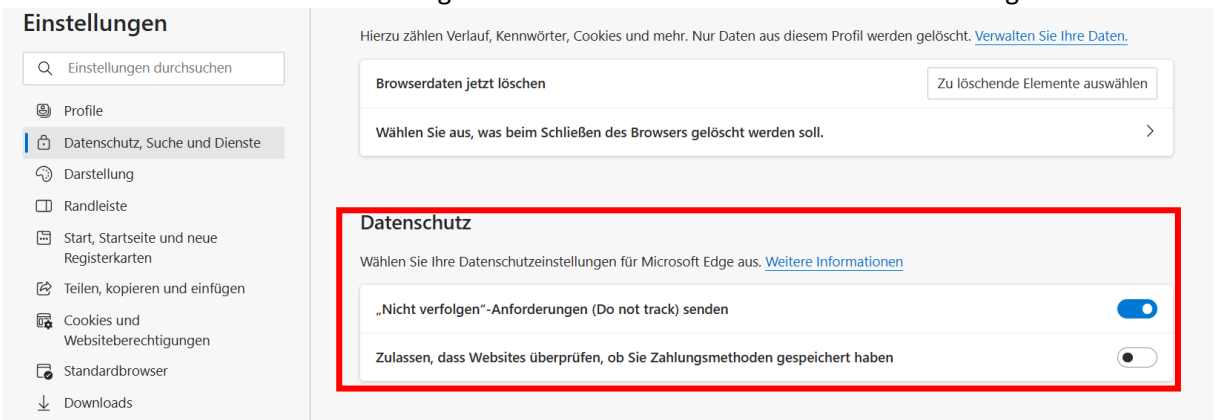


Einfach: blockiert als schädlich bekannte Tracking-Elemente und lässt ansonsten alles zu. Problem mit der Darstellung der Webseiten gibt es hier in der Regel nicht.

Ausgewogen: Empfohlene Standardeinstellung. Guter Basisschutz, weil es schädliche Tracker und Elemente blockiert, die von externen Adressen in Webseiten eingebunden werden.

Streng: Hier wird fast alles blockiert, unter Umständen auch die Darstellung von der Webseite selbst

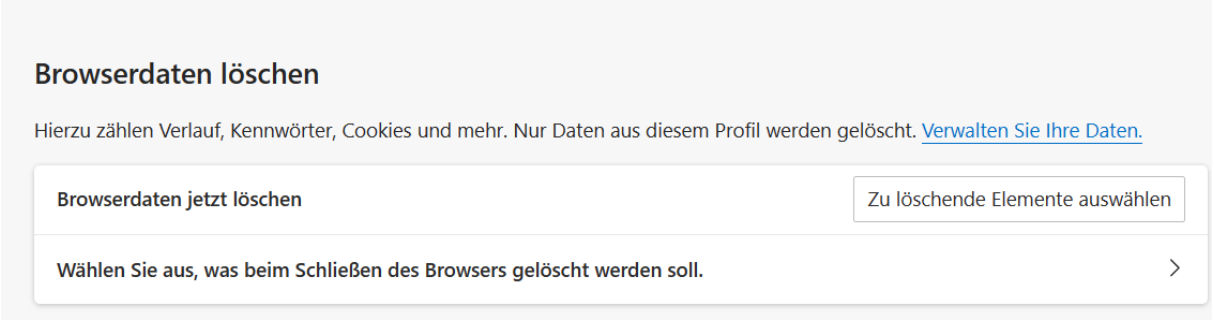
Etwas weiter unten in den Einstellungen findet sich auch die Do-not-Track Einstellung

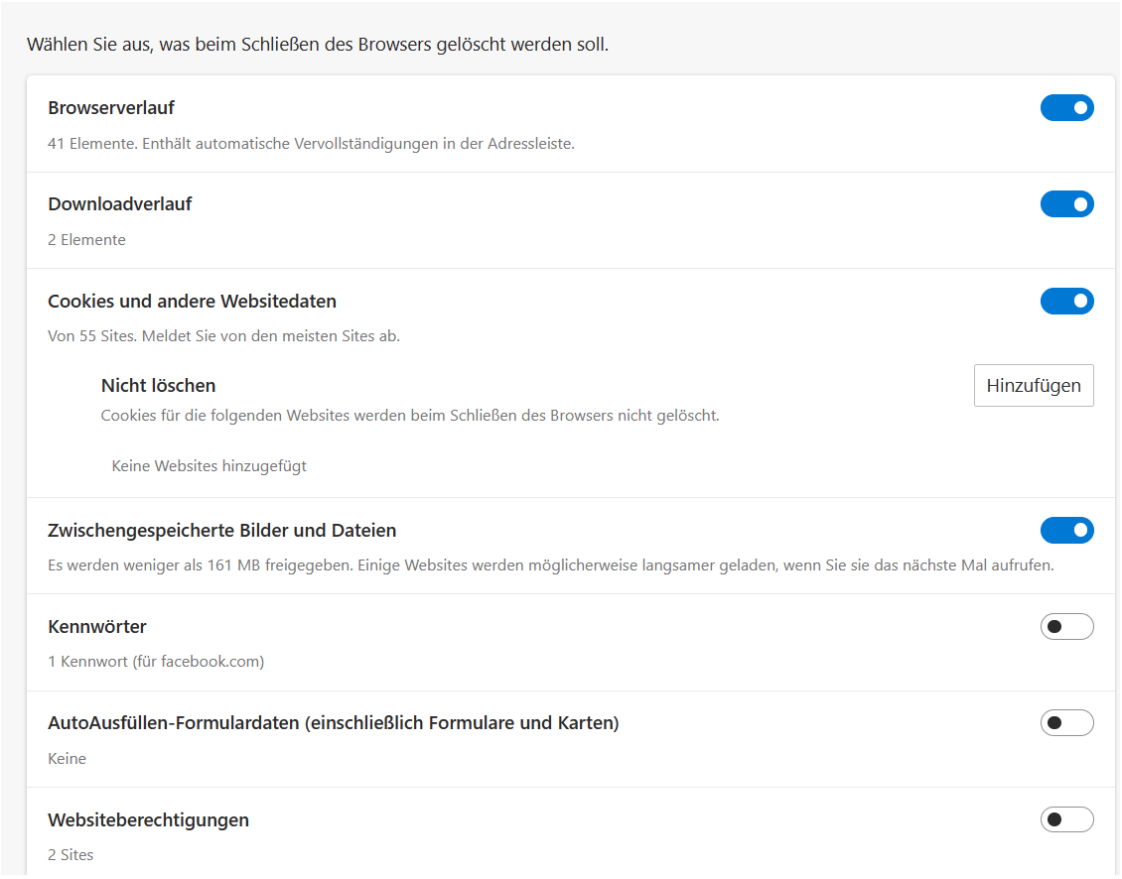


Eine gängige Annahme ist es, die „Do Not Track“-Option bei Browsern schützt vor übermäßiger Datensammlung durch die Webseiten.
Dies ist leider ein Irrtum, denn diese Option signalisiert lediglich den Wunsch des Anwenders nach Anonymität bei der Webseitennutzung.

4. **Weitere in dem Datenschutz dienende Einstellungen wären hier gleich auch noch folgendes:**

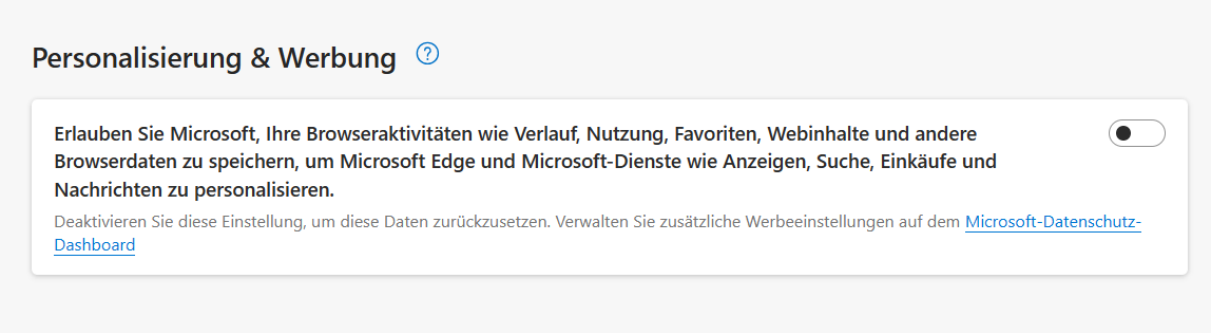
   Browserdaten löschen: man kann die Browserdaten zwischendurch mal löschen oder gleich angeben, welche Daten gelöscht werden sollen, wenn der Browser geschlossen wird.





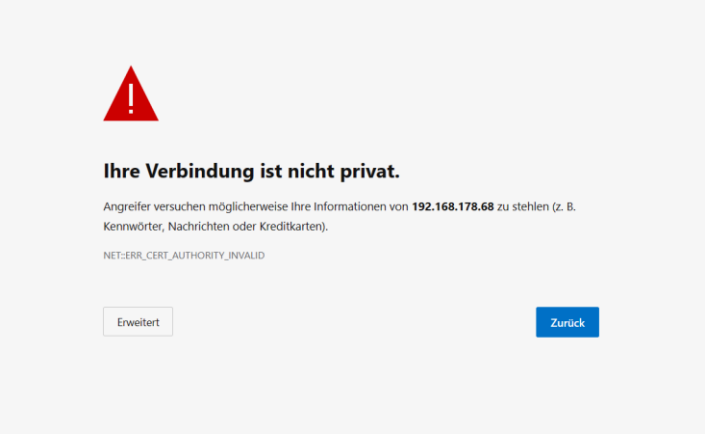
Hier werden wirklich nur die Daten im Browser-Speicherbereich gelöscht. Alle anderen Daten bleiben erhalten! Beim Internet-Provider, auf Proxy- Systemen oder Web-Gateways, auf den Ziel-Webseiten – nur die lokalen Daten auf dem eigenen System werden gelöscht. Diese Funktion erschwert neugierigen Dritten die Infoformationsgewinnung durch die Browserdaten.

Euch die Einstellung für die Personalisierung &Werbung kann ausgeschaltet werden

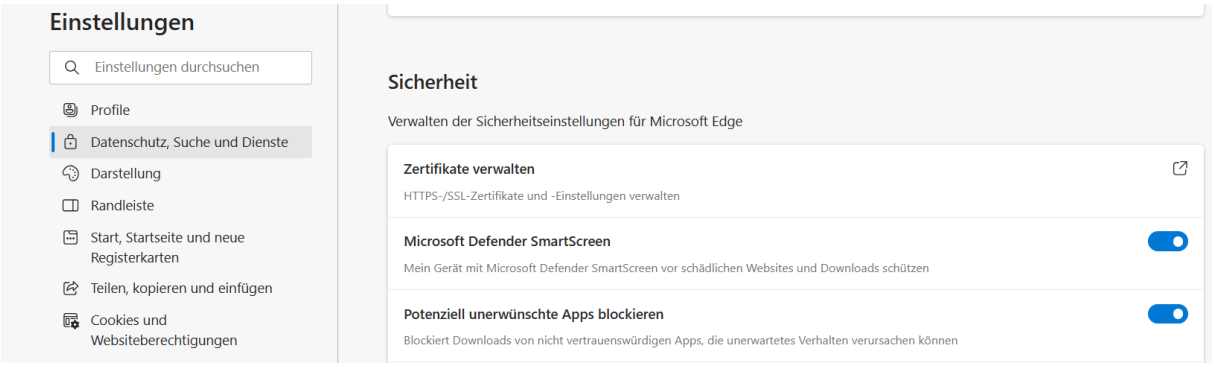


5. Der SmartScreen-Filter

Der SmartScreen-Filter ist eine Sicherheitsfunktion, die von Microsoft entwickelt wurde und in Microsoft Edge integriert ist. Es dient dazu, Benutzer vor schädlichen Websites, Downloads und Phishing-Angriffen zu schützen, indem es verdächtige Inhalte erkennt und blockiert. Der Filter analysiert Websites und Downloads in Echtzeit und warnt den Benutzer, wenn er auf potenziell gefährliche Inhalte stößt.
Das führt dazu, dass, wenn ein Link angeklickt oder eine Webseite geöffnet wird die Adresse mit einer internen Liste abgeglichen wird. Sollte die Adresse vermerkt sein, verweigert Edge den Zugriff auf die Seite.

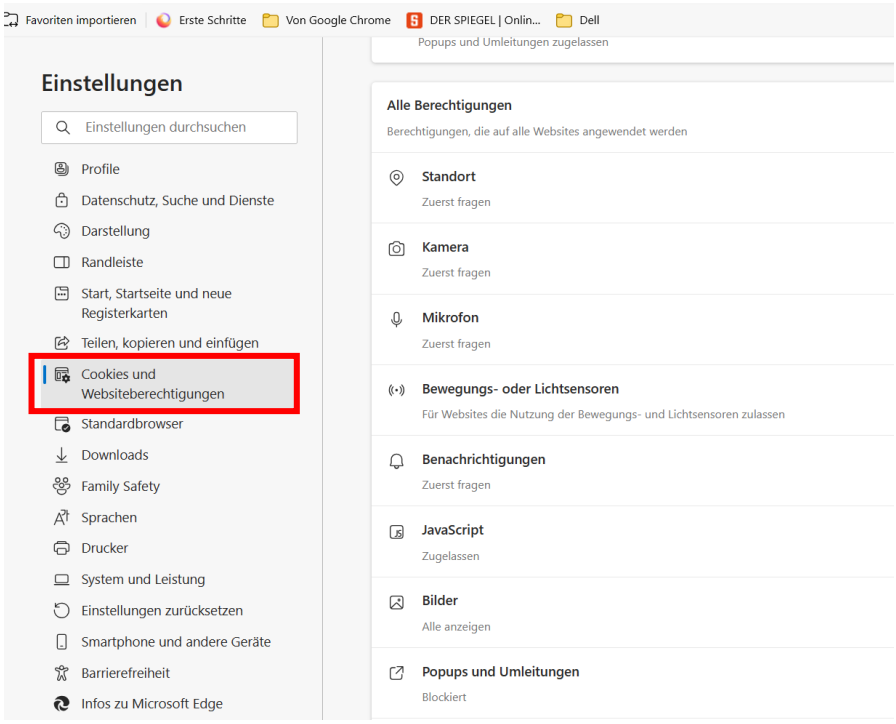


Du kannst aber trotzdem noch entscheiden (über Erweitert) ob du das Risiko eingehen möchtest oder nicht.
SmartScreen deaktivieren:
da der SmartScreen-Filter standardmäßig aktiv ist hat man die Möglichkeit ihn zu deaktivieren. Dazu geht man ebenfalls wieder in die Einstellungen des Browsers unter Datenschutz, Suche und Dienste. Im Abschnitt Sicherheit findest du den SmartScreen-Filter. Es ist allerdings davon abzuraten den Filter zu deaktivieren!

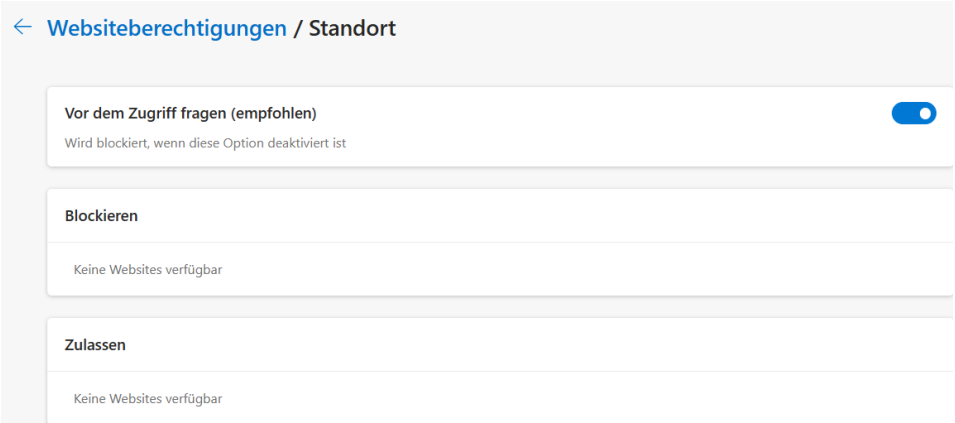


6. Benachrichtigungen von Webseiten einstellen

Pop-up-Fenster sind kleine Browserfenster, die plötzlich auftauchen, meistens beim Besuch einer Website. Sie enthalten oft Werbung, Benachrichtigungen oder andere Inhalte. Pop-ups können störend sein, aber sie werden auch für legitime Zwecke verwendet, z. B. um Benutzer über wichtige Informationen zu informieren oder um Anmeldeformulare anzuzeigen.
Auch hier hat man wieder die Möglichkeit dies zu unterbinden. In den Einstellungen des Browser unter Cookies und Websiteberechtigungen:



Hier kann die einzelne Berechtigung aufgerufen und eingestellt werden



Hier besteht auch die Möglichkeit ausgewählte Webseiten doch zuzulassen!

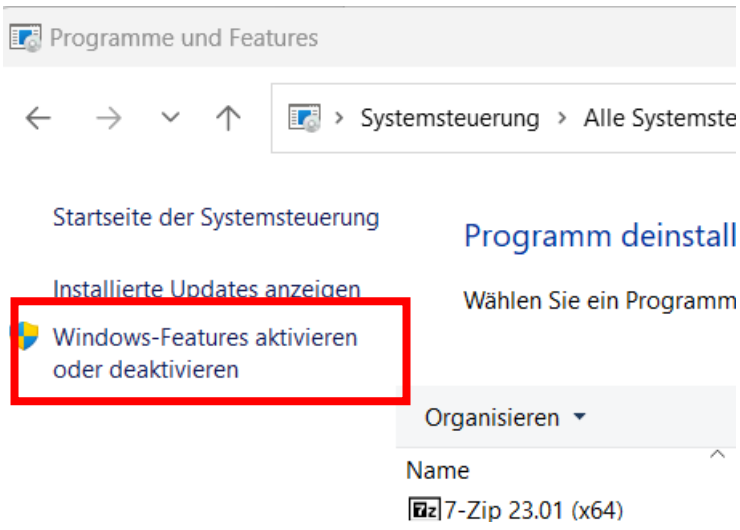
7. Application Guard

Der Application Guard von Microsoft ist eine Sicherheitsfunktion, die in Microsoft Edge integriert ist. Sie isoliert den Browser in einer virtuellen Umgebung, um das System vor schädlichen Websites und Dateien zu schützen. Wenn ein Benutzer auf potenziell gefährliche Inhalte stößt, werden diese in einer isolierten Umgebung geöffnet, um das Hauptsystem zu schützen. Dies hilft, das Risiko von Malware-Infektionen und anderen Sicherheitsbedrohungen zu reduzieren.

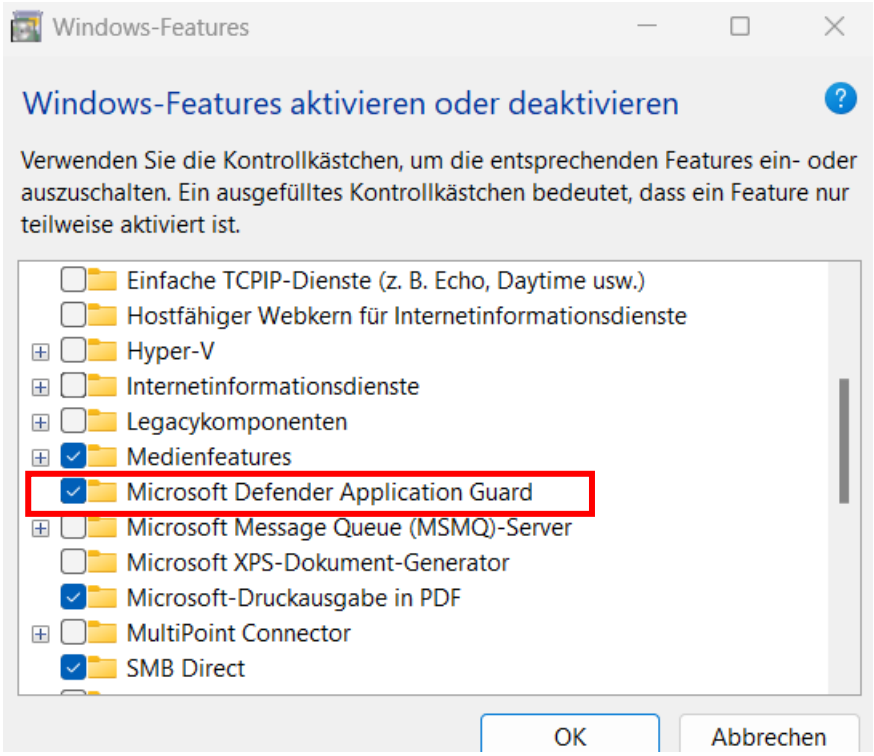
Application Guard aktivieren

Der Application Guard ist im Lieferumfang von Windows integriert, aber standardmäßig deaktiviert!

1. Öffne die Systemsteuerung und die Rubrik Programme und Features
2. Wähle links "Windows-Features aktivieren"



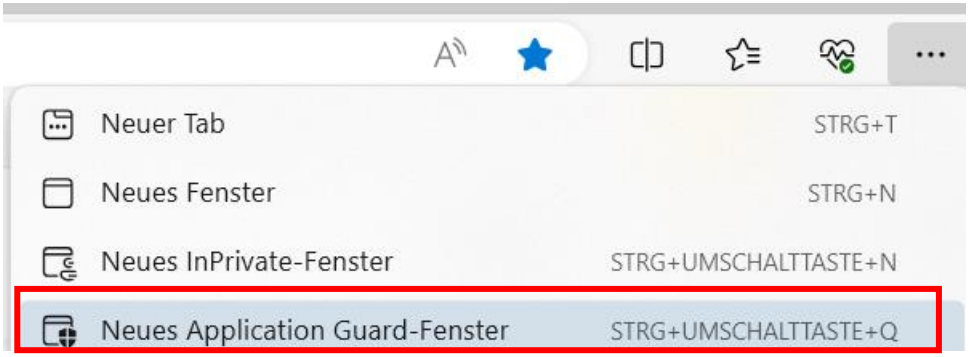
3. Suche in dem geöffneten Fenster Microsoft Defender Application Guard und setze dort ein Häkchen



4. Starte den PC neu, damit die Einstellungen übernommen werden.

Application Guard beginnen

Es gibt jetzt einen neuen Eintrag im Menü namens "Neues Application Guard-Fenster"



Der erste Start kann einige Sekunden dauern!

Das Fenster unterscheidet sich vom normalen Browserfenster kaum. In der Statusleiste findet man ein zusätzliches Symbol, das anzeigt das im geschützten Bereich gesurft wird