Sicherheit im Internet
(Windows Betriebssystem)

Updates: Betriebssystem schützen (Win 10, Win 11)

Virenscanner (Windows Defender)

Browser

E-Mail

WLAN

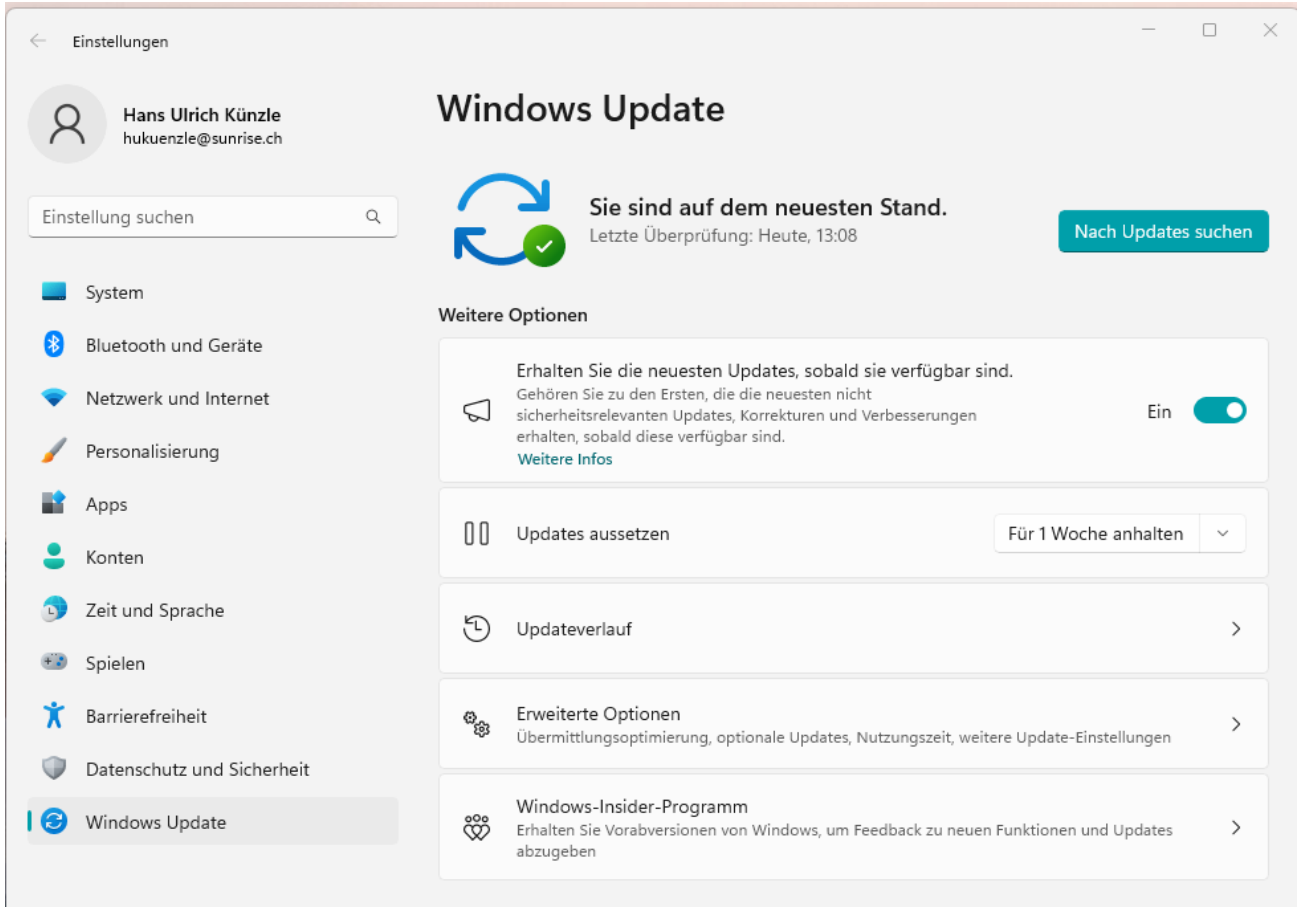
Passwörter

Daten sichern / Backup

Bedrohungen

- Infizierte Apps via Download vom Browser
- Schadsoftware als Anhänge von E-Mails
- Modifizierte Word-Dokumente
- Gefälschte E-Mails mit Aufforderung zur Übermittlung persönlicher Daten
- Ransomware Angriffe (Verschlüsselung oder Diebstahl von Daten) und Entschlüsselung nur gegen Lösegeld
- Phishing von Passwörter (Angeln)

Updates Windows 10 + 11



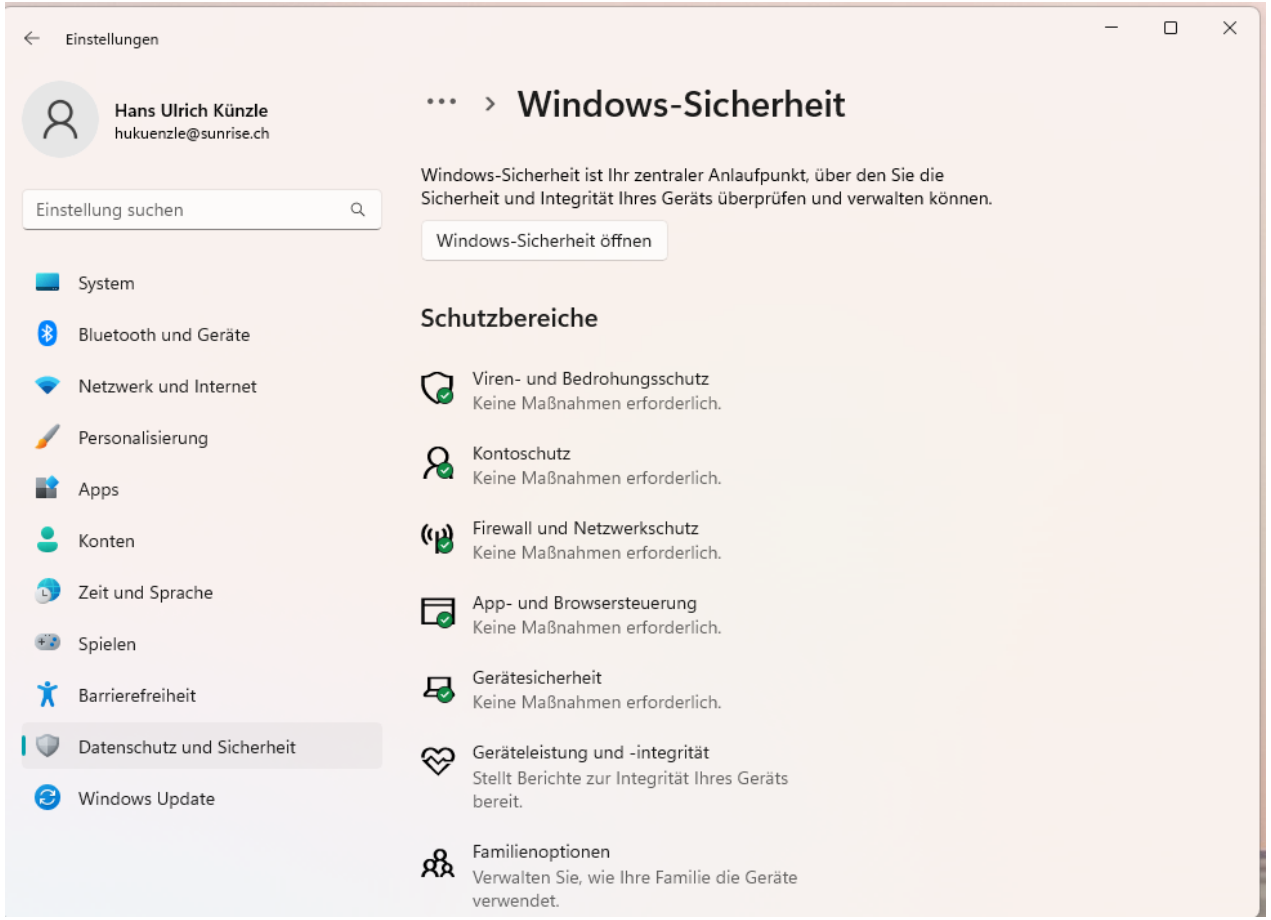
Einstellungen → Windows Update

Um die Windows-Sicherheit zu gewährleisten ist es unerlässlich, dass die Updates auf dem neuesten Stand sind.

Ist dies nicht der Fall, so können über die Taste “Nach Updates suchen” allfällige neue Updates gesucht und installiert werden.

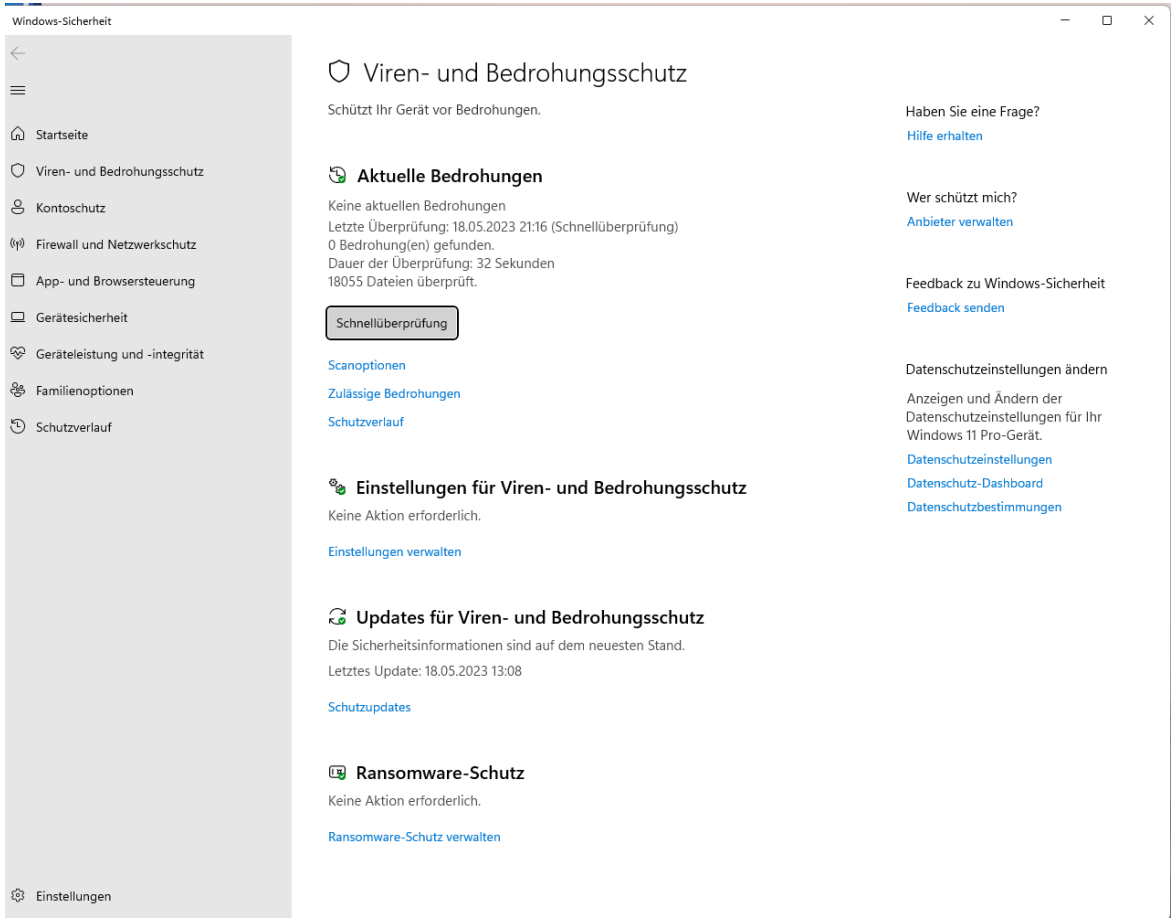
Updates für den Virenscanner (Defender) werden fast täglich neu installiert.

Windows Sicherheit



Einstellungen → Datenschutz und Sicherheit → Windows Sicherheit

Virenscanner (Windows Defender)



Bei Windows 10 + 11 ist mit dem Defender ein eingebauter Virenscanner bereits vorhanden.

Es braucht keinen fremden Virenscanner.

Der Defender wird täglich mit entsprechenden Updates versehen.

Einstellungen → Datenschutz und Sicherheit → Viren & Bedrohungsschutz

Browser (Das Tor zum Internet)

- Die meistbenutzten Browser sind Chrome (Google), Safari (Apple), Firefox (Mozilla, Open Source) und Edge (Microsoft)
- MS Internet Explorer 11 wird seit Juni 2022 nicht mehr unterstützt
- Grundsächlich sind die Bedienung und die Funktionen der verschiedenen Browser gleich.

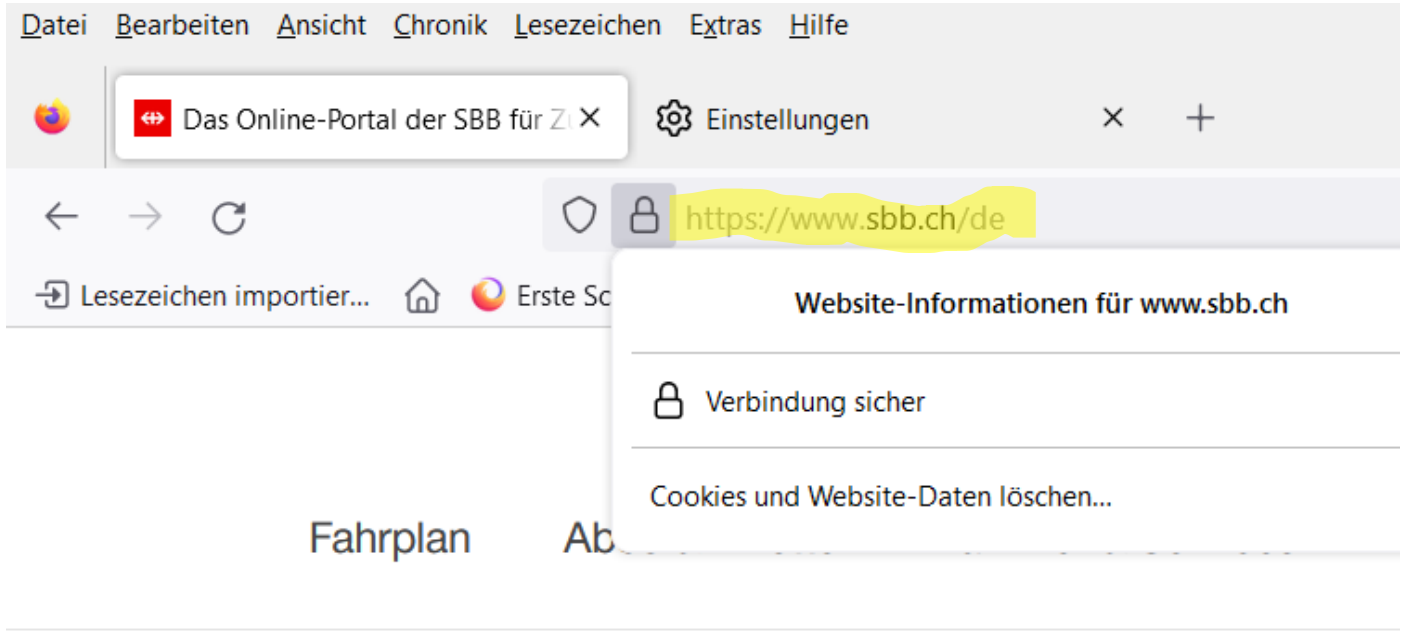
Google Chrome
Logo: Google
Erhältlich über:
➔ Google-Homepage

Apple Safari
Logo: Apple
Erhältlich über:
➔ Apple-Homepage

Mozilla Firefox
Mozilla
Erhältlich über:
➔ Mozilla-Homepage

Microsoft Edge
Logo: Microsoft
Erhältlich über:
➔ Microsoft-Homepage

Sicher Surfen

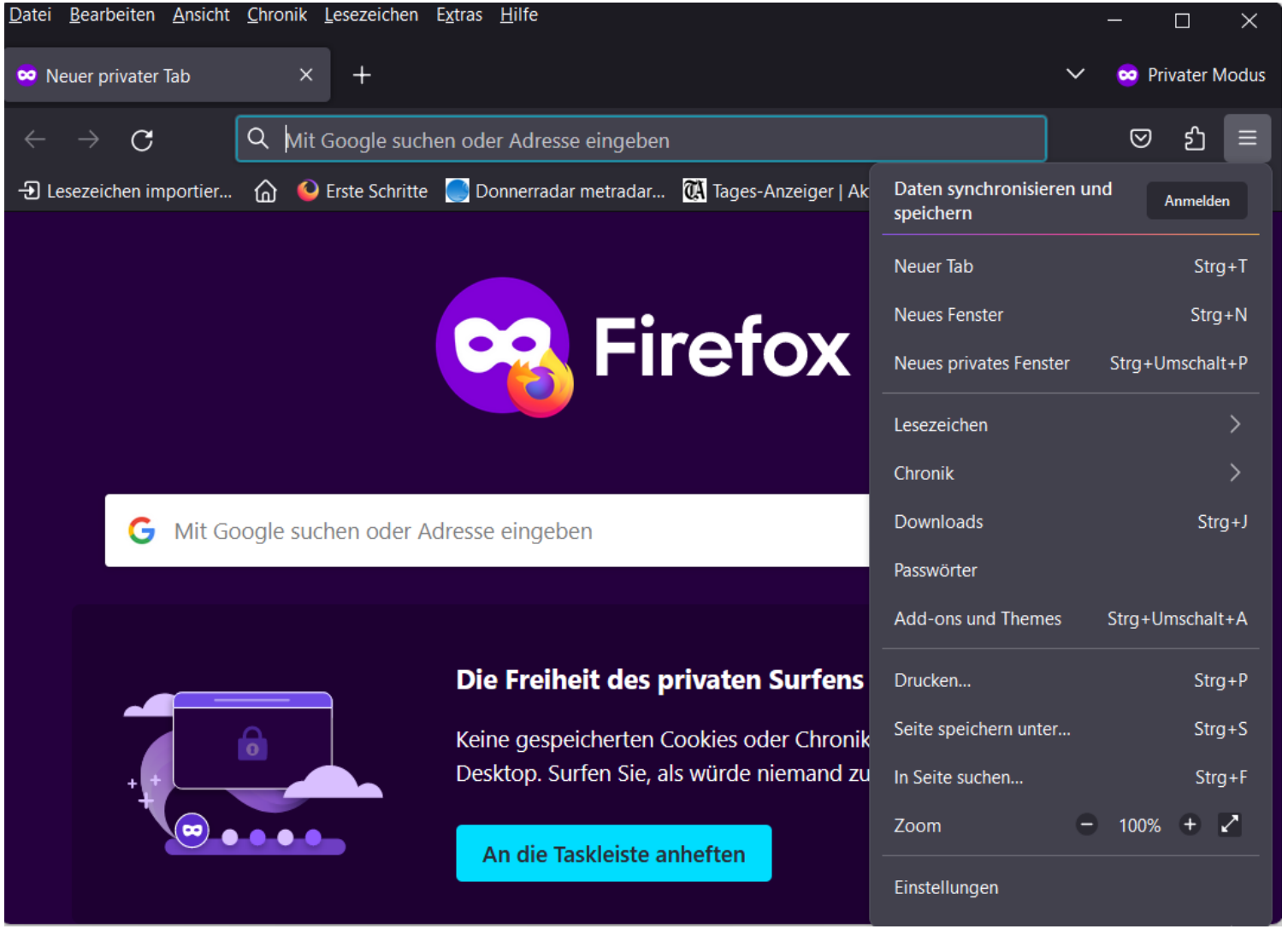


HTTPS = Sichere Verbindung zwischen Webserver und Browser

Die Daten zwischen Webserver und Webbrowser sind verschlüsselt

Eingabe von persönlichen Daten (z.B. Eröffnung eines Kundenkontos) nur über sichere Verbindung (HTTPS)

Privat Surfen



Über das Anwendungsmenu (drei waagrechte Striche oder drei Punkte) kann ein neues privates Fenster eröffnet werden.

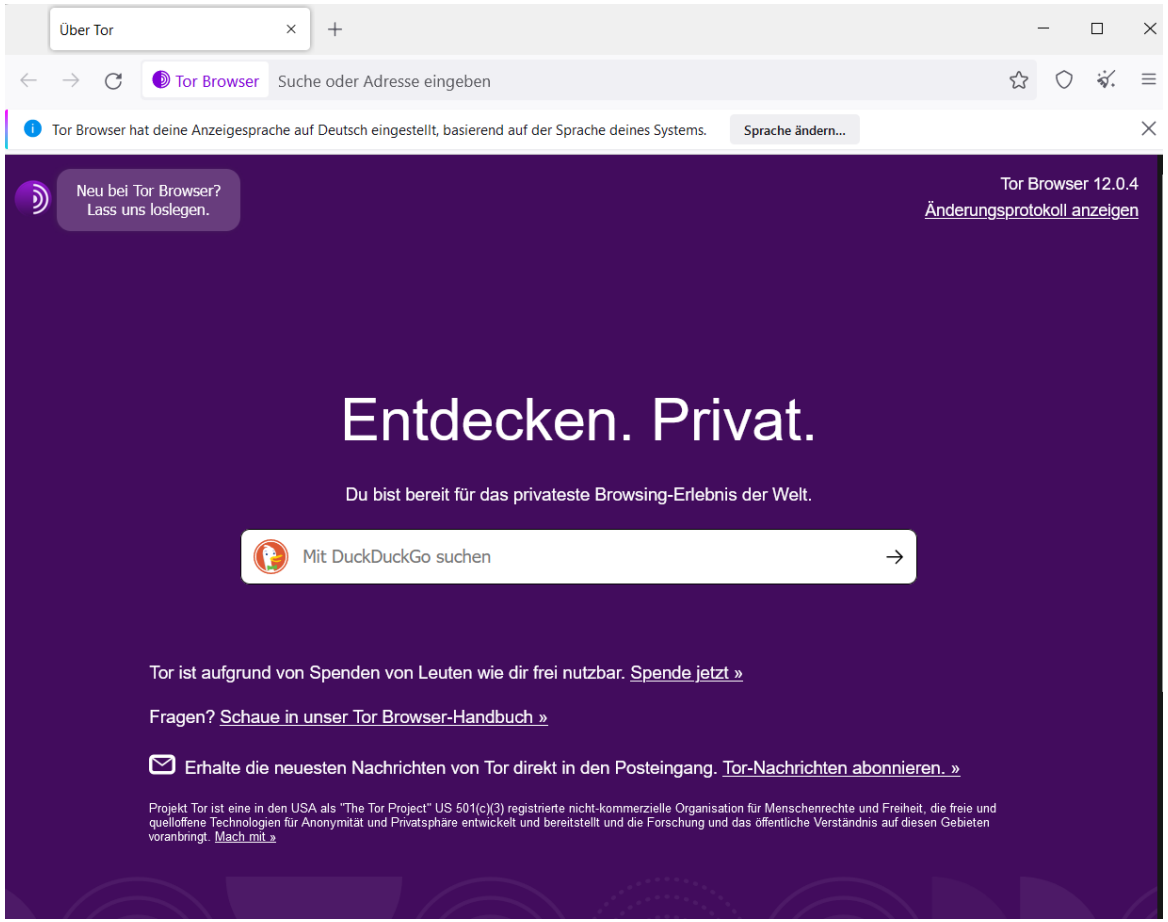
Firefox = Neues privates Fenster
Edge = Neues InPrivate Fenster
Chrome = Neues Inkognitofenster

In diesem Modus kann normal gesurft werden, jedoch wird kein Browserverlauf (Chronik), keine Cookies und keine Webseitendaten auf dem PC gespeichert.

Für den Internetanbieter ist jedoch die besuchte Webseite sichtbar.

Privat ist nicht Anonym !

Anonym Surfen mit dem TOR Browser



Über „torproject.org“ kann der Tor-Browser heruntergeladen und installiert werden.

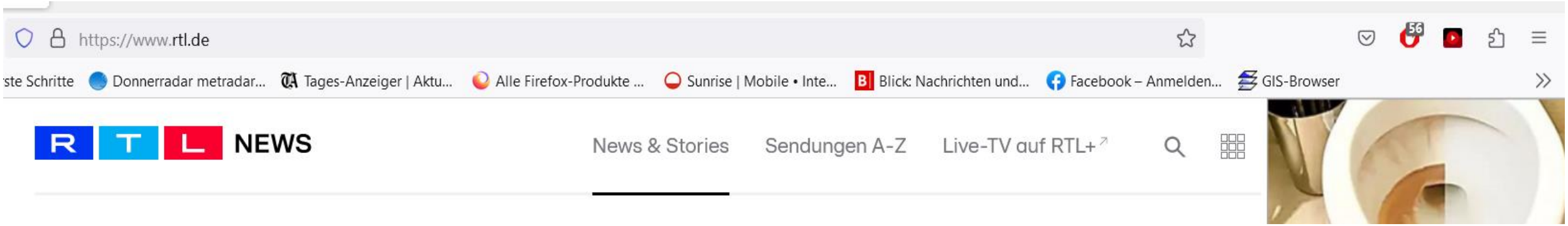
Mit dem Tor-Browser navigiert man vollständig anonym im Internet.

Die Daten werden mehrschichtig verschlüsselt, die besuchten Webseiten können nicht verfolgt werden (Tracker). Das Gleiche gilt für den Browser-Verlauf.

Das Tor-Netzwerk besteht aus Tausenden von Servern, betrieben von Freiwilligen, die als Tor-Relays bekannt sind.

Die Anonymität des Surfen mit dem Tor-Browser kommt daher, dass die Internetverbindung auf dem Weg von uns zu der Internetseite mehrfach umgeleitet wird. Dies hat jedoch auch Einfluss auf die Geschwindigkeit, das Surfen wird langsamer.

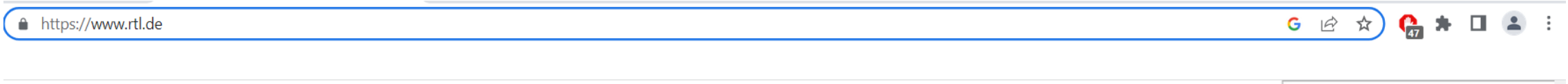
Werbeblocker Installieren



Firefox AdBlock

- Über Einstellungen --> Add-ons und Themes → AdBlock suchen oder Auswählen und installieren

Werbeblocker Installieren



Chrome AdBlock

- Über Einstellungen → Erweiterungen→ Menu → Erweiterungen und Chrome Webstore öffnen
- Im Chrome Webstore „AdBlock“ suchen und installieren

Edge AdBlock

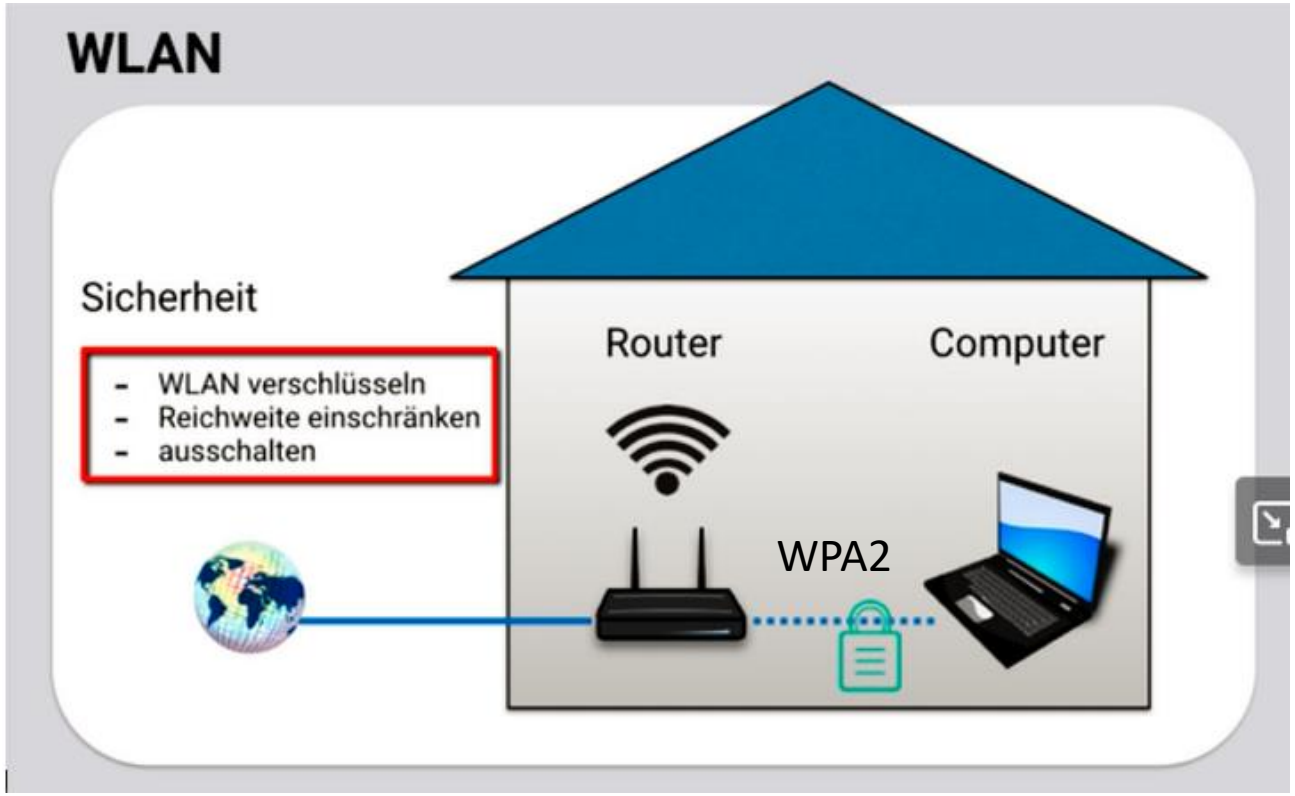
- Über Einstellungen → Erweiterungen → Erweiterungen für Microsoft Edge abrufen (suchen) und installieren

E-Mail Sicherheit

Typische Merkmale einer gefälschten E-Mail

- Absender verdächtig
- Fehlende persönliche Anrede
- Rechtschreibefehler, seltsamer Satzbau, schlechter Schreibstil
- Drohungen und gesetzte Fristen, die dringenden Handlungsbedarf suggerieren
- Aufforderung persönliche Daten einzugeben
- Aufforderung Anhänge oder Links anzuklicken

WLAN Sicherheit



Das WLAN-Netzwerk muss mit dem Sicherheitsprotokoll WPA2 verschlüsselt werden (Netzwerksicherheitsschlüssel)

Die Reichweite kann im Router eingeschränkt werden

Bei Benützung eines LAN-Kabel zwischen Computer und Router, muss im Router WLAN ausgeschaltet werden

Sichere Passwörter

Passwörter – die schlechtesten

123456	Zahlenfolgen
abcdefg	Buchstabenfolgen
wertzuiop	Tastaturfolgen
asdfgh	
Passwort	Wörter aus dem Lexikon
Sabine	Namen

Passwörter – so werden sie geknackt

- Kriminelle probieren die Passwörter aus
- Computer können Millionen Passwörter innerhalb kürzester Zeit austesten
- Zuerst werden dabei bekannte Passwörter, Wörter aus dem Lexikon, Zahlenfolgen und Namen abgeglichen
- Auch ein Passwort wie Manfred123 oder Sonnenblume1950 ist daher in Sekundenschnelle erraten
- Deshalb: Solche PW nicht verwenden!

Sichere Passwörter

Passwörter – so werden sie sicher

Es gibt mehrere Faktoren, die die Sicherheit eines Passworts erhöhen

- Zufällige Zeichenfolge
- Zeichenraum (welche Zeichen werden genutzt)
- Länge (wieviele Zeichen werden genutzt

Zeichenraum

Zahlen	0-9	10	
Kleines Alphabet	a-z	26	
Grosses Alphabet	A-Z	26	
Sonderzeichen	#(+	43	
	Total	96	Zeichen

Daher sollte man alles miteinander kombinieren!

Passwörter können auch abhanden kommen

- Trojaner liest Passwort mit
- Datei mit Passwörter wird gestohlen
- Firma, bei der man angemeldet ist wird gehackt

In diesen Fällen hilft auch ein starkes Passwort nicht

Deshalb:

- Ein eigenes Passwort für jede Seite
- So können Kriminelle ein gestohlenes Passwort nicht auf anderen Internetseiten verwenden

Passwörter verwalten

Für zahlreiche Anwendungen im Internet benötigt man ein Passwort. So kommen schnell 10-25 verschiedene Passwörter zusammen. Um die verschiedenen Passwörter zu verwalten gibt es eigene Programme, welche in einer sicheren Datenbank die Passwörter speichern.

Passwort-Manager „KeePass“

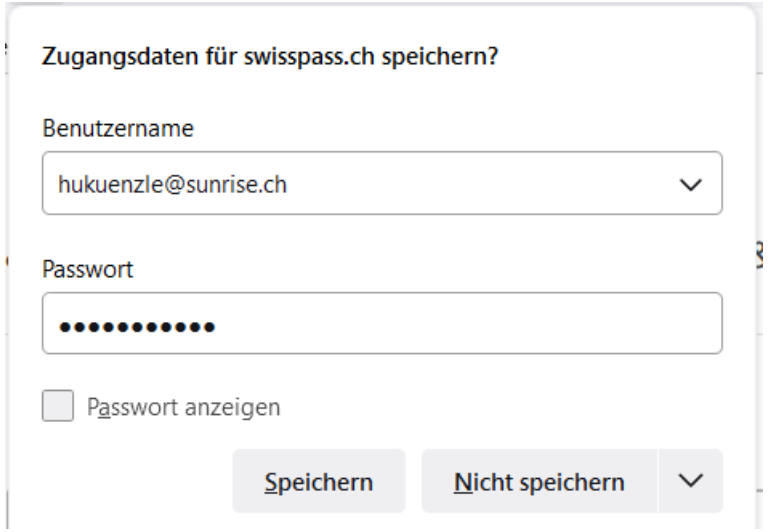
- Ist ein kostenloses Programm für Win 10 +11
- Legt eine Datenbank mit allen Passwörtern an (Tresor)
- Zugang wird mit einem sicheren Masterpasswort gewährt
- Kann auch auf einen USB-Stick installiert werden (portabel)

Passwörter im Browser speichern

Passwörter können auch in folgenden Browser gespeichert werden: Chrome, Firefox, Edge und Safari

Passwörter im Firefox speichern

- Über Einstellungen → Datenschutz und Sicherheit → Zugangsdaten und PW speichern, kann konfiguriert werden, ob Internet-Zugangsdaten (Logon-Daten) gespeichert werden sollen.
- Zugang über Hauptpasswort
- Wenn Firefox zur Speicherung der Zugangsdaten konfiguriert ist, erscheint bei einem Logon die Aufforderung, ob Firefox diese Daten speichern soll.
- Beispiel SBB Swisspass
- Mit Speichern werden die Zugangsdaten gespeichert.



Daten Sichern / Wiederherstellen (Backup / Recovery)

Vollständige Sicherung (Abbild / Image)

- Apps „Paragon CE“, „Acronis“, „Drive Snapshot64“ oder andere
- Seit Win11 gibt es bei Microsoft keine Sicherungs-App mehr
- Sicherung immer auf externe Festplatte oder Server (NAS)