Firefox einrichten und optimieren

Tipps zu Einstellungen und AddOns
about:config

In eigener Verantwortung

Firefox Einstellungen im Menü

Menü Einstellungen	Wert	Bedeutung	Kommentar
Allgemein: Start	Häkchen entfernen	Vorherige Fenster und Tabs öffnen wird verhindert.	
Einstellungen: Startseite und neue Tabs	Auf leere Seite setzen	Es werden keine externen Server kontaktiert.	Damit werden Google und Co. nicht mehr für die Startseite herangezogen.
Suche: Standardsuchmaschine	Eine andere Suchmaschine auswählen, z. B. Startpage oder DuckDuckGo.	Google als Standardsuchmaschine abwählen.	
Datenschutz und Sicherheit	Benutzerdefiniert auswählen und alle Häkchen setzen.		
Datenschutz und Sicherheit: Cookies	Alle Cookies von Drittanbietern blockieren.	Damit wird größtmöglicher Schutz vor der Aktivitätenverfolgung erreicht.	
Datenschutz und Sicherheit: Cookies und Website-Daten	Häkchen setzen.	Cookies und Website-Daten werden beim Beenden von Firefox gelöscht.	
Datenschutz und Sicherheit: Datenerhebung durch Firefox und deren Verwendung	Alle Häkchen entfernen	Firefox erhält keine Berichte mehr.	
Datenschutz und Sicherheit: Sicherheit	Alle Häkchen setzten	Erhöht die Sicherheit	

Firefox mit Plugins (AddOn) erweitern

Plugin	Bedeutung	Kommentar
Cookie AutoDelete von CAD Team	Löscht Cookies bereits beim Schließen der Seite	Ergänzung zu den Einstellungen „Cookies beim Beenden löschen“
I don’t care about Cookies	Akzeptiert in der Regel alle Cookies ohne Benutzereingabe.	Bitte auch alle Cookies beim Beenden löschen aktivieren.
Privacy Badger		
uBlock Origin	Unerwünschte Werbung unterdrücken	
HTTPS everywhere	Vorwiegend sichere https-Seiten anwählen.	

Firefox Einstellungen über „about:config (Die Verantwortung übernimmt der Benutzer)

about:config	Wert einstellen auf	Bedeutung	Kommentar
browser.tabs.closeWindowWithLastTab	false	Firefox wird beim Beenden des letzten Fensters nicht geschlossen	
browser.tabs.warnOnCloseOtherTabs	false	Der nervende Hinweis, dass mehrere Tabs geschlossen werden erscheint nicht mehr	
dom.webnotifications.enabled	false	PUSH Nachrichten werden nicht mehr angezeigt	
browser.privatebrowsing.autostart	true	Startet den Browser immer im privaten Modus	
browser.sessionstore.interval	300000	Tab-Wiederherstellung erfolgt seltener (alle fünf Minuten	
network.http.proxy.pipelining	true	Webseiten-Teile werden parallel und damit schneller geladen	
network.http.pipelining.ssl	true	Webseiten-Teile werden parallel und damit schneller geladen	

network.http.pipelining.maxrequests	8	Webseiten-Teile werden parallel und damit schneller geladen	
network.dns.disablePrefetch	true	Verhindert das Vorab-Laden von Webseiten mit zum Teil überflüssigen Elementen	
network.prefetch-next	false	Verhindert das Vorab-Laden von Webseiten mit zum Teil überflüssigen Elementen	
beacon.enabled	false	Verhindert das Vorab-Laden von Webseiten mit zum Teil überflüssigen Elementen	
network.http.max-persistent-connections-per-server	10	Beschränkt die Anzahl der Verbindungen je Server	
network.http.max-connections	256	Maximale Serververbindungen	
browser.tab.animate	false	Animierung in Tabs ausschalten (in FF 60 nicht vorhanden)	
browser.panorama.animate_zoom	false	??? (Animierte Tabs abschalten) (in FF 60 nicht vorhanden)	
nglayout.initialpaint.delay	1	Ladepausen verringern	
network.captive-portal-service.enabled	false	Mit dem Verbindungsaufbau zu »detectportal.firefox.com« prüft Firefox auf die Existenz eines Captive Portals, das insbesondere in öffentlichen WiFi-Netzwerken anzutreffen ist. Bei Bedarf wird der Browser dann zu einem Anmeldebildschirm umgeleitet. Mit einem Aufruf der about:config und der folgenden Einstellung kann der Captive-Portal-Check deaktiviert werden: network.captive-portal-service.enabled = false	
geo.enabled	false	Mozilla betreibt den Mozilla Location Service (MLS) – ein Dienst, der anhand von verfügbaren Daten wie Mobilfunkmasten, WiFi-Netzwerkinformationen oder Bluetooth-Beacons den (ungefähren) Standort eines	

		Nutzers ermitteln kann. Als Rückgabe erhält Firefox in meinem Beispiel folgende Information: *{„country_code“: „DE“, „country_name“: „Germany“}*Mit einem Aufruf der about:config und der folgenden Einstellung kann der Location-Service deaktiviert werden: geo.enabled = false	
browser.topsites.contile.enabled	false	Bei der Gegenstelle »contile.services.mozilla.com« handelt es sich um den Contile Tile Server von Mozilla. Hintergrund ist die Startseite bzw. Kachelansicht, bei der Kacheln von Amazon, eBay, YouTube, Facebook, Wikipedia und Reddit geladen werden. Eine Server-Antwort sieht folgendermaßen aus (Beispiel Amazon): Mit einem Aufruf der about:config und der folgenden Einstellung kann der Aufruf unterbunden werden: browser.topsites.contile.enabled = false	
extensions.pocket.enabled	false	Über die Adresse »getpocket.cdn.mozilla.net« lädt Firefox die neuesten Pocket-Informationen. Das sind meist Artikelteaser von Nachrichtenportalen wie ntv, Spiegel, Zeit, FAZ etc. Hier bspw. die Antwort zu einem Artikel zur FAZ mit dem Titel »Von Mafia gebaute Brücke in Italien beschlagnahmt«: Mit einem Aufruf der about:config und der folgenden Einstellung kann der Aufruf unterbunden werden: extensions.pocket.enabled = false	

Ergänzende Informationen

Die initiale Startseite des Browsers ist eine Mischung aus Suche (via Google), Kacheln (Amazon, eBay etc.) und Mozilla-Pocket-Meldungen. Mit dem Starten des Browsers/öffnen eines neuen Tabs geht das Nachladen von etlichen Ressourcen (JavaScript, Stylesheet, Bilder, Schrift (WOFF2) etc.) einher. Über »Einstellungen -> Startseite -> Neue Fenster und Tabs« lässt sich das Verhalten beeinflussen. Dort einfach jeweils »Leere Seite« wählen. Anschließend kommen die Verbindungen nicht mehr zustande.	Einstellungen -> Startseite -> Neue Fenster und Tabs« →“LeereSeite“

Während der Eingabe einer URL in der Adresszeile wird der Name der Domain an die Suchmaschine Google übermittelt. Google erhält über die Adresszeile also Kenntnis über jede Suchanfrage bzw. Webseite, die jemand besucht. Über »Einstellungen -> Suche« sollte eine andere Suchmaschine (bspw. Startpage) festgelegt werden. Ebenso ist es sinnvoll die Option »Suchvorschläge anzeigen« zu deaktivieren, damit nicht jede Eingabe der Tastatur an die ausgewählte Suchmaschine übermittelt wird.	Einstellungen -> Suche« sollte eine andere Suchmaschine (bspw. Startpage) festgelegt werden
Firefox kontaktiert ca. alle 30 Minuten die Adresse »safebrowsing.googleapis.com«, um die Blockliste herunterzuladen. Das Verhalten lässt sich über die about:config (oben beschrieben) oder »Einstellungen -> Datenschutz & Sicherheit -> Schutz vor betrügerischen Inhalten und gefährlicher Software« deaktivieren. Es ist darauf zu achten, alle Häkchen zu entfernen.	Einstellungen -> Datenschutz & Sicherheit -> Schutz vor betrügerischen Inhalten und gefährlicher Software« deaktivieren
Mozilla verfolgt/trackt den Nutzer im Auslieferungszustand. Unter anderem werden Informationen zum Nutzungsverhalten und auch Absturzberichte versendet. An sog. Firefox-Studien nimmt man auch automatisch teil. Über »Einstellungen -> Datenschutz & Sicherheit -> Datenerhebung durch Firefox und deren Verwendung« lässt sich die Übermittlung deaktivieren bzw. ein Opt-Out vornehmen.	Einstellungen -> Datenschutz & Sicherheit -> Datenerhebung durch Firefox und deren Verwendung« lässt sich die Übermittlung deaktivieren

Weiterführende Artikel:

Mike Kuketz: https://www.kuketz-blog.de/mozilla-firefox-datensendeverhalten-desktop-version-browser-check-teil20/
PC-Magazin: https://www.pc-magazin.de/ratgeber/firefox-schneller-machen-langsam-tipps-tuning-3198119-15932.html

Hier wird beschrieben, wie man seine Einstellungen vereinfachen kann!!
GnuLinux/CH https://gnulinux.ch/firefox-konfiguration-automatisieren

Für Profis:

Herkunft: Privacy Handbuch – Lizenz: Public Domain
https://www.privacy-handbuch.de/handbuch_21n.htm

Safebrowsing im Firefox ausschalten/deaktivieren.

Die Safebrowsing Engine lässt sich unter Firefox deaktivieren. Dies sollte stets unter Berücksichtigung des Mehrwertes geschehen: Wer sich im Internet tendenziell unsicher fühlt, der sollte überlegen den Schutz aktiviert zu lassen. Schlussendlich schützt aber auch die Safebrowsing Engine nicht endgültig vor Phishing. So lässt sich die Anbindung deaktivieren:

Aufruf im Browser: about:config

browser.safebrowsing.phishing.enabled	false
browser.safebrowsing.malware.enabled	false
browser.safebrowsing.blockedURIs.enabled	false
browser.safebrowsing.downloads.enabled	false
browser.safebrowsing.downloads.remote.enabled	false
browser.safebrowsing.downloads.remote.block_dangerous	false
browser.safebrowsing.downloads.remote.block_dangerous_host	false
browser.safebrowsing.downloads.remote.block_potentially_unwanted	false
browser.safebrowsing.downloads.remote.block_uncommon	false
browser.safebrowsing.downloads.remote.url	(leerer String)
browser.safebrowsing.provider.*.gethashURL	(leerer String)
browser.safebrowsing.provider.*.updateURL	(leerer String)