Bayerisches Staatsministerium für
Unterricht und Kultus

Browser

Stand: 16.09.2024

→ www.km.bayern.de / gestalten / digitalisierung / datensicherheit / browser

Inhaltsverzeichnis

Sichere Nutzung von Browsern

Browsersicherheit schafft Datensicherheit ©Robert Avgustin - stock.adobe.com

Empfehlungen zur Nutzung von Browsern

Die nachfolgenden Inhalte widmen sich der Aufklärung wichtiger Aspekte, die bei der sicheren Nutzung von Browsern berücksichtigt werden sollten. Dazu gehören

- die Vermeidung von Tracking-Mechanismen,
- der sensible Umgang mit personenbezogenen Daten im Zusammenhang mit Downloads und Cache,
- sowie die Risiken, die von unsicheren Servern ausgehen können.

Ein fundiertes Verständnis dieser Themen ist unerlässlich, um die Sicherheit jeglicher Daten zu gewährleisten. Die folgenden Empfehlungen geben ein Mindestmaß an Schutz vor.

Empfehlung 1: Der Privat-Modus

Der Begriff Privat-Modus wird hier anstelle der produktspezifischen Bezeichnungen der einzelnen Browser, wie „Inkognito-Modus“, „Privates Fenster“, „Privates Surfen“ und "InPrivate-Fenster“ verwendet. Er wird zur grundsätzlich empfohlen und bietet folgende Vorteile:

Privatsphäre

Im Privat-Modus werden keine Informationen wie Cookies, Verlauf oder Suchanfragen

gespeichert, wenn das Fenster geschlossen wird. Dadurch bleiben Ihre Aktivitäten auf dem Gerät privat und werden nicht in Ihrem Browserverlauf gespeichert.

Schutz vor Tracking

Fenster oder Tabs des Browsers im Privat-Modus blockieren normalerweise das Tracking durch Websites und Werbenetzwerke. Da Cookies und andere Tracking-Mechanismen nach dem Schließen des Fensters gelöscht werden, können Websites Ihre Aktivitäten nicht über verschiedene Sitzungen hinweg speichern und verfolgen.

Separate Sitzung

Der Privat-Modus ermöglicht es separate Sitzungen ohne Interferenzen mit anderen regulären Browsersitzungen zu haben. Das bedeutet, gleichzeitig in einem normalen Fenster und einem privaten Fenster gesurft werden kann, ohne dass Daten zwischen ihnen ausgetauscht werden. Verwendet man mehrere Privat-Modus-Fenster oder –Tabs, kann man sich beispielsweise auf der gleichen Website mit verschiedenen Konten anmelden.

Sicheres Surfen auf privaten Endgeräten bzw. Computern, die von mehreren Personen benutzt werden

Wenn man einen öffentlichen Computer (Lehrerzimmer) verwendet und keine Spuren seiner Aktivitäten hinterlassen möchten, ist der Privat-Modus ideal. Nachdem das Privat-Modus-Fenster geschlossen wurde, werden alle Daten gelöscht, was sicherstellt, dass der nächste User des Computers auf die Daten keinen Zugriff hat, da keine persönlichen Informationen zurückbleiben.

Hinweis

Dennoch ist es wichtig zu beachten, dass man im Privat-Modus nicht vollständig anonym ist.

Empfehlung 2: Regelmäßige Bereinigung und Datensparsamkeit

Es ist wichtig, regelmäßig den Download-Ordner sowie Cookies und Cache des Browsers zu bereinigen, um unter anderem Speicherplatz freizugeben und um mögliche Sicherheitsrisiken, durch unerwünschte und veraltete Cookies zu minimieren und um **personenbezogene Daten** nicht unnötig vorzuhalten.

In den Browsern lässt sich dies auch automatisieren, so dass beispielsweise nach jeder Sitzung alle Cookies gelöscht werden. Es kann auch eine automatische Ablehnung von Cookies (auch von Drittanbietern) durch Einstellungen oder Funktionserweiterungen mit

Plug-Ins oder Add-Ons eingestellt werden.

Empfehlung 3: Verschlüsselung und Zertifikate

Es sollte immer darauf geachtet werden, dass Websites das TLS-Protokoll verwenden, um eine sichere Verbindung zu gewährleisten. Am Symbol eines Vorhängeschlosses, meist vor der Adressleiste des Browsers, kann man erkennen, ob eine Website TLS unterstützt bzw. ob das HTTPS-Protokoll verwendet wird. Ist das Vorhängeschloss geschlossen oder grün, deutet dies auf eine sichere, verschlüsselte Website hin. Fehlende, ungültige und selbsterstellte Zertifikate können auf unsichere Verbindungen (offene Vorhängeschlosssymbol bzw. rot) hinweisen. Daher warnen die Browser, durch ein Pop-up vor dem Zugriff auf eine solche Website und verlangen eine Bestätigung durch den Nutzer über das Bewusstsein des Zugriffs auf eine unsichere Website. Dieser Mechanismus ist bei den aktuellen Browsern Standard.

Empfehlung 4: Speicherung von Formulardaten

Sollte es mehreren Personen, ohne personalisierte Anmeldung, möglich sein auf einem Client (z. B. PC im Lehrerzimmer) zu zugreifen, so muss das Speichern von Formulardaten (z. B. persönliche Anschrift, Bankdaten) ausgestellt sein. Nutzt man den Computer mit personalisierten Konten kann das Speichern von Formulardaten die Arbeitseffizienz erhöhen und eine Zeitersparnis kann mit einhergehen. Gespeicherte Formulardaten können ein potenzielles Sicherheitsrisiko darstellen, insbesondere, wenn jemand unbefugten Zugriff auf den Computer erhält. In diesem Fall könnten sensible Informationen an andere weitergegeben oder kompromittiert werden.

Empfehlung 5: Speicherung von Passwörtern

Meldet man sich im Browser bei verschiedenen Websites mit Passworten an, so werden diese können diese verschlüsselt durch den Browser gespeichert werden. Beim Schließen des Browserfensters werden die Passwörter nicht automatisch gelöscht. Stattdessen bleiben sie im Speicher des Browsers, bis man sie aktiv löscht. Es ist wichtig zu beachten, dass das Speichern von Kennwörtern im Browser ein potenzielles Sicherheitsrisiko darstellen kann, insbesondere, wenn jemand unbefugten Zugriff auf den Computer hat oder beim Gebrauch eines öffentlichen PC (Lehrerzimmer) ohne personalisierte Anmeldung. Im letzteren Fall sollten keine Kennwörter im Browser gespeichert werden. Grundsätzlich wird die Nutzung eines Passwort-Managers empfohlen. Dieser generiert sichere und eindeutige Passwörter und speichert diese verschlüsselt ab.

Empfehlung 6: Kamera-, Mikrofon- und Standorteinstellungen

Um unkontrollierten Zugriff auf die Kamera, das Mikrofon oder den Standort zu vermeiden, sollten entsprechende Einstellungen vorgenommen werden, die den Benutzer darüber informieren, wenn eine Webanwendung den Zugriff anfordert.

Empfehlung 7: Plug-Ins/Add-Ons

Plug-Ins und Add-Ons sollten immer mit Bedacht und nur aus vertrauenswürdigen Quellen verwendet werden. Um Sicherheitslücken zu schließen ist dringend darauf zu achten, dass die Plug-Ins und Add-Ons regelmäßig aktualisiert werden. Nicht benötigte Plug-Ins und Add-Ons sollten deaktiviert oder gelöscht werden, um potenzielle Angriffspunkte zu minimieren.