



# SBRM ONLINE PC-KURS 2: NICHTSZUVERBERGEN

## SCHÜTZEN SIE SICH UND IHRE DATEN

### A) BEGRIFFE:

- Webbrowser:  
das englische Verb „to browse“ bedeutet durchblättern. Mit dem Webbrowser „blättern“ Sie das Internet (Web) nach Seiten zu einer von Ihnen gestellten Anfrage durch. Als Ergebnis erhalten Sie eine Liste passender Antworten, aus der Sie die Beste auswählen.  
Beispiele für Webbrowser sind: Mozilla Firefox, Google Chrome, Opera, Internet Explorer.  
Ich beziehe mich hier auf Firefox, einen schnellen und sicheren OpenSource Browser.
- Open Source Programme  
Sie sind quelloffen, das bedeutet, dass jeder der programmieren kann in der Lage ist, die interne Programmierung (das Quellprogramm, die Source) nachzuvollziehen und somit auch sicherheitsrelevante Bereiche erkennen. Open Source Programme sind meist kostenlos  
Dem gegenüber stehen die kommerzielle Programme, auch Betriebssysteme wie WINDOWS, deren Quellcode geheim ist.
- Suchmaschine  
Genau genommen ist es nicht der Webbrowser, der Ihnen die Antworten auf Ihre Suchanfrage liefert, sondern es ist die im Browser integrierte Suchmaschine, sehr oft Google.
- Add ons  
das sind Erweiterungen, die nachträglich dem Browser hinzu gefügt werden können.
- Cookies  
dies ist kurz gesagt eine kleine Textdatei, die von der besuchten Webseite auf Ihrem PC abgelegt wird. Cookies enthalten Informationen zu Ihrem Besuch und ermöglichen es zB dass Ihre Einstellungen oder Ihr Warenkorb beim nächsten Besuch wieder erkannt wird.
- Ad Blocker  
blockieren Adware ( werbefinanzierte Software), die Sie eigentlich gar nicht wollen. Auch Malware (Schadprogramme) werden als Adware bezeichnet. Ad steht als Abkürzung für Advertisement

### B)WIE GEHT DAS ?

1. Das Add-on Startpage als Suchmaschine an Stelle von Google einrichten:  
Startpage übergibt die Suchanfrage anonym an Google und das Suchergebnis zurück an den Webbrowser. Somit hat Google keine Information über Sie und Ihre Interessen.
  - Öffnen Sie das Anwendungsmenü in *Firefox* (oder Ihres Browsers). Das sind die 3 waagerechten Striche (auch Sandwichmenü genannt).meist rechts oben zu finden
  - Wählen Sie „*Einstellungen*“ und dann „*Suche*“.  
Unter „*Standardsuchmaschinen*“ wählen Sie „*Startpage.com*“  
Sollte *Startpage* dort nicht auftauchen, gehen sie auf „*Weitere Suchmaschinen hinzufügen*“, geben in das Suchfeld „*Startpage*“ ein, markieren den Treffer und fügen ihn zu



## SBRM ONLINE PC-KURS 2: NICHTSZUVERBERGEN

Firefox hinzu.

2. die *Aktivitätsverfolgung* im Browser deaktivieren  
Wählen Sie im „Sandwichmenü“ „*Einstellungen*“, dann „*Datenschutz und Sicherheit*“.
  - Den „*verbesserten Schutz vor Aktivitätenverfolgung*“ können Sie auf „*Standard*“ lassen und markieren weiter unten „*immer*“ bei „*Do not track information senden*“
3. *Add-Blocker*-add-ons im Browser aktivieren:
  - Sandwichmenü → *Erweiterungen*
  - in das Suchfeld „*Weitere Add-ons finden*“ geben Sie „*Adblock plus*“ ein. In der Liste finden Sie das Gesuchte, wählen es mit Linksklick aus und fügen es hinzu.
  - Keine Browser Historie speichern:  
*Einstellungen* → *Datenschutz&Sicherheit* → *Chronik*:  
*eine Chronik niemals anlegen* wählen. Sodann die bisherige Chronik löschen
    - auf derselben Seite: wählen Sie: „*Cookies und Website-Daten beim Beenden löschen*“
4. Über die Daten Sammelwut und Sicherheitslecks von Whatsapp & Co wurde bereits oft in Zeitungen berichtet.  
Es gibt bessere Alternativen. Ich bevorzuge *Ginlo* und *Telegram*.
5. „*opt out*“ einrichten:  
*opt-out* bedeutet, sich gegen etwas zu entscheiden; hier :die Vermarktung Ihrer Daten.
  - Am einfachsten folgen Sie der Anleitung unter diesem Link:  
<https://blog.hubspot.de/marketing/google-analytics-deaktivieren>  
hier finden Sie auch weitere Erläuterungen.
  - laden Sie das Browser add-on herunter, klicken Sie auf „*akzeptieren und installieren*“
6. neben Ihrer privaten Mailadresse sollten Sie mindestens noch eine weitere besitzen.  
Diese nutzen Sie für die Kommunikation mit Unbekannten, auch Anbietern von Waren im Netz wie Ebay ua.  
einen weiteren Vorteil bietet diese zweite Adresse, wenn Sie einmal ihr Passwort für die private mail verloren haben: Sie können sich dann ein temporäres Passwort an die zweite Adresse schicken lassen.
7. Geben Sie keine privaten Daten ohne Not preis, stellen Sie keine Fotos von sich selbst oder der Familie ins Netz, veröffentlichen Sie Ihre private Adresse oder Ihre Urlaubspläne nicht in den sozialen Netzwerken . s.a.  
<https://daserste.ndr.de/panorama/archiv/2021/Geklaut-Private-Kinderfotos-auf-Kinderpornografie-Seiten,kinderpornografie210.html>

Man sieht, es gibt viel zu tun .....