



**bnmsp.de**

"Internet für Main-Spessart"  
Hotline: 09352 / 60 33 76



# Bürgernetze Main-Spessart

## Sicher Surfen

Christoph Purrucker  
cp@bnmsp.de

17. November 2015

# Inhalt

- Definition „Sicher“
- Mobil- Betriebssysteme (wenig Möglichkeiten)
- Desktop- Betriebssysteme (schon besser)
- Surf- Betriebssystem (Dual-Boot, VM)
- Remote-Verbindung
- Verschlüsselte Verbindungen

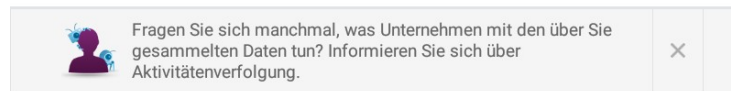
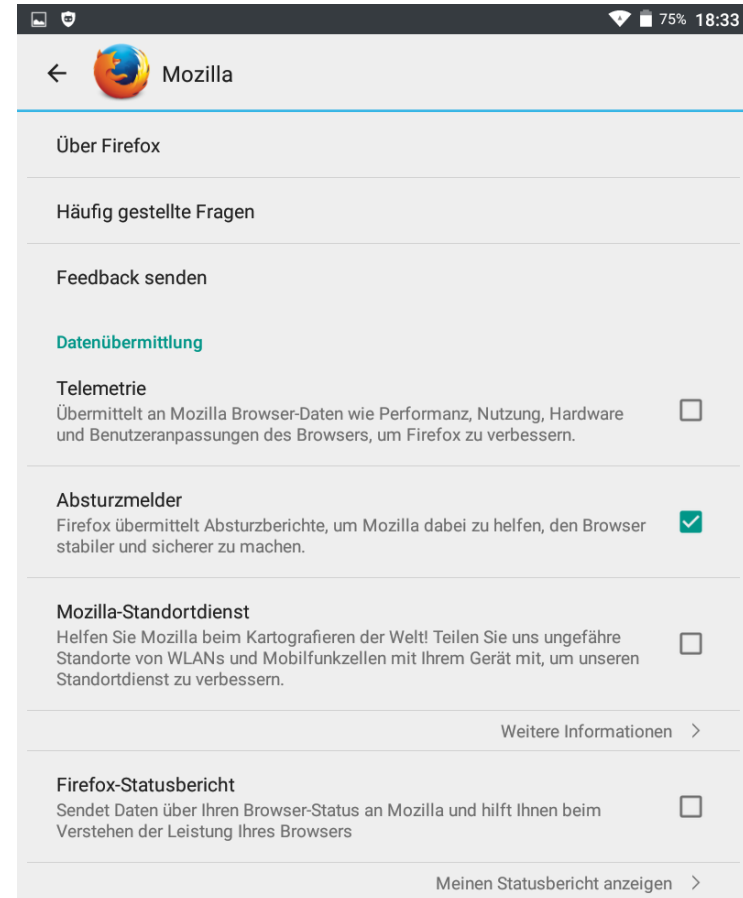
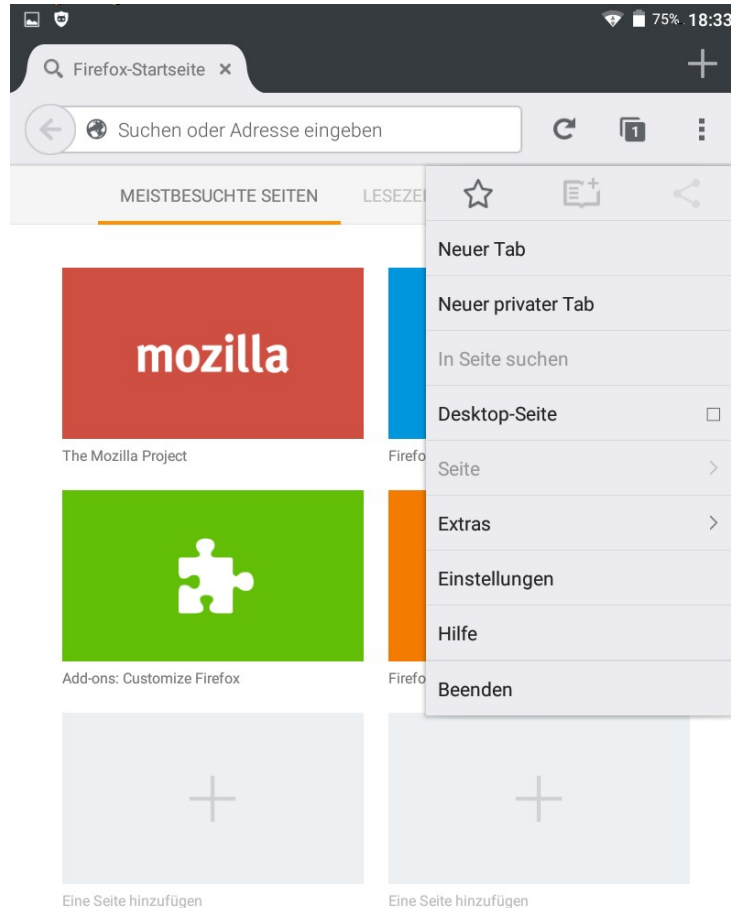
## Definition „Sicher“

- Beim Surfen darf mein Rechner/mein Betriebssystem keinen Schaden nehmen.
- Ich will nicht unwillkürlich Daten über mich preisgeben; ich will nicht von der Werbeindustrie verfolgt werden.
- Ich will sicher verschlüsselte Verbindungen zu Servern nutzen.

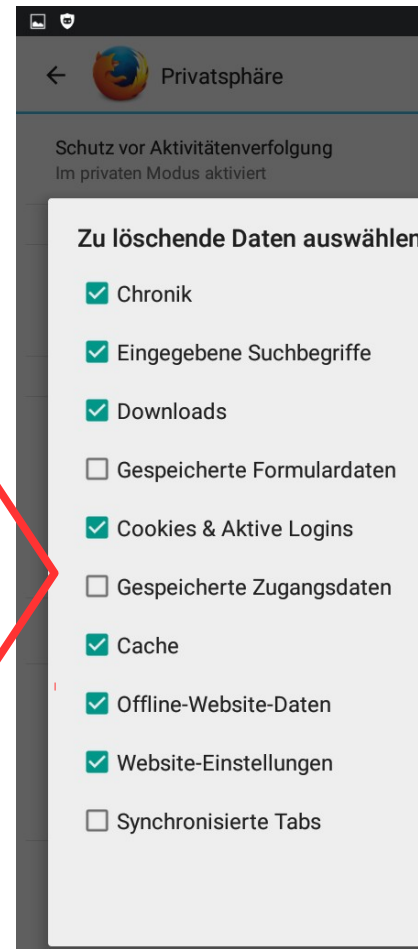
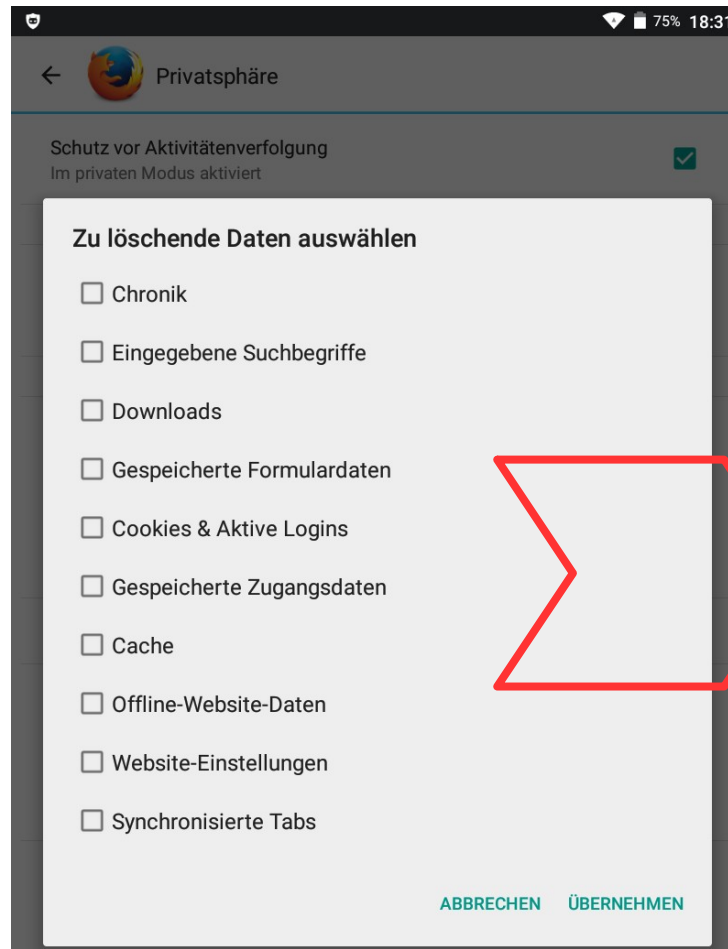
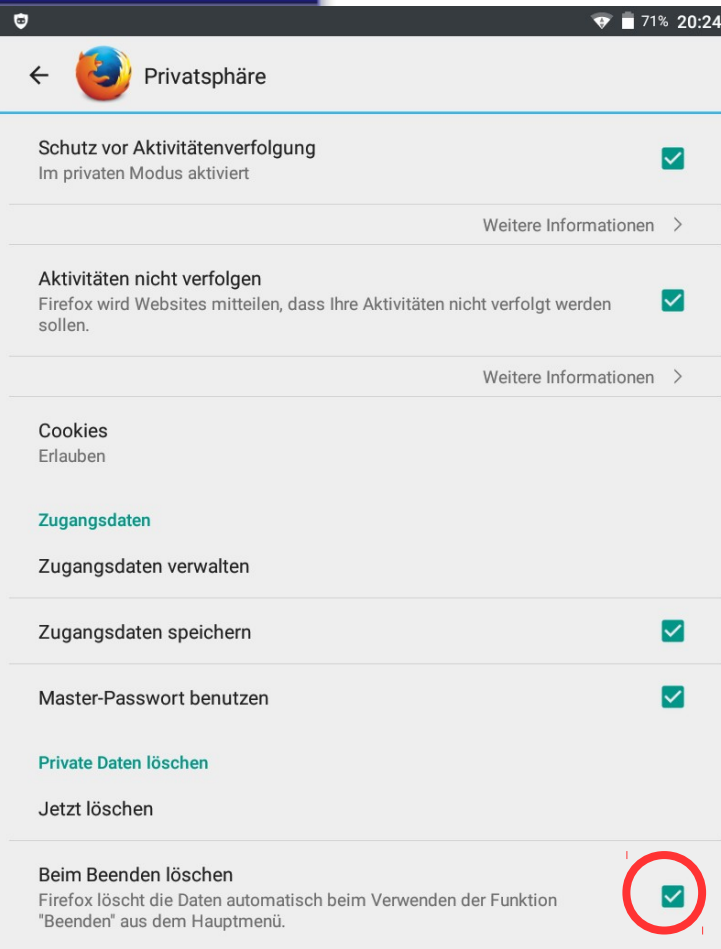
# Mobil-Betriebssysteme

- Windows 8/10 Mobile: kein Testgerät zur Hand.
- iOS: Kein aktuelles Testgerät zur Hand.
- Android:
  - Achtung: Prüfen, ob die App **Adobe Flash** installiert ist: Deaktivieren ist wichtig!
  - Der integrierte Browser hat wenig nützliche Einstellungen, da Google Geld mit Werbung verdient.
  - Mobile Firefox ist am vertrauenswürdigsten. „Private-Mode“ vorhanden. Die wenigen Einstellungen zeigen die folgenden Seiten...

# Firefox Mobile 1



# Firefox Mobile 2



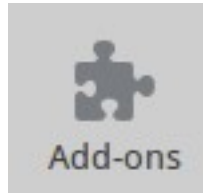
# Desktop-Betriebssysteme

Relevante, sichere Browser (u.a. mit „Private-Mode“):

- Firefox
- Chromium

Sicherheit steht und fällt mit den Plugins:

- „NoScript“ und insb. AdBlocker sind wichtige Plugins.
- Diverse Toolbars und Erweiterungen gefährden die Sicherheit



Daher wichtig: Regelmäßiger Blick in die Plugins

Gerade unter Windows finanzieren sich viele Tools mit für den Anwender ungünstigen Um-Konfigurationen der Browser (prominent: Java,...)

# Plugins 1

Sinnvoll: AdBlocker „uBlock Origin“



- Seiten laden schneller, da Verbindungen zu Werbenetzwerken blockiert werden.
- Sicherer: Über Werbenetzwerke werden oft Viren verbreitet, die so gar nicht erst geladen werden.

Gefährlich aber manchmal nützlich:

- Adobe Flash: Ständig Sicherheitslücken. Unter Windows schlechter Update-Mechanismus.
- Oracle Java: das gleiche.



## Plugins 2

Gefährlich aber selten nützlich:

- Alle Formen von Toolbars
- Weitere Codecs
- Adobe PDF-Plugin (weil auch hier Adobe keinen stabilen Update-Mechanismus hinbekommt)
- Skype Plugin
- ...

Firefox: Plugins regelmäßig auf Aktualisierung prüfen:  
<http://www.mozilla.com/en-US/plugincheck/>

# Firefox Einstellungen 1

## Datenschutz

### Verfolgung von Nutzeraktivitäten

- Websites auffordern, meine Aktivitäten nicht zu verfolgen [Weitere Informationen](#)
- Schutz vor Aktivitätenverfolgung in privaten Fenstern verwenden [Weitere Informationen](#)

### Chronik

Firefox wird eine Chronik:

- Immer den privaten Modus verwenden
  - Besuchte Seiten und Download-Chronik speichern
  - Eingegebene Suchbegriffe und Formulardaten speichern
  - Cookies akzeptieren

[Ausnahmen...](#)

Cookies von Drittanbietern akzeptieren:

Behalten, bis:

[Cookies anzeigen...](#)

- Die Chronik löschen, wenn Firefox geschlossen wird

[Einstellungen...](#)

### Adressleiste

Vorschläge beim Verwenden der Adressleiste:

- Einträge aus der Chronik
- Einträge aus den Lesezeichen
- Offene Tabs

[Einstellungen für Suchvorschläge öffnen...](#)

# Firefox Einstellungen 2

## Sicherheit

### Allgemein

- Warnen, wenn Websites versuchen, Add-ons zu installieren
- Webseite blockieren, wenn sie als attackierend gemeldet wurde
- Webseite blockieren, wenn sie als Betrugsversuch gemeldet wurde

[Ausnahmen...](#)

### Passwörter

- Passwörter speichern
- Master-Passwort verwenden

[Ausnahmen...](#)

[Master-Passwort ändern...](#)

[Gespeicherte Passwörter...](#)

# Surf- Betriebssysteme

Immer auf Linux basierend und auf spezielle Einsatzzwecke zugeschnitten.

Lassen sich auf USB-Stick oder als zweites Betriebssystem auf die Festplatte installieren.

Komfortabler: Installation in eine virtuelle Maschine, dann muss man den Rechner nicht umständlich neu starten.

- Speziell für Homebanking: **c't Bankix**  
(<http://www.heise.de/ct/projekte/Sicheres-Online-Banking-mit-Bankix-284099.html>)
- Allgemein zum Surfen: **c't Surfix**  
(<http://www.heise.de/ct/projekte/c-t-Surfix-Sicher-im-Web-1380126.html>)

# Remote-Verbindung

**Idee:** Man surft auf einem entfernten Rechner und überträgt nur den Bildschirminhalt, aber nicht die Schadsoftware auf den eigenen PC.

- Wir bieten bei uns einen solchen Rechner an, auf dem man sich einloggen und surfen kann. Dabei kann der lokale Rechner keinen Schaden nehmen.
- Aktuell Testbetrieb, Zugangsdaten über mich.
- Trotzdem sollte man natürlich auch hier die Tipps bezüglich Plugins und Browser-Einstellungen beachten.



**bnmsp.de**

"Internet für Main-Spessart"  
Hotline: 09352 / 60 33 76



# Sichere Verbindungen 1

Browser zeigen verschlüsselte Verbindungen an:



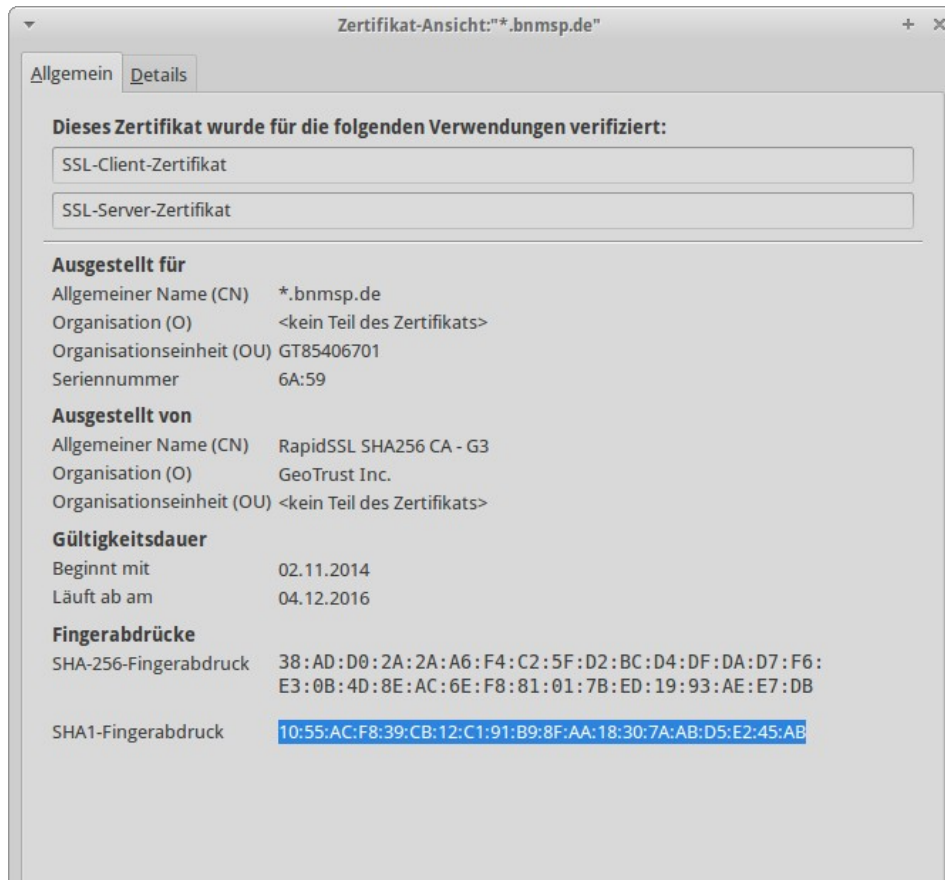
... je nach dem, wie viel Geld man für ein Zertifikat ausgegeben hat.

Sicher ist das trotzdem alles nicht, weil der Browser hunderten Zertifikats- Ausgabestellen vertraut, u.a. so seriösen wie: TürkTrust, China INIC, u.v.a.

Jede dieser Stellen kann Zertifikate ausstellen mit denen ein Angreifer sich zwischen Client und Server platzieren kann, um Daten mitzulesen.

# Sichere Verbindungen 2

**Abhilfe:** Fingerabdruck prüfen und vergleichen (am sichersten aber sehr umständlich):



## Bnmsp.de-SHA1:

10:55:AC:F8:39:CB:12  
C1:91:B9:8F:AA:18:30  
7A:AB:D5:E2:45:AB



## Sichere Verbindung 3

Automatisierte Verfahren zur Zertifikatsprüfung sind noch nicht sehr weit verbreitet:

- **DANE:** Im DNS werden Fingerabdrücke mitgeliefert. Funktioniert nur mit DNSsec- Infrastruktur.
- **Certificate Transparency:** Mit dem Logbuch mit Fingerabdrücken kann man im Nachhinein gefälschte Zertifikate entdecken: Google setzt auf den Abschreckungs-Effekt.
- **Certificate Pinning:** Server sendet seinen Fingerabdruck mit. Browser merkt sich diesen und kann bei Abweichungen Alarm schlagen.