

*Folgende Tipps sollen dir helfen, deine persönlichen Daten am Computer zu schützen:*

### 1. **Betriebssystem**

Benutze ein aktuelles Betriebssystem und halte es immer auf dem neuesten Stand (installiere grundsätzlich alle Sicherheitsupdates).

- Windows XP wird nur noch mit Service Pack 3 unterstützt
- Windows Vista benötigt Service Pack 2
- Windows 7
- Apple OSX „Snow Leopard“
- Linux Kernel 2.6.35

### 2. **Benutzerprofile**

Lege für jeden Benutzer des Computers ein Benutzerprofil mit eingeschränkten Rechten an und arbeite niemals als Administrator.

### 3. **Firewall**

- Computer: Aktiviere die Firewall von Windows
- Router: Aktiviere die Firewall im Router
- Teste die Firewall unter: [www.heise.de/security](http://www.heise.de/security) - Netzwerkcheck – Test starten

### 4. **Antivirenprogramm**

Verwende unter Windows immer ein aktuelles Antivirenprogramm, das täglich aktualisiert wird.

- Avira Antivir Personal: [free-av.de](http://free-av.de)
- Avast Free Antivirus: [www.avast.com](http://www.avast.com)

Zusätzlich solltest du dich unter Windows durch ein Antispywareprogramm schützen, das dafür sorgt, dass deine Daten nicht ausgespäht werden.

- Spybot - Search & Destroy: [www.safer-networking.org](http://www.safer-networking.org)

### 5. **Browser**

Arbeite nur mit einem aktuellen Browser. Aktiviere die automatische Updatefunktion.

- Firefox 3.6.11
- Opera 10.63
- Internetexplorer 8.0
- Safari 5.02
- Chrome 7.0

### 6. **WLAN**

- Nutze WLAN nur, wenn es sich nicht umgehen lässt.
- Aktiviere unbedingt die WPA/WPA2-Verschlüsselung.
- Schalte das WLAN ab, wenn es nicht genutzt wird.
- Ändere das Routerpasswort
- Verwende öffentliche Access-Points niemals für private Dinge wie E-Mail oder gar Banking.

## 7. Verschlüsselung

Mit dem Programm Truecrypt lassen sich sehr einfach Daten verschlüsseln, so dass sie nur noch nach Eingabe eines Passwortes zu entschlüsseln sind. Dazu wird eine Datei (Volume) angelegt, die als ein eigenes Laufwerk eingebunden wird. Die Größe des Volumes kann nachträglich nicht mehr verändert werden.

- *Create Volume*
- *Create an encrypted file container* → Next
- *Standard TrueCrypt Volume* → Next
- Speicherort und Name (Endung .tc) für die verschlüsselte Datei auswählen:  
*Select File* → Next
- *Encryption Algorithm „AES“* → Next
- Größe des verschlüsselten Laufwerks angeben → Next
- Passwort eingeben, möglichst lang und sicher.  
Achtung: Ist das Passwort vergessen, sind alle Daten für immer verloren!
- *Filesystem type: „FAT“*
- Volume Format: Maus hin und her bewegen, dann *Format* anklicken – abwarten, es dauert ein bisschen. → OK → Exit
- Über *Select File* kann die verschlüsselte Datei nun angewählt und mittels *Mount* als ein Laufwerk (Zuordnung im oberen Feld) eingebunden werden.
- Download unter: [www.truecrypt.org/downloads](http://www.truecrypt.org/downloads)

## 8. E-Mail

- Öffne nur Anhänge, von denen du ganz sicher bist, dass du sie haben willst.
- Verwende ein gutes E-Mail-Programm, z.B. Thunderbird
- Lege dir zwei E-Mail-Adressen zu (privat/öffentlich).
- Verwende zum Lesen von E-Mails möglichst nur das Text- und nicht das HTML-Format.
- Versende Dokumente am besten nur im PDF-Format.

## 9. Software

Grundsätzlich sollte nur mit aktueller Software gearbeitet werden. Besonders wichtig ist es folgende Programme stets aktuell zu halten:

- Adobe Reader
- Flashplayer
- Java
- E-Mail-Programm (Thunderbird, Outlook...)
- Medienplayer (Mediaplayer, VLC...)
- Chatprogramme (MSN, ICQ...)