

Das Verbinden des Computers mit dem Netz erhöht die Risiken, die beim unvernetzten Bürocomputer nur bei der Nutzung von externen Datenträgern aus dubiosen Quellen bestanden:

Die Wahrscheinlichkeit, sich über E-Mail oder Internetnutzung Schädlinge (Viren, Spy- oder Hackerprogramme etc.) einzufangen, ist hoch nicht nur, weil es viel Müll gibt im WWW, sondern auch, weil dort viel kriminelle Energie aufgewendet wird, um an unsere Rechner (und oft auch an unser Geld) heran zu kommen.

Deshalb ein paar **Grundregeln** für ungetrübtes Mitmachen:

1. Der vernetzte Rechner benötigt ein leistungsfähiges **Schutzsystem**. Dies gibt es kostenlos (z. B. AntiVir 7 Classic); die besseren kosten eine jährliche Lizenzgebühr (Kaspersky steht in vielen Tests vorn und kostet jährlich ca. 30 Euro).
2. Dieser Schutz muss regelmäßig (am besten täglich) **aktualisiert** werden im Hinblick auf neu bekannt gewordene Schädlinge.  
Diese Aktualisierung erfolgt online, lässt sich automatisieren und ist bei schnellen DSL Leitungen (Flatrate!) eine Sache von Sekunden.
3. Die größte Gefahr geht vom E-Mail aus. Deshalb muss erstens ein „**Spamfilter**“ her, der unerwünschte Werbung gleich aussortiert, und zweitens allerhöchste **Sorgfalt und Disziplin** im Umgang mit E-Mail-Anhängen oder E-Mail-Links.  
Grundsätzlich sollte kein Anhang geöffnet und keinem Link gefolgt werden, wenn der E-Mail-Absender nicht bekannt und vertrauenswürdig ist.
4. Von Browsern und Mail-Programmen immer die **aktuellsten Versionen** nutzen.  
Derzeit hat (obwohl der Explorer aufgeholt hat) in den Augen der meisten Sachverständigen die Kombination Firefox/Thunderbird die Nase vorn.
5. Die von den Browsern als Standard empfohlene Sicherheitsstufe sollte nicht unterschritten werden.
6. Vorsicht mit den Keksen  
**Cookies** (Kekse) werden von Internetseiten, die Sie besucht haben, auf Ihrem Rechner abgelegt, damit der Seitenaufruf oder die Eingabe von Benutzerdaten bei erneutem Besuch der gleichen Seiten schneller vonstatten gehen. Wenn man z. B. im VDW-Vorstandszimmer mehrere Seiten nacheinander aufruft, dann bewirken Cookies, dass man sich nicht immer wieder neu einloggen muss.  
Das klingt nach mehr Komfort, hat jedoch durchaus seine Tücken, denn Anbieter von Internetseiten können z. B. mit Hilfe von Cookies von Ihren Besuchern Profile ermitteln und speichern. (Wenn Sie Amazon-Kunde sind und sich wundern, wie genau deren Empfehlungen auf Sie passen, dann stecken da Cookies hinter.)  
Den Umgang mit Cookies kann man im Browser einstellen. Sie können (Firefox: Extras/Einstellungen/Cookies) akzeptieren oder nicht, auf Anforderung akzeptieren oder akzeptieren bis der Browser geschlossen wird. Wenn Sie sehr restriktiv mit Cookies umgehen, sollten Sie vertrauenswürdige Seiten (wie [www.wachtelhund.de](http://www.wachtelhund.de)) als Ausnahme zulassen.

## 7. Cache, der Puffer-Speicher

Um den Aufbau komplexer Seiten zu beschleunigen, legen alle Browser besuchte Seiten oder Teile davon auf der Festplatte ab; das führt dann dazu, dass Sie bei zwischenzeitlich veränderten Seiten möglicherweise noch eine ältere Version angezeigt bekommen. Da helfen auch die Schalter „neu laden“ (Explorer) oder „aktualisieren“ (Firefox) wie auch die rechte Maustaste häufig nicht.

Was tun?

Im **Explorer** haben Sie die Möglichkeit, unter Extras/Internetoptionen/ Erweitert unter der Überschrift Sicherheit „leeren des Ordners temporary internet files beim Schließen“ zu aktivieren (das ist von Zeit zu Zeit ohnehin eine sinnvolle Maßnahme, weil dort auf die Dauer eine riesige Sammlung entsteht). Im **Firefox** können Sie über Extras/Einstellungen/Datenschutz den Cache löschen; das hat die gleiche Wirkung.

## 8. Die Stilfragen zum Schluss

Mit „**Netikette**“ (Kunstwort aus *Net* und *Etikette*) bezeichnet man einen - ungeschriebenen – Verhaltenskodex für die Netzkommunikation.

Auch wegen einiger Erfahrungen mit [www.wachtelhund.de](http://www.wachtelhund.de), aber unter Verzicht auf Beispiele, einige Hinweise:

- Wer in seinem Briefbogen, in beruflichen Zusammenhängen oder als Vereinsfunktionär eine E-Mail-Adresse veröffentlicht, muss auch sicherstellen, dass er auf diesem Weg **schnell erreichbar** ist.

- Das bedeutet erstens, dass der Rechner funktioniert, zweitens, dass der elektronische Briefkasten nicht verstopft ist und drittens, dass Mails mindestens täglich abgerufen werden.

- Anders als beim Postbrief ist mit dem E-Mail die Erwartung **kurzfristiger Beantwortung** verbunden. Wer sich also nicht in der Lage sieht, seine E-Mails umgehend oder innerhalb weniger Tage abzuarbeiten, sollte die Finger von dieser Kommunikationsform lassen.

- E-Mail-Sicherheit hat über den Schutz des eigenen Rechners hinaus noch einen anderen Aspekt: Nicht selten sind z. B. Outlook-Adressensammlungen Gegenstand von Spy-Attacken. Wer sich also mit seinem Rechner leichtfertig ungeschützt im Netz bewegt, riskiert auch, dass seine vielen, unter **Kontakte** abgelegten Freunde auf Verteilerlisten geraten, die Böses im Schilde führen.

- Weil wir auf Bildschirmen flüchtiger lesen und schreiben als auf Papier, ist die Sprache in Mails oder in Chats häufig irgendwas zwischen unabgewogen und ruppig. Die Qualität der Rechtschreibung ist signifikant geringer als bei anderen Texten.

Deshalb die Empfehlung: Beim Schreiben eher konservativ sein und beim Lesen duldsam und liberal.