

# Damit Privates privat bleibt

**Praktische Tipps:** So schützen Sie Ihre persönlichen Computerdaten

**Wer nicht vom Chef, von Bürokollegen oder kommerziellen Datenschnüfflern belauscht werden will, sollte E-Mails verschlüsseln, anonym surfen und die PC-Daten schützen.**

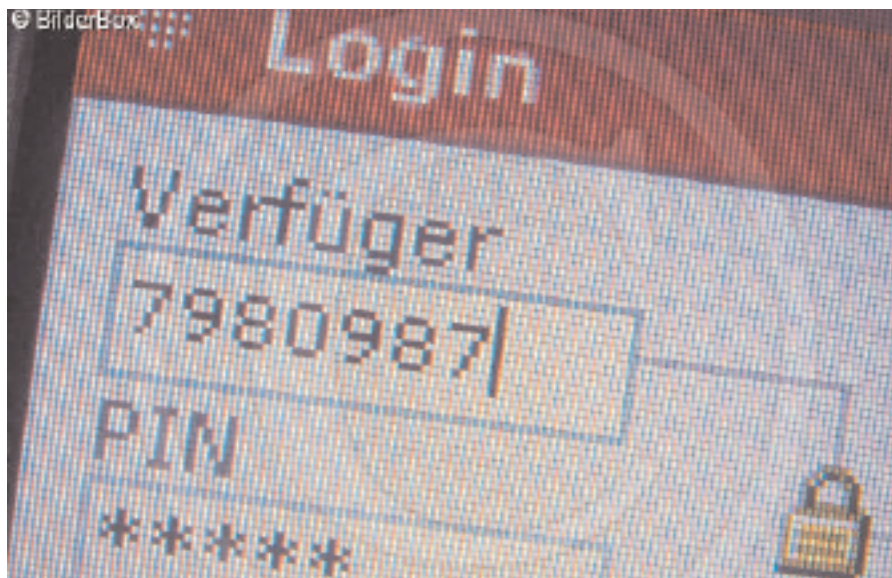
Kurt Haupt

redaktion@ktipp.ch

Der erste Angriff auf die Privatsphäre kann schon beim vermeintlich harmlosen Lesen von E-Mails erfolgen. Versender von kommerziellen Newslettern versuchen, vom Empfänger persönliche Informationen zu erschöpfeln. Zu diesen so genannten Webbugs und Schnüffelmails hat inzwischen der eidgenössische Datenschutzbeauftragte ein Merkblatt (<http://snurl.com/pst02>) verfasst.

Glücklicherweise alarmieren inzwischen moderne E-Mail-Programme, wie das kostenlose Mozilla Thunderbird ([www.mozilla.com/thunderbird/](http://www.mozilla.com/thunderbird/)), bei solchen Schnüffelversuchen.

**E-Mails verschlüsseln:** Zunehmend werden aber auch E-Mails von Firmen oder gar dem Staat überwacht. Wer vertraulich kommunizieren will, muss deshalb seine E-Mails verschlüsseln. Eine sichere und kostenlose Lösung für Windows bietet GNU-PGP ([www.gpg4win.org/index-de.html](http://www.gpg4win.org/index-de.html)). Bedienung und Installation sind allerdings anspruchsvoll, eine gute Einführung findet sich unter <http://kai.iks-jena.de/pgp/>.



**Sicheres Senden von Daten:** Nicht nur für Online-Banking, sondern auch bei Liebesbriefen

Einfacher geht die Verschlüsselung eines E-Mail-Textes mit Clip Secure (<http://snurl.com/pst01>). Nach dem Tippen der E-Mail klickt man auf das Clip-Secure-Symbol und wählt «Encrypt». Dann muss man ein Passwort eingeben und der Text wird damit verschlüsselt und gleich in der E-Mail ersetzt. Der Empfänger muss ebenfalls Clip Secure installieren und das Passwort kennen.

Mit Steganografie kann man eine vertrauliche Mitteilung sogar unbemerkt verschicken. Steganog (<http://www.gaijin.at/dlsteg.php>) versteckt Texte unsichtbar in einem beliebigen Digitalbild, was nur der Empfänger weiss. Er kann die Infos nach Passwordeingabe wieder aus dem Bild herausholen.

**«Toter Briefkasten»:** Die Mailüberwachung kann man auch umgehen, indem man die Mails gar nicht erst versendet. Die Kommunikationspartner teilen sich

dazu einfach eine Adresse bei einem Web-Mail-Anbieter. Die Meldungen werden aber nie verschickt, sondern einfach im Entwurfsordner hinterlegt und dort auch wieder gelesen. Dieser Trick ist sozusagen der «tote Briefkasten» im Internetzeitalter».

**Anonym surfen:** Will man einen solchen «toten Briefkasten» nutzen, sollte man natürlich anonym surfen. Denn normalerweise erfährt der Betreiber einer Website viel über einen Besucher.

Dies beweist eindrücklich die Site [www.yourip.de](http://www.yourip.de), die vom Browser übertragene Infos übersichtlich auflistet. Vor allem die IP-Adresse lässt einen direkten Rückschluss auf den Nutzer zu. Will man anonym surfen, kann man einen Anonymisierungsdienst wie JAP (<http://anon.inf.tu-dresden.de/>) verwenden. Der Dienst ist kostenlos und gilt als sicher. Bei der Suchmaschine Meta Crawler ([\[crawler.de\]\(http://crawler.de\)\) kann man Suchtreffer anonym besuchen. Kommerzielle Anbieter wie Megaproxy \(\[www.megaproxy.com\]\(http://www.megaproxy.com\)\) Steganos \(\[www.steganos.com\]\(http://www.steganos.com\)\) und Safersurf \(\[www.safersurf.com\]\(http://www.safersurf.com\)\) bieten mehr Tempo beim anonymen Surfen als die kostenlosen Alternativen.](http://www.meta</a></p>
</div>
<div data-bbox=)

Eine komplette Lösung für anonymes Surfen unterwegs bietet TorPark (<http://torpark.nfshost.com/>).

**Daten verschlüsseln:** Wer sicherstellen will, dass private Daten auf dem Büro-PC, Notebook oder Familienrechner vertraulich bleiben, sollte diese verschlüsseln. Nicht zu trauen ist den leicht zu knackenden Passwortfunktionen von Word oder Excel und Co.

Zuverlässig kann man einzelne Dateien mit Blowfish Advanced CS ([www.hotpixel.net/software.html](http://www.hotpixel.net/software.html)) verschlüsseln. Noch praktischer ist es, ein komplett verschlüsseltes Laufwerk (Container) zu haben. Die-

ses wird von allen Programmen wie eine normale zusätzliche Festplatte behandelt. Eine kostenlose, sichere Verschlüsselung für solche Container bietet das deutschsprachige True Crypt ([www.truecrypt.org](http://www.truecrypt.org)). ■

## PASSWÖRTER

### Zum Beispiel Meer3bälligOnfi

Die Sicherheit von Datenverschlüsselungen steht und fällt mit der Passwortvergabe. Passwörter sollten mindestens zwölf Zeichen lang sein und Sonderzeichen enthalten. Mundartaussprüche sind schwerer zu erraten als hochdeutsche Wörter. «Meer3bälligOnfi» ist also «Johannisbeergelee» vorzuziehen.

Entscheidend ist ferner auch, dass sich auf dem PC keine Schadprogramme befinden, die Tastatureingaben überwachen und so Passwörter aufzeichnen und übermitteln.

Windows-Systeme sind für solche Schädlinge sehr anfällig. Mehr Sicherheit bieten Live-CDs mit Linux, die beim Einschalten des Rechners gestartet werden. Schädlinge haben so keine Chance und die Live-CDs verändern auch keine Daten auf der Festplatte. Phantomix (<http://phantomix.ytternhagen.de/>) ist eine solche Live-CD, die bereits für anonymes Surfen vorkonfiguriert ist.