

PRAKTISCHE TIPPS ZUM DATENSCHUTZ

Veröffentlicht am 28. Januar 2013 von Annette

Heute ist europäischer Datenschutztag. Dieser geht auf den Jahrestag der Unterzeichnung der Europäischen Datenschutzkonvention [...]

Heute ist **europäischer Datenschutztag**. Dieser geht auf den Jahrestag der Unterzeichnung der Europäischen Datenschutzkonvention am 28.1.1981 zurück und wird dieses Jahr schon zum siebenten Mal begangen. Heute sollen Europäerinnen und Europäer besonders für den Datenschutz sensibilisiert werden. Wir leisten einen kleinen Beitrag und haben einige **Tipps** zusammen gestellt, mit denen Sie **Ihre persönliche Daten im Internet schützen** können.

Zuallererst sollte man sich fragen: **Was ist eigentlich Datenschutz** und warum ist er überhaupt wichtig? Der Begriff "Datenschutz" ist in den 60er-Jahren entstanden, als die Bundesregierung plante, jedem Bürger ein "Personenkennzeichen" zu verpassen und sämtliche verfügbaren Daten in einem zentralen System zu sammeln. Was damals noch verhindert wurde, ist heute bereits durch die lebenslange Steuernummer Realität. Dennoch wird Datenschutz seit dem Voranschreiten der digitalen Revolution viel diskutiert. Er bezeichnet das grundsätzliche Recht eines Menschen auf **informationelle Selbstbestimmung**, also das Recht, zu bestimmen, wie und wo seine Daten gespeichert und verwendet werden. Dies schützt uns nicht nur davor, "gläserne Menschen" zu werden, sondern auch vor Mißbrauch und Angriffen von Kriminellen.

Was kann man selbst für seinen Datenschutz tun?

1. Überlegen Sie zwei mal, was Sie im Internet preisgeben.

Vor allem Social Media laden dazu ein: Hemmungslos Informationen teilen, persönliche Mitteilungen machen, Fotos und Videos hochladen und anzeigen, wo man sich gerade befindet. Alles schön und gut, aber man sollte darauf achten, dass man solche Informationen nicht öffentlich zugänglich macht. Viele vergessen, dass alles über Suchmaschinen auffindbar ist. Und es ist nicht unwahrscheinlich, dass zum Beispiel ein zukünftiger Arbeitgeber danach sucht oder jemand veröffentlichte Handynummern oder gar Bankdaten missbraucht. In Sachen digitaler Offenherzigkeit gilt also häufig: weniger ist mehr.

2. Verwenden Sie mehrere E-Mail-Adressen.

Nutzen Sie nicht immer die gleiche E-Mail-Adresse für alles, was Sie im Internet tun. Man sollte insbesondere Privates und Berufliches strikt trennen und darauf achten, wo E-Mail-Adressen öffentlich einsehbar sind, zum Beispiel in sozialen Netzwerken oder Foren.

3. Vorsicht vor Spam und Phishing!

Reagieren Sie niemals auf Emails, in denen Sie aufgefordert werden, persönliche Daten oder Passwörter anzugeben. Auch, wenn der Absender Ihnen seriös erscheint, kann es sich hier um

kriminelle Absender handeln. Wer sich vor Werbe-E-mails, Werbepost und Werbeanrufen schützen möchte, dem sei übrigens die **Robinsonliste** ans Herz gelegt. Die Robinsonlisten sind Schutzlisten mit Kontaktdaten von Personen, die keine unaufgeforderte Werbung erhalten wollen, und sind in der Regel sehr effektiv.

4. Lesen Sie die AGB von Diensten, die Sie nutzen.

Kaum jemand tut es, aber man sollte es sich angewöhnen: die allgemeinen Geschäftsbedingungen lesen. Wichtig ist vor allem, ob man die Daten, die man zum Beispiel in einem Netzwerk eingibt, hinterher komplett wieder löschen kann. Geht das nicht, wird man vermutlich noch Jahre später über Suchmaschinen gefunden.

5. Meiden Sie unseriöse Gewinnspiele.

Gewinnspiele sind ein beliebter Köder, um an Daten zu kommen, die dann an Dritte weitergegeben werden. Lesen Sie sich die Datenschutzbestimmungen durch, bevor Sie teilnehmen und entscheiden Sie sich lieber dagegen, teilzunehmen, wenn Ihnen irgendetwas dubios vorkommt.

6. Surfen Sie sicher im Internet.

Achten Sie bei Ihrer täglichen Internet-Routine, aber vor allem beim Online Banking und Shopping auf sicheres Surfen. Hier sollte man nach anerkannten Gütesiegel und SSL-gesicherten Seiten Ausschau halten. Sensible Daten wie Bankdaten oder Passwörter sollten niemals auf unverschlüsselten Internetseiten eingegeben werden, da sonst jeder einfach mitlesen könnte. Wie Sie eine sichere Seite erkennen? Eine verschlüsselte Adresse beginnt mit „https“ statt mit „http“. Auch gilt: Regelmäßiges Löschen der Browser-Chronik sowie aller gespeicherten Formulare und Passwörter verhindert, dass die Daten ausgelesen werden können.

Wenn man all diese Tipps beherzigt, dürften die eigenen Daten sehr sicher sein, auch wenn man nie eine Garantie hat - schließlich entwickelt sich die Technik mit all ihren Möglichkeiten rasend schnell. Was tun Sie zusätzlich für den **Datenschutz**? Wir freuen uns über weitere Tipps!