

Schutz persönlicher Daten



Man sollte sich gut überlegen, welche Daten man im Internet über sich selbst teilt und auch wo genau man sie preisgibt. Kommen individuelle Informationen nämlich in die falschen Hände, kann es zu **Missbrauch der Daten** kommen, wie zum Beispiel zum Identitätsklau. Darum ist es wichtig auf die persönlichen Informationen aufzupassen. Oft sind zum Beispiel Online-Services an unseren Daten interessiert, um aufgrund unserer „Likes“ zu sehen was unsere Interessen sind. Diese Informationen erleichtern es den Konzernen personalisierte **Werbung** zu schicken, um mehr Gewinn zu machen. Das Problem daran ist: Je mehr Informationen wir online über uns preisgeben, desto genauer und zielgerichteter kann Werbung für uns gestaltet werden.

Zusätzlich darf nicht vergessen werden, dass Daten, die frei im Netz zugänglich sind, von jedem eingesehen und auch zurückverfolgt werden können. Darum sollte man nicht nur darauf achten, welche Informationen man online gibt, sondern auch welche Fotos man postet, wenn man nicht möchte, dass diese von jedem Menschen gesehen werden können.

Daten sind sehr vielfältig: Sie reichen von **privaten Daten**, wie Name und Adresse (=schutzbedürftige Daten), über weniger persönliche Angaben, wie das Lieblingsgericht oder die Lieblingsfarbe. Das Lieblingsgericht sagt nichts Spezifisches über eine Person aus und kann daher kaum missbräuchlich verwendet werden. Es ist aber schon problematisch, wenn eine fremde Person Zugriff auf den Namen und die Adresse hat, da es hierbei zu Identitätsklau oder anderem Datenmissbrauch kommen kann. Einem besonderen Schutz unterliegen die **sensiblen Daten**. Dazu gehören Informationen über die Gesundheit, die politische Einstellung, oder religiöse oder philosophische Überzeugungen. Diese Informationen sind sehr persönlich und sollten nicht in den öffentlichen Umlauf geraten.

Um im Internet möglichst sicher mit Daten umzugehen, könnten folgende Tipps helfen:

- Bei Registrierungen sollten **Nicknames anstatt echter Namen** benutzt werden.
- Die **Privatsphäre-Einstellungen auf sozialen Netzwerken**, oder auf Plattformen, auf denen man registriert ist, sollten immer wieder überprüft und gegebenenfalls geändert werden.
- Es sollte immer hinterfragt werden, **ob und wann es sinnvoll ist**, schutzbedürftige Daten anzugeben. Bestelle ich zum Beispiel ein Geschenk, macht es Sinn, die Adresse anzugeben, damit der/die Postausträger:in weiß, wohin das Paket geliefert werden muss. Fragt aber eine Spiele-App nach meiner Wohnadresse, ist dies sehr kritisch, da es keinen guten Grund gibt, wieso diese Information von der App benötigt wird.
- E-Mails, die **unbekannt sind oder fragwürdige Anhänge beinhalten**, sollten nicht aufgemacht werden. Dahinter könnte sich zum Beispiel eine Spionage-Software befinden, die die persönlichen Daten ausliest.
- Passwörter sollten sehr **sicher und geheim** gehalten sein.
- Für Registrierungen kann eine **zweite Email-Adresse** angelegt werden, die nicht den eigenen Namen verwendet.

