

Impressum

Herausgeber:
Initiative D21 e.V. und Bayerisches Staatsministerium
der Justiz und für Verbraucherschutz

Redaktion:
Martin Falenski (Initiative D21) – V.i.S.d.P.

Gestaltung:
Ulrike Miller, www.miller-partners.com

Kontakt:
Initiative D21, Reinhardtstraße 38, 10117 Berlin
kontakt@initiated21.de, www.initiated21.de

Bayerisches Staatsministerium der Justiz und für Verbraucherschutz
Prielmayerstraße 7, 80335 München
poststelle@stmjv.bayern.de, www.justiz.bayern.de

Bildnachweis:
dreamtimes.com
stockfoto.com

**Aufbruch
Bayern**

Google+



Bereits ein Jahr nach der Gründung 2011 soll Google+ nach eigenen Angaben 250 Millionen Nutzer haben. Ähnlich wie Facebook richtet sich das Netzwerk sowohl an Privatnutzer, als auch an Unternehmen. Auch ansonsten gibt es große Ähnlichkeiten zwischen den Netzwerken. So ist zum Beispiel der bekannte „Gefällt mir-Button“ bei Facebook der „+1“-Button bei Google. Anders als Facebook ist jedoch Google+ datenschutzfreundlicher konzipiert; die Einteilung in die sogenannten „Circles“ erlaubt eine einfachere Auswahl, was man mit wem teilen möchte. Dennoch sind auch hier einige Verhaltensregeln zu beachten, um die Vorteile des Sich-Vernetzens ungetrübt genießen zu können.

Sicherheitseinstellungen Google+

- ▶ Gefunden werden: Name und Profilbild sind immer für alle sichtbar. Alle anderen Bereiche sind durch den Nutzer anpassbar über „Profilsymbol“ -> „Profil bearbeiten“ -> „Über mich“ -> **entsprechenden Profibereich anklicken**.
- ▶ Festlegen, wer eigene Beiträge („Posts“) sehen kann: Mithilfe der Einstellungen zum Teilen lässt sich festlegen, ob man seine Bilder „öffentlich“ macht oder sie nur „erweiterten Kreisen“ beziehungsweise „eingeschränkt“ zugänglich macht. Die höchste Sicherheitsstufe hat die Option „nur für mich“.
- ▶ Nennungen von Personen auf einem Bild: Namensnennungen von Personen auf Bildern („Taggen“) aus den Kreisen eines Abgebildeten werden automatisch zugelassen, alle anderen bedürfen dessen Zustimmung. Wird diese verweigert, kann der Abgebildete auf diesem Bild nicht getaggt werden.

Ausführliche Informationen findet man im Hilfebereich von Google+ unter: <http://support.google.com/plus/?hl=de>

Weitere Netzwerke:

Es gibt noch eine Vielzahl weiterer sozialer Netzwerke. Oftmals sprechen diese eine bestimmte Zielgruppe an oder weisen bestimmte konkrete Funktionen auf. So richten sich etwa Xing und LinkedIn primär an Nutzer, die sich beruflich vernetzen wollen, StayFriends an Personen, die aufgrund gemeinsamer schulischer Erfahrungen in Kontakt bleiben wollen und die Dienste Twitter und Youtube an Nutzer, die sich in punkto gegenseitiger Unterrichtung und Versorgung mit Neuigkeiten miteinander verbinden möchten.



Diesen Diensten ist gemein, dass sie aufgrund ihrer Funktion oder ihrer Ausgestaltung keine so große Gefahr für eine umfassende Profilbildung oder -nutzung darstellen. Dies gilt erst recht, wenn sie kostenpflichtig sind. Nichtsdestotrotz ist auch hier Vorsicht geboten. Das Netz vergisst nichts, im Zweifel daher immer lieber weniger Informationen über sich preisgeben – und die zahlreichen Vorteile, die das Internet und das „Sich-Vernetzen“ bieten, auf Dauer ungetrübt genießen.

Gut zu wissen!

Sicher in sozialen Netzwerken



INITIATIVE D21

Bayerisches Staatsministerium der
Justiz und für Verbraucherschutz



Einführung



Soziale Netzwerke finden immer mehr Anhänger. Bis zu einer Milliarde Nutzer sollen mittlerweile Mitglieder bei Facebook, Google+ und Co. sein. Die meisten Angebote sind dabei – vermeintlich – kostenfrei. Man bezahlt jedoch mit seinen Daten. Viele Social-Networking-Geschäftsmodelle basieren auf der Verwertung der Daten ihrer Nutzer. Das geht von der einfachen Weitergabe an Dritte bis zur vollumfänglichen Profilbildung. Die Voreinstellungen sind oft auf die Weitergabe von Daten und die völlige Sichtbarkeit der Nutzer eingestellt. Wenn man aber einige Dinge berücksichtigt, dann kann man die Netzwerke sinnvoll nutzen und trotzdem auf der sicheren Seite sein. Eine kleine Hilfe soll Ihnen dabei dieser Flyer bieten!

Ihre Dr. Beate Merk MdL

Bayerische Staatsministerin der Justiz und für Verbraucherschutz

Überblick Gefahren durch soziale Netzwerke

Die Nutzung sozialer Netzwerke birgt eine Vielzahl von Gefahren. Wenn man nicht einige Sicherheitsvorkehrungen trifft, können Phishing, Mobbing, Stalking oder auch Probleme bei der Jobsuche die Folge sein.

- ▶ **Daten werden ohne ausdrückliches Einverständnis des Nutzers weitergegeben. Auch Daten nicht registrierter Nutzer werden von einigen Anbietern erfasst und verarbeitet.**
- ▶ **Mithilfe der Daten können umfangreiche Profile ohne Wissen der Nutzer erstellt werden. Oft auch mit dem „passendem“ Bild dazu.**
- ▶ **Daten sind unter Umständen auch für Dritte einsehbar.**



Checkliste

- ▶ **Geizen Sie mit Ihren Daten:** Nicht jeder muss alles über Sie wissen. Jede Angabe mehr erhöht die Gefahr, Opfer einer Phishing-Attacke oder eines Identitätsmissbrauchs zu werden.
- ▶ **Fügen Sie nur Personen, die Sie kennen oder die vertrauenswürdig sind, Ihrem Netzwerk hinzu.**
- ▶ **Melden Sie jede Form des Missbrauchs Ihrer Daten umgehend dem Betreiber.** Gleiches gilt für Mobbing- oder Stalking-Attacken.
- ▶ **Achten Sie darauf, was Sie in Ihrem Netzwerk posten. Auch Dritte können Kenntnis davon bekommen. Einmal eingestellte Informationen sind kaum wieder löschar.**
- ▶ **Klicken Sie nicht wahllos auf Links, auch wenn diese von Freunden/Kontakten kommen.** Oftmals werden Adressbücher oder Freundeslisten gehackt und für kriminelle Aktivitäten genutzt.
- ▶ **Prüfen Sie die AGB und die Datenschutzerklärung des Anbieters. Nicht selten räumt man diesem schon durch das Hochladen von Dateien umfangreiche Nutzungsrechte daran ein.**
- ▶ **Verwenden Sie sichere Passwörter (Tipp: Kombination aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen).**

Weiterführende Links/Infoseiten

- ▶ **www.bsi-fuer-buerger.de:** Infoseite des Bundesamtes für Sicherheit in der Informationstechnik über die Gefahren des Internets und wie man ihnen am besten begegnet.
- ▶ **www.vis.bayern.de:** Verbraucherportal der Bayerischen Staatsregierung zu allen wichtigen Verbrauchertemen wie zum Beispiel Rechte der Verbraucher. Die Sicherheit im Netz bildet im Bereich Daten und Medien einen eigenen Schwerpunkt.
- ▶ **www.bfdi.bund.de:** Webseite des Bundesdatenschutzbeauftragten mit zahlreichen Hinweisen rund um das Thema Datenschutz im Netz.
- ▶ **www.surfer-haben-rechte.de:** Aufklärungskampagne des Verbraucherzentrale Bundesverbandes (vzbv) mit dem Ziel, Verbraucher zu befähigen, sich sicher im Internet zu bewegen und aktiv zu partizipieren.
- ▶ **www.verbraucher-sicher-online.de:** Ein vom Bundesverbraucherschutzministerium gefördertes Projekt der TU Berlin mit dem Ziel, Verbraucher über die sichere Internetnutzung sowie den Zugang zu digitalen Inhalten verständlich zu informieren.



Facebook



Facebook ist mit großem Abstand Marktführer im Bereich Soziale Netzwerke. Zwar mahnen vor allem Datenschützer bei der Nutzung zur Vorsicht, aber gerade bei Jugendlichen gilt: Wer nicht dabei ist, ist „out“. Dabei geht gerade diese Zielgruppe oft leichtfertig mit ihren Daten um und gibt diese bedenkenlos frei. Und um möglichst viele „Freunde“ aufweisen zu können, akzeptieren sie oftmals jede Anfrage – ohne zu wissen, wer sich hinter „bubble 123“ verbirgt und vor allem was dieser Nutzer im Sinn hat.

Wie es auch anders geht, ohne dass man auf die Vorteile des social networking verzichten muss, erfahren Sie in kompakter Form hier:

Sicherheitseinstellungen bei Facebook

- ▶ **Gefunden werden:** Standardmäßig werden Facebookuser leicht gefunden. Die meisten Informationen wie Name, Geschlecht und Bild sind in der Grundeinstellung für alle sichtbar. Einstellung ändern: **Konto-Menü -> Privatsphäre-Einstellungen -> neben der Überschrift, „Funktionsweise von Verbindungen“ auf „Einstellungen bearbeiten“ klicken.**
- ▶ **Festlegen, wer eigene Beiträge („Posts“) sehen kann:** Grundsätzlich kann jeder Profilbesucher alles sehen, was im Profil bzw. auf der Pinnwand steht. Man kann aber zwischen den Optionen „Öffentlich“, „Freunde“ oder „nur ich“ wählen.
- ▶ **Nennungen von Personen auf einem Bild:** Welcher Nutzer sehen kann, dass eine Person auf einem Bild namentlich benannt wurde („Tagging“), richtet sich nach der eingestellten Publikumswahl. Wenn man die Markierung der eigenen Person durch einen anderen entfernen möchte und dieser sich weigert, dann muss man denjenigen in den Privatsphäre-Einstellungen blockieren.

Ausführliche Informationen findet man im Hilfebereich von Facebook unter www.facebook.com/help.