

FACEBOOK, MYSPACE & CO

Soziale Netzwerke im Internet, Analyse und Tipps

Daniela Zimmer (Konzept)

Österreichisches Institut für angewandte Telekommunikation (Durchführung)

Kammer für Arbeiter
und Angestellte für Wien

Wien, Mai 2009



WIEN

Arbeiterkammer Wien
Prinz-Eugen-Straße 20-22
A-1041 Wien
Tel: ++43-1-501 65/2144 DW
E-Mail: konsumentenpolitik@akwien.at
29/2009
Mai 2009

Inhalt

1.	Faszination „Soziale Netzwerke“	4
1.1.	Vier gute Gründe Soziale Netzwerke zu nutzen.....	4
1.2.	Welche Plattformen gibt es?	6
2.	Das Geschäft mit den Sozialen Netzwerken	9
3.	Herausforderung - Schutz der Privatsphäre.....	11
3.1.	Warum ist es wichtig, die eigene Privatsphäre zu schützen?.....	11
3.2.	Datenschutz und Kinder.....	12
3.3.	Ihre Rechte.....	13
4.	Soziale Netzwerke sicher nutzen	16
4.1.	So schützen sie Ihre Privatsphäre.....	16
4.1.1.	Bevor Sie ein Profil anlegen.....	16
4.1.2.	Nach der Anmeldung	18
4.1.3.	Während Sie Soziale Netzwerke nutzen.....	20
4.1.4.	Wenn Sie nicht mehr aktiv sind	22
4.2.	So schützen Sie sich vor Belästigung und Cyber-Mobbing	24
4.3.	Urheberrechte berücksichtigen.....	25
5.	Tipps für Eltern.....	27

Anmerkung: Stand der in dieser Broschüre angeführten Informationen und Tipps ist April 2009.

Einleitung

Soziale Netzwerke wie Facebook, MySpace & Co zählen zu den aktuellen Erfolgsgeschichten im Internet. Facebook hat es mittlerweile in Österreich auf Platz 4 der beliebtesten Websites geschafft. Die Frage „Sind Sie auch auf Facebook?“ ist Ihnen wahrscheinlich nicht fremd.

Kein Wunder, bieten diese Plattformen doch faszinierende Möglichkeiten: Online Kontakte pflegen, sich im Netz präsentieren und der einfache Austausch von Fotos und Videos sind ja auch wirklich gute Gründe in die Welt der Online-Communitys einzutauchen.

Andererseits: Haben Sie auch schon einmal ein ungutes Gefühl gehabt, wenn Sie private Daten online stellen? So geht es vielen, denn das Gedächtnis des Internet ist lang und einmal veröffentlichtes ist oft nur noch schwer zu entfernen.

Bei der Nutzung von Sozialen Netzwerke befindet man sich also häufig in einem Spannungsfeld: Die Verwendung von Facebook, MySpace & Co macht nur Sinn, wenn man etwas von sich preisgibt. Umgekehrt kann allzu große Freizügigkeit unangenehme Folgen haben.

Der Schutz der Privatsphäre ist also „die“ Herausforderung in Zeiten des online Netzwerkens. Freilich betrifft das nicht nur das eigene Nutzungsverhalten, sondern vor allem auch die Plattform-Betreiber: Welche Schutzmöglichkeiten bieten sie an und wie gehen sie mit den Ihnen anvertrauten Daten um?

Mit der vorliegenden Broschüre wollen wir Ihnen eine Unterstützung anbieten, die großartigen Möglichkeiten der Online-Communitys nutzen und gleichzeitig Risiken möglichst vermeiden zu können.

Die wichtigsten Tipps auf einen Blick: So nutzen Sie Soziale Netzwerke sicher

- Veröffentlichen Sie so **wenige Daten wie möglich** und machen Sie sich mögliche Risiken vor der Veröffentlichung bewusst.
- Nutzen Sie **Einstellungen zum Schutz der Privatsphäre**: Wer darf was einsehen und ist es Suchmaschinen erlaubt auf mein Profil zugreifen?
- **Trennen Sie Berufliches und Privates.**
- Verwenden Sie **sichere Passwörter**, damit nicht Unbefugte plötzlich in Ihrem Namen auftreten.
- **Löschen Sie Ihr Profil**, sobald Sie Ihren Auftritt in einem Sozialen Netzwerk nicht mehr pflegen möchten.
- Akzeptieren Sie **nur bekannte Personen als „Freunde“**.
- Veröffentlichen Sie **keine Bilder, auf denen Sie oder Dritte nachteilig dargestellt sind**.
- Veröffentlichen Sie Musik, Videos und Fotos nur, wenn Sie die **Zustimmung der UrheberInnen** besitzen.
- Verwenden Sie **Virenschutz-Programme** und aktualisieren Sie diese regelmäßig.

1. Faszination „Soziale Netzwerke“

Web 2.0, oft auch als „Mitmach-Web“ bezeichnet, hat sich in den vergangenen Jahren zu einem wichtigen Bestandteil des Internets entwickelt. Das Besondere daran: NutzerInnen stellen Inhalte selbst online – und das mit relativ geringem Aufwand. Ob Blogs oder Foren, Foto- oder Videoplattformen, oder Soziale Netzwerke – sie alle bieten die Möglichkeit sich zu präsentieren und neue Freunde oder Gleichgesinnte kennenzulernen. Vor allem Soziale Netzwerke wie *Facebook*, *MySpace* & Co erfreuen sich zunehmender Beliebtheit und haben sich zum Motor des Trends Web 2.0 entwickelt. Eigentlich wenig überraschend, handelt es sich beim Gemeinschaftsgefühl ja um ein menschliches Grundbedürfnis, das auch in der virtuellen Welt erfüllt werden will.

Allein in Europa nutzten im Jahr 2008 42 Millionen Menschen regelmäßig Soziale Netzwerke und mit jedem Tag werden es weltweit 250.000 mehr. Der Hype rund um die Sozialen Netzwerke hat natürlich auch längst Österreich erreicht: Mittlerweile zählen *Youtube*, *Facebook*, *MySpace*, *Netlog* und *StudiVZ* hierzulande zu den 20 meistbesuchten Internetseiten. Die einstigen Spitzenreiter bei den Besucherzahlen, Orf.at und Wikipedia, wurden in Österreich bereits von *Facebook* überholt.¹

Info: Soziale Netzwerke - so funktioniert's

Sie melden sich auf einer Plattform an, füllen ein so genanntes „Profil“ mit ihren persönlichen Daten aus und schon kann es losgehen: Fotos und Videos online stellen, einen eigenen Blog verfassen oder andere kommentieren und neue oder auch „alte“ „Freunde“ im Netzwerk finden.

Darin liegt auch das Besondere der Sozialen Netzwerke: Indem Sie ihr Profil mit dem anderer TeilnehmerInnen verknüpfen, sammeln sie „Freunde“, die wiederum selbst mit anderen „Freunden“ verknüpft sind. Dadurch entsteht schließlich ein riesiges Netzwerk von Beziehungen, das schon innerhalb kurzer Zeit die ganze Welt umspannen kann.

1.1. Vier gute Gründe Soziale Netzwerke zu nutzen

1. Kontakte pflegen

Mit Menschen, von denen man schon seit Jahren nichts mehr gehört hat, in Verbindung zu treten oder sich einfach mit FreundInnen, Verwandten, und GeschäftspartnerInnen auszutauschen, machen Soziale Netzwerke besonders interessant. Unterstützt wird diese Kommunikation von einer Vielzahl an Features:

- **Interne Nachrichtenfunktionen:** Diese lösen oft herkömmliche E-Mail-Programme ab.

¹ Quellen: http://ec.europa.eu/information_society/activities/social_networking/facts/index_en.htm und Alexa.com Pageranking Österreich

- **Statusmeldungen:** In kurzen Sätzen teilen Sie Ihren virtuellen „Freunden“ aktuelle Tätigkeiten, Gedanken oder Befindlichkeiten mit. Meldungen wie, „Max Meier ist sauer, weil es schon wieder regnet“ oder „Maria Mustermann geht jetzt schlafen“ scheinen einerseits trivial. Andererseits sind sie Ausdruck des Miteinanderlebens im virtuellen Raum. Schließlich spielen Small-Talk und Tratsch auch bei Treffen in der realen Welt eine wichtige Rolle.
- **Gästebucheinträge:** Auf den meisten Plattformen können Sie Fotos, Videos oder Statusmeldungen ihrer Freunde, sowie deren Profile kommentieren.

2. Neue Personen kennenlernen

Soziale Netzwerke sind auch die idealen Orte, um neue Personen kennenzulernen, mit denen Sie z. B. ähnliche Interessen teilen. Dies können „Freunde“ von „Freunden“ sein oder aber auch potenzielle neue GeschäftspartnerInnen.

Info: Der virtuelle Freundeskreis

In Sozialen Netzwerken erfährt der Begriff „Freund“ eine ganz neue Bedeutung. Alle können „Freunde“ werden, die einem eine Verlinkung im Netzwerk anbieten. „Freunde“, so formuliert es ein begeisterter *Facebook*-Nutzer, „sind alle, die nicht meine Feinde sind.“

Die Anzahl der „Freunde“ gilt als Indikator für die Verankerung in der jeweiligen virtuellen Gemeinschaft. So wird in Business-Netzwerken genau beobachtet, wer mit wem vernetzt ist und unter Jugendlichen ein regelrechter Wettbewerb betrieben, wer die meisten „Freunde“ besitzt.

3. Sich selbst präsentieren

Die Videoplattform *YouTube* trifft mit dem Slogan „Broadcast yourself“ den Hype um die Online Communitys auf den Punkt. In einer Zeit, in der das Internet einen wichtigen Stellenwert im Alltag vieler Menschen einnimmt, will man sich natürlich auch online entsprechend präsentieren.

Besonders junge Menschen wetteifern häufig mit Gleichaltrigen um das tollste Profil oder die meisten „Freunde“.

Die Motivation in Business-Netzwerken ist eine ähnliche: Wie kann man eigene Kompetenzen oder Produkte am besten für mögliche ArbeitgeberInnen oder KundInnen präsentieren?

4. Alternative zur eigenen Website

Online-Communitys sind „die“ Alternative zur eigenen Website. Ein eigenes Profil bei Facebook & Co zu erstellen ist um vieles einfacher, als eine eigene Website zu programmieren. Die Plattformbetreiber stellen dafür ein umfangreiches Angebot an Funktionen zu Verfügung: So ist es beispielsweise in den meisten Netzwerken ganz unkompliziert eigene Foto- und Videogalerien einzurichten.

1.2. Welche Plattformen gibt es?

Das Angebot an Sozialen Netzwerken ist mittlerweile sehr umfangreich. Nach der Ausrichtung der Communitys kann unterschieden werden in:

- **Allgemeine Soziale Netzwerke** („die Generalisten“): Dazu zählen *Facebook*, *MySpace*, *Netlog*, *StudiVZ*, *Szene1.at*
- **Inhalts-Plattformen**: NutzerInnen laden auf diesen Plattformen Videos oder Fotos hoch bzw. schauen sich diese an. Die wichtigsten Vertreter sind *YouTube* und *Flickr!*.
- **Business-Netzwerke**: Hier steht der berufliche Austausch im Mittelpunkt. Im deutschsprachigen Raum ist *Xing* sehr beliebt, im englischsprachigen *LinkedIn*.

Neben diesen drei Hauptgruppen gibt es zudem eigene **Netzwerke für bestimmte Zielgruppen**: Jugendliche vernetzen sich beispielsweise auf *SchülerVZ* und für SeniorInnen wurde mit *Seniorkom.at* ein eigenes Netzwerk geschaffen.

Auch sogenannte **Micro-Blogging-Plattformen** und **virtuelle Welten** gelten als Soziale Netzwerke. Auf *Twitter*, *Identi.ca* und ähnlichen Plattformen verfassen NutzerInnen Micro-Blogs – das sind kurze, SMS-ähnliche Mitteilungen. Diese kurzen Botschaften sind entweder nur für einen bestimmten Personenkreis (FreundInnen, ArbeitskollegInnen) oder öffentlich für alle InternetnutzerInnen zugänglich. In virtuellen Welten hingegen, bewegen sich NutzerInnen durch digital animierte Landschaften und können in diesen miteinander kommunizieren. Die bekanntesten Beispiele sind *Second Life* und, speziell für Kinder, *Habbo Hotel*.

Trend: Gründen Sie Ihr eigenes Netzwerk

Seit der Entstehung der Sozialen Netzwerke haben sich auch Anbieter etabliert, die es ihren NutzerInnen ermöglichen, ein eigenes Netzwerk zu gründen. Firmen wie Ning stellen dafür die entsprechende Software und den Webspaces zur Verfügung.

So entstehen etliche Gruppen, die auf Basis gemeinsamer beruflicher Interessen, persönlicher Vorlieben oder Hobbys zusammenfinden. Fans der deutschen Band Tokio Hotel treffen sich auf <http://tokiohotelofficial.ning.com>, E-Learning Lehrende tauschen ihre Erfahrungen in *classroom2.0* (www.classroom20.com) aus und JungunternehmerInnen organisieren sich auf *Sta.r tup.biz* (<http://sta.r tup.biz/>).

Hier finden Sie kurze Beschreibungen der in Österreich am häufigsten genutzten Sozialen Netzwerke:

Facebook

Rund 70 Millionen NutzerInnen sind jedes Monat weltweit auf Facebook aktiv. 200 Millionen sind, nach Angaben der Betreiber, angemeldet und nützen das Angebot. Damit ist *Facebook* weltweit das größte Soziale Netzwerk.

The Facebook logo, consisting of the word "facebook" in white lowercase letters on a blue rectangular background.

Genutzt wird *Facebook* vor allem für den direkten Austausch zwischen Personen, die einander auch im realen Leben kennen: Von großem Interesse sind daher der aktuelle Status und die Aktivitäten im Netz oder in den Themen-Gruppen. Der amerikanische Präsidentschaftswahlkampf 2009 hat jedoch recht eindrucksvoll gezeigt, dass *Facebook* auch erfolgreich für ganz andere Zwecke genutzt werden kann: Barack Obama nutzte *Facebook* als virtuelle Wahlkampfbühne und versuchte auf diese Weise auch online Wählerstimmen für sich zu gewinnen.

Die Plattform spricht tendenziell eher Erwachsene oder ältere Jugendliche an.

Kritisiert wird *Facebook* immer wieder für seine Datenschutzpolitik. Umstritten sind vor allem die umfassenden Verwertungsrechte an den NutzerInnen-Profilen und unangekündigte Änderungen der Geschäftsbedingungen.

MySpace

MySpace wurde ursprünglich für den Austausch von Musik entwickelt. Zwar präsentieren sich hier auch heute noch Nachwuchs-Bands und verbreiten ihre Musik, das Netzwerk hat sich mittlerweile aber für alle Zielgruppen geöffnet. Lange Zeit war *MySpace* das am weitesten verbreitete Netzwerk.



Derzeit wird es in Österreich besonders von den 13-16 Jährigen geschätzt. Ein Grund für die Beliebtheit innerhalb dieser jungen Zielgruppe liegt wohl auch darin, dass *MySpace* individuelle Gestaltungsmöglichkeiten der eigenen Website anbietet. Man geht von rund 40 Millionen aktiven NutzerInnen pro Monat aus, Aussagen des Betreibers zufolge sind 260 Millionen NutzerInnen registriert.

Netlog

Netlog ist ein europäisches Netzwerk, dessen Zielgruppe hauptsächlich Jugendliche sind. Hier können sie sich mit ihren Freunden austauschen, neue Freunde suchen, miteinander chatten oder Bilder austauschen. Das Netzwerk hat nach eigenen Angaben 42 Millionen Mitglieder, davon knappe drei Millionen im deutschsprachigen Raum.

The Netlog logo, consisting of the word "NETLOG" in bold, red, uppercase letters.

StudiVZ, SchülerVZ, meinVZ

StudiVZ und *SchülerVZ* sind Netzwerke für StudentInnen und SchülerInnen. *meinVZ* bietet den gleichen Service, aber ohne die Voraussetzung StudentIn oder SchülerIn sein zu müssen. Hier liegt der Schwerpunkt, neben dem Vernetzen, in der konkreten Zusammenarbeit, beispielsweise im Zusammenhang mit



Lehrveranstaltungen. Über zwölf Millionen aktive NutzerInnen sind nach eigenen Angaben auf diesen drei Plattformen registriert.

Szene1.at

Szene1.at ist das größte österreichische Party-Netzwerk. Auf dieser Plattform finden sich nicht nur die nächsten Partytermine, sondern auch Fotos, die auf eben diesen Partys geschossen wurden. Dabei sind nicht nur professionelle FotografInnen für Szene1.at unterwegs, jede/r kann entsprechende Partyfotos auf dieser Plattform veröffentlichen. Mit über 400.000 aktiven Mitgliedern ist Szene1.at – nach eigenen Angaben – eines der größten österreichischen Netzwerke und expandiert auch ins Ausland.



Xing

Während die bisher genannten Netzwerke sich nicht durch Beiträge der NutzerInnen sondern durch Werbung finanzieren, geht Xing in diesem Zusammenhang einen anderen Weg. Die Business-Plattform bietet, neben einem eingeschränkten kostenlosen Zugang, auch kostenpflichtige Nutzungsangebote mit Zusatzfunktionen. Ziel dieses Netzwerkes, das aus dem deutschen Sprachraum stammt, ist das Aufbauen und Aufrechterhalten von Geschäftskontakten. Dies reicht vom fachlichen Austausch innerhalb von Gruppen bis hin zur Suche nach neuen Geschäftsbeziehungen. Xing hat laut eigenen Angaben sieben Millionen Mitglieder davon drei Millionen im deutschsprachigen Raum.



Checklist: Wie wähle ich ein Soziales Netzwerk aus?

Folgende Fragen erleichtern Ihnen die Auswahl einer passenden Plattform:

- Was will ich in dem Netzwerk hauptsächlich machen?
 - FreundInnen finden bzw. mit FreundInnen in Kontakt bleiben → *Facebook, Netlog, StudiVZ, SchülerVZ* bzw. *MeinVZ*
 - Inhalte wie Videos oder Fotos veröffentlichen → *Flickr!, Youtube*
 - Geschäftskontakte pflegen → *Xing*
- Wo sind die meisten meiner FreundInnen, Bekannten oder ArbeitskollegInnen bereits registriert?
- Gehöre ich einer bestimmten Zielgruppe (Kinder/Senioren) an, für die es eigene Netzwerke gibt? → *SchülerVZ, Seniorskom.at*
- Unterstützen die Anbieter ausreichend den Schutz der Privatsphäre? → Studien, wie die des Frauenhofer-Instituts über Privatsphärenschutz in Sozialen Netzwerken, unterstützen Sie bei der Auswahl nach diesem Kriterium. Aktuelle Untersuchungen finden Sie zum Beispiel auf <http://www.saferinternet.at/themen/soziale-netzwerke/>

2. Das Geschäft mit den Sozialen Netzwerken

Die hohen Nutzungszahlen von Sozialen Netzwerken und der hohe Marktwert bei Unternehmens-Beteiligungen (z. B. zahlte Microsoft 2008 für eine 1,6-Prozent-Beteiligung an Facebook 240 Millionen US-Dollar²) lassen vermuten, dass der Betrieb von Sozialen Netzwerken ein sehr lukratives Geschäft ist. Bis jetzt ist es den meisten Plattformbetreibern aber noch nicht gelungen, ein richtig profitables Geschäftsmodell zu entwickeln. Die derzeit gängigsten Ansätze um Einkünfte zu erzielen sind:

- **Personalisierte Werbung:** Soziale Netzwerke eignen sich aufgrund der zahlreichen verfügbaren Informationen über Interessen und Bedürfnisse der NutzerInnen besonders gut für personalisierte Werbung. Von diesen individualisierten Werbeeinschaltungen erhoffen sich Unternehmen eine höhere Wirksamkeit.
- **Kostenpflichtige Features:** NutzerInnen erhalten einen kostenlosen Zugang zu einem Netzwerk mit den Basisfunktionalitäten – für darüber hinausgehende Anwendungen fällt z. B. eine monatliche Gebühr an.
- **Gesponserte Profile und Gruppen:** Unternehmen zahlen immer häufiger für die Einrichtung spezieller Profile und Gruppen, um so ihre Produkte und Marken zu promoten.
- **„Third-Party“-Anwendungen:** In manchen Sozialen Netzwerken bieten externe Unternehmen zusätzliche Features an (z. B. Geburtstagskalender, Spiele, Tests etc.). Bei *Facebook* etwa werden diese als „Anwendungen“ bezeichnet und bei *MySpace* als „Widgets“. Es ist davon auszugehen, dass externe Anbieter solcher Programme dafür eine Gebühr an die Netzwerk-Betreiber zu entrichten haben. Als Gegenleistung können die Unternehmen NutzerInnen-Daten sammeln – allerdings nicht nur von Ihrem Profil sondern auch von den Profilen all Ihrer „Freunde“.



Abb: *Facebook* macht auf die Einbindung Dritter bei Anwendungen aufmerksam (Quelle: www.facebook.com)

² Heise online: Microsoft kauft sich bei Social-Networking-Site Facebook ein: www.heise.de/newsticker/Microsoft-kauft-sich-bei-Social-Networking-Site-Facebook-ein--/meldung/97934

- **Marktforschung:** Die großen Mengen an NutzerInnen-Daten sind auch für Marktforschungsunternehmen von großem Interesse, da die Profile sehr viel über die Gewohnheiten und Vorlieben der AnwenderInnen verraten. Über die tatsächliche Nutzung dieser Einnahmequelle ist aber derzeit wenig bekannt.
- **Gewinnbringender Verkauf:** Die weitverbreitete Annahme, dass die Plattformen eines Tages mit hohen Gewinnen betrieben werden können, nährt die Hoffnung vieler Betreiber auf einen gewinnbringenden Verkauf des Netzwerks.

3. Herausforderung - Schutz der Privatsphäre

Soziale Netzwerke setzen die Veröffentlichung von Informationen zur eigenen Person voraus. Ihre Nutzung befindet sich daher automatisch in einem **Spannungsfeld zwischen öffentlicher Präsentation und dem Schutz der Privatsphäre**.

Dass AnwenderInnen ihre Privatsphäre den eigenen Anforderungen entsprechend schützen können, liegt zum einen in ihrer eigenen Verantwortung und zum anderen in der Verantwortung der Netzwerk-Anbieter. Für NutzerInnen ist es daher wichtig, sich der Risiken einer Verletzung der Privatsphäre bewusst zu sein und kritisch mit persönlichen Daten umzugehen. Betreiber wiederum sind gefordert, Einstellungen zum Schutz der Privatsphäre anzubieten und die Datenschutz-Bestimmungen verlässlich einzuhalten.

3.1. Warum ist es wichtig, die eigene Privatsphäre zu schützen?

Der Forderung nach einem besseren Schutz der Privatsphäre wird häufig mit dem Argument begegnet „wer nichts angestellt hat, muss auch nichts verbergen“. Dem ist leicht zu entgegenen: Der Schutz der Privatsphäre stellt einen Wert an sich dar und ist ein verfassungsmäßig zugesichertes Recht. Abgesehen davon sind sich viele NutzerInnen nicht über die möglichen Konsequenzen der Preisgabe persönlicher, auf den ersten Blick vielleicht unkritischer Daten, bewusst.

Gründe, warum es sich lohnt, vorsichtig mit persönlichen Daten umzugehen:

- Etwas worauf Sie heute stolz sind, kann Ihnen in einigen Jahren sehr unangenehm oder peinlich sein. Das Internet vergisst nicht. Einmal veröffentlichte Daten sind oft nicht mehr zu entfernen. Denken Sie z. B. an Partyfotos, die bei der Jobsuche ein ungünstiges Licht auf Sie werfen könnten.
- Das Publikum im Internet ist potenziell ein sehr Großes. Bedenken Sie, dass Ihre Daten nicht nur Ihre Freunde, sondern auch Ihnen unbekannte oder weniger gut gesonnene Personen einsehen können.
- Fühlen Sie sich wohl bei dem Gedanken, dass Ihre Geschäftspartner und Bekannten sich mithilfe Ihrer Angaben zu Interessen, Hobbys, Vorlieben, Freunden, politischer Meinung etc. ein umfassendes aber gleichzeitig einseitiges Bild von Ihrer Person bilden können?
- Auch Datensicherheit ist ein großes Thema: Immer wieder tauchen Meldungen über Pannen auf, durch die der unerlaubte Zugriff Dritter auf NutzerInnendaten in Sozialen Netzwerken möglich wurde. So konnten die Foto-Sammlungen von tausenden *MySpace*-NutzerInnen über Tauschbörsen heruntergeladen oder Userprofile von *Facebook* gekauft werden. Im Februar 2007 wurden bei einem Hackerangriff auf *StudiVZ* E-Mail-Adressen und Zugangsdaten ausgelesen.

Wie wichtig der Schutz der Privatsphäre ist, illustrieren auch folgende Beispiele:

Nach einer Party laden Sie Fotos auf eine Website. Einige Bilder zeigen Sie im angetrunkenen Zustand. Ein paar Wochen später bewerben Sie sich für einen neuen Job. Zuvor durchsuchen Sie das Internet nach Angaben zu Ihrer Person, die sich nachteilig auf Ihre Bewerbung auswirken könnten. Dabei stoßen Sie auch auf die Partyfotos. Die Bilder von Ihrer eigenen Website zu entfernen ist kein Problem. Leider müssen Sie jedoch feststellen, dass andere Partyteilnehmer die Fotos bereits kopiert und an anderer Stelle ebenfalls veröffentlicht haben. Sämtliche Kopien zu entfernen ist in der Praxis oft kaum möglich.

Informationen, die von Ihnen in Soziale Netzwerke gestellt werden, können auch Rückschlüsse auf ihre Adresse und Telefonnummer erlauben. Dies kann besonders im Falle von Cyber-Stalking problematisch werden. Immer wieder passiert es, dass aus einer Belästigung in der virtuellen Welt, ein Nachstellen in der realen Welt wird.

Auch gibt es immer wieder Berichte von Menschen deren Daten kopiert und auf anderen Seiten veröffentlicht wurden. Beispielsweise Strand-Fotos, die samt Telefonnummer auf eine Sex-Dating-Seite gestellt wurden. Außerdem können Sie mit einem allzu offenen Umgang mit Privat-Informationen Kriminellen ungewollt Hinweise geben: Wenn Sie z. B. in Ihrem Profil Anhaltspunkte liefern, von wann bis wann Sie auf Urlaub sind, kann diese Information verwendet werden, um bei Ihnen einen Einbruch zu planen.

Tipp: Vorsichtiger Umgang mit privaten Informationen

Sie vermeiden unangenehme Situationen, wenn Sie sich vor einer Veröffentlichung von privaten Informationen, Fotos etc. folgende Fragen stellen:

- Könnte jemand diese Angaben gegen mich oder zu meinem Nachteil verwenden?
- Könnten mir die privaten Informationen zu einem späteren Zeitpunkt peinlich oder unangenehm sein?
- Bin ich damit einverstanden, dass mein derzeitiger oder zukünftiger Arbeitgeber, Geschäftspartner etc. diese Informationen sieht?
- Könnte eine Veröffentlichung für eine andere Person Nachteile zur Folge haben?

3.2. Datenschutz und Kinder

Kinder tun sich oft sehr schwer, den Wert ihrer persönlichen Daten richtig einzuschätzen. Sie übersehen, dass nicht nur ihre FreundInnen und SchulkollegInnen ihre ins Netz gestellten Daten einsehen können, sondern im Prinzip alle Personen im Internet. Eltern sind daher gefordert, ihre Kinder über unangenehme Folgen zu informieren und ihnen Tipps zur sicheren Handhabung der persönlichen Daten zu geben.

Die bedeutenden Sozialen Netzwerke Europas (u.a. *Facebook, MySpace, Netlog, StudiVZ*) haben im Februar 2009, im Rahmen einer EU-Richtlinie, eine Selbstverpflichtungserklärung für den besseren Schutz von Kindern innerhalb ihrer Plattformen unterzeichnet³. In dieser

³ http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm

Erklärung verpflichten sie sich unter anderem, ihre Datenschutzeinstellungen zu verbessern und Funktionen zur Prävention und Verfolgung von Verstößen in ihren Netzwerken bereitzustellen.

Im Sinne des Jugendschutzes sind Anmeldungen für Jugendliche bei Sozialen Netzwerken erst ab einem bestimmten Alter möglich. Auf den meisten Plattformen ist das Mindestalter 13 Jahre (*MySpace, Facebook, Netlog*, 12 Jahre auf *SchülerVZ*), auf *Szene1.at* können sich unter 18-Jährige nur mit Zustimmung ihrer Eltern anmelden und auf *Xing* ist Volljährigkeit die Voraussetzung zur Anmeldung. In vielen Nutzungsbestimmungen wird auch darauf hingewiesen, dass alle Angaben wahrheitsgetreu gemacht werden müssen. Es ist jedoch nicht bekannt, ob das Alter auch tatsächlich jemals, z.B. durch Vorlage einer Ausweiskopie, überprüft wird.

3.3. Ihre Rechte

Wenn Sie sich auf einer Internet-Plattform anmelden und die Allgemeinen Geschäftsbedingungen (AGB) akzeptieren, schließen Sie formell gesehen einen Vertrag ab. Das heißt, Sie haben bestimmte Rechte und Pflichten. Zu Ihren Pflichten gehören zum Beispiel meistens, dass Sie sich mit korrekten Angaben anmelden, dass Sie ein Mindestalter haben, dass Sie keine rechtswidrigen Inhalte verbreiten etc. Umgekehrt haben Sie gegenüber dem Betreiber eine Reihe an Rechten, gerade was den Schutz Ihrer Daten betrifft.

Ihre Ansprüche nach österreichischem **Datenschutzrecht** sind:

1. Recht auf Verwendung für den vereinbarten Zweck

Sie haben das Recht, dass Ihre Daten ausschließlich für den vereinbarten Zweck verarbeitet bzw. nur an Dritte weitergegeben werden, wenn Sie dafür Ihre Zustimmung gegeben haben. Diese Vereinbarung bzw. Zustimmung kann zum Beispiel erfolgen, in dem Sie bei der Anmeldung die Allgemeinen Geschäftsbedingungen akzeptieren.

2. Recht auf Auskunft:

Sie haben das Recht einmal pro Jahr kostenlos beim Betreiber Auskunft einzuholen, welche personenbezogenen Daten zu Ihrer Person verarbeitet werden.

3. Recht auf Richtigstellung oder Löschung:

Sie haben das Recht auf Richtigstellung oder Löschung der über Sie gespeicherten Daten.

Prinzipiell betreffen diese Rechte sowohl die Daten, die Sie bei der Registrierung angeben, die Sie in Ihrem Profil eintragen als auch die Inhalte die Sie auf der Plattform hochladen.

Beispiel: Profil löschen bei StudiVZ:

In einem ersten Schritt können Sie das eigene Profil abmelden. Das hat zunächst zur Folge, dass Sie selbst nicht mehr auf Ihre Daten zugreifen kann. Erst in einem weiteren Schritt wird dann das Profil vom Betreiber tatsächlich gelöscht. Gepostete Beiträge in Gruppen bleiben jedoch anonymisiert erhalten.

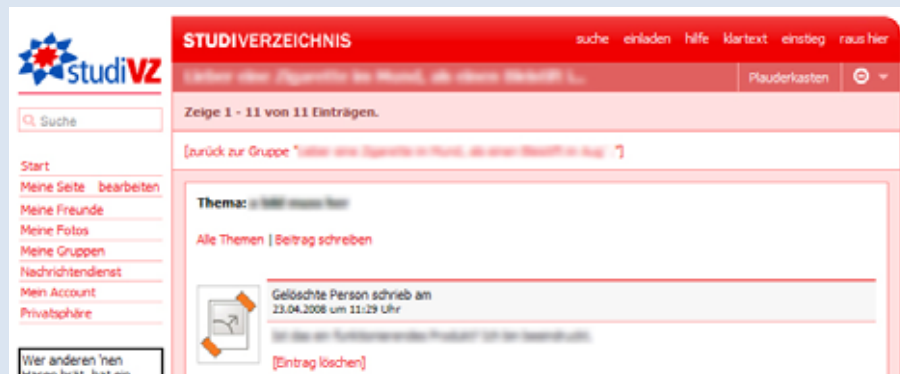


Abb: Posting einer „gelöschten Person“ in *StudiVZ*, Text unkenntlich gemacht (Quelle: www.studivz.net)

Abgesehen vom Datenschutzrecht haben Sie auch Ansprüche aufgrund des **„Rechtes am eigenen Bild“**: Bilder, auf welchen Sie erkennbar sind und die Ihre berechtigten Interessen verletzen, dürfen ohne Ihre Zustimmung nicht veröffentlicht werden. Berechtigte Interessen verletzen unter anderem Bilder, die die darauf abgebildeten Personen bloßstellen oder herabsetzen. Aufnahmen an öffentlichen Plätzen sind üblicherweise unbedenklich, ist der Kontext jedoch nachteilig (z. B. Oben-ohne Abbildungen am Strand) ist eine Veröffentlichung ebenfalls nicht erlaubt. Im privaten Bereich sind Interessen noch viel schneller beeinträchtigt. Dies gilt insbesondere auch für private, geschlossene Veranstaltungen (z. B. eine Party in einer Privatwohnung).

Um gegen eine Verletzung des Rechtes am eigenen Bild vorgehen zu können, reicht es aber nicht, wenn jemand meint, er würde auf dem Bild hässlich aussehen. Eine Bloßstellung muss objektiv nachvollziehbar sein. Das Recht am eigenen Bild betrifft übrigens nur die Veröffentlichung. Das Fotografieren an sich ist davon unberührt.

„Recht haben“ heißt nicht immer „Recht bekommen“

Ein Beispiel: Sie registrieren sich von Österreich aus bei einem Sozialen Netzwerk, das seinen Sitz in den USA hat. Nach wenigen Wochen verlieren Sie jedoch Ihr Interesse an der Plattform und melden sich wieder ab. Da Sie verhindern wollen, dass das Unternehmen weiterhin Daten über Sie besitzt, möchten Sie alle Angaben zu Ihrer Person löschen lassen. Dabei berufen Sie sich auf den Lösungsanspruch nach dem österreichischen Datenschutzgesetz. Soweit, so gut. Falls das Unternehmen Ihnen aber die Entfernung der Daten verweigert, wird es in der Praxis kompliziert:

1. Es ist zu klären, ob ein österreichisches oder ein US-amerikanisches Gericht für diesen Fall zuständig ist. Sollte dies geklärt sein, was aufwendig genug sein kann, ist auch noch zu entscheiden welches Recht (wiederum: österreichisches oder US-amerikanisches) anzuwenden ist.
2. Wenn Punkt 1 geklärt ist und das Gericht tatsächlich – nehmen wir an in Ihrem Sinn – zu einer Entscheidung kommt, bleibt immer noch die Frage, ob das Urteil in der Praxis durchzusetzen ist. Sie können zum Beispiel mit sehr großer Wahrscheinlichkeit davon ausgehen, dass das Urteil eines österreichischen Gerichts für ein Unternehmen in den USA keine unmittelbaren Konsequenzen hat.

Außerdem ist zu beachten, dass die US-Bestimmungen zum Datenschutz weniger streng sind als in Europa.

Welche Rechte treten Sie an die Plattformbetreiber ab?

Die Betreiber sichern sich – mit der Zustimmung der NutzerInnen zu den Geschäftsbedingungen – unterschiedliche Rechte für die Verwertung der veröffentlichten Inhalte zu. Wie umfassend diese Verwertungsrechte sein können, zeigt folgender Auszug aus den Nutzungsbedingungen von *Facebook*. Aufgrund dieser Vereinbarungen ist es beispielsweise ohne weiteres möglich, dass *Facebook* Urlaubsfotos von NutzerInnen im Rahmen einer Werbekampagne verwendet.

„Mit dem Posten von Benutzerinhalt auf einem beliebigen Teil der Site erteilst du dem Unternehmen automatisch eine unwiderrufliche, zeitlich unbegrenzte, nicht ausschließliche, übertragbare, vollständig bezahlte, weltweite Lizenz (mit dem Recht zur Vergabe von Unterlizenzen) für das Verwenden, Kopieren, öffentliche Aufführen, öffentliche Darstellen, Umformatieren, Übersetzen, Anfertigen von Auszügen (vollständig oder teilweise) und Weitergeben solcher Benutzerinhalte für kommerzielle, Werbe- oder sonstige Zwecke auf oder in Verbindung mit der Site oder mit dem Marketing für die Site, für das Erstellen abgeleiteter Werke oder die Einarbeitung solcher Benutzerinhalte in andere Werke und für das Vergeben und Autorisieren von Unterlizenzen zu Vorstehendem.“

Quelle: Facebook Nutzungsbedingungen (20.3.2009)

Facebook archiviert die Daten auch nach der Löschung Ihres Profils. Gemäß der aktuellen Nutzungsbestimmungen besitzt das Unternehmen ab diesem Zeitpunkt hierfür jedoch keine Verwertungsrechte mehr. Insgesamt wird die Frage, „Was darf der Netzwerk-Betreiber mit meinen Daten nach einer Abmeldung tun?“, heiß diskutiert. Anlass dazu geben unter anderem die laufenden Bestrebungen der Anbieter, die Nutzungsbestimmungen zu ihrem Vorteil zu verändern.

Anfang 2009 änderte *Facebook* beispielsweise die Nutzungsbedingungen ohne die registrierten Personen vorab davon in Kenntnis zu setzen. Diese Änderung hätte dem Plattformbetreiber auch nach Löschung des Profils umfassende Nutzungsrechte an den Daten gewährt. Nach massiven Protesten der NutzerInnen sah sich *Facebook* jedoch gezwungen, diese Veränderung der Nutzungsbedingungen wieder zurückzunehmen.

4. Soziale Netzwerke sicher nutzen

4.1. So schützen sie Ihre Privatsphäre

Sie finden in diesem Kapitel die wichtigsten Tipps zum Schutz der Privatsphäre unterteilt nach den Phasen der Nutzung – beginnend vor der Registrierung bis hin zur Abmeldung.

4.1.1. Bevor Sie ein Profil anlegen

Bevor Sie in einem sozialen Netzwerk ein Profil anlegen, sollten sie folgende Punkte beachten:

- **Geben Sie so wenige Daten wie möglich preis:** Das Internet hat ein langes Gedächtnis. Inhalte, die einmal online sind, können oft nur schwer kontrolliert oder gar gelöscht werden. Daher: Überlegen Sie genau, was Sie von sich selbst im Internet preisgeben!

Tipps: Pseudonym statt voller Name

Auf *Netlog* müssen Sie sich nicht mit Ihrem vollen Namen registrieren, sondern können sich auch unter einem fiktiven Namen (Nickname) anmelden. Sie müssen nur Ihren Vornamen, Ihr Geburtsdatum und Ihre E-Mail-Adresse verpflichtend angeben. Auch *MySpace* und *Szene1.at.at* erlauben die Nutzung unter einem Pseudonym. Allerdings müssen Sie bei der Anmeldung Ihren vollen Namen angeben und können in der Suche auch so gefunden werden.

Auf anderen Plattformen melden sich viele NutzerInnen nicht mit vollem Namen an, sondern kürzen ihren Nachnamen ab oder lassen einfach einzelne Buchstaben weg. Diese Vorgehensweise verstößt aber in den meisten Fällen gegen die Nutzungsbedingungen und kann zum Ausschluss führen.

- **Trennen Sie Privates von Beruflichem:** Aufgrund der zunehmenden Verbreitung von Sozialen Netzwerken erhält man „Freundschafts“-Anfragen aus unterschiedlichen Lebensbereichen, wie Beruf, Freizeit, Familie etc. Es ist empfehlenswert, diese Lebensbereiche auch in den Sozialen Netzwerken zu trennen. Z. B. ist für berufliche Kontakte die Nutzung eines Business-Netzwerks wie *Xing* sinnvoll. Durch die Vermischung der Lebensbereiche in einem einzigen Netzwerk vermitteln Sie einen sehr umfassenden Eindruck über Ihr soziales Umfeld, was nicht immer wünschenswert ist. Beispiel: Sind Sie wirklich damit einverstanden, dass Ihre Geschäftspartner über Ihre privaten Interessen und politischen Einstellungen Bescheid wissen?

-

- **Sichere Passwörter verwenden:** Verhindern Sie, dass Unbefugte Zugriff auf Ihr Profil haben und in Ihrem Namen Einträge in einem Sozialen Netzwerk veröffentlichen. Sicher sind Passwörter, die nur sehr schwer zu erraten sind. Dazu zählen Passwörter, die aus Buchstaben, Ziffern und Sonderzeichen zusammengesetzt sind. Neben der Auswahl eines sicheren Passworts, ist auch der vorsichtige Umgang damit entscheidend: Geben Sie ein Passwort niemals weiter und wechseln Sie es regelmäßig.

Tipp: Sichere Passwörter leicht merken

Schreiben Sie einen Satz auf, dessen Anfangsbuchstaben, Ziffern und Satzzeichen dann das Passwort bilden. Ein Beispiel: Der Satz „Ein sicheres Passwort hat mindestens 8 Zeichen!“ ergibt das Passwort: esphm8z!

- **Unterschiedliche NutzerInnen-Namen und Passwörter in jedem Netzwerk:** Sind Sie in mehreren Communities aktiv, ist es natürlich verlockend, immer die gleichen Zugangsdaten zu verwenden. Für den Fall aber, dass Ihr Passwort missbräuchlich verwendet wird, kann der potenzielle Schaden dann um ein Vielfaches größer ausfallen.
- **Vorsicht bei der Nutzung von Sozialen Netzwerken über öffentliche Netze:** Fast alle Plattformen (eine Ausnahme ist *Xing*) verwenden für die Datenübertragung keine Verschlüsselung. Oft werden nur die Login-Daten, also der BenutzerInnen-Name und das Passwort sicher übertragen. Aber sogar hier gibt es „schwarze Schafe“: Die Community-Plattform *MySpace* verschlüsselt auch diese heiklen Daten nicht. Daher ist besondere Vorsicht geboten, wenn Sie in öffentlichen Wireless-LAN-Netzen (Cafés, Hotspots), Internetcafés oder in Firmennetzwerken auf diesen Seiten surfen denn hier kann Ihr gesamter Datenverkehr sehr leicht mit verfolgt werden.
- **Lesen Sie die Nutzungsbedingungen (AGBs):** Wenn Sie sich für einen Anbieter entschieden haben, lesen Sie sich die Nutzungsbedingungen genau durch. Dort erfahren Sie, welche Rechte Sie an den Plattform-Betreiber abtreten und welche Rechte bzw. Pflichten Sie als NutzerIn haben.
- **Virenschutz-Programme verwenden und regelmäßig aktualisieren,** am besten automatisch. Führen Sie auch regelmäßig Updates der Programme auf Ihrem Computer durch und verwenden Sie eine Firewall.

4.1.2. Nach der Anmeldung

Passen Sie **nach der Anmeldung** sofort die Datenschutzeinstellungen an Ihre Bedürfnisse an. Die Beschäftigung mit diesen Einstellungen bedarf zwar einiger Zeit – es zahlt sich jedoch in jedem Fall aus, diese zu investieren!

- **Einstellungen im Profil – Wer darf was sehen?** In Ihrem Profil können Sie festlegen, wer welche Angaben lesen darf. Empfehlenswert ist beispielsweise die Einstellung, dass das Profil nur für „Freunde“ zugänglich ist.

The screenshot shows the 'Privatsphäre' (Privacy) settings for a Facebook profile. The 'Allgemeines' (General) tab is selected. At the top, there is a search box for 'So sehen Freunde dein Profil:' with the placeholder text 'Namen eingeben'. Below this, several settings are listed, each with a lock icon, a dropdown menu, and a help icon (?). The settings are: 'Profil' (Friends of Friends), 'Allgemeine Informationen' (Friends), 'Persönliche Angaben' (Friends), 'Status und Links' (Friends), 'Fotos, auf denen du markiert bist' (Friends), 'Videos, in denen du markiert bist' (Friends), 'Freunde' (Friends of Friends), 'Pinnwandeinträge' (checked: Friends can write on my timeline, Friends of Friends), 'Ausbildung' (Friends), and 'Berufliche Angaben' (Friends of Friends). At the bottom, there are two buttons: 'Änderungen speichern' (Save changes) and 'Abbrechen' (Cancel).

Abb: Allgemeine Datenschutzeinstellungen bei *Facebook* (Quelle: www.facebook.com)

- **Suche – Wie werde ich gefunden?** Eine weitere wichtige Option ist, welche Angaben aus Ihrem Profil Sie für die Suche freigeben. Dabei wird meistens unterschieden zwischen der Suche im Sozialen Netzwerk selbst und der Suche mithilfe externer Suchmaschinen, wie Google, 123people oder yasni. Die Einstellungen für die Suche sind bei allen Anbietern sehr unterschiedlich. Aber auch hier gilt: Geben sie so wenig Daten wie möglich von sich preis.

Suchfreigaben

Welche deiner Daten sollen für die Usersuche freigegeben werden?

E-mail: freigeben

Vorname: freigeben

Nachname: freigeben

Landkartenposition: freigeben

Speichern

Abb.: Gesucht und gefunden werden auf *Szene1.at* (Quelle: www.szene1.at)

Tipp: Personensuchmaschinen blockieren

Ein wichtiger Aspekt des Datenschutzes in Sozialen Netzwerken ist der Zugriff von Suchmaschinen auf die veröffentlichten Inhalte. Gerade spezialisierte Personensuchmaschinen, wie www.123people.com oder www.yasni.de durchsuchen gezielt Profile in Sozialen Netzwerken, um anderen InternetnutzerInnen umfassende Suchergebnisse (z. B. auch mit Profilfotos und Telefonnummer aus öffentlichen Verzeichnissen) liefern zu können.

Überlegen Sie, ob es notwendig ist, dass jede/r ganz einfach herausfinden kann, bei welchen Sozialen Netzwerken Sie registriert sind. Sie können in den Datenschutzeinstellungen der meisten Plattformen, externen Suchmaschinen den Zugriff auf Ihr Profil verweigern.

Optionen

- Mein Profil darf auch für Nicht-Mitglieder abrufbar sein. Bearbeiten
- Mein Profil darf in Suchmaschinen auffindbar sein.
- Meine Artikel und Kommentare in den Gruppen können über Suchmaschinen und RSS abgerufen werden.

Abb: Einstellung in den Privatsphären-Optionen von *Xing*, ob man in Suchmaschinen gefunden werden will oder nicht (Quelle: www.xing.com)

4.1.3. Während Sie Soziale Netzwerke nutzen

Richten Sie Ihre Aufmerksamkeit auch während der Nutzung auf den Schutz der Privatsphäre. Nur so können Sie unangenehmen Situationen vorbeugen.

- **Einstellungen bei der Veröffentlichung einzelner Beiträge:** Manche Soziale Netzwerke erlauben Ihnen individuelle Einstellungen für einzelne Beiträge wie etwa Postings, Fotos oder Videos. Auf diese Weise legen Sie fest, ob einzelne Inhalte öffentlich oder nur für „Freunde“ sichtbar sind. Gerade bei Fotos und Videos ist es empfehlenswert diese nur für „Freunde“ freizuschalten.

The screenshot shows the 'Album bearbeiten - Marias Party' interface. At the top, there's a red header with the album name and a 'Plauderkasten' button. Below the header, there are navigation links: '[Zu meinen Fotos]', 'Albuminfo bearbeiten', 'Titelbild ändern', 'Fotos bearbeiten', and 'Fotos hinzufügen'. The main content area is titled 'Marias Party' and includes a red 'Album löschen' button. The form contains the following fields:

- Name (max. 80 Zeichen): Marias Party
- Ort (max. 80 Zeichen): Marias Wohnung
- Beschreibung: Geburtstagsparty von Maria 01.02.09
- Sichtbar im studivZ für: meine Freunde
- Sichtbar bei meinVZ für: meine Freunde
- Wer darf verlinken?: alle, für die das Album sichtbar ist

At the bottom, there are two red buttons: 'Änderungen übernehmen' and 'Vergiss es'.

Abb: Einstellungen für die Privatsphären bei einzelnen Fotoalben auf *StudivZ* (Quelle: www.studivz.net)

- **Nur bekannte Personen als „Freunde“ akzeptieren:** Sinnvoll ist es, nur jene Personen als „Freunde“ zu akzeptieren, die man auch persönlich kennt. Gerade für Jugendliche ist es jedoch reizvoll, möglichst viele „Freunde“ zu sammeln. Was spricht dennoch dafür, nur bekannte Personen als „Freunde“ zu akzeptieren?
 - Personen, die Sie tatsächlich kennen, haben bereits ein gewisses Maß an Informationen über Ihr Leben. Sie sind nicht ausschließlich auf Angaben aus dem Netz angewiesen, um sich ein Bild über Sie zu machen.
 - Bei bekannten Personen lässt sich besser einschätzen, welche Informationen man ihnen anvertrauen kann und welche nicht.

- Immer wieder werden in Sozialen Netzwerken Schadprogramme (Viren, Trojaner etc.) verbreitet. Dies passiert auch häufig über Personen auf der „Freundesliste“, die man nicht kennt.

Tipp: Wenn Fremde Sie einladen, Sie als „Freund“ zu verlinken, nehmen Sie diese Personen vorab in jedem Fall genau unter die Lupe, bevor Sie die Freundschaftseinladung annehmen.

- **Keine kompromittierenden Bilder veröffentlichen**, auch nicht für „Freunde“. Denn aus „Freunden“ können später einmal „Feinde“ werden. Beispielsweise werden nicht selten Bilder, die zu Zeiten einer engen Freundschaft ausgetauscht wurden, später für Cyber-Mobbing missbraucht. „Witzige“ Bilder, intime Aufnahmen etc. können leicht auch gegen einen selbst verwendet werden.
- **Externe Anwendungen (Widgets):** Viele Plattformen bieten externe Anwendungen an. Mit diesen von Drittanbietern hergestellten Programmen können Sie z. B. Geburtstagsgrüßkarten versenden, Tests ausfüllen, kleine Spiele spielen usw. Vor allem auf *Facebook* und *MySpace* sind diese Applikationen sehr beliebt.

Tipp: Anwendungen auf Facebook und MySpace

Facebook und *MySpace* erlauben ihren NutzerInnen, den Zugriff von externen Programmen auf private Daten einzuschränken. Sinnvoll ist es, wenn Sie hier besonders restriktiv vorgehen und nur wenige, bis gar keine Daten freigeben, da sie über keinerlei Kontrolle darüber verfügen, welche Programme ihre „Freunde“ ausführen. Wenn Sie sich entscheiden selbst gar keine Anwendungen zu verwenden, können Sie den Zugriff auf Ihre Daten auch gänzlich verbieten.

Widget-Kommunikationseinstellungen

Widgets dürfen mir Nachrichten und Kommentare senden

Änderungen speichern

Datenschutz für Widgets deiner Freunde

Warum benötigen Widgets meiner Freunde meine Daten?

Wenn deine Freunde ein Widget benutzen, benötigt dieses möglicherweise einige Informationen über dich, um funktionieren zu können.

Beispiel: Wenn deine Freunde ein Widget für "Beste Freunde" benutzen, möchten sie möglicherweise deinen Namen und dein Foto in einer Liste aller ihrer Freunde ansehen können, um dich als besten Freund auswählen zu können.

Widget-Datenschutz (Freunde):

- Basis-Informationen (Name, Foto, Freunde, Alter, Geschlecht, Ort) freigeben
 Keine Informationen freigeben

Änderungen speichern

Abb: Privatsphären Einstellungen für Anwendungen (Widgets) auf *MySpace*
(Quelle: www.myspace.com)

Die Nutzung ist meist kostenlos, dafür erlauben die Plattformbetreiber den Drittanbietern Zugriff auf die Daten des NutzerInnen-Profiles sowie auf die Daten aller „Freunde“. Wenn einer Ihrer „Freunde“ ein solches Programm ausführt, kann es folglich auch auf Ihre Daten zugreifen. Zudem haben ForscherInnen in den USA

herausgefunden, dass 90 Prozent der *Facebook*-Anwendungen auf weitaus mehr private NutzerInnen-Daten zugreifen, als sie eigentlich für die angebotenen Dienste benötigen würden.⁴

- **Denken Sie an die Privatsphäre Ihrer „Freunde“:** Wie Sie hat auch jede/r andere ein Anrecht auf Datenschutz. Bevor Sie private Informationen über „Freunde“ veröffentlichen, überlegen Sie sich, ob diese Einwände haben könnten. Fragen Sie sicherheitshalber vor dem Hochladen bei den Betroffenen nach.

4.1.4. Wenn Sie nicht mehr aktiv sind

Das eigene Profil löschen: Wenn Sie auf einer Plattform nicht mehr aktiv sind, löschen Sie das eigene Profil. Denn nicht mehr aktualisierte Angaben können leicht einen falschen Eindruck von Ihrer Person vermitteln. Dieser Löschvorgang wird einem von den Betreibern aber nicht immer leicht gemacht:

- Die Löschfunktion ist oft schwer auffindbar und der Weg bis zur erfolgreichen Abmeldung erfordert mehrere Schritte.
- Auf manchen Plattformen wird Ihr Profil nicht wirklich gelöscht, sondern nur deaktiviert.

Nachrichten	in Ihren Postfächern	✓
Kontakte	Ihre Kontakte	✓
	Ihre Einladungen	✓
	Ihre Notizen	✓
	Ihre Tags	✓
Gruppen	Ihre Mitgliedschaften in Gruppen	✓
	Ihre Abonnements in Gruppen	✓
Termine	Ihre Termine (öffentlich und privat)	✓
	Ihre Teilnahme an Terminen	✓
Weitere Angaben	Ihre Bankdaten bzw. Kreditkarteninformationen	✓

Grund für den Austritt

Bitte erläutern Sie in kurzen Worten, warum Sie Ihre Mitgliedschaft beenden möchten.

Bitte geben Sie den Code ein, der rechts steht:



Mitgliedschaft beenden

Abbrechen

⁴ Adrienne Felt, David Evans: Privacy Protection for Social Networking APIs. <http://www.cs.virginia.edu/felt/privacybyproxy.pdf>

Abb: Das Abmeldeformular auf *Xing* (Quelle: www.xing.com)

Entscheidend bei der Abmeldung ist auch welche Daten tatsächlich gelöscht werden: Werden alle Daten, die mit dem/der NutzerIn verknüpft sind (z.B. auch Postings und Bilder), gelöscht oder nur die Angaben im Profil? Wenn die von den NutzerInnen hochgeladenen Inhalte nicht gelöscht werden, werden sie zumindest anonymisiert?⁵

4.2. So schützen Sie sich vor Belästigung und Cyber-Mobbing

Mit zunehmender Beliebtheit von Sozialen Netzwerken, steigt leider auch die Gefahr zum Opfer von Cyber-Mobbing-Attacken zu werden. Cyber-Mobbing umfasst beispielsweise das Bloßstellen von Personen im Internet, andauernde Belästigungen oder die Verbreitung von Gerüchten im Netz. Neben den, in den vorangegangenen Unterkapiteln beschriebenen Tipps, helfen folgende Ratschläge gezielt dem Cyber-Mobbing vorzubeugen:

- **Unerwünschte Personen blockieren:** Soziale Netzwerke bieten Ihnen die Möglichkeit, bestimmte Personen zu blockieren. Blockierte NutzerInnen sind dann nicht mehr berechtigt auf Ihr Profil zuzugreifen und Ihnen Nachrichten zu senden. In einigen Netzwerken können Sie zusätzlich eine so genannte „Whitelist“ nutzen, um ausgewählten Personen für einen bestimmten Zeitraum den Zugriff auf das eigene Profil zu erlauben. Diese Einstellungen finden Sie normalerweise im eigenen Profil oder in den Einstellungen zur Privatsphäre.



Abb.: Whitelist in *Netlog* (Quelle: www.netlog.com)

⁵ Die Studie „Privatsphärenschutz in Soziale-Netzwerke-Plattformen“ des Fraunhofer Instituts für Sichere Informationstechnologie SIT (August 2008) bietet einen guten Überblick über das Löschverhalten der wichtigsten Sozialen Netzwerke (www.sit.fraunhofer.de/Images/SocNetStudie_Deu_Final_tcm105-132111.pdf)

- **Auf Belästigungen nicht reagieren, aber Beweise sammeln:** Kommt es dennoch weiterhin zu Belästigungen, sollten Sie auf diese nicht reagieren. Manchmal erledigt sich dann die Sache von selbst. Wichtig ist aber, Beweise zu sammeln. Denn sollte die Belästigung sich fortsetzen oder gar schlimmer werden, können diese helfen, jemanden als „TäterIn“ zu identifizieren. Dadurch kann der jeweilige Nutzer bzw. die jeweilige Nutzerin von der Plattform verwiesen werden.
- **Belästigungen melden:** Alle Sozialen Netzwerke bieten zudem die Möglichkeit, Belästigungen oder kompromittierende Bilder zu melden.

Verstoß melden

Verwende dieses Formular nur dazu, Verstöße gegen die [Nutzungsbedingungen](#) von MySpace zu melden. Beschreibe den Verstoß so ausführlich wie möglich, damit wir uns schnellstmöglich informieren können.

* Pflichtfelder

Vorname:

Nachname:

* **E-Mail-Adresse:**

* **Beschwerde:**

* **Zusätzliche Informationen:**

Abb.: Möglichkeit, einen Missbrauch auf *MySpace* zu melden (Quelle: www.myspace.com)

4.3. Urheberrechte berücksichtigen

Jeder Text, jedes Bild, jeder Film wurde ursprünglich von jemandem geschaffen, eben von einer/m „UrheberIn“. Der/Die UrheberIn genießt für diese Schöpfung einen rechtlichen Schutz, der im Urheberrechtsgesetz festgehalten ist. Verwenden Sie also Inhalte, die nicht von Ihnen geschaffen wurden, ist es wichtig, die Rechte des/der Urhebers/in zu wahren.

- **Auf Urheberrechte achten:** Möchten Sie zum Beispiel Musik, Fotos, Texte oder Filme, die Sie nicht selbst erstellt haben, in einem Sozialen Netzwerk veröffentlichen, müssen Sie die Urheberin/den Urheber zuerst um Erlaubnis fragen. Veröffentlichen Sie im Internet fremde Inhalte ohne Zustimmung der Urheberin/des Urhebers, kann dies im Falle einer Klage bis zu einigen tausend Euro Strafe kosten.
- **Richtig Verlinken:** Links im Internet können gesetzt werden, wenn man sich ausreichend davon überzeugt hat, dass die verlinkte Seite keine illegalen Inhalte enthält. Erfährt man von illegalen Inhalten auf einer verlinkten Website, müssen Sie den Link sofort entfernen.

Tipp: Infos zur sicheren Internetnutzung

Praktische Tipps zur sicheren Nutzung des Internet finden Sie laufend aktualisiert auf der Website von Saferinternet.at:
www.saferinternet.at

5. Tipps für Eltern

So unterstützen Sie Ihre Kinder bei der sicheren Internetnutzung⁶:

1. Entdecken Sie das Internet gemeinsam mit Ihrem Kind.

Suchen Sie interessante und spannende Websites entsprechend dem Alter Ihres Kindes und erforschen Sie sie miteinander. Die gemeinsamen Erfahrungen erleichtern es in Zukunft, positive und negative Erlebnisse bei der Internetnutzung zu besprechen.

2. Vereinbaren Sie mit Ihrem Kind Regeln für die Internetnutzung.

Diese beinhalten beispielsweise die Weitergabe persönlicher Daten, das Verhalten gegenüber anderen Online-NutzerInnen bzw. in Ihrer Familie akzeptierte Online-Aktivitäten. Vergessen Sie nicht, dass Regeln nur wirksam sind, wenn Kinder und Jugendliche die Regeln verstehen und deren Berechtigung akzeptieren.

3. Machen Sie Ihr Kind darauf aufmerksam, persönliche Daten mit Vorsicht weiterzugeben.

Erklären Sie die Gefahren leichtfertiger Datenweitergabe. Eine einfache Regel kann sein, dass Ihr Kind Name, Adresse, Telefonnummer und Fotos nur nach Absprache mit Ihnen weitergibt.

4. Sprechen Sie mit Ihrem Kind über die Risiken von realen Treffen mit Online-Bekanntschäften.

Das Internet ist ein fantastischer Ort, neue Menschen kennenzulernen. Um unangenehme Überraschungen zu verhindern, treffen Sie mit Ihrem Kind die Abmachung, dass bei solchen Treffen immer ein vertrauter Erwachsener oder zumindest eine Freundin oder ein Freund dabei sein soll.

5. Diskutieren Sie mit Ihrem Kind den Wahrheitsgehalt von Inhalten im Internet.

Zeigen Sie Ihrem Kind, wie die Richtigkeit von Inhalten durch Vergleiche mit anderen Quellen überprüft werden kann.

6. Melden Sie illegale Internetinhalte an www.stopline.at.

Kinderpornografie und neonazistische Inhalte sind in Österreich gesetzlich verboten.

7. Ermutigen Sie Ihre Kinder zu guter Netiquette.

Netiquette sind die informellen Verhaltensregeln im Internet. Einfach gesagt: Was im realen Leben erlaubt ist, ist auch im Internet erlaubt. Was im realen Leben verboten ist, ist auch im Internet verboten.

8. Informieren Sie sich über die Internetnutzung Ihres Kindes.

Lassen Sie sich die Lieblingsseiten zeigen und versuchen Sie zu verstehen, was es dort tut. Dies ermöglicht Ihnen, Ihr Kind bei der Internetnutzung gezielt anzuleiten.

⁶ Quelle: Saferinternet.at www.saferinternet.at/tipps/fuer-eltern/

9. Seien Sie nicht zu kritisch in Bezug auf die Entdeckungsreisen Ihres Kindes im Internet.

Ihr Kind kann durch Zufall auf ungeeignete Inhalte stoßen. Nehmen Sie dies zum Anlass, um über diese Inhalte zu diskutieren und eventuell Regeln zu vereinbaren. Drohen Sie Ihrem Kind aber nicht sofort mit Internetverbot o.ä. Sie möchten ja, dass es sich auch in Zukunft wieder an Sie wenden wird, wenn es in einer unangenehmen Situation ist.

10. Vergessen Sie nicht: Chancen und Nutzen des Internets übertreffen die Risiken bei Weitem!

Das Internet ist ein ausgezeichnetes Medium zum Lernen und zur Freizeitbeschäftigung. Ermutigen Sie Ihr Kind, das Internet bewusst zu nutzen und alle positiven Möglichkeiten zu erforschen.