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

31/2013
Juni/2013

FACEBOOK, WHATSAPP & CO.

KONSUMENTINNEN-TIPPS FÜR SOZIALE NETZWERKE

Durchführung im Auftrag der AK-Wien:
Österreichisches Institut für angewandte Telekommunikation

Inhalt

Anmerkung:
Stand der in diesem Ratgeber angeführten Informationen und Tipps ist Juni 2013.

Einleitung

Soziale Netzwerke wie *Facebook, WhatsApp* & Co. zählen zu den „Erfolgsgeschichten" im Internet. *Facebook* rangiert in Österreich bereits auf Platz zwei der beliebtesten Websites[1]. Die Frage „Bist du auf *Facebook*?" ist Ihnen wahrscheinlich nur allzu bekannt.

Andererseits: Haben Sie auch schon einmal ein ungutes Gefühl dabei gehabt, private Daten online zu stellen? So geht es vielen Menschen, denn das Gedächtnis des Internets ist lang und einmal Veröffentlichtes ist oft nur schwer wieder zu entfernen.

Bei der Nutzung von Sozialen Netzwerken befindet man sich häufig in einem Zwiespalt: Die Verwendung von *Facebook, WhatsApp* & Co. macht nur Sinn, wenn man persönliche Informationen von sich preisgibt und sich mit anderen NutzerInnen über die Plattform austauscht. Umgekehrt kann allzu große Freizügigkeit mit privaten Daten, Fotos etc. unangenehme Folgen haben.

Der Schutz der Privatsphäre ist in Zeiten des „Online-Netzwerkens" also eine große Herausforderung. Freilich betrifft das aber nicht nur das eigene Nutzungsverhalten, sondern auch die Plattform-Betreiber: Welche Schutzmöglichkeiten bieten sie an und wie gehen sie mit den ihnen anvertrauten Daten um? Fragen, die in der Öffentlichkeit immer wieder für Kritik und Diskussionen sorgen, auch auf politischer und juristischer Ebene.

Der vorliegende Ratgeber soll Sie dabei unterstützen, Soziale Netzwerke sicher zu nutzen und dabei gleichzeitig von den vielen Vorteilen und Möglichkeiten zu profitieren.

Die wichtigsten Tipps – so nutzen Sie Soziale Netzwerke sicher:

- Veröffentlichen Sie so **wenige persönliche Daten wie möglich**. Machen Sie sich die etwaigen Risiken vor einer Veröffentlichung bewusst.
- Nutzen Sie die **Privatsphäre-Einstellungen**: Wer darf was einsehen und ist es Suchmaschinen erlaubt, auf Ihr Profil zuzugreifen?
- Verwalten Sie **Berufliches und Privates** klug. Bedenken Sie bei allen Veröffentlichungen, dass unter Umständen auch Chefs und KollegInnen mitlesen könnten.
- Verwenden Sie **sichere Passwörter**, damit Unbefugte nicht plötzlich in Ihrem Namen auftreten.
- **Löschen Sie Ihr Profil**, sobald Sie in einem Sozialen Netzwerk nicht mehr aktiv sein möchten.
- Akzeptieren Sie **nur bekannte Personen als „Freunde"**.
- Veröffentlichen Sie **keine Bilder, auf denen Sie oder andere Personen nachteilig dargestellt sind**.
- Veröffentlichen Sie Musik, Videos und Fotos nur dann, wenn Sie die **Zustimmung der UrheberInnen** besitzen.
- Verwenden Sie ein **Anti-Viren-Programm** und aktualisieren Sie es regelmäßig.

[1] Vgl. http://www.alexa.com/topsites/countries/AT (28.06.2013)

1. „Faszination“ Soziale Netzwerke

Soziale Netzwerke und die zahlreichen damit verbundenen Anwendungen haben sich in den letzten Jahren zu einem zentralen Bestandteil des Internets entwickelt. Für viele Menschen ist das „Online-Netzwerken“ alltäglich geworden. In Sozialen Netzwerken kann man sich mit anderen austauschen, Fotos, Videos und Links teilen, Interessensgruppen bilden, gemeinsam Spiele spielen, chatten, neue Kontakte knüpfen u.v.m. Die NutzerInnen präsentieren sich in einem persönlichen Profil mit Angaben wie z.B. Hobbys, Interessen, aktuellen Aktivitäten, Fotos, Videos etc. Wenn zwei NutzerInnen einwilligen, „verlinken“ sie ihre Profile und werden zu „Freunden“.

Info: Soziale Netzwerke – so funktioniert’s:

Sie melden sich auf einer Plattform an, füllen ein sogenanntes „Profil“ mit ihren persönlichen Daten aus und schon kann es losgehen: Fotos und Videos online stellen, Links teilen, eigene Meldungen verfassen oder andere kommentieren und neue oder auch „alte“ Freunde im Netzwerk (wieder)finden.

Darin liegt auch das Besondere der Sozialen Netzwerke: Indem Sie Ihr Profil mit dem anderer NutzerInnen verknüpfen, sammeln Sie „Freunde“, die wiederum selbst mit anderen „Freunden“ verknüpft sind. Dadurch entsteht schließlich ein riesiges Beziehungs-Netzwerk, das schon nach wenigen „Verknüpfungen“ die ganze Welt umspannen kann.

1.1. Fünf gute Gründe Soziale Netzwerke zu nutzen

1. Kontakte pflegen

Die Möglichkeit, sich jederzeit mit FreundInnen, Verwandten, ArbeitskollegInnen, GeschäftspartnerInnen etc. austauschen zu können oder Menschen wiederzufinden, von denen man schon seit Jahren nichts mehr gehört hat, macht Soziale Netzwerke besonders interessant. Unterstützt wird diese Kommunikation von einer Vielzahl an Anwendungen innerhalb der Plattformen:

- **Nachrichtenfunktionen & Chats:** Diese lösen zunehmend die herkömmliche E-Mail-Kommunikation ab. Die „Gesprächsverläufe“ bleiben im Netzwerk gespeichert.
- **Statusmeldungen:** In kurzen Sätzen werden den virtuellen „Freunden“ aktuelle Tätigkeiten, Gedanken oder Befindlichkeiten mitgeteilt. Meldungen wie „Max Meier ist sauer, weil es schon wieder regnet“ oder „Maria Mustermann geht jetzt nach einem feinen Grillabend schlafen“ scheinen einerseits trivial, andererseits sind sie Ausdruck des „virtuellen Miteinanders“. Schließlich spielen Small-Talk und Tratsch auch bei Treffen in der realen Welt eine wichtige Rolle.
- **Kommentarfunktionen:** Über Kommentare entstehen mitunter sehr lebendige Diskussionen zu Statusmeldungen oder zu geposteten Videos, Fotos oder Links. In den meisten Sozialen Netzwerken können Inhalte zudem mit nur einem Klick mit weiteren Personen „geteilt“ werden – so entstehen „Schneeballeffekte“.
- **Gruppen:** Hier treffen sich Gleichgesinnte, die sich zu einem bestimmten Thema oder Ereignis austauschen. Zeitliche oder geografische Grenzen spielen keine Rolle mehr.

2. Neue Personen kennenlernen

Soziale Netzwerke sind auch die idealen Orte, um neue Menschen kennenzulernen, mit denen Sie z.B. ähnliche Interessen teilen. Dies können „Freunde von Freunden" sein oder aber auch potenzielle 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 Profilbild oder die meisten „Freunde". Die Motivation in Business-Netzwerken ist eine ähnliche: Wie kann man die eigenen Kompetenzen oder Produkte am besten für mögliche ArbeitgeberInnen oder KundInnen präsentieren?

4. Alternative zur eigenen Website

Soziale Netzwerke sind eine Alternative zur eigenen Website. Ein eigenes Profil bei *Facebook* & Co. zu erstellen, ist um vieles einfacher als etwa eine eigene Website zu gestalten. Die Plattform-Betreiber stellen dafür ein umfangreiches Angebot an Funktionen zu Verfügung: So ist es beispielsweise in den meisten Sozialen Netzwerken ganz unkompliziert, eigene Foto- und Videogalerien einzurichten.

Auch Unternehmen und Organisationen können oft eigene Seiten in Sozialen Netzwerken einrichten und darüber direkt mit KundInnen, InteressentInnen, PartnerInnen etc. kommunizieren.

5. Neues entdecken

Nicht zuletzt sind es die Aktivitäten und die Kreativität der NutzerInnen, die eine Plattform interessant machen. Durch den regen Austausch an Gedanken und Inhalten, der über Soziale Netzwerke stattfindet, wird eine breite Palette an „Neuem" geboten – seien es neue Songs, lesenswerte Artikel, lustige Bilder, Anregungen für das eigene Hobby oder berufliche Tipps. Durch die zunehmende Vernetzung zwischen Sozialen Netzwerken und anderen Plattformen (z.B. Musik- oder Fotoplattformen), wird dieser Austausch weiter vorangetrieben und gleichzeitig vereinfacht.

1.2. Welche Plattformen gibt es?

Das Angebot an Sozialen Netzwerken ist mittlerweile sehr vielfältig. Durch die zunehmende Verschmelzung der verschiedenen Dienste im Internet ist eine trennscharfe Abgrenzung längst nicht mehr möglich. Ganz grob kann unterschieden werden in:

- **Allgemeine Soziale Netzwerke** („die Generalisten"): Dazu zählen *Facebook* und *Google+*. Hier präsentieren und vernetzen sich NutzerInnen jeden Alters und aus den unterschiedlichsten Motiven.
- **Einfache Kommunikations-Netzwerke:** Hier stehen kurze Nachrichten zwischen den NutzerInnen im Vordergrund. Bekannte Beispiele sind *WhatsApp* und *Twitter*.
- **Inhalts-Plattformen:** NutzerInnen laden auf diese Plattformen (eigene) Videos, Fotos oder Musik hoch bzw. konsumieren diese dort. Wichtige Vertreter sind *YouTube, Flickr, Instagram, Pinterest, Spotify, Tumblr* …
- **Business-Netzwerke:** Hier steht der berufliche Austausch im Mittelpunkt. Im deutschsprachigen Raum ist *Xing* sehr beliebt, im internationalen Kontext wird *LinkedIn* verwendet.

Auch **virtuelle Welten** gelten weitestgehend als Soziale Netzwerke. Die NutzerInnen bewegen sich dort in Form eines „Avatars" durch digital animierte Landschaften und können untereinander chatten. Die bekanntesten Beispiele sind *Second Life* und speziell für Kinder *Habbo Hotel*.

Die in Österreich am häufigsten genutzten Sozialen Netzwerke sind:

Facebook – www.facebook.com

Rund 2,9 Millionen NutzerInnen sind alleine in Österreich jeden Monat auf *Facebook* aktiv. Mehr als eine Milliarde Menschen sind weltweit angemeldet und nützen das Angebot. Damit ist *Facebook* weltweit das größte Soziale Netzwerk.

Genutzt wird *Facebook* vor allem für den direkten Austausch zwischen Personen, die einander meist auch im realen Leben kennen: Die NutzerInnen sind daher vor allem an aktuellen Statusmeldungen und Fotos ihrer „Freunde" interessiert. Aber auch der Austausch mit „Gleichgesinnten" in Themen-Gruppen ist sehr beliebt. Ebenso nutzen Unternehmen, Organisationen und prominente Personen *Facebook* inzwischen erfolgreich für ihre Zwecke.

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

WhatsApp – www.whatsapp.com

WhatsApp ist eine Smartphone-App, mit der man kostenlos chatten (zu zweit oder in Gruppen) sowie sehr einfach Bilder und Videos austauschen kann. Unter Smartphone-NutzerInnen wird der Dienst immer beliebter. Bei Kindern und Jugendlichen ist *WhatsApp* fast schon beliebter als *Facebook*.

Aufgrund mangelnder Datenschutz-Einstellungen und immer wieder bekannt werdender Sicherheitslücken steht *WhatsApp* häufig in der Kritik. Auch Mobbing via *WhatsApp* nimmt stark zu.

Google+ – plus.google.com

Google+ ist das Soziale Netzwerk des „Suchmaschinenriesens" *Google*. Das Netzwerk gilt als Versuch von *Google*, sich im Bereich der Sozialen Netzwerke zu etablieren. Es ist sehr ähnlich aufgebaut wie *Facebook,* konnte bisher aber noch lange nicht so viele NutzerInnen ansprechen. Für die Nutzung von *Google+* ist die Registrierung eines *Google*-Kontos notwendig, mit dem man automatisch für alle *Google*-Anwendungen angemeldet ist (z.B. für den E-Mail-Dienst *Gmail* und die Videoplattform *YouTube*).

Twitter – www.twitter.com

Twitter (engl. für „Gezwitscher") ist eine Kommunikationsplattform, auf der SMS-ähnliche Kurznachrichten verbreitet werden. Diese Nachrichten, die nicht mehr als 140 Zeichen haben dürfen, sind in der Regel öffentlich für alle InternetnutzerInnen zugänglich. Für eine bessere Auffindbarkeit sind die Nachrichten mit Schlagworten, sogenannten „#Hashtags", versehen.

Momentan sind weltweit 200 Millionen Menschen auf *Twitter* aktiv. In Österreich wird *Twitter* sehr stark von PolitikerInnen, JournalistInnen und FachexpertInnen für den schnellen Informationsaustausch genutzt.

Instagram – www.instagram.com

Instagram ist eine Smartphone-App, mit der kostenlos Fotos aufgenommen, bearbeitet und mit anderen NutzerInnen geteilt werden können. *Instagram* wurde vor allem wegen der speziellen Art der Fotobearbeitung („Retro-Polaroids") so populär, vor allem bei Jugendlichen. Über *Instagram* gemachte Bilder können binnen Sekunden in anderen Sozialen Netzwerken weitergepostet werden.

Xing – www.xing.com

Das deutschsprachige Business-Netzwerk *Xing* bietet neben einem eingeschränkten kostenlosen Zugang auch kostenpflichtige Nutzungsangebote mit Zusatzfunktionen. Ziel von *Xing* ist das Aufbauen und Aufrechterhalten von Geschäftskontakten. Dies reicht vom einfachen Vernetzen von Personenprofilen über den fachlichen Austausch innerhalb von Gruppen bis hin zur Anbahnung von neuen Geschäften. *Xing* hat laut eigenen Angaben sieben Millionen Mitglieder.

Tumblr – www.tumblr.com

Tumblr (engl. „etwas durcheinanderbringen") ist eine Blogging-Plattform, auf der NutzerInnen Texte, Bilder, Zitate, Musik und Videos veröffentlichen können. Die Blogs sind stark untereinander vernetzt.

Spotify – www.spotify.com

Spotify (engl. spot „entdecken" + identify „identifizieren") ist eine Musikplattform, auf der man legal urheberrechtlich geschützte Musik anhören kann. Große Plattenlabels wie *Sony*, *EMI, Warner* und *Universal* stellen die Songs ihrer KünstlerInnen auf dieser Plattform zu Verfügung. *Spotify* ist mit *Facebook* vernetzt – so kann man die eigenen „Freunde" wissen lassen, welche Songs man gerade hört.

2. Das Geschäft mit den Sozialen Netzwerken

Die hohen NutzerInnen-Zahlen von Sozialen Netzwerken, der regelmäßige „Hype" um neue Features sowie die hohen Summen bei Unternehmens-Beteiligung lassen darauf schließen, dass der Betrieb von Sozialen Netzwerken ein sehr lukratives Geschäft ist. Die „großen Player" des Internet-Zeitalters *Facebook*, *Google*, *Apple* & Co. sind längst an der Börse und zählen zu den wertvollsten Marken der Welt. Die gängigsten Ansätze um Einkünfte zu erzielen sind:

- **Personalisierte Werbung:** Soziale Netzwerke eignen sich aufgrund der zahlreichen verfügbaren Informationen über Interessen und Gewohnheiten der NutzerInnen besonders gut für personalisierte Werbung. Und tatsächlich nehmen die Werbeeinschaltungen in Sozialen Netzwerken kontinuierlich zu. Erst kürzlich verkündete *Facebook*, monatlich bereits eine Million aktive Werbekunden zu haben.

- **Kostenpflichtige Features:** NutzerInnen erhalten einen kostenlosen Zugang zu einem Netzwerk mit den Basisfunktionalitäten – für darüber hinausgehende Anwendungen und Funktionen 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 Anwendungen an (z.B. Spiele, Tests etc.). Externe Anbieter solcher Programme müssen eine Gebühr an die Netzwerk-Betreiber entrichten. Als „Gegenleistung" dürfen die Unternehmen NutzerInnen-Daten sammeln – allerdings nicht nur von den tatsächlichen NutzerInnen, sondern auch von deren „Freunden".

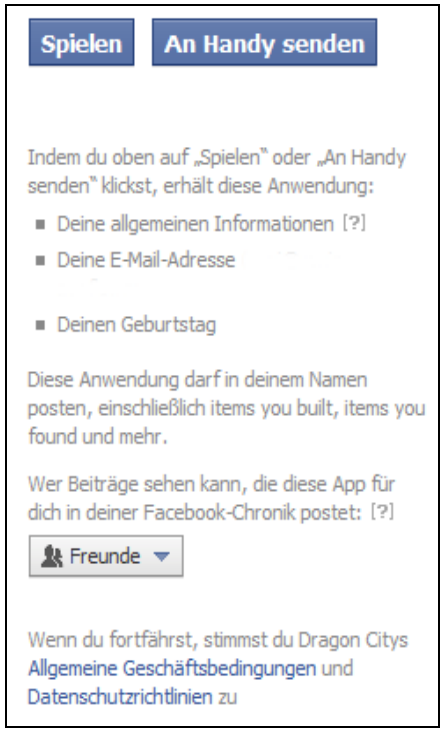


Abb.: *Facebook* macht auf die Einbindung Dritter bei Anwendungen aufmerksam – ein „falscher" Klick ist jedoch schnell gemacht. (Quelle: www.facebook.com)

- **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 Größenordnung dieser Einnahmequelle ist wenig bekannt.

- **Gewinnbringender Verkauf:** Die weitverbreitete Annahme, dass die Plattformen eines Tages mit hohen Gewinnen betrieben werden können, nährt die Hoffnung vieler BetreiberInnen und „Startup"-UnternehmerInnen auf einen gewinnbringenden Verkauf eines Netzwerks bzw. Dienstes.

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 NutzerInnen ihre Privatsphäre den eigenen Anforderungen entsprechend schützen können, liegt zum einen in ihrer eigenen Verantwortung und zum anderen in der Verantwortung der Netzwerk-Betreiber. Für NutzerInnen ist es unumgänglich, sich der Risiken einer allzu großen „Freizügigkeit" im Internet bewusst zu werden und folglich 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, braucht auch nichts zu verbergen". Dem ist leicht zu entgegnen: **Der Schutz der Privatsphäre stellt einen Wert an sich dar und ist ein verfassungsmäßig zugesichertes Recht** – das heißt, es gibt bestimmte Dinge im Leben, die andere einfach nichts anzugehen haben. Abgesehen davon, sind sich viele NutzerInnen gar nicht der möglichen negativen Folgen der Preisgabe persönlicher, auf den ersten Blick vielleicht „unverfänglicher" Daten, bewusst.

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

- **Das Internet vergisst nicht.** Etwas, worauf Sie heute stolz sind, kann Ihnen in einigen Jahren sehr unangenehm oder peinlich sein. Einmal veröffentlichte Daten sind weltweit zugänglich, schnell vervielfältigt und 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 sehr groß.** Alle Inhalte, die Sie ins Netz stellen, sind nicht nur für FreundInnen etc. zugänglich, sondern theoretisch auch für alle anderen InternetnutzerInnen auf der Welt. Auch Ihnen unbekannte oder weniger gut gesonnene Menschen können Ihre privaten Informationen unter Umständen einsehen und für böse Absichten missbrauchen.

- **Der erste Eindruck zählt.** Fühlen Sie sich wohl bei dem Gedanken, dass Ihre GeschäftspartnerInnen und Bekannten sich mithilfe Ihrer Online-Angaben zu Interessen, Hobbys, Vorlieben, politischer Meinung etc. ein umfassendes, aber gleichzeitig wahrscheinlich auch einseitiges Bild von Ihrer Person bilden könnten?

- **Nicht alles ist, wie es scheint.** Glauben Sie nicht alles, was andere Menschen im Internet behaupten – sich als jemand anderer auszugeben bzw. etwas vorzuspielen, ist im Web besonders einfach.

- **Ein Paradies für Datensammler.** Immer wieder wird von Sicherheitslücken, durch die der unerlaubte Zugriff Dritter auf NutzerInnen-Daten möglich wird, berichtet. Die möglichen Folgen: E-Mail-Adressen und andere private Daten werden für z.B. Spam missbraucht, Fotoalben widerrechtlich auf Tauschbörsen zum Download angeboten oder NutzerInnen-Profile weiterverkauft.

Ein Beispiel:

Nach einer durchfeierten Partynacht laden Sie Fotos in ein Soziales Netzwerk. Einige Bilder zeigen Sie im offensichtlich 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 auf die Partyfotos. Die Bilder aus Ihrem eigenen Profil zu entfernen ist kein Problem. Leider müssen Sie jedoch feststellen, dass andere Party-TeilnehmerInnen die Fotos bereits kopiert und sowohl innerhalb des Netzwerks wie auch auf anderen Plattformen weitergepostet haben. Sämtliche Kopien zu entfernen ist jetzt nicht mehr möglich.

Informationen, die von Ihnen in Soziale Netzwerke gestellt werden, können auch Rückschlüsse auf ihre Adresse und Telefonnummer bzw. auch auf Ihren aktuellen Aufenthaltsort 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 NutzerInnen, deren Profile bzw. Daten kopiert und auf anderen Websites veröffentlicht wurden. Beispielsweise Bikini-Fotos vom letzten Strandurlaub, die sich plötzlich auf einer Sex-Dating-Website wiederfinden.

Außerdem können Sie mit einem allzu offenen Umgang mit privaten 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 dazu verwendet werden, um bei Ihnen einen Einbruch zu planen.

Tipp: Vorsichtiger Umgang mit privaten Informationen

Sie können unangenehme Situationen vermeiden, wenn Sie sich vor der 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 oder Fotos zu einem späteren Zeitpunkt peinlich oder unangenehm sein?
- Bin ich damit einverstanden, dass mein derzeitiger oder zukünftiger Arbeitgeber, GeschäftspartnerInnen etc. diese Informationen sehen?
- Könnte eine Veröffentlichung für eine andere Person nachteilig sein?

3.2. Datenschutz und Kinder

Kinder tun sich oft sehr schwer damit, den Wert ihrer persönlichen Daten richtig einzuschätzen. Sie übersehen, dass nicht nur ihre FreundInnen und SchulkollegInnen ihre online gestellten Daten einsehen können, sondern im Prinzip alle Personen im Internet. **Eltern sind daher gefordert**, ihre Kinder über die Risiken einer allzu leichtfertigen Datenweitergabe aufzuklären und ihnen Tipps zum sicheren Umgang mit persönlichen Daten zu geben *(siehe dazu auch Punkt 5)*.

Facebook und andere Soziale Netzwerke haben im Februar 2009, im Rahmen einer EU-Richtlinie, eine Selbstverpflichtungserklärung für den besseren Schutz von Kindern innerhalb ihrer Plattformen unterzeichnet. In dieser Erklärung verpflichten sich die Betreiber unter anderem dazu, ihre Datenschutzeinstellungen zu verbessern und Funktionen zur Prävention und Verfolgung von Verstößen in ihren Netzwerken bereitzustellen. In den meisten Sozialen Netzwerken können anstößige oder widerrechtliche Inhalte tatsächlich gemeldet werden.

Im Sinne des Jugendschutzes sind Anmeldungen für Jugendliche bei Sozialen Netzwerken erst ab einem bestimmten Alter möglich. Auf den meisten Plattformen ist das **Mindestalter für eine Anmeldung** mit 13 Jahren (*Facebook*) festgesetzt. In vielen Nutzungsrichtlinien wird auch darauf hingewiesen, dass alle Angaben wahrheitsgetreu gemacht werden müssen.

3.3. Datenschutz – 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 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 werden. Ihre Daten dürfen nur an Dritte weitergegeben werden, wenn Sie dafür Ihre Zustimmung gegeben haben. *Achtung:* Diese Vereinbarung bzw. Zustimmung kann bereits erfolgen, indem 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 *Facebook*

Bei *Facebook* kann man sein Profil löschen oder lediglich deaktivieren. Deaktiviert man sein Profil, bleiben die persönlichen Daten unverändert gespeichert und man kann den Account jederzeit wieder aktivieren. Solange das Profil deaktiviert ist, können es andere NutzerInnen nicht aufrufen.

Abb.: In den „Sicherheitseinstellungen" kann das eigene Profil auf *Facebook* deaktiviert (das heißt: still gelegt) werden. (Quelle: www.facebook.com)

Abb.: Über einen Link in den FAQs kann man die Löschung des eigenen *Facebook*-Profils beantragen. *Facebook* wird stark dafür kritisiert, dass die Profilinformationen danach aber trotzdem intern gespeichert bleiben. (Quelle: www.facebook.com)

Das „Recht am eigenen Bild"

Abgesehen vom Datenschutzrecht haben Sie auch Ansprüche aufgrund des **„Rechts am eigenen Bild"**, das im österreichischen Urheberrechtsgesetz festgeschrieben ist: Bilder und/oder deren Begleittext, die die „berechtigten Interessen" der Personen auf dem Bild verletzen, dürfen nicht veröffentlicht werden. Aufnahmen an öffentlichen Plätzen sind üblicherweise unbedenklich. Wenn aber die Situation für die Abgebildeten nachteilig ist (z.B. Oben-ohne-Foto am Strand), ist die Abbildung in jedem Fall schützenswert.

Im privaten Bereich sind Interessen noch viel früher beeinträchtigt, dies gilt auch für private geschlossene Veranstaltungen (z.B. Partys bei FreundInnen). Es reicht allerdings nicht, wenn sich der/die Abgebildete auf einem Foto einfach nur hässlich findet – 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 Löschungsanspruch 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 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 jene in Europa.

Welche Rechte treten Sie an die Plattform-Betreiber ab?

Die Netzwerk-Betreiber sichern sich – mit der Zustimmung der NutzerInnen zu den Allgemeinen Geschäftsbedingungen (AGB) – 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 wird der/die „gläserne NutzerIn" mehr als deutlich.

> *„(…) Wir stellen auch Daten aus denjenigen Informationen zusammen, die wir bereits über dich und deine Freunde haben. Beispielsweise stellen wir gegebenenfalls Daten über dich zusammen, um festzulegen, welche Freunde wir dir in deinen Neuigkeiten anzeigen oder welche Freunde wir dir zur Markierung in den von dir geposteten Fotos vorschlagen sollten. Wir können deinen derzeitigen Wohnort mit GPS-Daten und anderen Ortsangaben, die wir über dich haben, zusammenführen, um dich und deine Freunde beispielsweise über Personen oder Veranstaltungen in eurer Nähe zu informieren oder dir Angebote anzubieten, an denen du eventuell interessiert bist. Gegebenenfalls stellen wir auch Daten über dich zusammen, um dir Werbeanzeigen anzuzeigen, die für dich von größerer Relevanz sind. (…)*"
>
> Quelle: *Facebook*-Nutzungsbedingungen (28.06.2013)

Facebook archiviert Ihre persönlichen Daten auch nach der Löschung Ihres Profils. Gemäß den 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 meiner Abmeldung tun?" heiß diskutiert. Anlass dazu geben unter anderem die laufenden Bestrebungen der Anbieter, die Nutzungsbestimmungen zu ihrem Vorteil zu verändern.

4. Soziale Netzwerke sicher nutzen

4.1. So schützen sie Ihre Privatsphäre

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

Bevor Sie ein Profil anlegen

Bevor Sie sich in einem Sozialen Netzwerk registrieren, sollten sie folgende Punkte beachten:

- **Geben Sie so wenige persönliche 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 schon vorher genau, was Sie von sich selbst im Internet preisgeben möchten!

- **Verwaltung von privaten und beruflichen Kontakten**: Durch die Allgegenwart von Sozialen Netzwerken erhält man „Freundschaftsanfragen" aus unterschiedlichen Lebensbereichen wie Beruf, Freizeit, Familie etc. Bevor Sie neue „Freunde" annehmen, sollten Sie sich fragen, was Sie aus Ihrem Leben mit wem teilen wollen.

  Beispiel: Sind Sie wirklich damit einverstanden, dass Ihr/e ChefIn, Ihre GeschäftspartnerInnen oder flüchtige Bekannte über Ihre privaten Interessen, Ihre Freizeitaktivitäten, Ihre familiären Angelegenheiten etc. Bescheid wissen?

- **Sichere Passwörter verwenden**: Verhindern Sie, dass Unbefugte Zugriff auf Ihr Profil bekommen und in Ihrem Namen Einträge veröffentlichen. Am sichersten sind Passwörter, die aus Buchstaben, Ziffern und Sonderzeichen zusammengesetzt und von Dritten nicht zu erraten sind – der Name Ihres Haustieres oder Ihr Geburtsdatum wären beispielsweise keine sehr sicheren Passwörter!

  Neben der Auswahl des Passworts, ist aber auch der vorsichtige Umgang damit entscheidend: Geben Sie ein Passwort niemals weiter, hinterlegen Sie es besser nicht am Computer oder Handy und ändern 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 Zugangsdaten in jedem Netzwerk**: Sind Sie in mehreren Communitys aktiv, ist es natürlich verlockend, immer die gleichen Zugangsdaten (E-Mail-Adresse, NutzerInnen-Name, Passwort) zu verwenden. Für den Fall aber, dass Ihre Zugangsdaten missbräuchlich verwendet werden, kann der potenzielle Schaden dann um ein Vielfaches größer ausfallen.

- **Vorsicht bei der Nutzung von Sozialen Netzwerken über öffentliche Netze:** Die meisten Plattformen verwenden inzwischen verschlüsselte Verbindungen für die Datenübertragung. Dennoch sollten Sie hier vorsichtig bleiben, denn Sicherheitslücken können immer wieder auftreten – auf der sicheren Seite sind Sie nur, wenn Sie in geschlossenen und gut gesicherten Netzwerken surfen.

- **Lesen Sie die Nutzungsbedingungen:** Wenn Sie sich für einen Anbieter entschieden haben, lesen Sie sich die Nutzungsbedingungen bzw. AGB vor Registrierung genau durch. Dort erfahren Sie, welche Rechte Sie an den Plattform-Betreiber abtreten und welche Rechte bzw. Pflichten Sie als NutzerIn haben.

- **Computer schützen:** Verwenden Sie ein Anti-Viren-Programm und aktualisieren Sie es regelmäßig. Aktualisieren Sie auch laufend Ihre Software, am besten per automatischem Update, installieren Sie eine Firewall und verschlüsseln Sie Ihre WLAN-Verbindung.

Nach der Anmeldung

Passen Sie gleich nach der Anmeldung in einem Sozialen Netzwerk die **Privatsphäre-Einstellungen** an Ihre Bedürfnisse an. Die Beschäftigung mit diesen Einstellungen bedarf zwar einiger Zeit – es zahlt sich jedoch in jedem Fall aus!

- **Profilsichtbarkeit einschränken – wer darf was sehen?** Sie können für Ihr Profil festlegen, wer welche Angaben lesen darf. Empfehlenswert ist beispielsweise die Einstellung, dass das Profil nur für „Freunde" zugänglich ist.

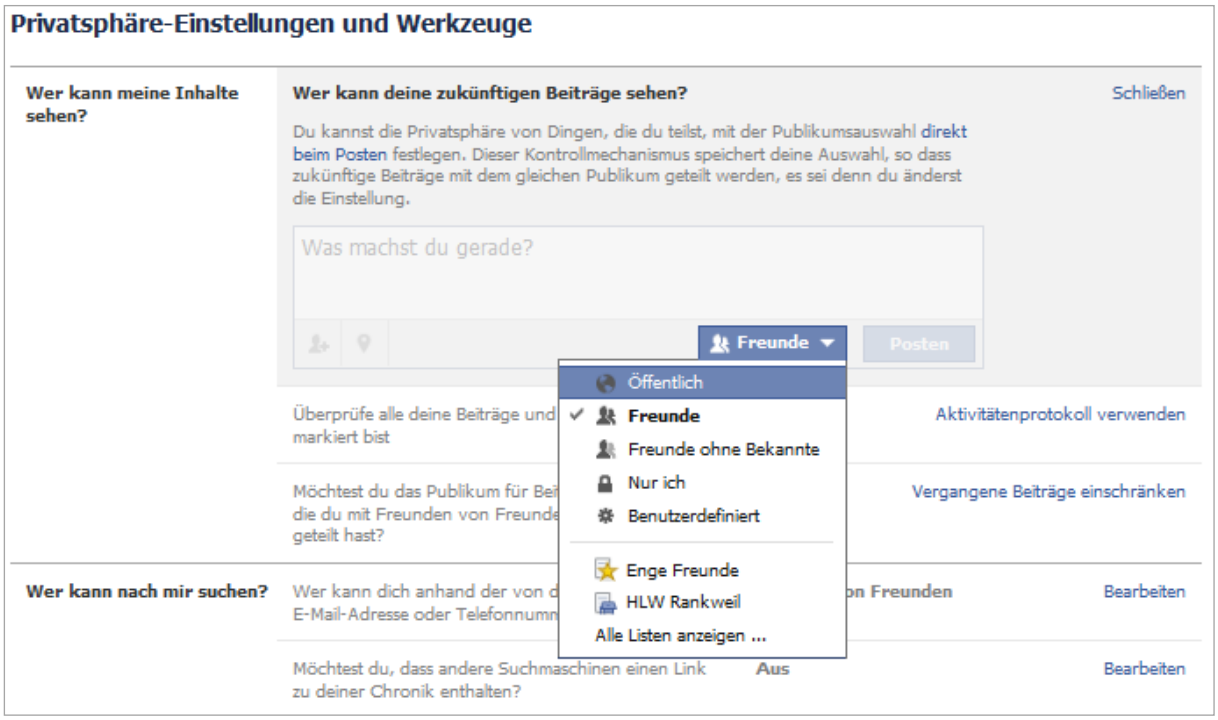


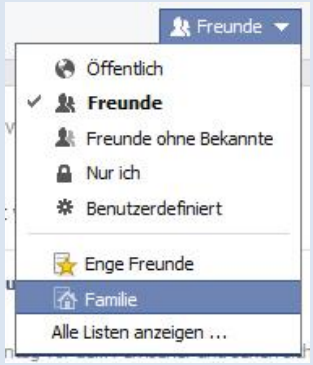
Abb.: Allgemeine Privatsphäre-Einstellungen bei *Facebook* (Quelle: www.facebook.com)

Tipp: „Listen"-Funktion bei *Facebook*

Mit diesem praktischen Feature können Sie Ihre *Facebook*-Freunde in unterschiedliche Gruppen einteilen (z.B. „enge Freunde", „Bekannte", „Arbeit" …) und die von Ihnen geposteten Inhalte dann auch nur für die gewünschten Gruppen sichtbar machen.

***„Freunde" einer Liste hinzufügen*:** Für die Einteilung klicken Sie in der eigenen Chronik auf den Tab „Freunde". Rechts neben jedem „Freund" findet sich ein Button, über den die entsprechende Einstellung gemacht werden kann. Direkt dort können Sie auch neue Listen anlegen.

Eigene Inhalte zielgerichtet steuern: Wenn Sie nun eigene Statusmeldungen, Fotos oder Videos posten, können Sie in einem eigenen Menü unterhalb des Eingabefeldes (*siehe Abbildung*) die entsprechenden Freundesgruppen auswählen. Die Auswahl lässt sich übrigens auch noch für ältere, bereits gepostete Inhalte anpassen.



- **Suche – wie werde ich gefunden?** Eine weitere wichtige Option ist, ob Sie Ihr Profil für öffentliche Suchmaschinen (*Google, 123people*, …) freigeben wollen oder nicht. Die Einstellungen für die Suche sind bei allen Anbietern sehr unterschiedlich. Auch hier gilt: Geben sie besser so wenige Daten wie möglich von sich preis!

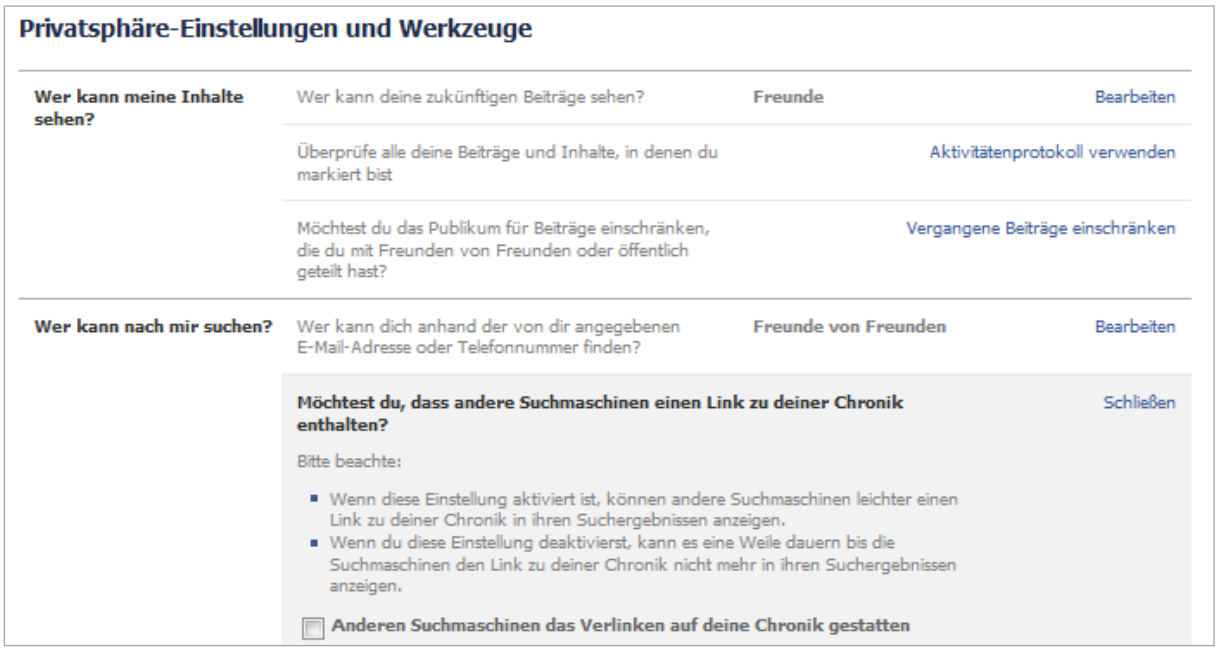


Abb.: Gesucht und gefunden werden auf *Facebook* (Quelle: www.facebook.com)

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 Statusmeldungen, 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. Für eine noch feinere Steuerung der eigenen Inhalte bietet *Facebook* eine praktische „Listen"-Funktion (*siehe Infobox auf Seite 17*).

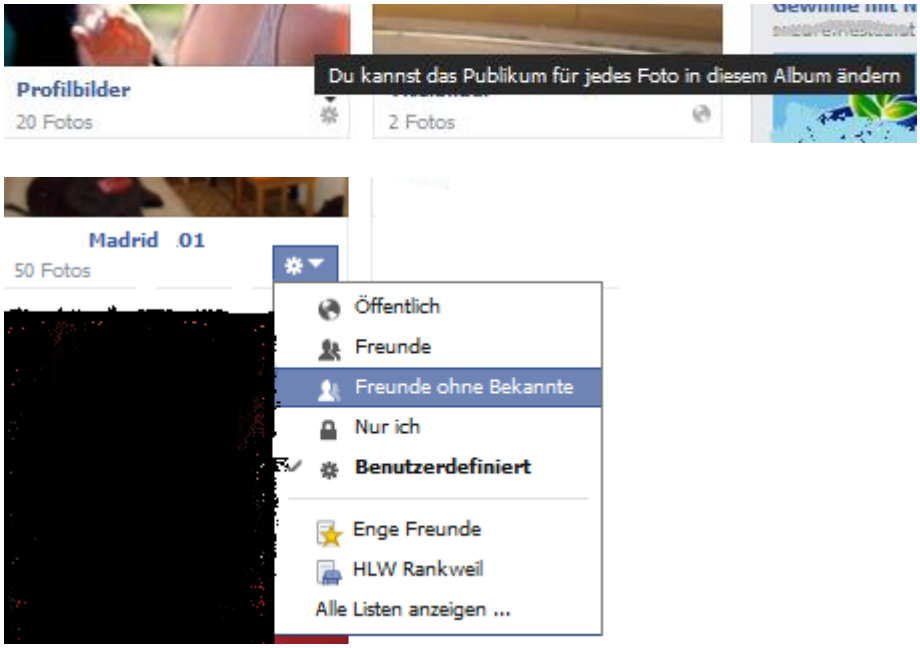


Abb.: Privatsphäre-Einstellungen bei einzelnen Fotoalben auf *Facebook*
(Quelle: www.facebook.com)

- **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 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 Internet 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 häufig über Personen auf der „Freundesliste", die man nicht kennt.

  Tipp: Wenn Fremde Ihnen eine „Freundschaftsanfrage" schicken, nehmen Sie diese Personen vorab genau unter die Lupe und hinterfragen Sie, was für Vorteile Sie von einer gegenseitigen „Freundschaft" haben.

- **Keine peinlichen Bilder veröffentlichen,** auch nicht für „Freunde". Denn aus jedem „Freund" kann später einmal ein „Feind" werden. Immer wieder werden Bilder, die zu Zeiten enger Freundschaft ausgetauscht wurden, später für Cyber-Mobbing missbraucht. Bedenken Sie: „Witzige" Bilder, Intimaufnahmen etc. können von anderen leicht zu Ihrem Nachteil verwendet werden!

- **Externe Anwendungen (Apps):** Viele Plattformen bieten externe Anwendungen von Drittanbietern an. Über diese Anwendungen können Sie z.B. Geburtstagsgrüße versenden, Tests ausfüllen, Spiele spielen etc. Vor allem auf *Facebook* sind solche Apps sehr beliebt.
  Die Nutzung externer Anwendungen ist meist kostenlos, dafür erlauben die Plattform-Betreiber den Drittanbietern Zugriff auf die persönlichen Daten der NutzerInnen sowie auf die Daten aller „Freunde". Wenn einer Ihrer „Freunde" eine solche App ausführt, kann diese – ohne entsprechende Privatsphäre-Einstellungen – folglich auch auf Ihre Daten zugreifen! ForscherInnen in den USA haben herausgefunden, dass 90 Prozent der *Facebook*-Anwendungen auf weitaus mehr private NutzerInnen-Daten zugreifen als für den angebotenen Dienst notwendig wäre.[2] *Beispiel:* Eine Geburtstagskalender-App braucht bestimmt nicht Ihren aktuellen Ort zu wissen!

Tipp: Datenfreigabe für Drittanwendungen beschränken

Facebook erlaubt seinen NutzerInnen, den Zugriff von externen Anwendungen auf private Daten einzuschränken. Sinnvoll ist es, wenn Sie hier besonders restriktiv vorgehen und nur wenige oder gar keine Daten freigeben. Anwendungen, die Sie nicht mehr nutzen oder die Ihnen unseriös erscheinen, sollten Sie unbedingt löschen.

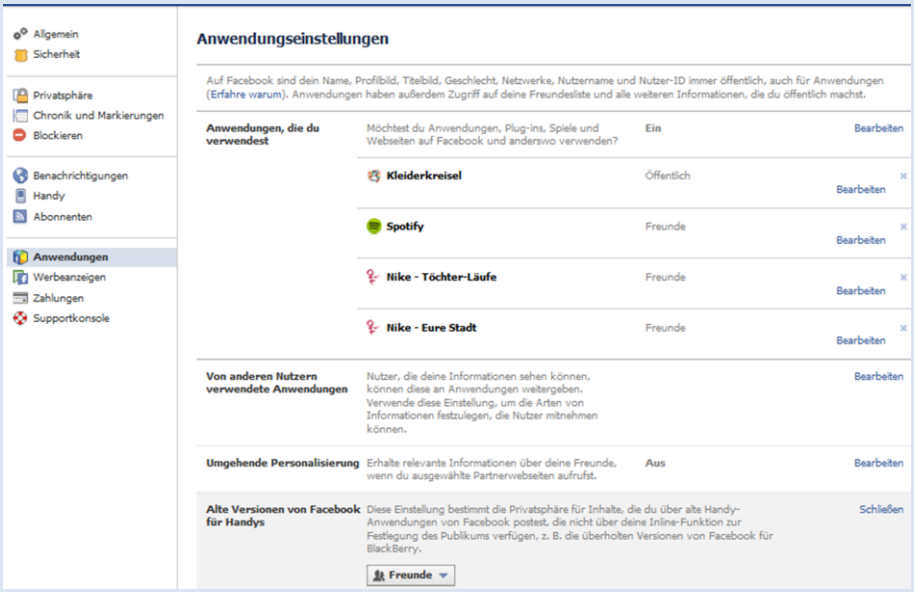


Abb.: Privatsphäre-Einstellungen für Anwendungen auf *Facebook* (Quelle: www.facebook.com)

[2] Adrienne Felt, David Evans: Privacy Protection for Social Networking APIs. http://www.cs.virginia.edu/felt/privacybyproxy.pdf (29.06.2013)

- **Achten Sie die Privatsphäre Ihrer „Freunde":** Genauso wie Sie, hat auch jede andere Person ein Anrecht auf Datenschutz. Bevor Sie private Informationen über „Freunde" oder Fotos, auf denen Dritte abgebildet sind, veröffentlichen, überlegen Sie sich, ob diese Einwände haben könnten. Fragen Sie sicherheitshalber vor der Veröffentlichung bei den Betroffenen nach!

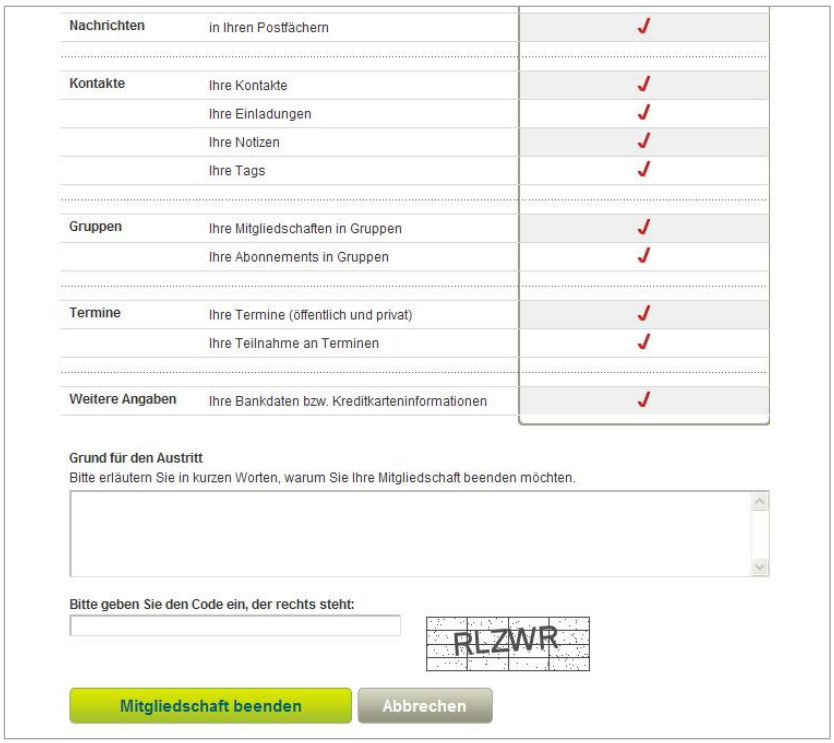
  Als Eltern sollten Sie übrigens dasselbe auch für Ihre Kinder berücksichtigen – nur allzu oft vergessen Eltern jegliche „Hemmungen" in Sozialen Netzwerken und posten quasi öffentlich alle nur erdenklichen Ereignisse und Fotos Ihrer Kinder. Der elterliche Stolz in Ehren, bedenken Sie aber, dass die veröffentlichten Inhalte Ihren Kindern später einmal sehr unangenehm sein könnten.

- **Privatsphäre-Einstellungen kontrollieren:** Überprüfen Sie die Privatsphäre-Einstellungen regelmäßig, da sich diese oft ändern.

Wenn Sie nicht mehr aktiv sind

Das eigene Profil löschen: Wenn Sie auf einer Plattform nicht mehr aktiv sind, löschen Sie Ihr Profil. Denn nicht mehr aktualisierte Angaben können leicht einen falschen Eindruck von Ihrer Person vermitteln. Der Löschvorgang wird einem von den Betreibern 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 – informieren Sie sich am besten bereits im Vorfeld, was genau mit Ihren Daten nach Ihrer Abmeldung passiert und ob Sie darauf Einfluss nehmen können (z.B. Anonymisierung der Daten).



Info: Digitaler Nachlass

Als „digitaler Nachlass" werden jene Daten bezeichnet, die unabhängig vom Tod eines Nutzers oder einer Nutzerin im Internet weiter bestehen. Der Umgang damit stellt Hinterbliebene vor eine große Herausforderung, da sie meist weder wissen, wo der oder die Verstorbene im Internet aktiv war, noch welche Zugangsdaten und Passwörter für die Online-Aktivitäten benutzt wurden.

Auch wenn es für die meisten Menschen ein unangenehmes Thema ist, so ist es dennoch ratsam, für den Fall des Falles vorzusorgen: Legen Sie **eine Liste über alle Mitgliedschaften, Profile, genutzten Dienste und die zugehörigen Zugangsdaten an** und pflegen Sie diese regelmäßig. Ergänzend können Sie in einem Dokument festhalten, was genau nach Ihrem Ableben mit Ihren Online-Daten passieren soll (löschen, archivieren, „Trauerseiten" einrichten, weiterführen, …). Einige Plattformen (etwa *Facebook* und *Google+*) bieten für Ihre Mitglieder inzwischen eigene Angebote zur „Nachlassverwaltung".

Weitere Tipps und Informationen zum „digitalen Nachlass" können Sie auf der Website der *Internet Service Providers Austria* nachlesen: www.ispa.at/digitaler_nachlass

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

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

Mobbing ist an sich kein neues Phänomen. Mit der Verbreitung von Internet und Handy findet das systematische Belästigen, Bloßstellen und Fertigmachen aber auch im „virtuellen Raum" statt. Die Besonderheiten von Cyber-Mobbing: Es kann rund um die Uhr erfolgen, erreicht ein großes Publikum und die TäterInnen agieren (scheinbar) anonym. Neben den vorangegangenen Tipps zum Schutz der Privatsphäre, sollten Sie Folgendes zur Vermeidung von Cyber-Mobbing beachten:

- **Unerwünschte Personen blockieren**: Soziale Netzwerke bieten Ihnen die Möglichkeit, bestimmte Personen, die Sie belästigen, zu blockieren. Blockierte NutzerInnen können nicht mehr auf Ihr Profil zugreifen oder Ihnen Nachrichten senden. In der Regel finden Sie die Einstellungen zum Blockieren direkt im Profil der betreffenden Person (z.B. bei *Facebook* über das Zahnradsymbol rechts oben).

Abb.: Eine Person blockieren auf *Facebook* (Quelle: www.facebook.com)

- **Auf Belästigungen nicht reagieren, aber Beweise sammeln**: Je mehr Sie auf Belästigungen reagieren, desto eher werden die TäterInnen in der Regel dazu animiert, weiterzutun. Zeigen Sie den TäterInnen hingegen die „kalte Schulter", erledigt sich die Sache häufig von selbst. Sollten die Belästigungen andauern, sammeln Sie unbedingt Beweise, z.B. indem Sie Chatprotokolle speichern oder Screenshots anfertigen. Das kann maßgeblich dazu beitragen, die TäterInnen zu identifizieren und im Extremfall auch rechtlich zu belangen.

- **Belästigungen melden:** Alle Sozialen Netzwerke bieten zudem die Möglichkeit, Belästigungen oder bloßstellende Bilder zu melden.

Abb.: Ein Foto auf *Facebook* melden (Quelle: www.facebook.com)

Tipp: Sollten diffamierende Inhalte trotz Meldung nicht gelöscht werden oder die Belästigungen weitergehen, hilft Ihnen der *Internet Ombudsmann* (www.ombudsmann.at) kostenlos weiter.

Vorfälle, die möglicherweise gegen das Gesetz verstoßen, sollten unbedingt zur Anzeige gebracht werden. **Stalking** (also die beharrliche Verfolgung einer Person, §107a StGB) ist seit 2006 in Österreich **strafbar** – das gilt auch für den „virtuellen Raum".

4.3. Urheberrechte berücksichtigen

Nur weil Fotos, Videos, Texte etc. frei im Internet abrufbar sind, heißt das noch lange nicht, dass man diese beliebig verwenden kann. Immer mehr InternetnutzerInnen sehen sich deshalb mit anwaltlichen Abmahnungen aufgrund der Verletzung von Urheberrechten konfrontiert.

Die wichtigste Regel: Will man ein Foto, Video oder ein anderes Werk, das man nicht selbst hergestellt hat, ins Internet stellen, **muss zuvor die Zustimmung des Urhebers/der Urheberin eingeholt werden** (am besten schriftlich). Das gilt z.B. auch für das Hochladen von fremden Inhalten in Soziale Netzwerke.

Dabei ist es egal, ob die Veröffentlichung privaten oder kommerziellen Zwecken dient. Unerheblich ist auch, wie viele Personen tatsächlich auf das Foto, Video etc. im Internet zugegriffen haben bzw. ob es überhaupt jemand angesehen hat. Für eine „Zurverfügungstellung im privaten Rahmen" gibt es zwar Ausnahmeregelungen, meist ist die Rechtssprechung hier aber sehr streng.

Tipp: Creative Commons-Inhalte als Alternative

Manche Werke werden von den UrheberInnen unter eine sogenannte „Creative Commons-Lizenz" (creativecommons.org) gestellt. Damit geben sie anderen Menschen die Möglichkeit, die eigenen **Werke unter bestimmten Bedingungen weiterzuverwenden, ohne ausdrücklich um Erlaubnis fragen zu müssen.** Die private bzw. nicht-kommerzielle Nutzung ist in der Regel kostenlos, wenn der/die UrheberIn sichtbar genannt wird. Der genaue Umfang der Verwendung (z.B. ob Werke auch verändert werden dürfen) hängt von der jeweiligen Lizenz ab – die Bedingungen, unter denen die Werke verwendet werden dürfen, sollten Sie daher immer genau lesen und einhalten.

CC-lizenzierte Inhalte finden:

- Suchmaschine: search.creativecommons.org
- Musik: jamendo.com, freemusicarchive.org, ccmixter.org
- Fotos: flickr.com (die „Erweiterte Suche" auf CC-lizenzierte Bilder einschränken), pixelio.de, openphoto.net

4.4. So schützen Sie sich vor Internet-Betrug

Nirgendwo sonst im Internet findet Betrug so geballt statt wie in Sozialen Netzwerken. Die große Zahl an potenziellen Opfern lockt BetrügerInnen und Daten-Diebe an. Ihre Tricks zielen auf die Neugier und die Unbekümmertheit der NutzerInnen ab: Der fatale Klick auf einen verlockend klingenden Link oder Banner ist schnell passiert – und schon schnappt die Betrugs-Falle zu. Die unangenehmen Folgen sind dann etwa **unwissentlich abgeschlossene Abos**, **überwiesene Geldbeträge** ohne je eine Leistung oder ein Produkt dafür zu bekommen, die **ungewollte Weitergabe persönlicher Daten** an AdresshändlerInnen oder ein **gehacktes Profil**.

Folgende Tipps helfen Ihnen dabei, Betrugs-Fallen in Sozialen Netzwerken zu entgehen:

- Klicken Sie nicht unüberlegt auf allzu verlockend klingende Links in Statusmeldungen, Werbeanzeigen oder Chat-Nachrichten. Auch nicht, wenn die „Empfehlung" scheinbar von „Freunden" kommt. Angebote, die zu schön sind, um wahr zu sein, sollten bei Ihnen die Alarmglocken schrillen lassen!

- Ignorieren Sie alles, was mit Superlativen wie „OMG", „unglaublich", „spektakulär" etc. angekündigt wird.

- Wenn Sie etwas per Klick bestätigen sollen, lesen Sie genau durch, was Sie damit bestätigen („Kleingedrucktes"). Das betrifft auch das Ausfüllen von Gewinnspiel-Formularen.

- Informieren Sie sich immer zuerst über den Seitenbetreiber, z.B. über das Impressum.

- Seien Sie generell vorsichtig mit der Angabe persönlicher Daten wie Adresse, Handynummer, Geburtsdatum etc. im Internet.

- Nehmen Sie nur „Freundschaftsanfragen" von Personen an, die Sie auch tatsächlich kennen. Seien Sie kritisch, wenn Ihnen Fremde irgendwelche Versprechungen machen.

- Verwenden Sie immer ein täglich aktualisiertes Anti-Viren-Programm auf Ihrem Computer.

- Melden Sie verdächtige Statusmeldungen, Fotos, Videos, Profile, Seiten, Werbeanzeigen oder Apps an die Plattform-Betreiber, damit diese gelöscht werden.

Tipp: Infos und Warnungen zu Internet-Betrug

Tagesaktuelle Warnungen und Erklärungen zu den gängigsten Betrugsarten im Internet finden Sie unter: www.watchlist-internet.at

Beratungsanfragen können Sie kostenlos an den Internet Ombudsmann (www.ombudsmann.at) oder die Beratungsstellen der Arbeiterkammern (www.arbeiterkammer.at) stellen. Eine Straftat können Sie auf jeder Polizeidienststelle zur Anzeige bringen.

5. Tipps für Eltern

1. **Entdecken Sie das Internet gemeinsam mit Ihrem Kind.**

Suchen Sie interessante und spannende Websites entsprechend dem Alter Ihres Kindes und erforschen Sie diese miteinander. Gemeinsame Erfahrungen erleichtern es, über positive und negative Erlebnisse bei der Internetnutzung zu sprechen.

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

Diese können z.B. den zeitlichen Umfang, die genutzten Inhalte, den Umgang mit Bildern und persönlichen Daten etc. betreffen. Bedenken Sie: Regeln sind nur dann wirksam, wenn Ihr Kind diese versteht und akzeptiert!

3. **Erklären Sie Ihrem Kind, warum persönliche Daten mit Vorsicht weiterzugeben sind.**

Sprechen Sie mit Ihrem Kind über die Risiken einer leichtfertigen Datenweitergabe im Internet. Name, Adresse, Telefonnummer und persönliche Fotos sollte Ihr Kind nur nach Absprache mit Ihnen weitergeben.

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

Es ist ok, sich mit Bekanntschaften aus dem Netz zu treffen – aber nur an öffentlichen Orten (z.B. Kinocenter, Café) und in Begleitung (Erwachsener oder zumindest FreundIn).

5. **Diskutieren Sie mit Ihrem Kind den Wahrheitsgehalt von Online-Inhalten.**

Zeigen Sie Ihrem Kind, wie die Richtigkeit von Inhalten aus dem Internet durch Vergleiche mit anderen Quellen überprüft werden kann. Auch Werbung ist für Kinder oft nur schwer zu durchschauen. Sensibilisieren Sie Ihr Kind dafür, dass es im Internet sehr einfach ist, etwas vorzuspielen.

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

Kinderpornografie und neonazistische Inhalte sind in Österreich gesetzlich verboten.

7. **Ermutigen Sie Ihr Kind zu guter Netiquette.**

Auch im Internet gibt es Regeln. Einfach gesagt: Was im realen Leben erlaubt ist, ist auch im Internet erlaubt. Was im realen Leben verboten ist, ist auch im Internet verboten.
Beispiel: Vor der Veröffentlichung eines Fotos immer zuerst die abgebildeten Personen um Erlaubnis fragen.

8. **Informieren Sie sich über die Internetnutzung Ihres Kindes.**

Lassen Sie sich von Ihrem Kind aktuelle Lieblingsseiten, -spiele oder -apps zeigen und versuchen Sie zu verstehen, warum es diese toll findet. Machen Sie die Internetnutzung zu einem gewohnten Thema in Ihrer Familie.

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 nicht mit Internetverbot! Sie möchten ja, dass es sich auch in Zukunft wieder an Sie wendet, wenn es in eine unangenehme Situation geraten ist.

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

Das Internet ist ein ausgezeichnetes Medium zum Lernen, zur Kommunikation und auch für die Freizeitbeschäftigung. Ermutigen Sie Ihr Kind, das Internet bewusst zu nutzen und alle positiven Möglichkeiten zu erforschen. Unter Anleitung können die Risiken sehr gut eingeschränkt werden.

Tipp: Infos zur sicheren Internetnutzung

Weitere praktische Tipps zur sicheren und verantwortungsvollen Nutzung des Internets finden Sie laufend aktualisiert auf der Website von *Saferinternet.at*: www.saferinternet.at