KANTON LUZERN

Datenschutzbeauftragter
des Kantons Luzern
Bahnhofstrasse 15
6002 Luzern
Telefon 041 228 66 06
dsb@lu.ch
www.datenschutz.lu.ch

Merkblatt "Richtiger Umgang mit den Sozialen Netzwerken"

1. Zweck des Merkblattes

Die Bedeutung von Sozialen Netzwerk Anwendungen im Internet ist in den letzten Jahren kontinuierlich gestiegen. Alleine in der Schweiz sind heute 2.48 Mio. Facebook Benutzer aktiv. Anbieter wie Facebook und Co. ziehen nach eigenen Angaben weltweit jeden Monat jeweils weit mehr als 100 Millionen Besucher auf Ihren Webseiten an.

Soziale Netzwerke und die in ihnen abgelegten persönlichen Profile (Daten) haben heute einen wichtigen Stellenwert bekommen. Sie repräsentieren die virtuellen Identitäten der Nutzer im Internet. Hier stellt sich die Frage: wie können soziale Netzwerke und ihre positiven Aspekte sinnvoll genutzt, die eigene Privatsphäre jedoch in ein vertretbares Verhältnis dazu gesetzt werden?

2. Risiken für den Anwender

Was passiert, wenn Ihr (zukünftiger) Arbeitgeber Ihre Fotos der letzten feucht-fröhlichen Party sieht? Wofür könnten Betrüger Informationen über Ihre Arbeit oder geplante Urlaube ausnutzen? Diese und andere Fragen sollten Sie sich stellen, bevor Sie ein Profil in einem sozialen Netzwerk anlegen beziehungsweise bevor Sie dort jede Menge Informationen über sich preisgeben.

Offenlegung privater Informationen
In sozialen Netzwerken können Nutzer E-Mail-Adressen, Telefonnummern, Hobbys, Vorlieben und diverse persönliche Informationen angeben. Diese Daten können von Firmen dazu missbraucht werden, die Nutzer gezielt mit Werbung zu bombardieren.
Die Voreinstellungen zum Schutz der Privatsphäre sind bei Eröffnung eines Accounts oft nicht ausreichend vorgenommen. Alle Daten sind so automatisch für alle Nutzer des sozialen Netzwerks sichtbar. Auszüge der Profile können teilweise sogar über Suchmaschinen gefunden werden und sind so allen Internetnutzern weltweit zugänglich.

Im Bewerbungsprozess nutzen Arbeitgeber soziale Netzwerke, um Informationen über potentielle Mitarbeiter herauszufinden. Freizügige Fotos oder verfängliche Äusserungen werden da schnell zum k.o.-Kriterium. Auch Vermieter und Versicherungen könnten an den preisgegebenen Hintergrundinformationen interessiert sein.

Informationen, Texte und insbesondere Bilder werden häufig von Privatpersonen auch ausserhalb der Netzwerke auf dem eigenen Computer archiviert. So können Daten plötzlich

auf anderen Seiten im Internet auftauchen oder für andere Zwecke missbraucht werden – auch nachdem diese vermeintlich aus dem sozialen Netzwerk gelöscht wurden.

Identitätsdiebstahl
Kriminelle versuchen zunehmend, bestehende Nutzer-Accounts zu hacken, um diese Identität für ihre Betrügereien zu nutzen. Oftmals täuschen sie nach Übernahme eines Accounts eine Notsituation vor und bitten die vernetzen Freunde um finanzielle Hilfe. Das über das Nutzerprofil erlesene Wissen kann dazu beitragen, das Vertrauen zu untermauern und Freunde zu täuschen. „Unechte" Profile werden zunehmend dazu genutzt, Personen zu schaden: Diebe können so zum Beispiel ausspionieren, wann jemand im Urlaub ist und die Wohnung leer steht.

Verbreitung von Schadsoftware
Das Vertrauen der Nutzer in die sozialen Netzwerke ist meist gross. Betrüger haben deshalb eine gewohnte Masche auf diese Plattformen übertragen: Sie verschicken Nachrichten, die einen Link auf manipulierte Webseiten enthalten. Über diese Seiten werden dann die Schadprogramme verbreitet. Ein bekanntes Beispiel hierfür ist der Wurm „Koobface", der zum Beispiel über Facebook verbreitet wurde. Von zuvor infizierten Konten aus wurden Einladungen an andere Nutzer verschickt, sich ein Video anzusehen. Klickte der Empfänger auf den angegebenen Link, wurde er jedoch auf eine gefälschte Facebook- oder YouTube-Seite geleitet, auf der er zum Download des Flash-Players aufgefordert wurde. Hinter dem angebotenen Download verbarg sich aber der Wurm, der sich so immer weiter verbreiten konnte.

Einige soziale Netzwerke bieten Zusatzanwendungen an, die Nutzer ihrem Profil hinzufügen können. Ein Beispiel hierfür sind Mini-Spiele, die die Nutzer auch vernetzt spielen können. Problematisch ist, dass diese Anwendungen von Drittanbietern stammen, deren Sicherheitsstandards nicht zwangsläufig denen der sozialen Netzwerke entsprechen müssen. Auf diese Weise können – ob beabsichtigt oder ungewollt – Schadprogramme verbreitet werden.

Mobbing
Soziale Netzwerke haben Mobbing auf eine neue Ebene gebracht. Personen können zum Beispiel bewusst aus Freundesgruppen ausgeschlossen oder ihre digitalen Pinnwände mit Beleidigungen bombardiert werden. Dies kann vor allem für Jugendliche zu einer Belastung werden. Mobbing wird strafrechtlich verfolgt.
Freundschaften sind in sozialen Netzwerken schneller geschlossen als in der „realen" Welt. So gelangen Informationen an Personen, die diesen sonst vielleicht nicht anvertraut worden wären. Wer böswillige Absichten hat, kann diese Informationen dafür nutzen, um jemanden bewusst bloss zustellen oder gegen ihn zu intrigieren.

So genannte „Cyberstalker" können sich auch „unechte" Profile anlegen, in denen sie sich als eine reelle oder fiktive andere Person ausgeben. So können sie in vollkommener Anonymität andere Personen über das soziale Netzwerk belästigen.

3. Verhaltensregeln zum sicheren Umgang mit Sozialen Netzwerken

Millionen Internet-Benutzer knüpfen Kontakte und pflegen Freundschaften über das Internet. Sie legen in Facebook & Co. ein persönliches Profil an, das neben grundlegenden Angaben zu ihrer Person auch Informationen über Hobbys, die Familienverhältnisse oder den beruflichen Werdegang enthalten kann. Das Ziel sozialer Netzwerke ist, sich mit Freunden zu vernetzen und Inhalte zu teilen. Damit sich alle Nutzer in einem sozialen Netzwerk wohl fühlen, ist es wichtig, dass Sie sich an einige Verhaltensregeln - die auch im realen Leben gelten - halten. Die soziale Vernetzung soll Spass machen, und damit es auch so bleibt, ist

ein freundlicher und respektvoller Umgang miteinander vorausgesetzt. Mit den folgenden 12 Verhaltensregeln sind Sie gut gerüstet für das soziale Leben im Internet.

1. **Seien Sie zurückhaltend mit der Preisgabe persönlicher Informationen!** Nicht alles, was Sie über sich wissen, müssen andere Menschen wissen. Überprüfen Sie kritisch, welche privaten Daten Sie „öffentlich" machen wollen. Bedenken Sie zum Beispiel, dass immer mehr Arbeitgeber Informationen über Bewerber im Internet recherchieren. Auch Headhunter, Versicherungen oder Vermieter könnten an solchen Hintergrundinformationen interessiert sein.

2. **Erkundigen Sie sich über die Allgemeinen Geschäftsbedingungen und die Bestimmungen zum Datenschutz des genutzten sozialen Netzwerks!** Mit beidem sollten Sie sich gründlich vertraut machen – und zwar bevor Sie ein Profil anlegen. Nutzen Sie unbedingt die verfügbaren Optionen des sozialen Netzwerks, mit denen die von Ihnen eingestellten Informationen und Bilder nur eingeschränkt „sichtbar" sind: Sollen nur Ihre Freunde Zugriff darauf haben oder auch die Freunde Ihrer Freunde oder alle Nutzer?

3. **Seien Sie wählerisch bei Kontaktanfragen – Kriminelle „sammeln" Freunde, um Personen zu schaden!** Bei Personen, die Sie nicht aus der „realen" Welt kennen, sollten Sie kritisch prüfen, ob Sie diese in Ihre Freundesliste aufnehmen wollen. Der oder die Unbekannte könnte auch böswillige Absichten haben. Kriminelle könnten zum Beispiel ausspionieren, wann Ihre Wohnung leer steht. „Unechte Profile" werden nachweislich dazu genutzt, Personen zu schaden – sei es aus Rache, Habgier oder anderen Beweggründen.

4. **Melden Sie „Cyberstalker", die Sie unaufgefordert und dauerhaft über das soziale Netzwerk kontaktieren!** Dafür können Sie sich meistens direkt an die Betreiber des jeweiligen sozialen Netzwerkes wenden. Diese können der Sache nachgehen und gegebenenfalls das unseriöse Profil löschen. In besonderen Fällen sollten Sie auch die Polizei für eine Strafverfolgung informieren.

5. **Verwenden Sie für jede Internetanwendung, insbesondere auch wenn Sie in verschiedenen sozialen Netzwerken angemeldet sind, ein unterschiedliches und sicheres Passwort!** Seien Sie sich aber auch darüber bewusst, dass Ihre Daten auf fremden Rechnern gespeichert sind. Das heisst die Sicherheit Ihrer Daten hängt nicht nur von Ihnen ab, sondern auch von den Betreibern des sozialen Netzwerks: wird deren Server gehackt, sind Ihre Daten nicht mehr sicher. Wenn Missbrauch bekannt wird, informieren Sie auch Ihre Freunde.

6. **Geben Sie keine vertraulichen Informationen über Ihren Arbeitgeber und Ihre Arbeit preis!** Berufliche Informationen haben in sozialen Netzwerken nichts verloren. Auch Wirtschaftsspione haben soziale Netzwerke für sich entdeckt und versuchen dort, wertvolle Informationen abzuschöpfen. Das kann Ihre Firma Geld und Sie den Job kosten.

7. **Prüfen Sie kritisch, welche Rechte Sie den Betreibern sozialer Netzwerke an den von Ihnen eingestellten Bildern, Texten und Informationen einräumen!** Keine Leistung ohne Preis: Die Eintrittskarte in soziale Netzwerke kostet Sie die Preisgabe von Informationen. Viele Firmen sind bereit, für diese Daten Geld zu bezahlen, um gezielt Werbung verschicken zu können. Geben Sie den sozialen Netzwerken die Rechte an Ihren Bildern, können diese theoretisch von den Betreibern weiterverkauft werden. Prüfen Sie auch, ob das gewährte Nutzungsrecht womöglich bestehen bleibt, wenn Sie Ihr Profil löschen.

8. **Wenn Sie „zweifelhafte“ Anfragen von Bekannten erhalten, erkundigen Sie sich ausserhalb sozialer Netzwerke nach der Vertrauenswürdigkeit dieser Nachricht!** Identitätsdiebstahl ist ein Risiko des digitalen Zeitalters. Eine fremde Person kann mit Hilfe eines gehackten Accounts, eine fremde Identität übernehmen und deren Freunde täuschen. Betrüger können zum Beispiel Nachrichten verschicken, in denen sie eine Notsituation beschreiben und um finanzielle Hilfe bitten. Mit Hilfe des angelesenen Wissens über die gestohlene Identität kann dabei die Vertrauenswürdigkeit untermauert werden.

9. **Klicken Sie nicht wahllos auf Links – Soziale Netzwerke werden verstärkt dazu genutzt, um Phishing zu betreiben!** Auf einen Link ist schnell geklickt. Aber Vorsicht: die Zieladresse könnte eine gefälschte Startseite eines sozialen Netzwerkes sein. Geben Sie dort Ihren Benutzernamen und Kennwort ein, werden die Daten direkt an die Betrüger weitergeleitet. Besonders beliebt sind bei solchen Attacken so genannte Kurz-URLs, bei denen der Nutzer die eigentliche Zieladresse nicht erkennen kann.

10. **Sprechen Sie mit Ihren Kindern über deren Aktivitäten in sozialen Netzwerken und klären Sie sie über die Gefahren auf!** Viele Kinder und Jugendliche sind sich oft nicht bewusst, welche Gefahren in sozialen Netzwerken lauern – Spass geht ihnen häufig vor Sicherheit. Die Stärkung der „Medienkompetenz“ ist eine neue Aufgabe, die Eltern in der Erziehung übernehmen müssen. Aber auch mit anderen Familienangehörigen und Freunden sollten Sie sich über Risiken und Bedenken austauschen.

11. **Arbeitgeber**, die die Verwendung von Social Networks wie Facebook etc. im Unternehmen erlauben, sollten eine sogenannte Social Media Weisung erstellen und die Mitarbeitenden mit dem Umgang entsprechend sensibilisieren. Die Social Media Weisung soll als Ergänzung zum Arbeitsvertrag von jedem Mitarbeiter unterschrieben werden.

12. **Benutzen** Sie Facebook auf mobilen Geräten, können die Facebook-Benutzer ihren aktuellen Standort erkennen. So wissen mögliche Einbrecher, dass Sie im Moment nicht zu Hause sind. Achten Sie darauf, dass Sie diese Funktion deaktivieren oder nur gezielt einsetzen.

4. Fragen und Informationen

Dieses Merkblatt wurde in Zusammenarbeit mit dem Verein InfoSurance erstellt und dient zur Sensibilisierung der Schweizer Bevölkerung im Umgang mit dem Computer und Internet. Haben Sie Fragen in Bezug auf den Datenschutz von Sozialen Netzwerken bitten wir Sie sich direkt mit dem EDÖB, dem eidgenössischen Datenschutzbeauftragten in Bern in Verbindung zu setzen.

Postadresse:	Datenschutzbeauftragte des Kantons Luzern Bahnhofstrasse 15 6002 Luzern
Telefon:	+ 41 41 228 66 06
Fax:	+ 41 41 228 69 13
eMail:	dsb@lu.ch
Internet:	www.datenschutz.lu.ch

InfoSurance
und Ihr Computer ist sicher.

Luzern, März 2011, v1.0