Sicherheitstipp April 2012 / Soziale Netzwerke

Einführung

"Das Netz vergisst nichts“. Damit Nutzer sich über die möglichen Gefahren von Facebook, Twitter und Co. bewusst werden, bieten wir Ihnen zehn Tipps für sicheres Surfen in sozialen Netzwerken.

1. Zurückhaltung bei persönlichen Informationen

Wer persönliche Daten im Internet preisgibt, sollte sich das vorher genau überlegen. Arbeitgeber, Headhunter, Versicherungen oder Vermieter können an Hintergrundinformationen interessiert sein und diese im Internet recherchieren.

2. Informieren Sie sich über AGBs und Datenschutzbestimmungen

Mit den Allgemeinen Geschäftsbedingungen und den Datenschutzbestimmungen eines sozialen Netzwerks sollte man sich vertraut machen, bevor man sich ein Profil einrichtet. Bei Facebook etwa kann man festlegen, dass nur bestätigte Kontakte Informationen und Bilder sehen können.

3. Nicht jeden Kontakt bestätigen

Bei Kontaktanfragen darf man ruhig wählerisch sein. Denn Unbekannte könnten auch böswillige Absichten haben. Kriminelle könnten beispielsweise ausspionieren, wann eine Wohnung leer steht.

4. Melden Sie Cyberstalker

Wenn Personen Sie unaufgefordert und dauerhaft über das soziale Netzwerk kontaktieren, müssen Sie das nicht ertragen. Wenden Sie sich direkt an den Betreiber des sozialen Netzwerks. In besonderen Fällen empfiehlt das BSI, auch die Polizei für eine Strafverfolgung zu informieren.

5. Verwenden Sie nie das gleiche Passwort

Sie sollten für jede Internetanwendung, auch wenn Sie in verschiedenen sozialen Netzwerken angemeldet sind, ein unterschiedliches und sicheres Passwort verwenden. Die Sicherheit Ihrer Daten hängt immer auch von den Betreibern des sozialen Netzwerks ab. Werden deren Server gehackt, sind Ihre Daten trotz guter Passwörter nicht mehr sicher. Wenn Missbrauch bekannt wird, informieren Sie auch Freunde und Bekannte.

6. Vorsicht bei vertraulichen Informationen über den Arbeitgeber

Vertrauliche Informationen aus Ihrem Job können Ihren Arbeitgeber Geld und Sie den Job kosten.

7. Prüfen, welche Rechte Betreiber an eingestellten Bildern, Texten und Informationen bekommen

Geben Sie sozialen Netzwerken die Rechte an Ihren Bildern, können diese theoretisch von den Betreibern weiterverkauft werden. Oft bleiben solche Nutzungsrechte gar bestehen, wenn man sein Profil löscht.

8. Zweifelhaften Anfragen von Bekannten nachgehen

Wenn Sie zweifelhafte Anfragen von Bekannten erhalten, könnte ein Identitätsdiebstahl vorliegen. Deshalb sollten Sie sich bei einem Verdacht außerhalb des sozialen Netzwerks nach der Vertrauenswürdigkeit der Nachrichten und damit der Identität von Bekannten erkundigen. Betrüger können zum Beispiel Nachrichten verschicken, in denen Sie eine Notsituation beschreiben und um finanzielle Hilfe bitten.

9. Klicken Sie nicht wahllos auf Links

Soziale Netzwerke werden verstärkt dazu genutzt, um Phishing zu betreiben. Die Zieladresse eines Links könnte etwa eine gefälschte Startseite eines sozialen Netzwerks sein. Gibt man dort Benutzernamen und Kennwort ein, werden die Daten direkt an den Betrüger weitergeleitet. Häufig kommen Kurz-URLs zum Einsatz, bei denen der Nutzer die eigentliche Zieladresse nicht erkennen kann.

10. Mit Kindern über soziale Netzwerke sprechen

Eine wichtige Aufgabe von Eltern besteht darin, die Medienkompetenz ihrer Kinder zu stärken. Sprechen Sie mit Ihren Kindern über ihre Aktivitäten in sozialen Netzwerken und klären Sie sie über Gefahren auf.

Zumikon, 30.01.2012

FP2 Security Solutions
Schwäntenmos 15
8126 Zumikon
T +41 79 416 74 10
www.fp2.ch
info@fp2.ch