



Gemeinsames Präventionsprojekt von Polizei und VKP **Gefahr durch neue Medien – Wie sicher Sie leben, entscheiden Sie selbst!**

Serienbeitrag 5

Soziale Netzwerke wie Facebook, StudiVZ, SchülerVZ pp.

Soziale Netzwerke bieten den unterschiedlichsten Menschen die Möglichkeit, sich über die verschiedensten Themen auszutauschen. Sie sind grundsätzlich harmlos, denn deren Betreiber verfolgen keinerlei kriminelle Absichten.

Aber der Mensch ist nun mal ein kommunikatives Lebewesen, der auch andere an seinem Leben teilhaben lassen will und sich dadurch angreifbar macht!

Sehr häufig kennen sich die Personen nämlich nicht persönlich, sondern nur über das digitale Kommunikationsmittel Computer. Trotzdem vertrauen Sie den dort hinterlegten Einträgen und Angaben über die jeweilige Person blind. Manchmal zu Recht, doch häufig zu Unrecht.

Aber nicht jeder benötigt alle Informationen von seinen Mitmenschen. Überprüfen Sie deshalb regelmäßig ihre Datenschutzeinstellungen und hinterfragen Sie kritisch, wer welche Informationen sehen darf und welchen Applikationen Sie den Zugriff auf Ihr Profil erlauben möchten.

Allzu große Offenheit macht angreifbar: Denn nicht nur Spammer, also die Versender von unerwünschten Mitteilungen (z.B. Spam-Mails), auch Datendiebe interessieren für die öffentlich zugänglichen Informationen. Längst hat sich ein Online-Schwarzmarkt etabliert, auf dem persönliche Daten in großen Paketen gehandelt werden.

Von Interesse sind alle möglichen Datensätze, nicht nur Ihre Shopping - Gewohnheiten. Die Polizei und der VKP-WHV meinen dazu:

„Nicht jeder Facebook-Kontakt ist auch wirklich Ihr Freund“!

Wenn Sie „zweifelhafte“ Anfragen von Bekannten erhalten, erkundigen Sie sich **außerhalb sozialer Netzwerke** nach der Vertrauenswürdigkeit dieser Nachricht und der Quelle! Identitätsdiebstahl ist ein Risiko des digitalen Zeitalters. Eine fremde Person kann mit Hilfe verschiedener Techniken problemlos Ihren Account „hacken“ und so Ihre Identität annehmen. Betrüger können zum Beispiel in Ihrem Namen Nachrichten verschicken, in denen sie eine Notsituation beschreiben und um finanzielle Hilfe in Ihrem Freundeskreis bitten.

Sicherheitsregeln für Social-Network-Nutzer:

1. Seien Sie stets zurückhaltend mit der Preisgabe persönlicher Informationen und machen Sie sich nicht angreifbar!
Denn nicht alles, was Sie über sich wissen, müssen andere Menschen wissen. Überprüfen Sie kritisch, welche privaten oder beruflichen Daten „öffentlich“ sein müssen. Bedenken Sie zum Beispiel, dass immer mehr Firmen Informationen über Konkurrenten und Arbeitssuchende im Internet recherchieren.
2. Allzu private Bilder, das sind solche mit freizügigen Posen oder von feuchtfröhlichen Partys, können Ihnen langfristig nur schaden!
3. Verwenden Sie niemals dasselbe **Password** für mehrere Anwendungen, besonders nicht für das E-Mail-Konto und das soziale Netzwerk. Ändern Sie diese regelmäßig.
4. Geben Sie keinesfalls persönliche Daten, wie etwa Handynummern oder den Wohnort, auf Ihrer öffentlich einsehbaren Seite bekannt.
5. Verwenden Sie bestenfalls **FreeMail-Adressen** (z.B. von Web.de oder GMX.de), die sie leicht entsorgen können, falls Sie mit unerwünschten eMails überflutet werden.
6. Seien Sie vorsichtig bei Einladungen von „Freunden“ die man nicht kennt, und beantworten Sie niemals Anfragen von völlig fremden Mitgliedern. Verstehen Sie derartige „Communitys“ als Teil Ihres privaten Telefonbuches und nicht als Ihren engsten Freundeskreis.
7. Benutzen Sie keinen Computer, bei dem Sie nicht sicher sind, dass er frei von Viren oder Trojanern ist. Dies ist z.B. häufig bei sog. Internet-Cafes der Fall!
8. Verwenden Sie stets und ausnahmslos aktuelle Sicherheits-Software auf Ihrem eigenen PC.
9. Installieren Sie immer die neuesten Updates für das verwendete Betriebssystem, am besten aktivieren Sie die Funktion „automatisches Update“ und wählen die höchsten Sicherheitseinstellungen.

Siehe dazu auch:

www.bsi-fuer-buerger.de

Die Beauftragte für Kriminalprävention der Polizei, Polizeioberkommissarin Katja Reents, bietet darüber hinaus Vorträge und persönliche Beratungen zu diesem Thema an. Sie ist dienstlich unter der Rufnummer 04421-942-108 zu erreichen.

Für Rückfragen stehen wir Ihnen gerne zur Verfügung:

Markus Wallenhorst
Presse- und Öffentlichkeitsarbeit
Polizeiinspektion Wilhelmshaven/Friesland
04421-942-404
markus.wallenhorst@polizei.niedersachsen.de

Andrea Papenroth, Pressesprecherin des
VKP,
Tel. 04421-942-437
andrea.papenroth@polizei.niedersachsen.de