Spam Mails in Ihrem Namen oder mit dem Absender Ihrer Schule?

Ist das bei Ihnen vielleicht auch schon vorgekommen?
In Ihrem Namen und mit Ihrer E-Mail-Adresse im Absenderfeld wurden E-Mails verschickt – und das ohne, dass Sie es wussten und vor allem wollten?

Immer häufiger passiert es in der letzten Zeit, dass Spammer Absenderadressen fälschen, um unerkannt ihr Unwesen treiben zu können. Wie leicht sich die E-Mail-Adressen fälschen lassen, ist erschreckend: Es sind keinerlei Spezialkenntnisse dafür notwendig, lediglich ein Zugang zu einem E-Mail-Server ist nötig, um E-Mails mit beliebigem Absender zu verschicken.

Wie Sie erkennen, ob ein E-Mail-Absender gefälscht ist und wie Sie sich gegen Spam wehren können...

Wie können Sie gefälschte E-Mail-Absender erkennen?

Wie können aber Sie erkennen, ob die E-Mail wirklich von dem Absender stammt, der in dem Adressfeld aufgeführt ist? Einen ersten Hinweis finden Sie im sogenannten E-Mail-Header.

Der E-Mail-Header ist die Informationen, die am Anfang einer E-Mail steht. Er zeigt den Zustellweg der E-Mail chronologisch rückwärts an: Im Header sind Sender und Empfänger der E-Mail sowie Name und IP-Adresse der Server eingetragen, über die die Mail verschickt wurde. Auch der E-Mail-Betreff findet sich in im Header wieder.

Um zu identifizieren, von wem die Mail stammt, können Sie beispielsweise in Outlook unter "Ansicht“ und "Optionen“ den kompletten E-Mail-Header aufrufen. Beispiel:

E-Mail-Header-Screenshot

Wichtig ist hierbei die Zeile "Received from“. Es werden alle Server und Mail-Dienste aufgezählt, die bei dem E-Mail-Versand beteiligt waren. Der letzte Server ist der Server, über den die E-Mail versandt wurde. Die Absender werden mit "from“ gekennzeichnet, die Empfänger mit "by“.

Es ist also nur über die letzte Received-Zeile im Header normalerweise eine eindeutige Identifikation des Senders möglich. Die weiteren Zeilen, wie beispielsweise die E-Mail-Adresse des Senders, können zwar Hinweise geben, sind aber keine sicheren Quellen, da sie leicht manipulierbar sind.

Jedoch nutzen viele Spammer mittlerweile für ihre Zwecke so genannte Open-Relay-Server. Das sind E-Mailserver, die es Dritten durch fehlerhafte Konfigurationen erlauben, die eigene Identität – somit auch die E-Mail-Adresse – zu verschleiern bzw. zu fälschen.
Somit ist eine Rückverfolgung und die Ermittlung des Verursachers des Mail-Mülls schwierig bis nahezu unmöglich.

Sehr ausführliche Informationen zum Thema E-Mail-Header finden Sie unter:

FAQ E-Mail-Header lesen und verstehen.
http://sites.inka.de/ancalagon/faq/headerfaq.php3