SO SCHÜTZEN SIE SICH VOR PHISHING-MAILS UND SPAM

Veröffentlicht am 17. Januar 2013 von Annette

Jeder Deutsche bekommt täglich 9 Spam-Mails. Auch wenn die Zeiten klassischer Spam-Mails lange vorbei sind, ist die Bedrohung [...]

Jeder Deutsche bekommt täglich 9 Spam-Mails. Auch wenn die Zeiten klassischer Spam-Mails lange vorbei sind, ist die Bedrohung durch Emails nicht weniger geworden. Mittlerweile sorgen zielgerichte Phishing-Aktionen für erheblichen Schaden. Worum handelt es sich dabei genau und wie kann man sich davor schützen?

Nervige Werbemails: Spam
Spam bezeichnet **Emails, die ein Empfänger unerwünscht erhält** und die häufig **werbenden Inhalt** haben. Das Wort "Spam" ist ursprünglich ein Name für Dosenfleisch - eines der wenigen Nahrungsmittel, die während des zweiten Weltkrieges in Großbritannien in großer Menge vorhanden und somit einige Zeit quasi omnipräsent waren. Ein Sketch von Monty Python's Flying Circus verdeutlicht die nervige, übermäßige Verwendung des Produkts. Dies trug dazu bei, dass auch Mail-Müll im Netz als Spam betitelt wurde. Ein Begriff, der sich etabliert hat.

Eine Geschichte der Email ohne Spam gibt es wohl kaum. Und ein Ende ist nicht abzusehen. Im letzten Jahr wurden **pro Tag rund 300 Millionen Spam-Nachrichten** in deutschen Email-Postfächern zugestellt. Dadurch, dass der Email-Verkehr zum Standard geworden ist und Benutzer an vielen Stellen im Netz ihre Emailadresse hinterlegen, bieten sich vielfältige Möglichkeiten für Spammer, um Werbemails zu versenden. Wie kann man sich schützen? **In diesem Artikel** haben wir Ihnen bereits viele hilfreiche Tipps zusammengestellt. Am Wichtigsten ist es, seine Emailadresse **nicht unüberlegt preiszugeben** und verdächtige Nachrichten direkt zu **löschen**. Ein effektiver **Spamfilter** kann helfen, nur noch relevante Nachrichten zu erhalten.

Gefährliche Datenkraken: Phishing Mails
Mittlerweile lassen sich viele Mails aber nur noch sehr schlecht von authentischen Nachrichten unterscheiden. Sogenannte **Phishing-Mails** (das Wort "Phishing" ist eine Zusammensetzung aus "password harvesting" und "fishing") zielen darauf ab, an Passwörter und private Daten von Benutzern zu gelangen. Die Absender der Mails **geben sich als vertrauenswürdige Personen aus** und fordern den Empfänger auf, Passwörter, Online-Banking-Daten oder Kreditkartennummern preiszugeben.

Für Benutzer wird es zunehmend schwerer, Phishing-Mails zu erkennen. Eine Möglichkeit ist, sich zu informieren: Die Verbraucherzentrale NRW stellt beispielsweise einen sehr informativen **Phishing-Radar** zur Verfügung, den es lohnt, regelmäßig zu beobachten. Ebenfalls sollte man darauf achten,

sensible Daten nur auf sicheren Webseiten einzugeben. Achten Sie hierbei darauf, dass die Seite mit https statt http beginnt. Erscheint Ihnen irgendetwas merkwürdig oder finden Sie auffällige Rechtschreibfehler in der Webadresse, könnte dies auf eine Phishing-Aktion hinweisen. Im Zweifel **kontaktieren Sie den Anbieter**, der angeblich als Absender der Mail auftritt. So sind Sie immer auf der sicheren Seite.

Was tun Sie, um sich vor Spam und Datenklau zu schützen? Wir freuen uns über Ihre Kommentare.