

10 Tipps gegen Spam-Mails

Während einige kein oder kaum ein Problem mit Spam-Mails haben: „Ist kein großes Problem. Verstehe das ganze Tra-ram bezüglich Spam nicht.“, gehen andere in der Flut unter und wissen nicht genau, wie sie sich schützen können. Überraschend viele Befragte glauben, dass es außer Anti-Spam-Filter keine wirksamen Mittel oder Vorsichtsmaßnahmen gegen Spam-Mails gibt. Die erkennbare Hilflosigkeit gegenüber Spam soll dieses Kapitel mindern und Anwendern effektive Tipps zur Vorbeugung und Verhinderung von Spam-Mails geben.

Offene Fragen zum Spam-Schutz ...

„Kann man sich überhaupt davor schützen?“

„Bin hilflos. Spamfilter können wir leider auch nur teilweise einsetzen.“

„Leider kann man sich davor kaum schützen.“

„...es gibt kaum eine Lösung - ich kann ja seitens des Unternehmens nicht die E-Mail-Adresse zyklisch ändern. Das wird der Kunde nicht akzeptieren.“

„Ich sehe keine Möglichkeit.“

„Abgesehen von einem Spam-Filter gibt es leider keinen wirksamen Schutz.“

„Gar nicht. Wie denn auch???“

Neben dieser Unwissenheit ist oft die Verantwortungsabgabe ein Herd der Spam-Problematik in einem Unternehmen. Die Einstellung: „Spam Vorbeugung und Verhinderung geht mich nichts an, das ist Aufgabe der EDV-Abteilung.“ kann schnell zu

vollen Postkästen führen. Für ein Unternehmen ist es daher sehr wichtig klare Sicherheitsregeln festzulegen, um die Gefahr aus dem Netz zu minimieren und ein Sicherheitsbewusstsein unter den Mitarbeitern zu schaffen. In diesem Zusammenhang könnte die Herausgabe von monatlich aktuellen Information mit Zahlen und Fakten zu wichtigen Sicherheitsthemen die Mitarbeiter sensibilisieren. Dies ist insbesondere so wichtig, da der Trend immer mehr wächst, mit Hilfe von Spyware, Trojanern und Phishing-Aktionen Internetbenutzer auszukundschaften und u.a. Passwörter zu erfahren. Spammer nutzen diese Möglichkeiten, um Computer von ahnungslosen Nutzern zu kidnappen und damit Inhalte im Netz zu vertreiben. Mittlerweile stammt rund ein Drittel der versendeten Spams von Unschuldigen. Das wird besonders ärgerlich, wenn Sie fälschlicherweise beschuldigt werden Spams zu verschicken. Bevor Sie in Erklärungsnot kommen ist es ratsam eine Schutzsoftware zu installieren und die Gefahren aus dem Internet kennen und einschätzen zu lernen. Ein Leitfadens für den sicheren Umgang mit E-Mail sollte unter anderen die nachfolgenden Tipps beinhalten.

„Schulung der Mitarbeiter hinsichtlich Umgang mit E-Mail-Adressen“

„Sicherheitsbewusstsein verstärken“

Laut Florian Klein von AntiSpam.de

gibt es ein wachsendes Aufkommen von sogenannten „Pinc Contracts“, in denen Spammer Provider an ihren Gewinnen beteiligen. So wird es immer schwerer ersichtlich, wem sie ihre Daten geben und was dieses Unternehmen mit diesen macht. Sie sollten sich deshalb sehr gut überlegen, ob und wem Sie Ihre E-Mail Adresse geben. Generell gilt, je weniger Spuren Sie im Netz hinterlassen, desto geringer die Wahrscheinlichkeit durch Spam-Mails belästigt zu werden. Sollte es doch einmal nötig sein, dass Sie Ihre geschäftliche E-Mail Adresse angeben müssen, lesen Sie sich sorgfältig die Allgemeinen Geschäftsbedingungen durch und überprüfen Sie diese auf den Datenschutz Ihrer Angaben.

„Sorgfältige (Nicht-)Weitergabe meiner E-Mail-Adresse“

„Preisgabe meiner `wichtigen` E-Mail-Adresse nur an mir `wichtigen` Stellen“

„Ich mache meine persönlichen Angaben bei der Bestellung von Newslettern sehr überlegt und bestelle wirklich nur ganz notwendige“

Harmlos aussehenden Fallen können Gewinnspiele sein. Die kleine Change, sollte es wirklich real einen Preis geben, diesen zu gewinnen steht die große Wahrscheinlichkeit der Zusendung von Spam-Mail gegenüber. An Gewinnspielen und Umfragen sollte man deshalb nur teilnehmen, wenn der Veranstalter seriös und eine Weitergabe Ihrer Daten ausgeschlossen ist. Auch Ihre

Angaben in Telefonbüchern, Chats und Foren können mit Hilfe von Harvestern schnell auf eine Spammer-Liste gelangen. Ein weiterer Trick von Spammern sind Kettenbriefe. Oft haben diese ein sehr emotionales Thema und bringen den Empfänger damit in einen moralischen Zugzwang. Auf diese Weise können schnell viele Adressen gesammelt werden.

„Keine Teilnahme an Preisausschreiben oder Umfragen (dies hier ist eine absolute Ausnahme!)“

„Die eigene E-Mail-Adresse auf Websites/-blogs und in Foren möglichst nicht veröffentlichen“

„Keine Teilnahme an Umfragen. Keine Weitersendung von Kettenbriefen“

Die guten Ratschläge aus vielen Artikeln, seine E-Mail Adresse (fast) nie anzugeben sind zwar richtig, jedoch nur sehr schwer durchführbar, da man heute für fast jede Information eine Mail Adresse hinterlegen muss. Um Informationen zu bekommen und trotzdem nicht „zugemüllt“ zu werden, sollten Sie ein Doppelleben führen. Schaffen Sie sich bei einen der vielen Freemail-Anbieter eine zweite E-Mail Adresse an, die Sie für Internetformulare benutzen. Durch die Verwendung spezifischer E-Mail-Adressen für spezifische Zwecke ist Ihre wichtige Mail Adresse mehr vor Spam-Mails geschützt. Um den Spam-Befall weiter zu minimieren sind Wegwerf-Adressen oder Änderungen der E-Mail-Adresse von Zeit zu Zeit sehr sinnvoll. Bei der Auswahl des E-Mail-Namens

sollten, wenn möglich, typische Kombinationen wie *ameier@domain.de*, *otto.wagner@domain.de* vermieden werden. Die Adresse sollte zudem nicht zu kurz sein *ab@domain.de*, *susi@domain.de*. Die Verwendung von Buchstabenkombinationen aus dem Ende des Alphabets können wie zum Beispiel *zebra@domain.de*, *xyandreas@domain.de* können die Spam-Wahrscheinlichkeit zusätzlich ein wenig eindämmen, da die Programme der Spammer zumeist nach dem Alphabet vorgehen.

„Wegwerf E-Mail Adressen (*@subdomain.meinedomain.de)“

„Die Firmen-Domain wird nur an direkte Geschäftskontakte gegeben. Newsletter und private Kontakte gehen über eine externe Domain (GMX)“

„Verwenden von Dummy E-Mail Adressen“

„Erster Kontakt mit Wegwerf E-Mail-Adressen (spamgourmet.com) um zu schauen was da so zurück kommt“

Auch das Angeben der E-Mail Kontakt Adresse auf Homepages ist gefährlich. Zum Adressen sammeln werden oft Suchroboter sogenannte Harvester genutzt, die das Internet nach E-Mail Adressen durchforsten. Wenn Sie auf einer Webseite trotzdem eine Kontakt-E-Mail-Adresse angeben möchten, ist es ratsam diese zu verschlüsseln oder als Bild (gif) einzufügen. Harvester suchen im Internet nach dem @-Zeichen und können somit die Bilddatei nicht als E-Mail Adresse identifizieren.

„Seitdem unsere allgemeine E-Mail-Adresse auf der CeBIT Webseite gelistet ist (wir waren Aussteller) erhalten wir in unserer Inbox für allgemeine Anfragen wesentlich mehr

Spam E-Mails“

„Adressen auf Webseiten verschlüsseln“

„Maskierung der E-Mail-Adresse gegenüber automatischen Suchroutinen“

Hat man erst einmal Spam-Mails erhalten heißt der wichtigste Sicherheitstipp: nie antworten. In der Umfrage gaben einige als Lösung an auf die Spam-Mails zu antworten oder sich abzumelden. Das ist jedoch ein großer Fehler. Mit Ihrer Antwort bestätigen Sie dem Spammer nämlich, dass Ihre Adresse richtig ist und genutzt wird. Mit dieser Bestätigung geht meist die Spamflut erst richtig los. Berücksichtigt werden sollten ebenso automatische Mitteilungen. Auch wenn Sie ganz bedacht mit E-Mails umgehen und auf keine Spam-Mail antworten war Ihre ganze Mühe umsonst, sollten Sie während Ihres Urlaubs eine automatische Abwesenheitsmitteilung aktivieren. Diese Systeme antworten auf alle eingehenden E-Mails, d.h. auch auf Spams und bestätigen damit diese. Deshalb sollten, wenn möglich, automatische Mitteilungen nicht benutzt oder deaktiviert werden. Einige Spams locken mit der Chance, sich aus dem Verteiler zu löschen und Abmelde-Links. Meist sind diese angeblichen Möglichkeiten sich von der Spamflut zu befreien nur Fallen. Deshalb gilt: gehen Sie nie auf einen Link und führen Sie nie die in der Mail beworbene Handlung durch.

„Nie reagieren“

„Offensichtliche Versender von

Werbemails werden sofort gelöscht“

„Möglichst aufgrund der Betreffzeile löschen“

Natürlich ist das alles kein hundertprozentiger Schutz. Spammer finden immer neue Tricks. Manche Spammer geben sich als Kontaktperson aus dem Chat aus und verlocken den Empfänger zu antworten. Grundsätzlich gilt deshalb, öffnen Sie nie eine E-Mail von Absendern, die Sie nicht kennen. Es kann sich dabei nicht nur um eine lästige SPAM Mail handeln, sondern auch um eine mit einem Virus infizierte E-Mail. Um dies möglichst vollständig zu vermeiden, sollten Sie die E-Mail Vorschau-Funktion in Ihrem Mail-Client deaktivieren. Bereits in der Vorschau hat der Virus die Möglichkeit auf Ihren Computer zu gelangen und einige Spammer können nachvollziehen, dass die E-Mail geöffnet wurde.

„Sofort löschen ohne Preview“

„Instinkt für idiotische Absender“

Beim Ausschauen und Einsatz einer Anti-Spam-Software ist einiges zu beachten. Einen Überblick über die unterschiedlichen Filtertechnologien, die Möglichkeiten des Filterplacements und den rechtlich unbedenklichen Einsatz von Spamfiltersoftware bietet die neue Studie von Absolit Dr. Schwarz Consulting: Der Weg aus der Spam-Flut www.absolit.de.

10 Tipps gegen Spam	
Sparsame Herausgabe der E-Mail-Adresse	Sie sollten sich sehr gut überlegen, ob und wem Sie Ihre E-Mail Adresse geben. Generell gilt je weniger Spuren Sie im Netz hinterlassen desto geringer die Wahrscheinlichkeit durch Spam-Mails belästigt zu werden.
Bedachte Teilnahme an Gewinnspielen & Umfragen	Zu den Tricks von Spammern E-mail-Adressen zu sammeln zählen Gewinnspiele, Kettenbrief und Umfragen. Sie sollten daher Gewinnspielen und Umfragen nur teilnehmen, wenn der Veranstalter seriös und eine Weitergabe Ihrer Daten ausgeschlossen ist.
Zweite Mail Adresse anlegen	Geben Sie nie Ihre wichtige / dienstliche E-Mail Adresse in Mailinglisten, Chat Foren oder in anderen Eingabefeldern an. Führen Sie lieber ein Doppelleben, nutzen Sie die kostenlosen Freemail Dienste und legen Sie sich einen zweiten Account zu.
Namensauswahl	Verwenden Sie wenn möglich keine typische Kombinationen (<i>ameier@domain.de</i> , <i>otto.wagner@domain.de</i>), legen Sie nicht zu kurze Adresse an (<i>ab@domain.de</i> , <i>susi@domain.de</i>) und nutzen Sie das Ende des Alphabets (<i>zebra@domain.de</i> , <i>xyandreas@domain.de</i>)
E-Mail auf Webseiten als Bild angeben	E-Mail Adressen auf Webseiten sollten nicht im Textformat angegeben werden, da Spammer mit sogenannten Harvester (Suchrobotern) das Internet nach E-Mail Adressen (...@...) durchforschen. Wenn Sie Ihre E-Mail Adresse auf Ihrer Homepage angeben wollen, speichern Sie diese als Bild (gif) oder verschlüsseln Sie sie.
Nie Antworten	Antworten oder leiten Sie nie eine unverlangte Werbe-E-Mail weiter. Durch das Antworten wird die Adresse, als genutzte Adresse bestätigt und dann geht es mit der Spam Flut erst richtig los. Eine Falle sind harmlos aussehende Kettenbriefe, mit denen leicht Mail Adressen gesammelt werden können. Generell gilt: Öffnen bzw. beantworten Sie möglichst keine E-Mails von unbekanntem Absendern.
Automatische Abwesenheitsmitteilungen deaktivieren	Auch automatische Abwesenheitsmitteilungen bestätigen dem Spammer, dass diese Adresse stimmt. Deshalb sollten automatische Mitteilungen deaktiviert werden.
Nachladbare E-Mail-Inhalte unterdrücken	Manche Spammer bauen Web-Bugs und andere nachladbare http Inhalte in ihre Spam-Mails ein und können so nachvollziehen ob die gesendete Spam-Mail geöffnet und damit die E-Mail-Adresse bestätigt wurde. Um dies zu verhindern sollte der E-Mail-Clients so eingestellt sein, dass keine externen Inhalte automatisch nachgeladen werden. Um Viren keine Chance zu geben, sollte außerdem die Vorschau-Funktion von E-Mails deaktiviert sein.
Nie Links / Handlungen in Spams befolgen	Gehen Sie nie auf einen Link in einer Junkmail bzw. führen Sie nicht die dort beworbenen Handlungen durch. Auch nicht, wenn es darum geht Ihre Adresse aus dem Verteiler zu löschen. Meist ist dieses angebliche Abmelden eine Falle.
Sicherheitsregeln festlegen	In einer Firma ist es wichtig klare Sicherheitsregeln festzulegen, um die Gefahr aus dem Netz zu minimieren und ein Sicherheitsbewusstsein zu schaffen.