Freitag, 22. September 2017
Aktualisiert am Mittwoch, 7. März 2018

Spam vermeiden ganz ohne Spamfilter

Spam ist elektronischer Müll und wer nicht gerade ein Müllliebhaber ist, der wird versuchen seinen Posteingang frei davon zu halten.

Die meisten nutzen dazu mehr oder weniger gut arbeitende SPAM-Filter, die aber das Problem mit sich bringen, dass man sich nicht immer auf sie verlassen kann.

Begriffserklärungen

Bevor es richtig los geht, möchte ich wichtige Begriffe erklären, die zum Verständnis meiner Anti-Spam-Methode wichtig sind.

Wer sich bereits gut mit dem Thema "E-Mail" auskennt oder sich vorab einen Überblick über meine Anti-Spam-Methode verschaffen möchte, der findet weiter unten eine Zusammenfassung.

1. **E-Mail-Adresse**
2. **E-Mail-Postfach**
3. **E-Mail-Konto**
4. **E-Mail-Weiterleitung**
5. **E-Mail-Alias**
6. **Sammelweiterleitung**
7. **Identität**

Zu 1.: Was eine **E-Mail-Adresse** ist, dürfte jedem Internetnutzer bekannt sein. Sie lautet z. B. "**nie-wieder@spam.org**" und kann verwendet werden, ohne, dass dafür ein Postfach, eine Weiterleitung oder einen Alias eingerichtet werden muss (siehe 6.).

Die Adresse unterteilt sich in zwei Abschnitte: vor dem "@" steht der Name des Postfaches und hinter dem "@" steht der Domainname. Wird eine E-Mail an "**nie-wieder@spam.org**" geschickt, bedeutet das ausgesprochen etwa "*Sende eine E-Mail an das Postfach **nie-wieder**, das auf dem Server **spam** mit der Endung **.org** (=TLD) liegt.*" Der Servername zusammen mit der Endung wird als "Domain" bezeichnet.

An dem Beispiel wird auch deutlich, wie Postfachname und Servername so kombiniert werden kann, damit sich daraus eine leicht zu merkende, bzw. sprechende E-Mail-Adresse ergibt.

Zu 2.: Ein **E-Mail-Postfach** ist zum Versand bzw. Empfang von E-Mails erforderlich. Ein Postfach muss zunächst bei einem Internetprovider auf dessen Server eingerichtet und mit einem Benutzernamen (in der Regel identisch mit der E-Mail-Adresse) und einem Kennwort versehen werden. Anschließend ist der Zugriff z. B. per Webmail darauf möglich.

Zu 3.: Soll nicht per Webmail auf das zuvor beim Internetprovider eingerichtete Postfach zugegriffen werden, weil es einem zu umständlich ist, sich jedes Mal dort einzuloggen, lässt sich alternativ das Postfach mit Hilfe eines **E-Mail-Kontos** verwalten, das anschließend auf dem Smartphone bzw. PC in einem E-Mail-Programm eingerichtet wird (z. B. Thunderbird oder Microsoft Office Outlook®).

Hierfür werden folgende Daten benötigt:

- Name des Anwenders

- Benutzername des Postfachs (in der Regel die E-Mail-Adresse)
- Kennwort des Postfachs
- Posteingangsserver des Postfachs (zum Empfangen von E-Mails)
- Postausgangsserver des Postfachs (zum Versenden von E-Mails)
- Die Ports der zuvor genannten Server, die zum Abrufen bzw. Versenden geöffnet sind

Der Name des Anwenders lautet z. B. "**Max Muster**" oder einfach nur "**Max**", während der Benutzername in der Regel die E-Mail-Adresse ist. Ist alles eingerichtet und der Max verschickt eine E-Mail, so wird seine Absenderadresse beim Empfänger (je nach E-Mail-Programm) z. B. als "**Max Muster <nie-wieder@spam.org>**" bzw. "**Max <nie-wieder@spam.org>**" dargestellt.

Exakte Anleitungen zum Einrichten von E-Mail-Konten finden sich auf den Supportseiten von Mozilla (Thunderbird) oder Microsoft (Outlook® oder dem normalen E-Mail-Programm von Windows 10).

Wer ein anderes E-Mail-Programm verwendet, sucht am besten bei Google nach e-mail-konto einrichten anleitung gefolgt von dem Namen des Programms.

Zu 4.: Eine **E-Mail-Weiterleitung** leitet, wie es der Name schon sagt, eine E-Mail an eine andere E-Mail-Adresse weiter. Dabei muss es sich bei der Zieladresse keineswegs um ein Postfach handeln, sondern es kann auch auf eine andere Weiterleitung weitergeleitet werden.

Zu 5.: Ein **E-Mail-Alias** verhält sich ähnlich wie eine Weiterleitung, kann in der Regel aber nur für ein bestehendes Postfach angelegt werden. D. h. existiert zum Beispiel das Postfach "**nie-wieder@spam.org**" und es wird ein zusätzlicher Alias "**ich-will@spam.org**" für dieses Postfach angelegt, so erhält man beim Abrufen dieses Postfachs alle E-Mails, die an "**nie-wieder@spam.org**" und "**ich-will@spam.org**" gesendet wurden, obwohl für "**ich-will@spam.org**" kein eigenes Postfach existiert.

Zu 6.: Eine **Sammelweiterleitung** "sammelt" alle E-Mails ein, die nicht an ein bestehendes Postfach oder eine bestehende Weiterleitung adressiert sind.

Diese dient dazu, dass keine E-Mails verpasst werden, sollte jemand eine E-Mail-Adresse nicht richtig geschrieben haben. Wurde z. B. das Postfach "**nie-wieder@spam.org**" eingerichtet und es wird diese Adresse telefonisch an sein Gegenüber durchgegeben, der sie falsch versteht und daraufhin eine E-Mail an "**knie-nieder@spam.org**" schreibt, so kommt diese E-Mail dennoch an.

Eine "Sammelweiterleitung" kann auch als "Catch-E-Mail-Adresse", "Catch-All-E-Mail-Account", "Catch-All-Weiterleitung" oder im Falle, dass jemand zur Administration das weit verbreitete cPanel nutzt, "Default Address" heißen. Der Zweck ist in allen Fällen jedoch derselbe.

Zu 6.: Unter einer "**Identität**" im Zusammenhang mit E-Mail-Konten wird ein Name und eine E-Mail-Adresse verstanden. Wurde einmal ein E-Mail-Konto in seinem E-Mail-Programm eingerichtet, so lässt sich mit Hilfe von mehreren Identitäten die Servereinstellungen dieses Kontos nutzen, um E-Mails unter einem anderen Absender zu versenden.

Wird in Thunderbird z. B. die Identität "**Moritz <nie-wieder@spam.org>**" hinzugefügt und man erstellt eine neue E-Mail, so lässt sich als Absender diese Identität im "Von-Feld" auswählen und damit eine E-Mail verschicken. Nutzer von Outlook® haben hier das Nachsehen, da sich dort keine Identitäten einrichten lassen.

Um eine Identität zum Versenden nutzen zu können, muss in der Regel zuvor eine Weiterleitung mit dieser E-Mail-Adresse eingerichtet werden (abhängig von der Konfiguration des Servers beim Provider). Es lassen sich nicht beliebige Absender, insbesondere nicht von fremden Domains, verwenden.

Vorbemerkungen

Mit dem Internet beschäftige ich mich seit über 20 Jahren. Meine erste, private Homepage mit einer eigenen Domain, hatte ich 1997/98 eingerichtet und kenne noch die Zeiten, in denen sich die Nutzer per Modem in Mailboxen eingewählt haben.

Meine in diesem Beitrag vorgestellte Anti-Spam-Methode beruht nicht auf theoretischen Überlegungen, sondern auf jahrelangem, praktischen Einsatz. Richtig verstanden und umgesetzt, ist sie meiner Meinung nach die effektivste Methode im Kampf gegen Spam, die dazu ohne jede Anti-Spam-Software auskommt.

Ich bezeichne die hier beschriebene Methode als "meine" Methode, weil ich sie mir ausgedacht und nicht woanders abgekupfert habe. Das heißt nicht, dass bereits andere vor mir dieselbe Methode verwenden und jeder, der "meine" Methode bereits kennt, möchte mir das nachsehen.

In diesem Beitrag nutze ich für Beispiele die Domain mit der Endung "**spam.org**"

für die aktuell keine Internetpräsenz eingerichtet ist. Ich stehe in keiner Beziehung mit dem Besitzer der Domain und es sollte klar sein, dass keine E-Mails an die genannten Beispiel-Adressen geschickt werden.

Voraussetzungen für meine Anti-Spam-Methode

Die wichtigste Voraussetzung damit sich meine Methode anwenden lässt, ist der Besitz einer eigenen Domain (Ausnahme, siehe unter Fragen und Antworten) . Eine eigene Domain ist bereits für wenige Euro pro Jahr erhältlich und es muss dazu keine Internetseite erstellt werden.

Auf der anderen Seite gibt es noch immer viele Internetseiten, die keine zur Domain passende E-Mail-Adresse eingerichtet haben, sondern z. B. mit ihrer T-Online oder Gmail-Adresse etc. arbeiten (meist sind es Freiberufler oder kleine Firmen).

Ich empfehle jedoch jedem eine zur Domain passende E-Mail-Adresse für seinen Internetauftritt einzurichten, weil alles andere unprofessionell wirkt und Fragen aufwirft.

Wenn z. B. auf einer Domain "**spam.org**" keine E-Mail-Adresse mit z. B. "**info@spam.org**" zu finden ist, sondern z. B. "**max.muster@t-online.de**", dann fragt sich der erfahrene Besucher, warum der Betreiber dieser Domain keine zur Domain passende E-Mail-Adresse eingerichtet hat? Gehört ihm die Domain am Ende gar nicht oder kennt er sich einfach nicht damit aus, wie man ein E-Mail-Konto einrichtet?

Ist aber eine E-Mail-Adresse angegeben, die zum Domainnamen passt, so wird damit die Inhaberschaft der Domain bestätigt und man baut Vertrauen beim Besucher auf.

Anmerkung: Ein E-Mail-Konto muss dazu nicht unbedingt eingerichtet werden. Es würde eine Weiterleitung von "**info@spam.org**" nach "**max.muster@t-online.de**" reichen, da die "**info@spam.org**" ohnehin nur zur ersten Kontaktaufnahme dient.

Für professionelles Arbeiten sollte man aber schon ein Postfach, das zur Domain passt, einrichten (z. B. "**max.muster@spam.org**"). Wenn ein Anwender eine E-

Mail an eine Adresse mit der Endung "**spam.org**" schreibt, dann erwartet er auch eine Antwort von einem Postfach dieser Domain.

Falls man aber (aus welchem Grund auch immer) kein weiteres Postfach einrichten möchte, so ist eine Weiterleitung allemal besser, als eine E-Mail-Adresse anzugeben, die nicht zur Domain passt.

Die zweite Voraussetzung, die aber nicht zwingend zur Anwendung meiner Anti-Spam-Methode ist, ist ein E-Mail-Programm, das mit "Identitäten" umgehen kann (siehe bei "Begriffserklärungen"). Microsoft Office Outlook® kann das z. B. nicht, so dass meine Methode hier zwar dennoch Anwendung findet, aber nicht vollständig und nicht so bequem umgesetzt werden kann wie z. B. bei der Verwendung von Thunderbird.

Wer zu Thunderbird* wechseln möchte, es aber noch nicht installiert hat, dem empfehle ich die portable Version, da diese nur entpackt werden muss, wozu keine Administratorenrechte erforderlich sind. Portable Software wird vorzugsweise mit dem dazu passendem Verwaltungstool installiert, mit dem sich u. a. bequem neue Programme installieren und vorhandene aktualisieren lassen.

* Thunderbird bietet nicht die gleiche Unterstützung bei der Formatierung von HTML-E-Mails an, wie zum Beispiel Outlook. Für Anwender ohne HTML-/CSS-Kenntnisse, die auf eine exakte Gestaltung von HTML-E-Mails angewiesen sind (z. B. für geschäftliche Newsletter), ist Thunderbird weniger gut geeignet.

Was mich an Spam stört

Früher, als ich noch kein Smartphone besaß, bekam ich auf meinem Notebook während der Arbeit Meldungen über neu eingetroffene E-Mails eingeblendet. An der Meldung erkannte ich bereits, ob es Spam war und ich somit gar nicht erst ins E-Mail-Programm wechseln und meine aktuelle Arbeit unterbrechen musste.

Im Jahr 2011 kaufte ich mein erstes Smartphone und habe darauf ein E-Mail-Programm installiert, das sofort eine Benachrichtigung auslöst, sobald eine neue E-Mail eingetroffen ist. Nachdem man ein Smartphone nicht ständig im Blickfeld hat, ist auch eine akustische Benachrichtigung erforderlich.

Die sofortige Benachrichtigung benötigte ich, weil ich zu dieser Zeit Kunden für meine programmierte Software zu betreuen hatte und mir schneller Kundensupport sehr wichtig war. Das war auch der Auslöser zur Anschaffung des Smartphones, damit ich auch von unterwegs aus zeitnah weiterhelfen konnte.

Trifft also eine neue E-Mail ein, so muss das Smartphone hervorgeholt und die E-Mails gelesen werden. Handelt es sich bei der neuen E-Mail nur um Werbung für irgendwelche Pillen oder jemand versucht einmal wieder an Zugangs- oder Kreditkartendaten zu gelangen, so ist das mit der Zeit frustrierend.

Der Frustfaktor steigert sich, wenn man gerade auf eine dringende E-Mail wartet. Was mich aber am meisten daran stört, ist die Tatsache, dass man diesen Spammern hilflos ausgeliefert ist. Spammer schreiben in der Regel unter gefälschten Absenderadressen und nutzen zum Versand noch nicht einmal ihren eigenen Computer dazu, sondern einen, den sie zuvor gehackt haben. Da ist jede Reaktion auf eine E-Mail zwecklos.

Das hat mich dazu gebracht den Spammern auf meine Weise das Handwerk zu legen, die zudem sehr befriedigend ist, weil man Spammern eben nicht mehr hilflos ausgeliefert ist, sondern mit wenigen Klicks einem Spammer für immer los wird und das ganz ohne Einsatz eines Spam-Filters.

Das Kernproblem von Spam

Wer täglich mehr als eine Handvoll oder gar dutzende Spam-E-Mails erhält, der hat mit großer Wahrscheinlichkeit bei der Verwendung seiner E-Mail-Adresse etwas falsch gemacht.

Immer wieder sieht man, dass Nutzer freigiebig ihre oft einzige E-Mail-Adresse öffentlich zur Kontaktaufnahme bereitstellen und offenbar nicht wissen, dass es Suchmaschinen von Spammern gibt, die genau nach diesen Adressen suchen.

Die fortgeschrittenen Nutzer versuchen ihre Adresse durch die Schreibweise etwas zu verschleiern (z. B. "**nie-wieder(at)spam(dot)org**"), aber die gängigen Methoden sind den Spammern bekannt und können nicht so leicht umgangen werden.

Ein Problem stellt dabei die Impressums-Pflicht für Personen und Firmen in Deutschland dar, bzw. Personen und Firmen, deren kommerziellen Angebote sich an deutsche Nutzer richten. Hier gibt es verschiedene Ansätze, um eine E-Mail-Adresse nicht im Klartext wiedergeben zu müssen.

In der Regel handelt es sich aber um E-Mail-Adressen, die nur für die erste Kontaktaufnahme gedacht sind, bzw. wirklich nur für die rechtlichen Belange der Internetseite von Bedeutung sind und die sich bei Bedarf einfach ändern lassen.

In jedem Fall sollte aber zusätzlich ein (funktionierendes!) Kontaktformular zur Verfügung gestellt werden, weil es immer einmal vorkommen kann, dass jemand keine E-Mail an die angegebene Adresse verschicken kann, weil die E-Mail-Domain gerade auf einer Blacklist steht.

Ein weiteres Problem sind Viren, die Adressbücher von E-Mail-Programmen auslesen und an Spammer versenden, sowie Anwender die falsch mit dem An-/Cc-Feld umgehen.

Spam-Ursache "Viren"

Noch immer arbeiten viele Privatnutzer von Windows als Administrator und öffnen so Viren Tür und Tor. Bereits seit Windows XP Service-Pack 2 (veröffentlicht am 9. August 2004) gibt es jedoch das Sicherheitscenter, das den Anwender auf verschiedene Sicherheitsprobleme aufmerksam macht (z. B. eine deaktivierte Firewall, einen fehlenden Virenscanner oder deaktivierten Updates).

In dieses Sicherheitscenter hätte auch eine Warnung integriert werden können, die aufpoppt, wenn ein Benutzer als Administrator arbeitet. Warum dies bis zum heutigen Tag nicht erfolgt ist, ist mir ein Rätsel.

Niemand arbeitet als Administrator an einem Windowsrechner, auch kein Systemadministrator. Ein Administratorkonto dient ausschließlich zur Installation von Software und zur Konfiguration von Windows. Software, die nur mit Administratorrechten funktioniert, ist Murks und sollte vom Rechner entfernt werden.

An dieser Stelle beschreibe ich daher ganz kurz, wie sich ein Administratorkonto herabstufen lässt, damit sich Viren nicht so leicht im System einnisten können: Zunächst wird ein zweites Administratorkonto angelegt und danach sein eigener Kontotyp auf "Standardbenutzer" geändert - fertig. Durch dieses Vorgehen bleiben alle Einstellungen und benutzerbezogenen Daten erhalten.

Am Anfang wird es eine Umstellung sein, wenn für jede Systemänderung das Kennwort des neu erstellten Administratorkontos eingegeben werden muss, aber Sicherheit gibt es nicht zum Nulltarif. Für Linuxanwender (und auch für mich) ist

das längst Gewohnheit, so dass man sich daran auch nicht mehr stört.

Auf diese Weise trägt wird ein kleiner, aber wichtiger Beitrag zur Verhinderung von Spam beigetragen.

Spam-Ursache "An-/Cc-Feld"

Neben Viren, die Adressbücher auslesen, machen leider sehr viele Anwender einen entscheidenden Fehler beim Versand einer E-Mail an mehrere Empfänger. Zur Adressierung von Empfängern gibt es in jedem E-Mail-Programm drei Felder:

1. **An**
2. **Cc**
3. **Bcc** (muss eventuell erst eingeblendet werden)

Das "**An**-Feld" wird für alle Adressen verwendet, die direkt und persönlich angesprochen werden sollen (soweit das in einer nicht persönlich adressierten E-Mail möglich ist).

Das macht man jedoch nur dann, wenn allen Empfängern die E-Mail-Adressen der anderen bekannt ist. Anderenfalls wird ohne deren Einverständnis eine sehr private Information weitergegeben, die dadurch auch leichter in die Hände von Spammern gelangen kann (z. B. durch einen verseuchten PC einer der Empfänger).

Das "**Cc**-Feld" (=Carbon Copy, zu Deutsch "Durchschlag", "Kopie") wird dagegen genutzt, um andere darüber zu informieren, dass die E-Mail an den Empfänger, der im "An-Feld" steht, geschickt wurde und sie selbst eine Kopie derselben erhalten haben.

Und auch hier gilt: Das sollte nur dann gemacht werden, wenn allen Empfängern die E-Mail-Adressen der anderen bekannt ist.

In allen anderen Fällen wird das "**Bcc**-Feld" (=Blind Carbon Copy, zu Deutsch etwa "unsichtbare Kopie") verwendet. Damit erhalten alle Empfänger die E-Mail, jedoch kann keiner der anderen Empfänger die Adresse der anderen sehen, weil sie in der E-Mail nicht enthalten ist.

In diesem Fall sollte im Nachrichtentext erwähnt werden, dass noch andere eine Kopie bekommen haben (eventuell mit den Namen, aber natürlich ohne deren E-Mail-Adressen).

Tipp: Wird eine E-Mail an mehrere Empfänger verschickt, die sich untereinander nicht kennen, so setzt man seine eigene E-Mail in das "An-Feld" und den Rest in das "Bcc-Feld".

Die sauberste Lösung für E-Mails, die sich an mehrere Menschen richtet, ist ein Serien-E-Mail-Programm. Dieses vermeidet das Problem der Adressweitergabe und spricht zudem jeden Kontakt mit seinem Namen an.

Spamfilter lösen das Problem nicht

Auch ich hatte lange Zeit Spamfilter im Einsatz, die relativ gute Dienste tun und helfen das Problem einzudämmen. Der größte Nachteil aber ist, dass sie nicht 100%ig zuverlässig arbeiten und es so sein kann, dass immer wieder einmal eine normale E-Mail im Spamordner landet.

Wartet man z. B. auf einen Kundenauftrag und erhält aber eine E-Mail nicht rechtzeitig, so kann daraus ein (beträchtlicher) finanzieller Schaden entstehen. Daher sind Spamfilter nur als Hilfe zu sehen, lösen aber das eigentliche Problem (Erhalt von Spam) nicht.

An dieser Stelle möchte ich noch kurz auf ein weiteres Problem in diesem Zusammenhang hinweisen: Nutzer, die ihre E-Mails per Pop3 herunterladen, haben nur Zugriff auf den Posteingang ihres Postfachs. Ist aber am Server ein Spamfilter aktiv, so werden diese E-Mails am Server in einen Unterordner verschoben und nie abgerufen.

Je nach Konfiguration des Spamfilters auf dem Server, erhält man eine Nachricht über neuen Spam oder aber auch nicht. D. h. es kann eine normale E-Mail im Spamordner auf dem Server liegen und der Anwender bekommt davon nichts

mit. Daher sollte jeder seine Einstellungen auf dem Server kontrollieren.

Da ich selbst ja keinen Spamfilter nutze und Pop3 verwende, mein Provider aber alle E-Mails immer über seine Antispamserver schickt, habe ich zwar alle Einstellungen am Server deaktiviert, lasse mir aber dennoch einmal pro Tag eine E-Mail mit einem Bericht zuschicken, um sicher zu gehen, dass (z. B. durch ein Update am Server) meine Einstellungen nicht geändert wurden und versehentlich E-Mails im Spamordner am Server landen.

Bei einem Konto, das per Imap-Protokoll abgerufen wird, besteht in der Regel nicht das Problem, da sich in diesem Fall auf alle Ordner des Postfachs zugreifen lässt.

Meine Methode zur Spamvermeidung

Der erste Grundsatz, auf dem meine Anti-Spam-Methode beruht, lautet:

Das beim Provider eingerichtete E-Mail-Postfach ist geheim zu halten und dessen E-Mail-Adresse wird unter keinen Umständen an Dritte weitergegeben.

Ja, ja, ich "höre" es schon: "*Wie soll mir dann jemand an diese Adresse eine E-Mail schicken können, wenn keiner von deren Existenz weiß?*"

Das soll ja gar keiner, denn das Zauberwort lautet "E-Mail-Weiterleitung". Wenn also keiner von der Existenz Deines E-Mail-Postfaches weiß, ist klar, dass auch kein Spammer dorthin eine E-Mail schicken kann. Das können nur die Menschen, die Du dazu mit Hilfe einer eigenen Weiterleitung auserwählst.

Etwas einschränkt werden muss diese Aussage für allgemein bekannte Adressen, wie z. B. "**info@spam.org**" oder "**kontakt@spam.org**" etc., die daher nach Möglichkeit nicht verwendet werden sollten, weder für das geheime Postfach, noch für Weiterleitungen.

Sammelweiterleitung deaktivieren

Weiter oben bei den Begriffserklärungen hatte ich bereits die Funktionsweise einer "Sammelweiterleitung" beschrieben.

Ist diese aktiv und sammelt wahllos alle E-Mails auch von nicht existierenden, bzw. generierten Adressen ein, macht meine Methode keinen Sinn. Der zweite Grundsatz zur Anwendung meiner Anti-Spam-Methode lautet daher:

Die Sammelweiterleitung muss deaktiviert werden.

Viele dürften dies ohnehin schon getan haben, um Spam zu vermeiden, der an allgemein bekannte oder zufällig generierte Adressen geschickt wird. Wer es aber noch nicht getan hat, bzw. unsicher ist, ob sie deaktiviert ist, der sollte die Einstellung dazu überprüfen.

E-Mail-Adressen für Internetdienste

In den meisten Fällen, in denen eine E-Mail-Adresse bei Diensten im Internet, wie z. B. "Paypal", "Amazon" oder "Ebay" angegeben werden muss, handelt es sich bei der Kommunikation um eine Einbahnstraße

D. h. das System verschickt automatische Bestätigungs- und Benachrichtigungs-E-Mails auf die in der Regel ohnehin nicht geantwortet werden kann (zu erkennen am Absender, z. B. "**noreply@spam.org**").

Das ist die gute Nachricht für alle Outlook-Nutzer, die aufgrund dieser Tatsache auch ohne Identitätsverwaltung einen Nutzen aus meiner Anti-Spam-Methode ziehen können. Sollte man dennoch in die eher seltene Lage kommen, auf eine E-Mail antworten zu müssen, so muss man das nicht zwangsläufig mit seinem eigenen E-Mail-Programm tun, sondern kann dafür das Kontaktformular des Dienstes nutzen.

Bei Thunderbird lohnt sich das Einrichten einer Identität ohnehin nur für Adressen, mit denen häufiger kommuniziert wird, weil der Absender in der E-Mail auch ohne Identität geändert werden kann.

Dazu kopiere ich meine eigene Adresse samt Namen mit der rechten Maustaste aus dem "An-Feld" der empfangenen E-Mail und wähle in der Antwort im "Von-Feld"

"Benutzerdefinierte Adresse..." aus. Dann kopiere ich meine eigene Adresse dort hinein und kann meine E-Mail unter dieser Identität versenden, obwohl sie nicht eingerichtet ist.

E-Mail-Adressen für Kontakte

Für Anwender, mit denen ich relativ viel kommuniziere, nutze ich ebenfalls eigene E-Mail-Adressen. D. h. anstatt des Domainnames, wird hier der Name des jeweiligen Kontakts verwendet. Wer viele Kontakte hat, für den bietet es sich an den vollständigen Namen aus der Geburtsurkunde zu verwenden.

In meinem Fall ist das nicht erforderlich. Kenne ich z. B. einen "Hans", so erstelle ich eine E-Mail-Adresse, die "**hans@spam.org**" lautet.

Läuft dann Spam auf dieser Adresse ein, lösche ich sie und erstelle eine neue (z. B. "**hans2@spam.org**"). Anschließend benachrichtige ich den Hans über die neue Adresse und empfehle ihm seinen Rechner auf Viren zu überprüfen, da nur er diese E-Mail-Adresse kannte.

Bei diesem System könnte es Verwirrung geben, insbesondere, wenn mit dem Namen aus der Geburtsurkunde gearbeitet wird. Ein "Max Muster", der eine E-Mail an den "Moritz" schicken möchte, könnte beim ersten Anblick der ihm mitgeteilten E-Mail-Adresse "**max.muster@spam.org**" denken: "*Was ist das denn? Ich will doch an den Moritz eine E-Mail schicken und nicht an mich?*"

Bei mir hat sich deswegen zwar noch keiner beschwert, aber ich wollte das nicht unerwähnt lassen. Alternativ könnte z. B. "**max.muster-an-moritz@spam.org**" verwendet werden. Hier kann jeder seine Kreativität walten lassen, da man an kein festes Schema gebunden ist.

Bei einer umfangreichen Kontaktsammlung ist der Aufwand für jeden Kontakt eine eigene E-Mail-Adresse einzurichten zu groß. Hier behilft man sich, indem Kontakte zu Gruppen zusammengefasst werden (z. B. "Freunde", "Familie", "Verein", "Beruf" etc.). Eine E-Mail-Adresse heißt dann z. B. "**verein@spam.org**".

Im Falle von Spam muss dann die ganze Gruppe über eine eventuell neu eingerichtete E-Mail-Adresse informiert werden.

Weiterleitungen einrichten

Die zuvor erwähnten E-Mail-Adressen sind alle ausnahmslos E-Mail-Weiterleitungen. Es wird nur ein einziges, geheimes Postfach verwendet (siehe ersten Grundsatz meiner Methode). Über die Jahre habe ich rund 140 Weiterleitungen eingerichtet. Eine Weiterleitung einzurichten dauert bei mir Dank RoboForm (RoboForm-v8-Setup.exe (21,44 MB)) nur etwa eine halbe Minute.

Da der Domainname, bzw. Kontakt(gruppen)name in der E-Mail-Adresse enthalten ist, weiß ich im Falle von Spam sofort wer meine Adresse weitergegeben hat, oder von wem sie gestohlen wurde. Auch betrifft das Löschen einer "verbrannten" Weiterleitung nur E-Mails, die im Zusammenhang mit dieser Domain bzw. Kontakt(gruppe) verschickt wurden.

Somit kommen wir zum dritten Grundsatz meiner Methode:

Für jeden Dienst (z. B. Paypal, Amazon, E-Bay, Facebook, Forum etc.) bzw. Kontakt/Kontaktgruppe wird eine eigene Weiterleitung eingerichtet.

Dabei ist es jedem selbst überlassen, ob er den Domainnamen des jeweiligen Dienstes verwenden will oder nicht. Man kann sich auch sein eigenes System ausdenken und z. B. mit dem Datum arbeiten. Anstelle von "**paypal.de@spam.org**" könnte man auch "**01-10-2017@spam.org**" verwenden.

In diesem Fall weiß man, wann diese E-Mail-Adresse erstellt wurde und wie lange es gedauert hat, bis Spam darauf eingegangen ist. Falls mehrere an einem Tag erstellt wurden, kann für die nächsten zusätzlich eine Nummer angehängt werden: **01-10-2017-1@spam.org**. Um bei diesem System aber nicht den Überblick zu verlieren, sollte eine Liste geführt werden, für welchen Dienst welche E-Mail-Weiterleitung verwendet wurde.

Um mir diese Liste zu sparen, nutze ich die zuvor erwähnte Methode mit den Domainnamen. Dabei kann es aber passieren, dass sich so eine E-Mail-Adresse nicht verwenden lässt. So konnte ich auf diese Weise kein Konto bei Samsung erstellen, weil die Programmierer auf "**samsung**" in der gesamten E-Mail-Adresse prüfen, anstatt sich nur auf den Domainnamen zu beschränken.

Damit wollen die Programmierer den Missbrauch der eigenen Domain verhindern, sind aber aus Schlamperei über das Ziel hinausgeschossen. D. h. "**samsung.com@spam.org**" ist eine gültige E-Mail-Adresse, die aber bei der Kontoerstellung von Samsung nicht akzeptiert wird.

Praxiserfahrung

Bei mir kommt es inzwischen nicht mehr vor, dass eine E-Mail-Adresse, die ich eigens für einen Dienst oder Kontakt angelegt habe, richtig zugespammt wird. Leute, die Probleme mit Spam haben, gehen in der Regel zu leichtfertig mit ihrer E-Mail-Adresse um und haben in der Regel auch nur eine einzige eingerichtet. Da ist es nur eine Frage der Zeit, bis Spam zu einem Problem wird.

In der Praxis erhalte ich mit meiner Methode keinen Spam. Wie es aber der Zufall will, bekam ich während ich diesen Beitrag verfasste, eine E-Mail mit Werbung zugeschickt. Diese hatte als Empfänger jedoch eine Adresse, die ich früher eine Zeitlang auf meiner Homepage zur Kontaktaufnahme veröffentlicht hatte und ich sozusagen selbst die Schuld daran trage.

Nachdem es aber vorher wochenlang vollkommen still war und es mehr Arbeit ist die Adresse zu ändern, als die E-Mail zu löschen, lösche ich diese Spam-E-Mail einfach, bzw. verschiebe sie zu Statistikzwecken in einen dafür erstellten Unterordner. Sollte sich das wider Erwarten häufen bzw. es anfangen mich zu nerven, kann ich die Adresse immer noch ändern.

> Aktualisierung vom 31.12.2017: Bereits einige Zeit vor Weihnachten hat der Spammer, der meine E-Mail-Adresse in die Finger bekommen hat, angefangen vermehrt Werbung zu versenden, so dass ich die Adresse zwischenzeitlich geändert und wieder 0 Spam habe.

Es folgt nun ein Praxis-Beispiel, wie mit meiner Methode verfahren wird. Nehmen wir dazu als Beispiel Workaway. Ich melde mich bei Workaway mit der E-Mail-Adresse "**workaway.info@spam.org**" an und erhalte eine automatische Eingangsbestätigung die mich auffordert meine Registrierung durch das Anklicken eines Links zu bestätigen.

Ich bestätige den Link und nutze die Plattform, um Stellplatzangebote für mein Wohnmobil zu finden. Nach einiger Zeit bekomme ich auf diese E-Mail-Adresse unerwünschte Werbung (ob von Workaway oder von Dritten, ist jetzt nicht wichtig).

Falls ich in der Zwischenzeit das Interesse an der Plattform verloren habe, lösche ich die Weiterleitung einfach und fertig. Möchte ich sie aber noch nutzen, erstelle ich zunächst eine neue Weiterleitung (z. B. "**workaway.info-2@spam.org**")

ändere meine E-Mail-Adresse bei workaway.info auf die neue und lösche dann die alte Weiterleitung.

Vorsicht: Die zuvor genannte Reihenfolge sollte eingehalten werden, denn es gibt manche Dienste, die schicken zunächst an die alte Adresse eine Änderungsbestätigung, bevor die neue aktiviert werden kann. Das ist in meinen Augen Unsinn, weil es sein kann, dass es sich dabei um eine Adresse handelt, auf die man keinen Zugriff mehr hat (z. B. wenn eine Domain verkauft/gelöscht wurde), habe ich aber selbst schon erlebt.

Jeder Mensch ist von seinem Gemüt her anders. Manche nehmen Spam als unvermeidbar hin und ärgern sich auch gar nicht über die unerwünschte Werbung oder sind mit ihrer Spam-Filter-Lösung zufrieden. Andere wieder (dazu zähle ich) empfinden Spam als Eingriff in die Privatsphäre, was sie zum Handeln nötigt und ihre Zeit verschwendet.

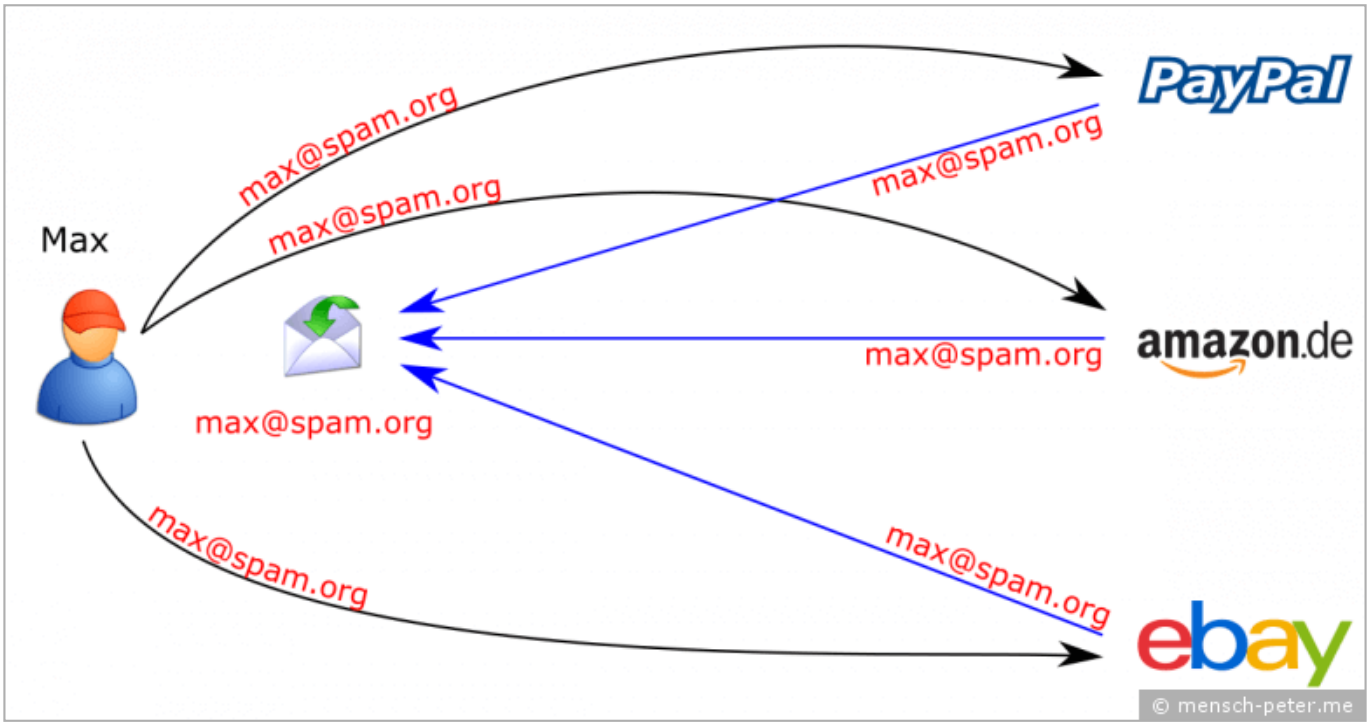
Mein vierter und letzter Grundsatz bei meiner Anti-Spam-Methode lautet daher:

Läuft (zu viel) Spam auf eine E-Mail-Adresse ein, wird einfach die Weiterleitung gelöscht und gegebenenfalls eine neue erstellt.

Zusammenfassung meiner Methode

1. Es wird nur ein einziges, geheimes Postfach eingerichtet, dessen E-Mail-Adresse nicht weitergegeben wird.
2. Die "Sammelweiterleitung" beim Provider wird deaktiviert.
3. Für alle genutzten E-Mail-Adressen, sei es ein Dienst im Internet oder einzelne Kontakte, bzw. Kontaktgruppen, wird eine eigene Weiterleitung auf das geheime Postfach eingerichtet.
4. Läuft (zu viel) Spam auf eine E-Mail-Adresse ein, wird einfach die Weiterleitung gelöscht gegebenenfalls eine neue erstellt.

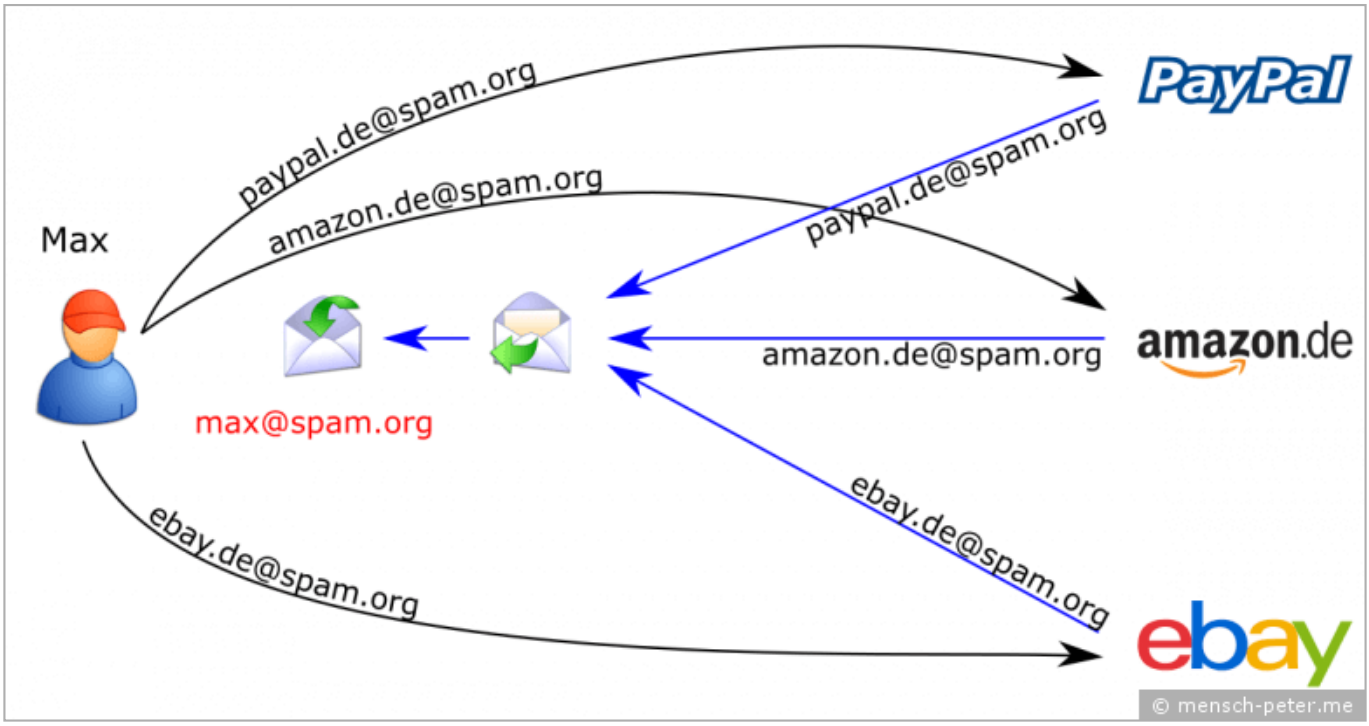
Im folgenden Bild ist grafisch der falsche Umgang mit einer E-Mail-Adresse dargestellt:



Falsch: Eine E-Mail-Adresse für alle Dienste (Bild 1/1)

Der Max gibt seine einzige E-Mail-Adresse "**max@spam.org**" an alle Dienste und Kontakte weiter, die wiederum alle dieselbe E-Mail-Adresse zur Kommunikation verwenden müssen.

Im Gegensatz dazu die Anwendung meiner Anti-Spam-Methode:



Richtig: Für jeden Dienst eine eigene E-Mail-Adresse (Bild 1/1)

Hier gibt der Max die E-Mail-Adresse seines geheimen Postfachs "**max@spam.org**" nicht an andere weiter, sondern jeweils nur spezifische Weiterleitungen, die er für jeden genutzten Dienst bzw. Kontakt eigens eingerichtet hat. Somit hat er eine Art "Firewall" vor sein Postfach geschaltet.

Sollte jetzt auf einer dieser Adressen Spam einlaufen, braucht er nur die entsprechende Weiterleitung zu löschen bzw. zu ändern und lässt sein Postfach unangetastet.

Erweiterte Anti-Spam-Methode

Zur Vorstellung meiner Methode habe ich diese vereinfacht beschrieben, damit sie leichter verstanden wird. In der Regel ist sie in dieser Form auch völlig ausreichend. Der Vollständigkeit halber gehe ich jetzt aber noch einen Schritt weiter.

Rein theoretisch könnte es passieren, dass das geheime Postfach bekannt wird und es dann gegebenenfalls gelöscht werden muss, um wieder Spamfrei zu werden.

Wer dann wie ich weit über 100 Weiterleitungen auf dieses Postfach eingerichtet hat, müsste nun alle diese Weiterleitungen auf ein neu eingerichtetes Postfach anpassen. Bei dem bereits erwähnten cPanel gibt es die Möglichkeit Weiterleitungen zu exportieren und anschließend wieder zu importieren.

Es werden also alle Weiterleitungen exportiert und mit einem Texteditor die E-Mail-Adresse des alten Postfachs durch die des neuen ersetzt. Danach werden die geänderten Weiterleitungen importiert und es kann wieder normal weitergearbeitet werden.

Nun gibt es aber auch Provider, die nicht das cPanel, sondern eine eigene Administrationsoberfläche verwenden. Gibt es bei dieser keine Ex-/Importmöglichkeit, so wäre das mit viel Arbeit verbunden, um meine Methode wieder zum Laufen zu bekommen.

Um sich diese Arbeit zu sparen, wird einfach eine geheime Zentralweiterleitung eingerichtet. D. h. alle Weiterleitungen zeigen nicht mehr auf das geheime Postfach, sondern auf die geheime Zentralweiterleitung. Diese wiederum zeigt auf das geheime Postfach.

Im Notfall müsste dann nur ein neues Postfach eingerichtet und die Zentralweiterleitung gelöscht werden. Danach wird eine neue Zentralweiterleitung eingerichtet, die auf das neue Postfach zeigt, und kann anschließend das alte Postfach löschen (E-Mails vorher sichern).

Ein alternativer Anwendungsfall für die Einrichtung so einer geheimen Zentralweiterleitung stellt ein Domainumzug dar. Hier lassen sich ganz einfach alle bestehenden E-Mail-Weiterleitungen, die ja auf die geheime Zentralweiterleitung zeigen, auf die neue Domain umleiten, indem nur die geheime Zentralweiterleitung geändert, bzw. neu erstellt wird.

Zur Verdeutlichung folgen ein paar Beispiele. Die E-Mail-Adresse des geheimen Postfachs soll dabei "**nie-wieder@spam.org**" lauten.

Einfache Methode:

paypal.de@spam.org -> **nie-wieder@spam.org**

amazon.de@spam.org -> **nie-wieder@spam.org**

ebay.de@spam.org -> **nie-wieder@spam.org**

Erweiterte Methode:

Es wird zunächst eine Zentralweiterleitung mit z. B. "**redirects@spam.org"** eingerichtet. Alle Weiterleitungen richtet man jetzt nicht mehr auf das geheime Postfach, sondern auf die geheime Zentralweiterleitung ein, die auf das geheime Postfach zeigt:

paypal.de@spam.org -> **redirects@spam.org** -> **nie-wieder@spam.org**

amazon.de@spam.org -> **redirects@spam.org** -> **nie-wieder@spam.org**

ebay.de@spam.org -> **redirects@spam.org** -> **nie-wieder@spam.org**

Domainumzug:

paypal.de@spam.org -> **redirects@spam.org** -> **info@anti-spam.net**

amazon.de@spam.org -> **redirects@spam.org** -> **info@anti-spam.net**

ebay.de@spam.org -> **redirects@spam.org** -> **info@anti-spam.net**

Wie bereits geschrieben, ist diese Vorgehensweise für den Normalanwender nicht von Bedeutung. In meinem Fall (ich nutze die erweiterte Methode) sind in all den Jahren weder das geheime Postfach, noch meine geheime Zentralweiterleitung bekannt geworden. Und nein: meine lautet nicht "**redirects@mensch-peter.me**" ;-).

Aktualisierung vom 07.03.2018: Nach vielen Jahren des störungsfreien Betriebs, hat heute das erste Mal ein Shopbetreiber eine E-Mail an meine geheime Sammelweiterleitung geschickt. Wie er diese herausgefunden hat, bin ich mir nicht ganz sicher. Die Weiterleitung, die ich für diesen Shop verwendet hatte, hatte ich bereits vor längerer Zeit gelöscht.

Ich habe jetzt im C-Panel alle Weiterleitungen heruntergeladen und die Adresse für die Sammelweiterleitung ersetzt. Dabei werden Adressen, die auf Autoresponder und E-Mail-Konten zeigen, mit einer Pipe dargestellt, die sich damit nicht wieder importieren lassen. D. h. diese Pipes müssen aus der Datei entfernt werden.

Weil sich im C-Panel Weiterleitungen nur einzeln löschen lassen, habe ich meinen Provider gebeten diese für mich auf einmal zu löschen, was er innerhalb von ein paar Minuten nach der Supportanfrage erledigt hatte.

Danach habe ich meine geänderten Weiterleitungen wieder importiert. Dadurch ging jedoch die Zuordnung von Weiterleitung und Autoresponder verloren. Nachdem ich aber alle Autoresponder einfach neu gespeichert habe, hat alles wieder wie zuvor funktioniert. Die Weiterleitung auf das geheime E-Mail-Konto war nicht davon betroffen und funktionierte nach dem Import sofort wieder.

Anmerkung: Meine erweiterte Methode hatte ich bereits bei verschiedenen Providern im Einsatz. Gab es Probleme mit dem E-Mail-Empfang so behauptete

der Support von zwei Providern es läge an meiner doppelten Weiterleitung. Es stellte sich aber in beiden Fällen heraus, dass das nicht die Ursache war und doppelte Weiterleitungen somit kein Problem sind.

Vorteile meiner Anti-Spam-Methode

- Spam ist kein Problem mehr, sondern eine seltene Ausnahmeerscheinung
- Man hat Kontrolle über den Spammer und kann ihn bei Bedarf abschalten
- Es lässt sich die Quelle von Spam (exakt) bestimmen und den Verursacher auf das Problem hinweisen
- Einmal eingerichtet benötigt sie einen minimalen Zeitaufwand um funktionsfähig zu bleiben
- Auf einen Spam-Filter kann verzichtet werden und man muss dessen Aktivitäten nicht auf Fehler kontrollieren
- Kein Ärger mit schlecht programmierter Anti-Spam-Software auf dem eigenen Rechner, da überflüssig

Nachteile meiner Anti-Spam-Methode

- Man muss sich in das Thema einarbeiten und seine Arbeitsweise ändern (gerade Letzteres fällt vielen schwer)

Mehr fällt mir nicht ein. Wer noch Vorschläge hat, darf diese gerne in die Kommentare schreiben, damit ich diese Negativliste erweitern kann.

Allgemeine Tipps

Zum Schluss folgen noch allgemeine Sicherheitstipps im Umgang mit E-Mails und dem Internet:

- Halte Deine Software auf dem neuesten Stand. Dazu zählen in erster Linie alle Programme, die eine Verbindung ins Internet aufbauen, allen voran Dein E-Mail-Programm und Dein Browser.
- Nutze zur Verwaltung jedes Deiner Konten im Internet ein eigenes, sicheres Kennwort. Ein Passwort-Manager, wie z. B. RoboForm (RoboForm-v8-Setup.exe (21,44 MB)), mit dem ich schon seit vielen Jahren arbeite, nimmt Dir nicht nur das Ausdenken von sicheren Kennwörtern ab, sondern meldet Dich per Mausklick an jedem Dienst automatisch an. In Zukunft brauchst Du Dir nur noch ein einziges, sicheres Kennwort zu merken, um den Passwort-Manager zu entsperren (optional).

Unknackbar aber einfach zu merken! - Passwörter einfach erklärt (1/5) (ca. 4,5 Minuten)

- E-Mails von unbekannten Absendern sind grundsätzlich zunächst als Spam

bzw. Betrugsversuch zu behandeln und im Zweifelsfall sofort gelöscht werden. Auf keinen Fall werden darin enthaltene Links oder Anlagen angeklickt, da dies u. U. bereits zu einem Virenbefall führen kann.

- Du solltest Dir auch bewusst sein, dass Spammer eine Absenderadresse leicht fälschen können. Sei daher auch vorsichtig, wenn Du völlig unerwartet eine E-Mail von einem bekannten Absender erhältst (z. B. Paypal).
- Weder Deine Bank, noch Paypal (naja, auch eine Art Bank) werden Dich jemals per E-Mail dazu auffordern Deine Zugangsdaten zu verifizieren. Im Falle des Passworts ist das auch gar nicht möglich, weil Dein Passwort auf keinem Server gespeichert wird. Es wird dort nur ein Hashwert des Passworts gespeichert, der bei der Anmeldung mit der Eingabe Deines Passworts verglichen wird.
- Falls Du von einem Dienst aufgefordert wirst, Dich dort einzuloggen, um z. B. auf ein Sicherheitsproblem zu reagieren oder um neue AGB zu bestätigen etc., so verwende dazu nie den in der E-Mail angegebenen Link. Dieser könnte zu einer gefälschten Seite führen, bei der Deine Logindaten abgefangen werden. Logge Dich daher **immer** über Deinen Passwort-Manager oder einem gespeicherten Lesezeichen ein.
- Besuche keine Internetseiten, die z. B. kostenlose Lizenzschlüssel, illegale Waren etc. anbieten. Auf solchen Seiten besteht eine erhöhte Gefahr sich einen Virus einzufangen, da sie ja von Menschen mit einer fragwürdigen Moral betrieben werden.
- Verwende E-Mail- und Internetadressen nur in Kleinschreibweise. Gemischte Groß-/Kleinschreibung (z. B. "**Max.Muster@spam.org**") mag schöner aussehen, spielt aber für die Funktion keine Rolle. Anwender, die das aber nicht wissen, werden dadurch überflüssigerweise genötigt die exakte Schreibweise zu verwenden.
- Installiere nur Software von vertrauenswürdigen Quellen und verzichte auf Download-Manager von Drittanbietern, die Dir vielleicht keinen Virus

installieren, jedoch ungefragt andere Programme. Im Zweifelsfall versuche immer die Herstellerseite ausfindig zu machen und von dort die Software herunterzuladen.

- Nutze zum Scannen heruntergeladener Software z. B. den Dienst von VirusTotal, der eine Überprüfung mit ca. 60 verschiedenen Scannern vornimmt und damit sicherer arbeitet, als jeder lokal installierte Virenscanner.
- Sei vorsichtig bei der Nutzung öffentlicher Hotspots. Auch, wenn der Betreiber keine bösen Absichten haben sollte, könnte ein anderer Nutzer Dir Schaden zufügen.

Fragen und Antworten

Frage: Kann ich von Deiner Methode auch profitieren, wenn ich keine eigene Domain habe?

Antwort: Das kommt auf den Provider an, bei dem Du Dein E-Mail-Postfach eingerichtet hast. Wenn es dort die Möglichkeit gibt E-Mail-Aliase einzurichten, so kannst Du diese anstatt Weiterleitungen bei den verschiedenen Internetdiensten verwenden.

Frage: Das ist ja alles schön und gut, aber ist das nicht etwas viel Aufwand?

Antwort: Der meiste Aufwand an meiner Methode war für mich das Schreiben dieser Anleitung und für Dich das Lesen und Verstehen derselbigen. Eine neue E-Mail-Weiterleitung einzurichten ist eine Kleinigkeit.

Im Vergleich zu einem Durchschnittsanwender nutze ich als Programmierer verhältnismäßig viele Dienste. Dennoch benötige ich eine neue Weiterleitung nicht jeden Tag. Gefühlt würde ich sagen 1-2 mal alle 14 Tage. Ein "Aufwand" von etwa zwei bis vier Minuten pro Monat, um Spamfrei zu bleiben - mir ist es das wert.

Frage: Ich habe bereits meine einzige E-Mail-Adresse bei vielen Diensten registriert. Die müsste ich dann bei der Anwendung Deiner Methode ja überall ändern, oder nicht?

Antwort: Meine Anti-Spam-Methode nutze ich wie geschrieben bereits seit vielen Jahren und "mensch-peter.me" ist während dieser Zeit meine dritte Domain. D. h. ich habe bereits zwei Umzüge mit allen Weiterleitungen hinter mir.

Durch das Ex-/Importieren von den bestehenden Weiterleitungen war die Änderung beim Domainwechsel kein Problem. Nun müsste ich aber auch alle E-Mail-Adressen ändern, die ich bei allen möglichen Diensten registriert habe?

Theoretisch ja, in der Praxis sieht es aber so aus, dass ich mit Hilfe des bereits erwähnten Passwort-Managers RoboForm (RoboForm-v8-Setup.exe (21,44 MB)) nur bei den noch aktuell genutzten Diensten in relativ kurzer Zeit die E-Mail-Adresse geändert habe.

Bei anderen Diensten mache ich das nach und nach nur bei Bedarf. Dort kann ich mich noch immer problemlos mit meiner alten E-Mail-Adresse anmelden und diese dann ändern.

Wenn Du aktuell eine Vielzahl von Diensten nutzt und Dich bisher ohne Passwort-Manager durchs Leben gequält hast, ist der Aufwand schon spürbar größer. In diesem Fall empfehle ich die Umstellung in zwei Schritten vorzunehmen:

1. Einen Passwort-Manager installieren und damit eine Zeitlang arbeiten
2. Erst, wenn die am meisten genutzten Dienste alle im Passwort-Manager gespeichert sind, nimmst Du die Umstellung vor

Frage: Ich möchte Deine Methode anwenden, komme damit aber nicht zurecht. Kannst Du mir weiterhelfen?

Antwort: Sofern es noch Verständnisprobleme oder allgemeine Fragen gibt, beantworte ich diese gerne in den Kommentaren.

Sind es spezifische Probleme bei der Einrichtung/Verwaltung einer Domain, dem Einrichten von E-Mail-Konten etc., helfe ich gerne per Fernwartung weiter. Dabei

erkläre ich Dir an Deinem eigenen Computer, was ich gerade mache und beantworte alle Deine Fragen.

Diesen Service kann ich nicht kostenlos anbieten und bitte bei Interesse um eine unverbindliche Anfrage über das Kontaktformluar.

Beitrag auf dem Smartphone lesen

Scanne das Bild mit Deinem Smartphone, um den Beitrag mit Deinem Smartphone zu lesen:

Mensch Peter

Auf meiner Homepage mensch-peter.me findest Du drei Rubriken mit weiteren Beiträgen:

Rezensionen | Tagebuch | Wohnmobil

Das Inhaltsverzeichnis gibt Dir eine Übersicht über alle meine Beiträge.

Hast Du Verbesserungsvorschläge, eine Frage oder einen Fehler gefunden, so schreibe mir bitte eine Nachricht oder hinterlasse einen Kommentar.

Sofern Du diesen Beitrag interessant findest, freue ich mich, wenn Du ihn mit anderen teilst:

WhatsApp	Facebook	Twitter	VKontakte

Pinterest	Tumblr	Reddit	LinkedIn
Xing	Google+		

Um den Beitrag in einem (älteren) Forum zu verwenden, kannst Du diesen BBCode verwenden:

```
[url=https://mensch-peter.me/go/p]Spam vermeiden ganz ohne Spamfilter[/url]
```

Oder als direkte Url (kann jedoch zu Problemen führen):

```
[url=https://mensch-peter.me/tagebuch/2017/09/spam-vermeiden-auch-ohne-spamfilter/]Spam vermeiden ganz ohne Spamfilter[/url]
```

Kurzlink (für E-Mails empfohlen, um zu verhindern, dass Links umgebrochen werden):

```
https://mensch-peter.me/go/p
```

Amazon Partnerprogramm

Hinweis: Peter ist Teilnehmer des Partnerprogramms von Amazon Europe S.à.r.l. und Partner des Werbeprogramms, das zur Bereitstellung eines Mediums für Websites konzipiert wurde, mittels dessen durch die Platzierung von Werbeanzeigen und Links zu amazon.de Werbekostenerstattung verdient werden können.

Links in dieser PDF-Datei, die zu Amazon führen, sind mit einer PartnerID versehen, um gemäß dem obigen Hinweis Werbekostenerstattungen erzielen zu können.

Die Vergütung aus dem Amazon Partnerprogramm zahlt dabei immer Amazon, nie der Käufer.