SG **August 2009**

Bekommen Sie von der Pressglas-Korrespondenz Spam-Mails?

Wikipedia: „Durch Spam entsteht allein in den Vereinigten Staaten pro Jahr ein Schaden von 22 Milliarden US-Dollar. Nach neueren Studien verbrauchen 62 Billionen [60.000.000.000.000] Spam-Mails jährlich zirka 33 Milliarden Kilowattstunden Energie sowie 100 Milliarden [100.000.000.000] User-Stunden zum Sichten und Löschen der Spam-Mails. Demnach macht Spam mittlerweile 97 % des gesamten Mail-Volumens aus.“

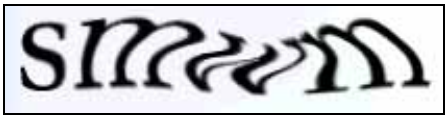
Haben Sie schon Spam mit meiner Mail-Adresse als Absender bekommen?

Wenn ja, dann bitte möglichst detailliert berichten - vielleicht kann ich etwas dagegen tun.

Auf der Website www.pressglas-korrespondenz.de wird meine Mail-Adresse nur als „**Captcha**“ angegeben: d.h. es ist eine Grafik, die bisher von den Programmen nicht gelesen werden kann, die Adressen als Empfänger und Absender für SPAM sammeln, so genannte „**Address-Harvester**“ [Erntemaschinen für Mail-Adressen].

Wikipedia: „Da die meisten E-Mail-Adressen aus dem Internet von so genannten **Address-Harvestern** automatisch aus den Newsgroups und Webseiten extrahiert werden, verspricht es einigen Erfolg, dort keine Adressen zu nennen oder die Adressen so zu verschleiern, dass sie von den Address-Harvestern nicht gefunden werden.“

Abb. 2009-3/447
Captcha „smwm“, aus Wikipedia: Captcha (2009-08)



Wikipedia: „**Hohe Sicherheit** bieten so genannte „**Captchas**“, mittels derer Menschen von Maschinen unterschieden werden sollen. So wird vorgeschlagen, die **Mail-Adresse in einem Bild** anzugeben oder in einer Audio-Datei zu buchstabieren. Allerdings sind diese Lösungen weder besonders komfortabel noch barrierefrei.“ „**Captcha“** ist ein Akronym für „**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part”. Captchas werden verwendet, um zu entscheiden, ob gegenüber Mensch oder Maschine ist.“

„**Address-Harvester**“ sind „**Webcrawler**“ (auch „**Spider**“), d.h. Computer-Programme, die automatisch das World Wide Web durchsuchen und Webseiten analysieren. Gutartige Webcrawler werden vor allem von **Suchmaschinen** wie **GOOGLE**, **YAHOO** ... eingesetzt. **Bösartige** Anwendungen sind das **Sammeln von Mail-Adressen**, RSS-Newsfeeds, oder anderen Informationen.“ [Wikipedia: Spam ...]

Übrigens „führte die Überprüfung der Gültigkeit von Absender-Adressen zur **Verwendung gültiger Adressen**. Dies hatte den Effekt, dass Unschuldige mit Tausenden bis zu Millionen von Bounces überschüttet wurden.“ [Wikipedia: Spam ...]

Da jedermann, der im Internet etwas einkauft, schon zur Benachrichtigung über die Bestellung seine richtige Mail-Adresse eingeben muss, gibt es im Lauf eines Jahres **Hunderte von Gelegenheiten, wo kriminelle Crawler und Spider diese Adresse abfangen können**. Da kann mann / frau gar nichts dagegen machen, auch wenn die Hersteller & Anbieter von Software für „Internet-Security“ und von Mail-Servern oder die Anbieter von Waren und Dienstleistungen (verschlüsselte Web-Verbindungen mit **https://**) zur Werbung gerne etwas anderes behaupten. (Eine nur für Profis nutzbare Möglichkeit ist, Mail-Adressen anzugeben, die nur für diesen Zweck gelten und danach und automatisch wieder verschwinden, „**Wegwerf-Mail-Adressen**“, z.B. Software „Spambox“).

Man könnte in unregelmäßigen Abständen seine **Mail-Adresse aufgeben** und eine ganz andere erfinden. Das würde aber jeden Mail-Verkehr z.B. zwischen www.pressglas-korrespondenz.de und den Abonnenten und Lesern der PK zugrunde richten!

Trotz aller empfohlenen **Sicherheitsmaßnahmen** von „Captchas“ bis Anti-Viren-Software auf dem eigenen Computer und Spam-Filtern beim Mail-Server wurde wahrscheinlich auch meine Mail-Adresse gekapert. Zumindest bei mir gehen seit einigen Wochen massenhaft Mails mit wegen ihrer Blödheit sofort erkennbaren **obskuren Absendern** und mit ebenso **blöder Anmache** im „Betreff“ ein: z.B. Sherika Owyyowq, Called lately?; Kivisto Davina, Skype ID; Chadwick Qxalim, Deadline for registering. Selbstverständlich sind das ohne Ausnahme so genannte „**Unverlangte kommerzielle E-Mails**“ (**UCE**), fast immer mit **unerwünschter Werbung** für Finanzdienstleistungen, gefälschte Uhren, illegale Online-Glücksspiel-Casinos, Lebensverlängerung, Markenprodukte, Medikamente, Nigeria-Scam der Nigeria-Connection (Vorschussbetrüger), Online-Sex, Penis-Verlängerung, Pornografie, angeblich günstige Software, **Viagra** und ähnlichen Mist.

Je nachdem, welchen Mail-Server (z.B. T-Online) und welchen Mail-Client (z.B. Firefox-Thunderbird) Sie verwenden, **bleiben die Mails auf dem Server** und werden beim Lesen nicht auf den eigenen Computer geladen. Das **verhindert** oder **behindert** wenigstens schon einmal, dass durch solche Spam-Mails auch noch Viren auf den eigenen Computer geladen werden. Den Rest sollte ein **Anti-Viren-Programm** auf dem eigenen Computer erledigen. (Man muss einstellen können, ob Mails beim Lesen vom Server auf den eigenen Computer verschoben werden!)

Übrigens sollten Sie „**Spam-Filter**“ der Mail-Software so einstellen, dass als Spam ausgefilterte Mails trotzdem

in einem eigenen Ordner auf dem Mail-Server angezeigt werden. Es gibt selbstverständlich nicht nur „**false negatives**“, d.h. Spam wird nicht erkannt und ausgefiltert, sondern auch „**false positives**“, d.h. Mails werden zu Unrecht ausgefiltert, und man sollte wissen, welche Absender ausgefiltert wurden.

Auch wenn sie „nur“ auf dem Mail-Server liegen, sollte man solche **Mails erst gar nicht öffnen**. Und man darf **auf keinen Fall in solchen Mails irgend etwas anklicken**. Hinter diesen angeblichen Werbe-Mails können nämlich ganz andere Schädlinge lauern, die auf dem eigenen Computer alle denkbaren Schäden anrichten können. Das geht bis dahin, dass der eigene Computer zu einem **ferngesteuerten** „**Bot-Server**“ wird, der seinerseits Spam und Schadsoftware weltweit auf anderen privaten Computern verbreitet. Ein besonders berüchtigtes Beispiel ist der seit Anfang 2009 von Fachpresse und Presse gemeldete „**Trojaner**“ „**Conficker**“. Übrigens kann jedermann einfach prüfen, ob „Conficker“ schon auf dem eigenen Computer gelandet ist: **http://www.heise.de/security/** ... Die-Infoseite-zu-Conficker--/artikel/135725

Die renommierte **Fachzeitschrift „c't“** für Computer-Freaks habe ich seit mehr als 15 Jahren regelmäßig gelesen bzw. abonniert. Dort habe ich jetzt um Rat gefragt, aber von den anscheinend überlasteten Experten **Wochen lang keine Antwort** bekommen, ganz zu schweigen von einer **praktikablen Lösung**. Das Abo weiter zu verlängern, halte ich jetzt für überflüssig!

Dass man vom Anbieter eines Mail-Servers, wie z.B. T-Online ..., in einem solchen Fall Hilfe bekommt, wird wohl von vorne herein niemand ernsthaft erwarten.

Ich könnte jetzt im Abstand von 3 Monaten meine **Mail-Adresse aufgeben und austauschen** - es wäre ein großer Aufwand, würde meinen ziemlich wichtigen Mail-Verkehr gründlich lahm legen und wäre sinnlos. Man kann dieser Schadsoftware und vor allem den Spam-Mails praktisch nicht entgehen!!!

Vor allem auch nicht, weil die wichtigsten Programme für den täglichen Arbeitsgebrauch wie MICROSOFT ... offenbar laufend weitere Löcher (Sicherheitslücken) für Schad-Software aufmachen, die jetzt in regelmäßigen Abständen an „**Patch-Days**“ angeblich durch „**Patches**“ [Flicken] gestopft werden. Selbst lange Zeit für sicher gehaltene, angesehene Hersteller wie ADOBE (PDF-Dokumente ...) oder MOZILLA (Webbrowser FIREFOX) müssen inzwischen ziemlich oft Patches für solche Löcher liefern!

Und vor allem:

Wenn meine Adresse als Absender von Spam-Mails gekapert wurde, kann ich auch durch laufende Änderungen meiner Adresse nicht verhindern, dass mit der alten Adresse bis zum Sankt Nimmerleins-Tag weiter Spam-Mails weltweit versendet werden!!!

Da behalte ich lieber meine Mail-Adresse!

Angeblich kann man **kriminelle Mail-Versender** bis zum Urheber zurückverfolgen und dann vor Gericht bringen! Wer glaubt, dass man einen solchen Kriminellen in Bulgarien, China, Deutschland, Nigeria, Russland, Südostasien, Ukraine oder USA ... wirklich findet und dann **mit der Polizei ergreifen und vor Gericht schleppen** lassen kann, wo er dann saftig verurteilt wird und bereut und nie wieder Schad-Mails versendet, der glaubt auch an den Klapperstorch, den Osterhasen und den Weihnachtsmann zusammen!

Schließlich wird mit Spam-Mails nicht nur ein **Schaden** von Milliarden Euros oder Dollars angerichtet, sondern mindestens genau so viel **Gewinn** gemacht: es gibt nämlich immer noch ausreichend viele Idioten, die glauben, ein „**Schnäppchen**“ gefunden zu haben und Schad-Links anklicken! **Längst wurde ausgerechnet, dass sich selbst bei einem winzigen Anteil von solchen Mail-Empfängern der Spam-Versand für kommerzielle und kriminelle Absender lohnt!!!**

Wikipedia: „Auch **eBay** oder **PayPal** verfolgen - natürlich primär im eigenen Interesse - **Spam-Versender**. Diese werden auf Unterlassung verklagt [...]. eBay und PayPal gehen jedem Hinweis nach und verfolgen die Versender von Spam-Mails weltweit. Dazu muss man Spam-Mails, die sich für eBay bzw. PayPal ausgeben, an folgende Adresse weiterleiten: **spoof@ebay.de** oder **spoof@paypal.de**.“ SG: Solche primitiven Phishing-Mails wurden nach meiner Erfahrung aufgegeben!

Wikipedia: Am 1. Juli 2005 hatte das vom Bundesministerium für Verbraucherschutz, Ernährung und Landwirtschaft (BMVEL) zusammen mit dem Verbraucherzentrale Bundesverband e.V. ein mittlerweile wieder eingestelltes Projekt einer **Beschwerdestelle zur Bekämpfung von Spam** gestartet. [...] Die Beschwerdestelle wurde am 31. Dezember 2006 jedoch vorläufig **eingestellt**, so dass man seit Mitte Dezember 2006 keinen Spam mehr melden kann. Ob und wann die Beschwerdestelle fortgeführt wird, steht noch nicht fest.“

Ein **Vorschlag für wagemutige Freaks**: „den **Täter an der Ausführung seiner Geschäfte hindern**. So können Empfänger von UCE zum Schein mit falschen persönlichen Daten auf die angebotenen Geschäfte eingehen. Dies bewirkt beim Händler, dem der Täter zuarbeitet, eine Flut von Fehlern bei Bestellungen von Kunden, die vom Täter angeworben wurden. Das führt möglicherweise sogar zur Beendigung des Geschäftsverhältnisses.“ [Wikipedia: Spam ...]

Das sollten Sie auf keinen Fall ausprobieren! Da fallen Sie heutzutage bestimmt auf Phishing oder einen Schad-Link herein!

Siehe unter anderem auch:

PK 2009-3 SG, Downloads / Security Updates Adobe Reader / Windows, Version 8.1.3 und 9.1.1
siehe auch: http://de.wikipedia.org/wiki/Spam ...
https://mail.google.com/mail/help/intl/de/about.html