

Spam von eigener Adresse [HVF&PH]

29.10.2024 06:33:32

FAQ-Artikel-Ausdruck

Kategorie:	E-Mail & Groupware	Bewertungen:	0
Status:	öffentlich (Alle)	Ergebnis:	0.00 %
Sprache:	de	Letzte Aktualisierung:	12:48:42 - 25.06.2020

Schlüsselwörter

E-Mail Spam

Symptom (öffentlich)

Es kommt vor, dass Mails scheinbar von der eigenen E-Mail-Adresse geschickt wurden, wodurch die Befürchtung auftritt, dass das eigene Mailkonto gehackt wurde. Meistens kriegt man dies von den Empfängern solcher Mails mit oder aber kriegt selbst Mails von anderen, die offensichtlich Spam sind oder gar Schadsoftware enthalten.

Problem (öffentlich)

Wurde das E-Mail-Konto übernommen/gehackt? Diese Frage lässt sich meist leicht beantworten, denn in der Regel wird die E-Mail-Adresse nur vorgetäuscht.

In den Feldern der E-Mail, in denen Sender und Empfänger stehen, kann man neben der Mailadresse auch beschreibende Informationen mitgeben. Üblicherweise wird hier ein Name im Klartext angegeben, der für die Kommunikationspartner leichter zu lesen ist, als die E-Mail-Adresse. Wenn zum Beispiel Frau Professor Marie Musterfrau die E-Mail-Adresse `marie.musterfrau@campus-lb.de` hat, so könnte das mit hinzugefügtem Klartext wie folgt aussehen: "Musterfrau, Marie, Prof." <marie.musterfrau@campus-lb.de>

In diesen Klartextbereich kann aber alles mögliche geschrieben werden, also auch E-Mail-Adressen die nicht so vom E-Mail-Programm ausgewertet werden, aber von Menschen gelesen werden. Als Beispiel: "marie.musterfrau@campus-lb.de" <die.eigentliche@spam-adresse.xx>

Es gibt auch Möglichkeiten die komplette Mailadresse vorzutauschen, doch diese Methoden werden heutzutage von den meisten E-Mail-Servern erkannt und schon vorab als Spam heraus gefiltert.

Ein E-Mail-Konto tatsächlich zu hacken ist mit erheblichem Aufwand verbunden, der zudem auch oft von den E-Mail-Servern schon im Versuch erkannt und unterbunden wird. Sollte man also keine einfachen Passwörter verwenden, diese regelmäßig erneuern und auch nicht verlieren, ist es recht unwahrscheinlich, dass ein E-Mail-Konto der Hochschule gehackt wird. Sollte man allerdings ein Endgerät wie Notebook oder Smartphone verlieren, von dem man mit E-Mails arbeitet, sollte man umgehend das Passwort ändern.

Warum bekommt man Spam? E-Mail-Adressen, die Spammer zusammentreiben können, können diese (von dubiosen Quellen) in Hunderttausender-Listen kaufen.

Die Adressen werden auf unterschiedlichen Wegen gesammelt. Zum Beispiel können ausgeschriebene Adressen von Internetseiten durch Roboter gesucht werden. Wenn man in einem Internetdienst wie einem Forum angemeldet ist und das System dort kompromittiert wurde, werden dort E-Mail-Adressen abgezogen. Sollte ein E-Mail-Konto kompromittiert worden sein, mit dem man Kontakt hatte, können die Informationen dort heraus gezogen werden. Wenn man Diensten erlaubt auf das eigene Adressbuch zuzugreifen kann das auch zu einem Datenleck führen.

Kurz: E-Mail-Adressen kommen auf vielen Wegen in die Spam-Listen, das ist fast nicht zu verhindern.

Warum sind die vermeintlichen Spammer bekannt? Auch das kann auf vielen Wegen herausgefunden werden, aber in der Regel liefern speziell E-Mail-Adressen die aus gekaperten E-Mails oder aus Adressbüchern kommen, sehr eindeutige Hinweise darauf, welche Kommunikationspartner miteinander zu tun haben. Diese Konstellationen sind für die Spammer von Vorteil, weil der Empfänger dann vielleicht weniger Vorsicht beim Klicken auf Links oder Öffnen von Anhängen walten lässt.

Lösung (öffentlich)

Wenn die Befürchtung besteht, dass das eigene E-Mail-Konto kompromittiert wurde, sollte man dringend das Passwort ändern.

Wenn es sich allerdings nur um eine Vortäuschung der Mailadresse handelt, so kann man leider nichts tun.

Auch ist es als Spam-Empfänger nur bedingt sinnvoll die E-Mail-Adresse zu wechseln, denn es dauert meist nicht lange, bis auch diese neue Adresse Spam bekommt. Der Aufwand die neue Adresse allen Kontakten mitzuteilen und ggf. auch bei allen Systemen, bei denen man sich mit dieser Adresse registriert hat, abzuändern ist dafür aber eventuell enorm.