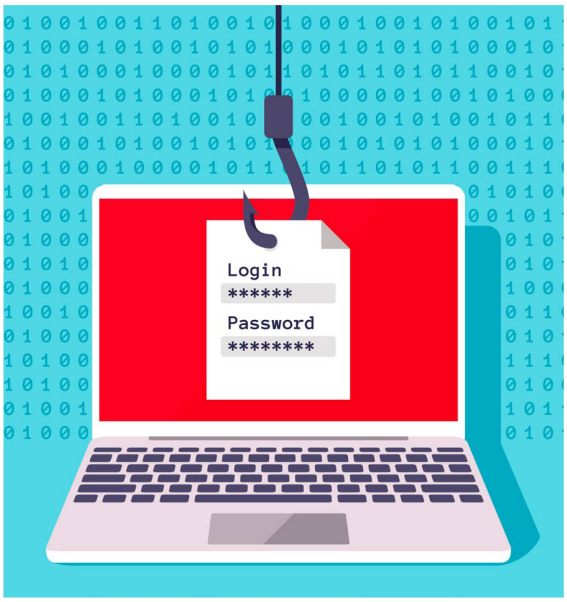
Zeitschrift: Zeitlupe : für Menschen mit Lebenserfahrung
Herausgeber: Pro Senectute Schweiz
Band: 96 (2018)
Heft: 10

Artikel: Digital : was ist eigentlich Phishing?
Autor: Bodmer, Marc
DOI: https://doi.org/10.5169/seals-1087778



Was ist eigentlich Phishing?

Über E-Mail versuchen Hacker und Online-Betrüger das Vertrauen der Nutzerinnen und Nutzer zu gewinnen. Aber auch im Web lauern Gefahren, die zur Vorsicht mahnen.

Kürzlich erreichte mich folgende E-Mail: «Hello ! Ich bin sicher, dass diese E-Mail als Überraschung zu Ihnen kommen würde, weil wir nicht wissen, einander persönlich, und Sie können auch fragen, warum ich sollte Ihnen in Verbindung setzen.»
In der Tat kenne ich keine Caroline Freund, wie sich die Dame später nennt, und noch viel weniger habe ich von einem Paul-Louis Haley gehört, der blosse acht Millionen Dollar vor 15 Jahren hinterlassen haben soll. Was mich das angeht? Die freundliche Frau Freund möchte mit mir das Geld teilen und 40 Prozent davon überweisen. Dazu bräuchte ich lediglich den Link im E-Mail anzuklicken.

Zum Glück sind die automatischen Übersetzungsprogramme von Google und Co. noch nicht so weit fortgeschritten und machen es einem dank dem Kauderwelsch einfach, die dubiose Botschaft als Betrugsversuch zu entlarven. Doch manche dieser sogenannten Phishing-Versuche sind weit raffinierter. Sie zielen nicht nur auf die Gier ab, sondern ähnlich den Enkeltrickbetrügereien werden Notlagen vorgetäuscht, und als Absender können auch Namen aus dem Bekanntenkreis erscheinen.

Wenn bekannte Namen auftauchen und man unsicher ist, ob das E-Mail echt ist, einfach schnell den Freund oder die Bekannte anrufen und fragen, ob das E-Mail tatsächlich von ihm oder ihr stammt. Sollte das E-Mail-Konto des Absenders gehackt worden sein, wird man Ihnen für den Hinweis danken. Das hilft auch bei Absendern von Firmen oder öffentlichen Stellen wie der Polizei. Einfach auf den Namen klicken, um die E-Mail-Adresse zu sehen. Oft handelt es sich dann um eine Yahoo-, Gmail- oder andere E-Mail-Server-Adresse, die nichts mit dem vermeintlichen Absender zu tun hat. Grundsätzlich gilt: Misstrauisch sein und keinesfalls den Link im E-Mail anklicken oder den Anhang öffnen, auch wenn er noch so Gutes verspricht!

In den Anhängen können sich nämlich Viren verbergen, die sich meist unerkannt auf dem Computer einnisten. Diese sogenannten Trojaner können zu einem späteren Zeitpunkt aktiv werden oder aber verschiedene andere Funktionen aktivieren. Verbreitet ist die Aufzeichnung von Passworteingaben, die dem Urheber des Virus anschliessend zugesendet werden oder aber das Sperren des Computerzugriffs, wie es im Beispiel von Markus S. (siehe Seite 20) geschehen ist, der auf einer Website einen entsprechenden Trojaner eingefangen haben muss. In Europa haben laut Spezialisten der Firma Datto solche Erpressungen im vergangenen Jahr allein bei kleineren und mittleren Betrieben einen Schaden von 80 Millionen Euro verursacht. Um solchen Problemen vorzubeugen, helfen auch Virenschutzprogramme.

Eine weitere, seit geraumer Zeit beliebte Betrugsmasche macht sich nicht den Computer zunutze, sondern das Telefon. Auf dem Telefonbildschirm mag eine Schweizer Telefonnummer oder gar ein Schweizer Name erscheinen, doch es melden sich Englisch sprechende Damen und Herren. Sie geben sich als Microsoft-Mitarbeitende aus, die festgestellt haben wollen, dass Ihr Computer von Viren infiziert und deshalb sehr langsam sei. Ziel der Betrüger ist es in diesem Fall, Sie zum Gehilfen zu machen: Sie sollen ihnen über Fernzugriff Ihren PC «öffnen». Hier gilt: Weder Microsoft noch eine Bank rufen Sie an und verlangen von Ihnen den Zugriff auf den Computer oder persönliche Kontodaten. In diesem Fall ist die einfachste Lösung, das Telefon sofort aufzuhängen. ✳

● **Marc Bodmer**
ist Jurist und Cyberculturist. Er beschäftigt sich seit über 25 Jahren mit digitalen Medien.