«Der Bund», 2.6.2017

Die pherräterischen Pheler der Phisher

Das fängt ja gut an: «Sie wurden als Gewinner für die Nutzung von Google-Services ausgewählt, …» Aber es geht weniger gut weiter: «… die an diese E-Mail angehängt ist, ist unser offizieller Benachrichtigungsschreiben für Ihre Durchsicht.» Spätestes jetzt merkt, wer halbwegs Deutsch kann, dass mit diesem E-Mail etwas nicht stimmt. Oder auch hier: «Ihre e-Mail wurde ausgewählt und hat 1'650'000 Euros, die bei ONU Office in Ihrem Namen registriert und versichert ist. Um mehr Informationen zu erhalten, wie man Ihr Geld beansprucht, wenden Sie sich bitte an …» oder: «Bitte setztzen sie sich dafuer mit unserer Deutsch Sprachigen Rechtsanwaelt in Verbindung.»

Auch wer keinen grossen Wert auf Grammatik und Rechtschreibung legt, wird zugeben müssen, dass es hier nützlich ist, richtig und falsch unterscheiden zu können. Denn dann blinken bei der Lektüre Warnlichter, und man wird stutzig, bevor man in Versuchung gerät. Nämlich das zu tun, was die Absender möchten: die Verbindung anzuklicken, hinter der angeblich ein Gewinn winkt. Tut man es doch, und hat man Pech, so hat der eigene Computer damit bereits einen Virus eingefangen, der früher oder später Unheil anrichten wird.

Hat man Glück, so kann man immer noch den nächsten Schritt verweigern, etwa die Angabe einer Bankverbindung, womöglich samt Passwort, oder eine Anzahlung für die Formalitäten, die leider vor dem Empfang des Geldsegens nötig sind. Die Aufforderung, Anmeldedaten und Passwörter preiszugeben, heisst mit einer köstlichen englischen Wortschöpfung «phishing» – ein Fischen, mit dem etwas nicht stimmt. Ein anderer derzeit grassierender Trick ist, dass das Anklicken des Links die Verschlüsselung des Computerspeichers auslöst, gefolgt von Lösegeldforderungen.

Nicht immer verraten sich die Täter durch läppisches Deutsch aus dem Übersetzungsautomaten. So bildete die «Sonntags-Zeitung» neulich einen eidgenössisch offiziell aussehenden Brief ab, der bloss einige Kommafehler enthielt, wie man sie leider heutzutage von Amtsstellen erwarten muss. Ein Arzt, der darin ein Schaltfeld anklickte, schleppte damit einen Virus in die Spitalcomputer ein. Stutzig hätte ihn ein unbeholfener Satz machen können, dessen Schluss auf dem Schaltfeld einfach wiederholt wurde: «Sie ihre Gerichtsverhandlung». Verräterisch war auch die Absenderadresse, laut welcher die «Bundespolizei der Schweiz» über einen britischen Dienst korrespondiert, der erst noch «spyglass-trading» heisst, (Spionage-)Fernrohrhandel. Aber wer achtet schon, vielleicht nach einer strengen Nachtschicht, auf solche Details?

So könnte man auch übersehen, dass sich der Absender des eingangs zitierten Mails als «Offizier» von Google Australien ausgibt. Oder dass ein wie echt aufgemachter Brief eines Internet-Zahlungsdiensts nicht an jene Mail-Adresse gerichtet ist, unter welcher der Empfänger sein Konto führt. Und dass der Link (anschauen statt anklicken!) nicht zu diesem Dienst führt, sondern zu einer Kauderwelsch-Adresse. Wer das übersieht, dem würden in diesem Fall auch perfekte Deutschkenntnisse nichts nützen: Der Brief, der vor angeblich drohender Kontosperre warnt, ist fehlerfrei abgefasst.

Muss ich nun befürchten, der Internet-Kriminalität Vorschub zu leisten, weil ich ausgerechnet jenen Kreisen zu makellosem Deutsch rate? Ich kann nur hoffen, dass sie die «Sprachlupe» nicht lesen und auch keine meiner Berufkollegen anstellen, um ihren Aussendungen den letzten Schliff zu verpassen. Das wäre freilich noch keine Garantie, dass die Lockbriefe fehlerfrei daherkommen. Oder eben «daher kommen», wie ein Kollege in der (echten) Einladung schrieb, bei seiner Video-Kolumne mitzumachen. Fein, da braucht man nichts zu schreiben, und er will «jede Woche einen freien Journalist … zu Wort kommen lassen». Das wird den freien Journalisten aber freuen!