

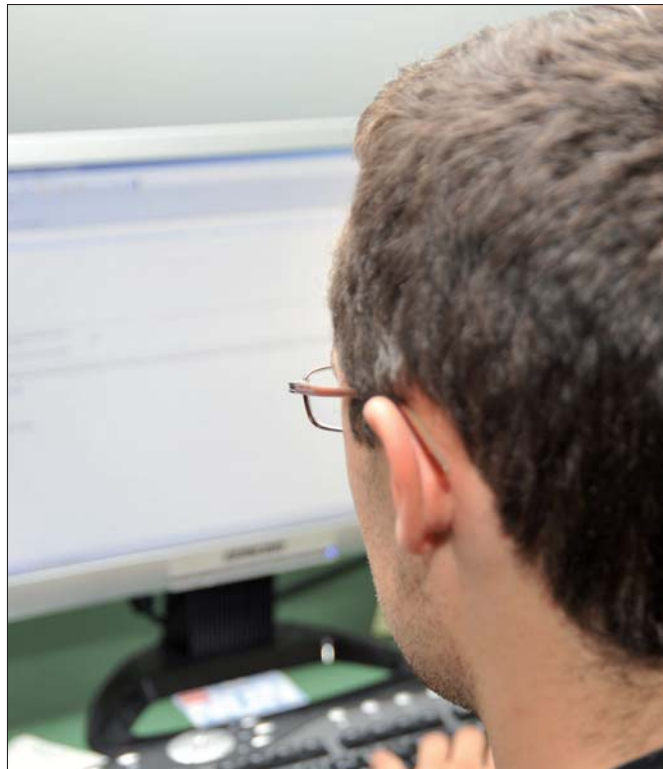
„Ausgeraubt“ in London

Seit einiger Zeit ist eine neue Form betrügerischer E-Mails im Umlauf: Eine befreundete Person meldet sich mit einer Nachricht, weil sie angeblich im Ausland bestohlen worden sei und dringend Geld benötige. Wer finanziell aushilft, fällt einem Internet-Trick zum Opfer.

Mails von Bankern oder Treuhändern in afrikanischen Staaten, die in Sicherheit gebrachtes Vermögen mit einem „Vertrauten“ teilen wollen, sind Internet-Usern seit längerem bekannt. Die Attraktivität des angeblich schnellen Geldes durch die Post von fremden Finanzverwaltern konnte durch Informationen und Warnungen über Internet-Betrügereien großteils genommen werden.

Wie sieht es aber aus, wenn plötzlich eine E-Mail einer bekannten Person einlangt, die in einer angeblichen Notlage um finanzielle Hilfe bittet? Eine Nachricht, die seit einiger Zeit in verschiedenen Varianten im Internet kursiert, trifft die Empfänger auf der emotionalen Seite. Sie kommt von der E-Mail-Adresse eines Freundes oder Familienmitglieds. Die Person berichtet darin verzweifelt, dass sie kurz zuvor im Ausland, meist in London, ausgeraubt worden sei und nun ohne Papiere, Handy, Flugtickets und Kreditkarte die Stadt nicht mehr verlassen könne. Der Zugang zum Internet sei auch nur eingeschränkt möglich. *„Es tut mir leid, dass ich euch auf diese Weise kontaktieren muss; ich brauche dringend Geld, um das Hotel und den Rückflug bezahlen zu können. Meine Bank würde zu viel Zeit benötigen, mir eine neue Kreditkarte zukommen zu lassen“*, steht in den E-Mails. Zum Teil soll die Botschaft oder die Polizei dazu geraten haben, via Internet im privaten Umfeld um Hilfe zu bitten, „um die Dinge zu beschleunigen“.

Eine E-Mail-Adresse und Telefonnummer des Hotels oder der Herberge des Betroffenen sind in den elektronischen Bitt-Briefen angegeben. Das Geld möge so schnell wie möglich an den Kontakt in der angegebenen Unterkunft geschickt werden – ansonsten dürfe der oder die Bekannte nicht ab-



Achtung vor E-Mails angeblicher Bekannter, in denen um Überweisung eines Geldbetrags ersucht wird.

reisen. Der Effekt erinnert an den „Neffentrick“, bei dem älteren Menschen zum Beispiel von einem Unbekannten per Telefon vorgegaukelt wird, ein Verwandter zu sein, der dringend um Geldmittel ersucht. Der Internet-Betrug geht jedoch einen Schritt weiter, da der Absender hier von Anfang an vertraut wirkt.

„Mein Account wurde gehackt und alle Personen in meinem Adressbuch wurden angeschrieben“, berichtet John Griesbacker, der Opfer einer solchen Attacke wurde. Da die Nachricht von seiner echten E-Mail-Adresse geschickt und mit seinem Namen unterschrieben war, waren viele Freunde und Verwandte höchst irritiert – vor allem, da er sich kurz darauf tatsächlich in London befand.

Zum Teil werden Adressdaten über Anwendungen in sozialen Netzwerken ausgespäht; *Malware* – etwa Trojanerprogramme – hilft dabei, die Zugangs-codes des E-Mail-Kontos zu knacken. Eine E-Mail sieht immer gleich aus,

egal wer sie abgeschickt hat. In verschiedenen Fällen antworten die Internet-Betrüger sogar auf verunsicherte Schreiben aus dem Freundes- oder Bekanntenkreis, denn sie besitzen ja das Passwort. Mit Informationen, die sie aus der Inbox des gehackten Accounts geholt haben, machen sie die Illusion perfekt. Unter der angegebenen Telefonnummer ist ein angeblicher Hotelangestellter erreichbar, der die Sachlage bestätigt.

Für John Griesbacker endete die Episode glimpflich: Er wurde von einem miss-trauischen Verwandten am Handy angerufen, der die Geschichte nicht geglaubt hatte, und konnte schnell von einer zweiten Mail-Adresse aus sein Umfeld warnen, kein Geld nach London zu verschicken. Noch sind die meisten betrügerischen Mails dieser Art auf Englisch oder

Französisch gehalten; eine deutsche Abwandlung wird nicht lange auf sich warten lassen.

Verhaltenstipps. Zum Schutz des eigenen Computers vor Passwort-Attacken sollten aktuelle Sicherheitslösungen installiert sein, die auch Spam-Mails erkennen. Beim Surfen im Internet und bei der Online-Übermittlung von persönlichen Daten ist stets größte Vorsicht geboten. Wenn ein „Hilferuf“ einer vertraut wirkenden Person per E-Mail einlangt, können gezielte Rückfragen zu Themen, die üblicherweise nicht öffentlich bekannt sein werden oder in E-Mails stehen, dabei helfen, einen betrügerischen Absender schneller zu erkennen. In Zeiten der verstärkten mobilen Kommunikation lassen sich Angaben aus einer E-Mail oft auch durch einen persönlichen Anruf beim Absender oder die Rückfrage bei einem gemeinsamen Freund oder Familienmitglied überprüfen.

Gregor Wenda