

Datenfischer im weltweiten Netz: Da sollten die Alarmglocken schrillen

Sie haben gewonnen! Sie haben geerbt! Sie wurden ausgewählt! Finger weg, sollten ähnliche Mails in Ihrem Postfach landen – sie dienen lediglich dazu, Sie auszuspionieren und an sensible Daten zu gelangen.

Drohungen und Versprechen

Wurde auch Ihnen schon einmal ein unerwartetes Millionenerbe angekündigt, das Sie nur noch anfordern müssen? Oder kam eine Nachricht, dass Ihr Mailaccount umgestellt wird und Sie Ihre Zugangsdaten neu eingeben müssen – oft verbunden mit der Drohung, dass Sie ansonsten keine Mails mehr empfangen können? Im Netz kursieren **viele Falschmeldungen**, die nur eines zum Ziel haben: Dass Sie in die Falle tappen ... Da wird die Notlage eines Freundes geschildert, mit der Aufforderung, eben mal einen höheren Betrag sofort zu überweisen ... Da taucht ein bis dato unbekannter Verwandter auf und bittet um Geld ... Unter falschen oder gehackten Adressen wird nach Konto- oder Geburtsdaten gefragt, doch im Gegensatz zu bloß lästigen und kommerziell ausgerichteten Werbemails/Spams haben Phishingmails **kriminelle Hintergründe**, und das macht sie gefährlich.

Was sind Alarmsignale?

Viele Fake-Mails lassen sich rasch „enttarnen“. Kontrollieren Sie zunächst die **Absenderadresse**: Kommt sie Ihnen „spanisch“ vor oder endet sie mit einem Länderkürzel, das Ihnen nicht geläufig ist, ist das ein erstes Warnzeichen. Der nächste Kontrollblick gilt dem **Betreff**: Häufig findet sich dort das Kürzel „Re“ oder „AW“, um zu suggerieren, dass Sie bereits in Kontakt stehen, auch wenn das ganz und gar nicht der Fall ist. Checken Sie dann den Inhalt des E-Mails: Ist die enthaltene **Botschaft plausibel**? Weist der Text **Fehler in Rechtschreibung und Grammatik** auf, sind Umlaute oder Anreden falsch geschrieben? Besondere Vorsicht ist geboten, wenn man Sie auffordert, einen **Link zu öffnen** oder ein beigefügtes Formular auszufüllen: Anhänge mit .exe-Endungen enthalten mit großer Wahrscheinlichkeit Schadsoftware, die Ihre Daten sammelt oder gar den Rechner lahmlegt – mit der nachfolgenden „höflichen“ Bitte, einen Obolus zu entrichten, damit Ihr System wieder läuft. Werden **sensible Daten per Mail abgefragt**, sollten Ihre Alarmglocken ebenfalls laut schrillen, auch wenn die Nachricht scheinbar von Banken, Behörden, Unternehmen oder Institutionen stammt – seriöse Absender würden das wohl nicht tun. Statt in die Falle zu tappen, löschen Sie verdächtige Mails am besten sofort.

Treffen Sie Gegenmaßnahmen

Geben Sie Ihre Mailadresse nur an Menschen weiter, denen Sie vertrauen. Das erspart Ihnen bereits einiges an Spam- und Phishingmails; wirklich geschützt sind Sie davor trotzdem nicht, denn E-Mail-Adressen werden mittlerweile fleißig gehandelt, zudem gibt es längst Programme, die das Web gezielt durchsuchen.

Sind Sie Vielbesteller oder häufiger Teilnehmer an Gewinnspielen, nutzen Sie eine **eigens dafür erstellte Mailadresse**, die Sie vor überquellenden Spams in Ihrem Hauptpostfach bewahrt. Apropos Spam: Nicht beantworten, sondern kennzeichnen, um Ihren Spam-Filter zu trainieren. Der wichtigste Tipp fasst abschließend alle Vorsichtsmaßnahmen zusammen: Bleiben Sie wachsam, damit Sie nicht leichtgläubig Opfer einer Phishing-Attacke zu werden!

Weiterführende Links:

→ Hier finden Sie aktuelle Phising-Warnungen: <https://konsument.at/aktuelle-warnungen/65937?page=0#comments-section>

→ Mehr Information und aktuelle Warnungen finden Sie hier: <https://www.watchlist-internet.at/warnungen-tipps/phishing-smishing-vishing/>