Helaba

PHISHING

5. APRIL 2018

So schützen Sie sich vor Betrugsversuchen

Betrüger versuchen immer wieder, durch E-Mails mit gefälschten Adressen persönliche Daten zu stehlen. Auf Kontodaten haben es die Internetkriminellen bei diesem „Phishing“ besonders abgesehen – seien es Kontonummern, persönliche Informationen, Passwörter, PIN oder TAN. Die E-Mails führen dann auf Internetseiten, die oft täuschend „echt“ aussehen.
Bitte melden Sie solche verdächtigen E-Mails an: warnung@helaba.de

Wie erkennen Sie als Kontoinhaber verdächtige E-Mails?

- Betrachten Sie E-Mails von unbekannten Absendern kritisch oder ignorieren Sie diese.
- Schauen Sie sich den Absender genau an: auch wenn der Name auf den ersten Blick bekannt klingt. Lassen Sie sich die komplette E-Mail-Adresse anzeigen und achten Sie auf Unstimmigkeiten.
- Lesen Sie sich die Betreffzeile und den Text kritisch durch. Viele Schreibfehler, falsche Grammatik, seltsame Formulierungen können ein Warnzeichen sein.
- Seien Sie vorsichtig, wenn eine E-Mail ungewöhnliche Aufforderungen oder Hinweise enthält. Etwa wenn Ihr Zugang zum Online-Banking „geschlossen“ wird oder Sie diesen „überprüfen/authentifizieren“ sollen. Oder wenn angeblich eine „Kontenauthentifizierung erforderlich“ ist.

Folgen Sie den Anweisungen in verdächtigen E-Mails nicht. Geben Sie vor allem nie PIN und TAN heraus. Ihre Zugangsdaten zum Online-Banking preisgeben, in einer E-Mail einen Link anklicken und dann Kontodaten eingeben: Die Helaba oder Ihre Sparkasse werden Sie dazu nie auffordern. Weder per E-Mail noch persönlich in einem Telefongespräch.

Wie erkennen Sie echte Internetseiten der Helaba?

- Achten Sie auf das Adressfeld: Dort steht https:// statt http://. Denn die Internetseiten für Online-Banking sind immer verschlüsselt.
- Schauen Sie, ob Ihr Browser das Schloss-Symbol anzeigt.

Was können Sie gegen Phishing tun?

- Tippen Sie die Adresse für das Online-Banking stets selbst ein.
- Nutzen Sie ein aktuelles Virenschutz-Programm und wenn möglich eine Firewall.
- Vermeiden Sie es, Bankgeschäfte an öffentlichen Computern zu tätigen.
- Wählen Sie komplizierte Passwörter und speichern Sie diese nicht auf Ihrem Computer ab.
- Seien Sie vorsichtig mit der Preisgabe persönlicher Daten, etwa in sozialen Netzwerken. Die Betrüger spähen solche Daten aus und versuchen sich so Ihr Vertrauen zu erschleichen.
- Richten Sie Benutzerkonten ein: Auch wenn nur Sie den Computer nutzen. Arbeiten Sie möglichst nicht permanent als „Administrator“.

Leiten Sie verdächtige E-Mails zum Online-Banking bitte an warnung@helaba.de weiter. Sie helfen damit, die von den Betrügern genutzten Server zu ermitteln und weiteren Schaden abzuwenden.
Bitte wundern Sie sich nicht, wenn Sie keine persönliche Antwort auf eine solche weitergeleitete Mail erhalten.
Für Ihre Unterstützung danken wir Ihnen schon heute!

Hotline Phishing:
Tel. +49 (0)69 9132-6600