Onlinebanking in Zeiten von Corona: Vorsicht, Phishing!

von Kathleen Altmann

Die aktuelle Nachrichtenflut rund um die Corona-Krise nutzen Kriminelle derzeit gezielt, um mit Bankkunden meist per E-Mail oder SMS, Kontakt aufzunehmen.

Wie funktioniert die Masche?

In solchen Nachrichten werden die Onlinebanking-Kunden etwa aufgefordert, ihre Kontaktdaten zu aktualisieren, um weiterhin die Kommunikation mit der Bank aufrechtzuerhalten. Die Betrüger versuchen damit, den Kunden über einen per E-Mail oder SMS zugesandten Link auf eine gefälschte Webseite zu locken, die dem Onlinebanking-Auftritt seiner echten, eigenen Bank sehr ähnlich sein kann. Loggt sich der Bankkunde nun auf der vermeintlichen Onlinebanking-Webseite mit seinen Zugangsdaten ein, werden diese von den Betrügern abgefischt.

Wie kann ich Phishing-Versuche erkennen?

Manchmal können Phishing-Mails oder -SMS schon auf den ersten Blick an einer fehlerhaften Rechtschreibung erkannt werden. Da viele dieser Nachrichten jedoch mittlerweile einen hohen Grad an Perfektion aufweisen, ist ein solcher Angriff oft nicht ganz so leicht erkennbar. Besondere Vorsicht ist immer geboten, wenn Sie zu einer der folgenden Handlungen aufgefordert werden; denn es könnte ein Phishing-Angriff dahinterstecken:

- Abfrage mehrerer TAN (Transaktionsnummern),
- TAN-Eingabe bei Androhung einer vermeintlichen Kontosperrung oder Laufzeitbeschränkung des TAN-Verfahrens,
- Bestätigung Ihrer Kontodaten per TAN,
- Rücküberweisung einer vermeintlich auf Ihrem Konto eingegangenen Zahlung,
- Anmeldung zu einem Demo-Konto,
- Durchführung einer Testüberweisung,
- Installation von Sicherheitszertifikaten oder Sicherheitssoftware/Apps.

Grundsätzlich gilt für die Sicherheit beim Onlinebanking: Beim Einloggen sollten Sie stets darauf achten, dass Sie tatsächlich die echte, verschlüsselte Seite Ihrer Bank aufrufen. Zu erkennen ist dies unter anderem an dem im Internet-Browser angezeigten Schloss- oder Schlüsselsymbol und daran, dass die Webadresse mit „https" beginnt. Kennwörter, persönliche Geheimzahlen (PINs) und TAN gehören niemals unverschlüsselt in Apps, in eine Cloud oder sollten auf der Festplatte gespeichert werden. Auch sollten die Zugangsdaten regelmäßig geändert werden.

Generelle Vorsicht, wenn sensible Daten abgefragt werden

Grundsätzlich sollte man auf E-Mails oder SMS, die zu einer Bestätigung von sensiblen Daten auffordern, etwa über die Abfrage von PINs oder TANs, gar nicht antworten. Auf Links zu klicken, die zu einer weiteren Eingabeseite führen, sollte man ebenfalls unbedingt unterlassen. Banken fragen solche Daten niemals ab, weder per E-Mail oder SMS, aber auch nicht telefonisch. Wenn ein vermeintlicher Bankmitarbeiter anruft und Sie dazu drängt, gemeinsam eine Transaktion vom Konto durchzuführen, sollte Sie das Gespräch umgehend beenden.

Im Verdachtsfall die eigene Bank informieren

Was tun, wenn Sie den Verdacht haben, doch eine gefälschte Onlinebanking-Seite oder Banking-App genutzt zu haben? Dann sollten Sie umgehend Ihre Bank darüber informieren! Sie wird mit Ihnen die weitere Vorgehensweise besprechen. Auf keinen Fall sollten weitere Bankgeschäfte erledigt werden. Vorsorglich können Sie auch Ihren Online-/Mobile-Banking-Zugang zum Konto sperren lassen.

Auch wenn Sie nicht selbst Opfer eines betrügerischen Phishing-Versuchs geworden sind, sollten Sie verdächtige E-Mails oder SMS Ihrer Bank melden, damit diese dagegen vorgehen und andere Bankkunden vor solchen kriminellen Angriffen schützen kann.