bankenverband

Presseinformation

16. September 2014

So betreiben Sie sicheres Online-Banking

Kontakt

Tanja Beller
Bundesverband deutscher Banken e.V.
Director, Pressesprecherin
Tel. +49 30 1663-1220
tanja.beller@bdb.de

Schlagworte

Verbraucher
PIN
TAN
Sicherheit
Onlinebanking

Online-Banking ist sehr sicher! Das glauben 53 Prozent der Deutschen. Unter denen, die Online-Banking nutzen, ist die Zahl sogar noch höher: 84 Prozent. Dennoch haben viele Menschen Angst vor „Phishing“, so nennt man es, wenn persönliche Daten abgefischt werden. Wer sich aber an bestimmte Regeln und Tipps hält, kann sowohl Mobile-Banking als auch Online-Banking sicher betreiben.

- Meist ist der PC zu Hause das Einfallstor für Kriminelle. Als Online-Banking-Kunde müssen Sie gewisse Sorgfaltspflichten einhalten: Installieren Sie einen Virenscanner und eine Firewall. Auch die Software sollte immer auf dem neuesten Stand sein. Sobald Sie ein Update angeboten bekommen, nutzen Sie es und zögern die Installation nicht hinaus. Sie sollten auch niemals Online-Banking auf fremden Rechnern (z.B. in einem Internet-Café) tätigen.

- Gleiches gilt für Ihr Smartphone. Es ist wie ein kleiner Computer. Sie müssen die Software auf dem aktuellsten Stand halten. Beim mobileTAN-Verfahren sollten Sie Ihr Smartphone nicht gleichzeitig zum Online-Banking und Empfang der SMS nutzen.

- Speichern Sie niemals Kennwörter, Ihre Geheimzahl (PIN) und TANs in Apps, in der Cloud oder auf Ihrer Festplatte. Auch nicht als Telefonnummern verschlüsselt im Handy.

- Bei Cyberattacken versuchen Betrüger Sie auf kopierte Online-Banking-Websites der Banken zu locken, um Daten abzufischen. Bevor Sie sich einloggen, überprüfen Sie, ob es sich wirklich um die verschlüsselte Seite Ihrer Bank handelt. Das erkennen Sie u. a. daran, dass im Browser ein Schloss-Symbol erscheint und die Webadresse mit https… beginnt.

- Antworten Sie niemals auf vermeintliche E-Mails Ihrer Bank, die Sie beispielsweise zu einer Bestätigung Ihrer Daten

auffordern. Klicken Sie keine Links an, um solche Daten einzugeben. Ihre Bank wird dies nicht abfragen.

- Beziehen Sie nur Apps aus autorisierten Quellen. Seien Sie bei Gratis-Versionen von ansonsten käuflich zu erwerbenden Apps skeptisch, denn es könnte sich um Schadsoftware handeln.

Auf keinen Fall sollten Sie folgenden Aufforderungen während der Banking-Sitzung nachkommen:

- einer Abfrage mehrerer TAN,
- einer TAN-Eingabe zur Aufhebung einer angeblichen Kontosperrung oder Laufzeitbeschränkung Ihrer iTAN-Liste,
- einer TAN-Eingabe zur Bestätigung der Kontodaten,
- einer Rücküberweisung einer (vermeintlich) eingegangenen Zahlung,
- einer Durchführung einer Testüberweisung,
- einer Installation von Sicherheitszertifikaten oder Sicherheitssoftware/App.

Wenn Sie diese Tipps beherzigen, können Sie Online-Banking sicher und bequem betreiben. Sollten Sie tatsächlich Opfer von Phishing-Betrügern werden, wenden Sie sich umgehend an Ihre Bank. Der Bankenverband hat zum Thema sicheres Online-Banking eine neue Broschüre herausgegeben, die Sie kostenlos herunterladen können.