bankenverband

fokus | verbraucher

Wie schütze ich mich vor Phishing?

Viele Menschen haben Angst, dass ihre Daten beim Online-Banking abgefangen werden. Dieses Ausspionieren wird in Fachkreisen Phishing genannt. Damit Bankkunden ihre Transaktionen sicher und ohne Sorge durchführen können, ist es wichtig, dass sie ein paar einfache Tipps und Regeln befolgen. In diesem Flyer hat der Bankenverband die wichtigsten Sicherheitsmaßnahmen zusammengestellt.

So erreichen Sie den Bankenverband

Per Post:
Bundesverband deutscher Banken
Postfach 040307
10062 Berlin

Per Telefon:
+49 30 1663-0

Per Fax:
+49 30 1663-1399

Per E-Mail:
bankenverband@bdb.de

Im Internet:
bankenverband.de
verbraucher.bankenverband.de

Scannen Sie diesen QR-Code für mehr Informationen zum Thema Online-Banking.

Social Media:

twitter.com/bankenverband
www.youtube.com/user/bankenverb
www.flickr.com/photos/bankenverband

Impressum | Herausgeber: Bundesverband deutscher Banken e. V., Postfach 040307, 10062 Berlin | Verantwortlich: Iris Bethge
Druck: druckpunkt GmbH, Berlin | Gestaltung: doppel:punkt redaktionsbüro janet eicher, Bonn | Fotos: actionpress, Jochen Zick, fotolia

Eine Information der privaten Banken
Berlin, August 2014

1 Der PC zu Hause kann ein Einfallstor für Kriminelle sein. Wenn er nicht abgesichert ist, steht die „Haustür“ für Betrüger offen. 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 Sie die Installation nicht hinaus. Es dient Ihrer eigenen Sicherheit. Deshalb sollten Sie auch niemals Online-Banking auf fremden Rechnern (zum Beispiel in einem Internetcafé) tätigen.

2 Das Gleiche gilt für Ihr Smartphone. Wenn Sie mit ihm Online-Banking betreiben, müssen Sie die Software auf dem aktuellen Stand halten. Denn Ihr Smartphone ist wie ein kleiner Computer. Beim mobileTAN-Verfahren sollten Sie Ihr Smartphone nicht gleichzeitig zum Online-Banking und Empfang der SMS nutzen.

3 Speichern Sie niemals Kennwörter, Geheimzahlen (PINs) und TANs in Apps, in der Cloud oder auf Ihrer Festplatte. Auch nicht als Telefonnummern verschlüsselt im Handy.

4 Bei Phishing-Angriffen versuchen Betrüger, Sie auf kopierte Online-Banking-Websites der Banken zu locken, um Ihre Daten abzufangen. Bevor Sie sich einloggen, überprüfen Sie, ob es sich wirklich um die verschlüsselte Seite Ihrer Bank handelt. Das erkennen Sie unter anderem daran, dass im Browser ein Schloss-Symbol erscheint und die Webadresse mit https... beginnt.

5 Antworten Sie niemals auf vermeintliche E-Mails Ihrer Bank, die Sie beispielsweise zu einer Bestätigung Ihrer sensiblen Daten auffordern. Klicken Sie auch niemals Links an, um solche Daten einzugeben. Ihre Bank wird niemals solche Daten abfragen.

6 Wenn Sie ein vermeintlicher Berater Ihrer Bank anruft und gemeinsam mit Ihnen eine Transaktion durchführen will, nutzen Sie Ihren gesunden Menschenverstand und beenden Sie das Gespräch. Ihre Bank wird Sie niemals zu so einer Aktion drängen.

7 Nutzen Sie eine geeignete App für den Zugang zu Ihrer Bank aus dem autorisierten App-Store Ihres Smartphones oder Tablets. Hierfür sollten Sie keinen „Hinweisen“ aus E-Mails oder von Webseiten nachgehen. Seien Sie bei Gratis-Versionen von ansonsten käuflich zu erwerbenden Apps skeptisch, denn es könnte sich um Schadsoftware handeln.

Wenn Sie diese Tipps beherzigen, können Sie Online-Banking sicher und bequem betreiben.

Sollten Sie tatsächlich Opfer eines Phishing-Falls werden, wenden Sie sich umgehend an Ihre Bank.