

4. Juli 2014

Wie schütze ich mich vor Phishing?

Viele Menschen haben Angst, dass ihre Daten beim Online-Banking abgefischt werden (Phishing). Damit Bankkunden ihre Transaktionen sicher und ohne Sorge durchführen können, ist es wichtig, dass sie ein paar einfache Tipps und Regeln befolgen:



- 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 Virenschoner 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. Es dient Ihrer eigenen Sicherheit. Deshalb sollten Sie auch niemals Online-Banking auf fremden Rechnern (z.B. in einem Internet-Café) tätigen.
- Das Gleiche gilt für Ihr Smartphone. Wenn Sie mit ihm Online-Banking betreiben, müssen Sie die Software auf dem aktuellsten Stand halten. Denn Ihr Smartphone ist wie ein

Kontakt

Julia Topar
Bundesverband
deutscher Banken
e.V.
Themengruppenlei-
terin, Director
Tel. +49 30 1663
1290
julia.topar@bdb.de

Schlagworte

Verbraucher
Onlinebanking
Phishing

Presseinformation

kleiner Computer. Beim mobileTAN-Verfahren sollten Sie Ihr Smartphone nicht gleichzeitig zum Online-Banking und Empfang der SMS nutzen.

- Speichern Sie niemals Kennwörter, Geheimzahlen (PIN) und TANs in Apps, in der Cloud oder auf Ihrer Festplatte. Auch nicht als Telefonnummern verschlüsselt im Handy.
- Bei Phishing-Angriffen versuchen Betrüger Sie auf kopierte Online-Banking-Websites der Banken zu locken, um Ihre 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 sensiblen Daten auffordern. Klicken Sie auch niemals Links an, um solche Daten einzugeben. Ihre Bank wird niemals solche Daten abfragen.
- 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.
- Nutzen Sie nur die von Ihrer Bank empfohlenen Apps. 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. Haftungsfragen werden im Einzelfall entschieden.