

Sicherheit

.....

Dieser Inhalt wird uns vom Bundesverband deutscher Banken e.V. zur Verfügung gestellt.
(www.bankenverband.de)

Online-Banking: Sicherheit fängt zu Hause an

Online-Banking wird für immer mehr Deutsche zu einer Selbstverständlichkeit. Dafür gibt es gute Gründe: So sind im Allgemeinen Finanztransaktionen, die online abgewickelt werden, preiswerter als Geschäfte am Bankschalter. Vor allem aber überzeugt die Kunden, dass sie Bankgeschäfte bequem und sicher von zu Hause aus abwickeln können - und das rund um die Uhr. Die Banken führen dazu umfangreiche Sicherungsmaßnahmen durch und schützen so von ihrer Seite zum Beispiel die Übertragung vertraulicher Daten via Internet.

Der Bankenverband hat verschiedene Publikationen zum Thema Sicherheit im Online-Banking zusammengestellt, die hier kostenlos bestellt oder heruntergeladen werden können.

Tätigkeit als Finanzagent? Finger weg von dubiosen Angeboten!

Geld verdienen ohne Mühen - wer möchte das nicht? In letzter Zeit sprechen Kriminelle gezielt per E-Mail oder direkt auf Internetseiten Bankkunden an, um sie für eine Tätigkeit als sogenannte Finanzagenten zu gewinnen: Der Bankkunde soll Zahlungen auf sein Konto entgegennehmen und das Geld dann per Bargeldversand an eine Person ins Ausland überweisen. Dafür winkt eine Provision, die vom Überweisungsbetrag abgezogen wird. Doch Vorsicht: Die auf das Konto des „Finanzagenten“ eingehenden Gelder stammen meistens von Opfern betrügerischer Handlungen.

Um vor derartigen kriminellen Tricks zu warnen, hat der Bankenverband Informationen und Tipps in einem Faltblatt „Tätigkeit als Finanzagent? Finger weg von dubiosen Angeboten!“ zusammengestellt.

Vorsicht: Phishing

Zur Sicherheit sollte jedoch auch jeder Online-Banker beitragen, indem er einige grundsätzliche Tipps sorgfältig beachtet. Denn auf die Sicherheit der Computer und Programme jedes Internetnutzers haben die Banken keinen Einfluss.

So häufen sich gerade in letzter Zeit erneut Berichte über das so genannte „Phishing“. Dabei wird der Kunde von Internetkriminellen beispielsweise per E-Mail aufgefordert, mit seinem Kreditinstitut Kontakt aufzunehmen. Folgt der Adressat dem in der E-Mail angegebenen Link, so landet er jedoch nicht bei seiner Bank, sondern auf einer gefälschten Website. So hoffen die Kriminellen, an vertrauliche Zugangsdaten - etwa PIN und TANs - zum Online-Konto zu kommen.

Wichtige Hinweise zu gefährlichen E-Mails, Phishing und Spyware erhalten sie in der Broschüre „Sicherheit im Internet“.

Websites genau prüfen

Grundsätzlich gilt: Der Kunde sollte sich immer vergewissern, mit wem er es zu tun hat. Vertrauliche Informationen sollte nur preisgeben, wer verlässlich weiß, dass es sich bei der Internetseite tatsächlich um die seines Kreditinstitutes handelt. Zum Beispiel sollten Abweichungen vom gewohnten Ablauf beim Online-Banking immer misstrauisch machen.

PIN und TANs sollten die Online-Banker insbesondere nur eingeben, wenn sie sich auf der geschützten Seite ihrer Bank befinden. Das erkennen sie unter anderem daran, dass die Internetadresse ihrer Bank mit „https://“ beginnt. Auch sollte jedes Mal in der Adresszeile des Internetbrowsers kontrolliert werden, ob die Internetadresse der Bank korrekt wiedergegeben ist. Bereits minimale Abweichungen können auf eine gefälschte Website hinweisen.

Zu den selbstverständlichen Vorsichtsmaßnahmen für jeden Online-Banker sollten auch gehören, dass sie regelmäßig ihre Virenschutzprogramme und ihre persönliche Firewall aktualisieren sowie immer die Sicherheitseinstellungen ihres Internetbrowsers aktiviert haben.

Der Bankenverband hat zehn Regeln für Sicherheit im Online-Banking in der Broschüre „Online-Banking-Sicherheit“ zusammengestellt. Sie enthält zudem ein Glossar mit einigen der wichtigsten Begriffe beim Online-Banking, wie Cookie, PIN, Trojaner, Viren.

Sicherheitstipps für die Nutzung Ihrer Bankkarte mit PIN enthält die gleichnamige Broschüre „Sicherheitstipps“.

Hier können Sie die Broschüren des Bankenverbandes bestellen oder herunterladen.