

Sicherheitstipps fürs Onlinebanking



Ihre Bank führt umfangreiche Maßnahmen zur Absicherung ihrer Online-Angebote durch. Diese gewährleisten unter anderem, dass Ihre vertraulichen Daten bei der Übertragung über das Internet nicht eingesehen und verändert werden können. Genauso wird die Verarbeitung auf dem Bankenserver geschützt.

Typische Gefahren im Internet sind das Mitlesen, Verändern und Löschen von Daten sowie das Erschleichen von Daten durch Vorgabe falscher Tatsachen.

Auf die Sicherheit Ihrer selbst ausgewählten Hard- und Software hat Ihre Bank keinen Einfluss. Damit die von Ihrer Bank vorgesehenen Sicherheitsvorkehrungen nicht durch Manipulation aus dem Internet umgangen werden können, müssen auch Sie Vorkehrungen zum Schutz treffen:

Eigenes Gerät

Für Bankgeschäfte benutzen Sie am besten Ihr eigenes Gerät. Ein fremdes Gerät oder ein PC in einem Internetcafé sollten Sie meiden. Hier besteht die Gefahr, dass Schadsoftware alle Ihre Tastatur- und Mauseingaben sowie



26.10.2018

von Kathleen Altmann

Kurzgefasst

Ihre Bank führt umfangreiche Maßnahmen zur Absicherung ihrer Online-Angebote durch. Diese gewährleisten unter anderem, dass Ihre vertraulichen Daten bei der Übertragung über das Internet nicht eingesehen und verändert werden können. Genauso wird die Verarbeitung auf dem Bankenserver geschützt.

Schlagworte

Verbraucher
PIN
Onlinebanking
TAN
Cyberkriminalität
Verbraucherschutz
Dossier Sicherheitstipps
Onlinebanking

Blog

Bildschirmhalte unbemerkt mitschneidet, manipuliert und an Dritte weiterleitet.

Sicherheitssoftware

Halten Sie das Betriebssystem und Virenschutzprogramme permanent aktuell.

Firewall

Auch eine persönliche Firewall gehört zum Sicherheitspaket dazu. Zum Schutz vor schädlicher Software sollten zudem alle Laufwerke des Computers regelmäßig überprüft werden.

Wachsam bleiben

Anhänge von E-Mails unbekannter Herkunft nicht öffnen. Treten bei der regelmäßigen Prüfung von Konto- bzw. Depotumsätzen Unstimmigkeiten auf, sollten Sie umgehend die Bank informieren. Vermuten Sie, dass ein Unbefugter die geheimen Zugangsdaten (z. B. PIN oder TANs) kennt, sollten Sie den Online-Zugang zum Konto sofort sperren lassen.

Daten schützen

Sensible Daten wie Passwörter, PIN und TANs dürfen niemals auf der Festplatte gespeichert oder am Telefon weitergegeben werden.

Verschlüsselte Verbindung

Zudem sollten Sie immer darauf achten, dass die Zugangsdaten nur eingegeben werden, wenn Sie sich auf der geschützten Seite der Bank befinden und eine verschlüsselte Verbindung besteht. Das lässt sich unter anderem

Blog

daran erkennen, dass die Internetadresse der Bank mit https:// beginnt.

Sicheres Passwort

Um Onlinebanking zu starten, müssen Sie sich mit einem Passwort ausweisen. Diese persönliche Identifikation autorisiert den berechtigten Nutzer für Transaktionen. Ein gutes Passwort sollte schwer zu knacken sein. Es sollte zum Beispiel aus einer Mischung von Groß- und Kleinbuchstaben sowie Ziffern und Sonderzeichen bestehen. Und: Das Passwort ist nur sicher, wenn es wirklich geheim gehalten wird.