

## Blog

# Schnell und jederzeit: Bankgeschäfte auf dem Smartphone



In Zeiten von Corona wird das Smartphone immer wichtiger: Wenn Sie mit Ihrem Mobilgerät Internetzugang haben, können Sie Ihre Bankgeschäfte auch von zuhause oder unterwegs schnell erledigen („Mobile Banking“). Einige Tipps, die sich speziell auf Bankgeschäfte mit dem Smartphone oder dem Tablet beziehen, können Ihnen dabei helfen, auch die Sicherheitsaspekte nicht aus den Augen zu verlieren.

Was Sie im Mobile Banking alles erledigen können, ist vom Angebot oder der App Ihrer Bank abhängig. In der Regel kann jeder seine Überweisungen, Umbuchungen oder Wertpapierorders über das Mobile Banking erledigen.

---

### **Besuchen Sie auch unsere Corona-Themenseite**

---

## Nutzen Sie Ihre eigenen Geräte und installieren Sie einen Virenschanner

Für die Sicherheit bei Ihren Bankgeschäften von unterwegs ist es wichtig, dass Sie nur Ihre eigenen Geräte verwenden. Sollten Sie das Gerät nicht kennen – beispielsweise, weil es sich um das Tablet eines Bekannten handelt – und deswegen keine Informationen über seinen „Gesundheitszustand“ haben, handeln Sie sich unnötige Risiken ein. Ist es

21.04.2020

von



Altmann, Kathleen

## Schlagworte

Corona  
Corona-Verbraucher  
PIN  
Onlinebanking  
Sicherheit  
Mobile Banking  
Dossier Mobile Banking  
Verbraucher

## Blog

beispielsweise mit einer Schadsoftware infiziert, könnten Ihre Tastatureingaben oder Bildschirminhalte unbemerkt aufgezeichnet und an Dritte weitergeleitet werden.

Wichtig ist auch, dass Ihr Gerät ausreichend vor Schadsoftware geschützt wird. Abhängig von Ihrem Benutzerverhalten kann es daher ratsam sein, beispielsweise einen Virenschanner zu installieren.



## Laden Sie Apps nur aus autorisierten App-Stores herunter

Für Ihre Bankgeschäfte können Sie die Banking-App Ihrer Bank verwenden. Wichtig ist, dass Sie Apps ausschließlich aus dem offiziellen App-Store herunterladen. Folgen Sie bitte keinen Angeboten zum Download aus fremden Quellen, etwa von Webseiten. Folgen Sie auch keinen Links, die Ihnen per E-Mail oder SMS zugeschickt wurden: Es besteht die Gefahr, sich eine infizierte App herunterzuladen.

## Schützen Sie Ihre Zugangsdaten

Wenn Sie sich im Mobile Banking anmelden, werden Sie nach Zugangsdaten gefragt, um sich zu identifizieren. Diese können beispielsweise eine Persönliche Identifikationsnummer (PIN) oder ein Passwort in Kombination mit Ihrer Teilnehmernummer sein. In zahlreichen Apps kann die Anmeldung auch mithilfe biometrischer Merkmale erfolgen. Für die Anmeldung kann zusätzlich auch eine Transaktionsnummer (TAN) gefordert werden. Hier gibt es je nach Bank Unterschiede: Bei einigen Banken muss die TAN jedes Mal eingegeben werden, andere Banken bitten Sie hingegen nur alle 90 Tage um die Eingabe einer TAN bei der Anmeldung. In jedem Fall gilt: Schützen Sie Ihre Zugangsdaten, die TAN sowie die für den TAN-Empfang erforderlichen Geräte vor unberechtigtem Zugriff.

## **Blog**

### Schließen Sie nicht einfach die App – melden Sie sich ab

Beenden Sie die Mobile-Banking-Sitzung, indem Sie auf den „Logout“ oder „Abmelden“-Button klicken. Schließen Sie also nicht einfach die App.

### Setzen Sie ein Tageslimit für Überweisungen

In den Sicherheitseinstellungen Ihres Onlinebankings lässt sich in der Regel auch ein Tageslimit für Überweisungen festsetzen. Damit können Sie festlegen, wie viel Geld maximal von Ihrem Konto einmalig oder in einem bestimmten Zeitraum überwiesen werden kann.

### Behalten Sie Ihre Kontobewegungen im Blick

Zu guter Letzt: Prüfen Sie regelmäßig Ihre Umsätze sowie Ihren Konto- und Depotstand. Sind alle Überweisungen, auch die vorgemerkten, von Ihnen veranlasst? Kontaktieren Sie anderenfalls umgehend Ihre Bank.

*Was Sie beim Smartphone-Wechsel beachten müssen, finden Sie in diesem **[Blogbeitrag](#)**.*