Bezahlung per Smartphone

Das Smartphone ist unser Begleiter im Alltag. Ob Terminkalender, Unterhaltungsprogramm, Kontaktbörse, es gibt Menschen, die nutzen ihr Mobiltelefon für fast alles. Sogar das Bezahlen mit dem kleinen Alleskönner – auch Mobile Payment genannt - ist in Deutschland immer mehr auf dem Vormarsch. Wie bei der Bezahlung mit der EC-Karte Handy kurz ans Gerät halten, warten und weiter. Super praktisch! Was aber steckt dahinter, dass man nun so einfach ohne Geldbörse bezahlen kann? Und ist das auch sicher?

Wie funktioniert Mobile Payment?

Die Technik, die hinter der digitalisierten Zahlung steckt, nennt sich Near Field Communication (NFC), zu Deutsch: Nahfeldkommunikation. Dabei tauschen sich zwei NFC-Chips kontaktlos aus. Um also mit dem Handy oder der Smartwatch bezahlen zu können, müssen diese so einen NFC-Chip haben. Bei aktuellen Geräten ist dies mittlerweile Standard. In den Einstellungen kann das NFC meist ein- oder ausgeschalten werden. Zusätzlich zur NFC-Funktion braucht es eine passende Bezahl-App (z. B. Google Pay, Apple Pay, PayPal etc.). In dieser App können die EC-Kartendaten oder sogar das Konto verbunden werden. Andernfalls kann auch Guthaben aufgeladen werden, um dieses für die Kaufabwicklung zu nutzen.

Um schließlich zu bezahlen, wird das Handy nah an das Kartenlesegerät gehalten. Die NFC-Chips tauschen sich miteinander aus und der Betrag wird über die App vom Konto oder Guthaben abgebucht. Nicht anders als mit der EC-Karte, die man meist auch nicht mehr stecken, sondern einfach an das Gerät halten muss.

Am sichersten ist natürlich das gute alte Bargeld. Aber wie schnell passiert es, dass man eben keines in der Tasche hat und der nächste Geldautomat nicht um die Ecke ist? Ist Mobile Payment also eine sichere Alternative? An sich, ja. Denn, damit eine Abbuchung klappen kann, muss das Handy sehr nah am Lesegerät sein. Das heißt, man kann nicht so einfach die Daten auslesen. Zudem wird von den

Daten nur eine verschlüsselte Kopie weitergeleitet, die nur für den Bezahlvorgang gilt, der gerade über das Handy freigegeben wird. Das heißt, die Bankdaten werden nicht so einfach offengelegt. Trotzdem sollte man wachsam bleiben und mit seinen persönlichen Daten nicht zu freizügig umgehen. Ein Angriff auf das Konto oder die Daten sind nicht unmöglich. Gerade, wenn die Bezahl-App nicht vom Kreditinstitut, sondern von einem Drittanbieter kommt, muss damit gerechnet werden, dass das Kaufverhalten analysiert und eventuell weitergegeben wird. Apps des eigenen Kreditinstituts sind daher eher von Vorteil, da Banken prinzipiell kein Interesse am Kaufverhalten haben. Dennoch schließt das nicht mit Sicherheit aus, dass Daten weitergegeben werden. Allerdings müssen die Datenschutzhinweise der Anbieter ausführlich erläutern, was mit den persönlichen Daten geschieht.

Was kann man darüber hinaus noch tun, um das mobile Bezahlen für sich sicherer zu gestalten?

- Bezahl-Apps nur von vertrauenswürdigen Quellen installieren – beispielsweise dem bekannten App-Store.
- Aktuellste Version der App verwenden und regelmäßig per Update aktualisieren. Auch das Betriebssystem des Smartphones oder der Smartwatch regelmäßig aktualisieren.
- Mit persönlichen Daten nicht zu freizügig umgehen. Etwa den Standort ausschalten oder die Einstellungen genau prüfen und festlegen.
- Wenn möglich nicht benötigte Zusatzfunktionen blockieren oder ausschalten.
- Eine automatische Sperre einrichten, die bei wiederholter Falscheingabe von TAN oder Passwort greift.
- Kein gerootetes/gejailbreaktes Smartphone benutzen.
- Bildschirmsperre des mobilen Geräts einrichten (PIN, Passwort, Fingerabdruck oder Gesichtserkennung).
- Sperren von SIM-Karte und Banking-Zugängen bei Verlust des Geräts.
- Regelmäßig das Konto überprüfen und der Bank melden, wenn etwas komisch ist.
- Bluetooth und NFC nur einschalten, wenn es gebraucht wird. Das erschwert eine Verbindung von Angreifern zum eigenen Smartphone.

Text: Tanja Bochmann