Bestellt und nichts geliefert >
< Wie Computer lernen, Menschen zu erkennen

Kontaktloses Bezahlen

Wie sicher sind funkfähige Kredit- und Girokarten?

Immer mehr Händler bieten das kontaktlose Bezahlen an

Das Bezahlen an der Kasse soll mit funkfähigen Kredit- und EC-Karten schneller und einfacher werden. Bei kleineren Beträgen bis 25 Euro ist der Vorgang ganz ohne Unterschrift oder PIN-Eingabe möglich. Doch wie sicher ist das kontaktlose Bezahlen? Dr. Julia Gerhards von der Verbraucherzentrale Rheinland-Pfalz klärt über die Vor- und Nachteile der Nutzung von funkfähigen Karten auf.

Ein Chip macht es möglich

Einfach die Karte ans Lesegerät halten, schon ist der Bezahlvorgang abgeschlossen. Die Technik, mit der das kontaktlose Bezahlen möglich ist, nennt sich „Near Field Communication“ (NFC). In vielen Giro- und Kreditkarten sind die Chips schon verbaut. Ob die eigene Karte NFC-fähig ist, erkennt man an einem auf die Karte aufgedruckten Wellensymbol. Es ähnelt dem WLAN-Symbol, das viele Computer und Smartphones anzeigen, wenn sie kabellos mit dem Internet verbunden sind. Um kontaktlos bezahlen zu können, muss das Kartenlesegerät im Geschäft oder im Restaurant allerdings ebenfalls NFC-fähig sein. Ist das der Fall, muss man die Karte nur kurz an das Gerät halten, um den gewünschten Betrag abzubuchen. Bei Beträgen bis 25 Euro ist das Bezahlen ohne PIN und Unterschrift möglich. Visa hat die Grenze bei seinen Kreditkarten auf 50 Euro erhöht.

Was praktisch klingt, birgt auch Gefahren

Eine Gefahr beim kontaktlosen Bezahlen ist die Möglichkeit, dass Kriminelle die auf der Karte gespeicherten Daten auslesen könnten, um sie im Internet für Einkäufe zu missbrauchen. Dafür genügt schon ein Smartphone mit einer Schnüffel-App, wie beispielsweise die Android-Anwendung „Scheckkartenleser“. Der Täter oder die Täterin hält das Telefon in die Nähe des Portemonnaies des potenziellen Opfers und liest mittels der App die Kartennummer und das Gültigkeitsdatum aus. „Mit diesen Informationen wird es Kriminellen allerdings nur eingeschränkt möglich sein, im Internet einzukaufen“, erklärt Dr. Julia Gerhards. „In der Regel wird bei Online-Zahlungsvorgängen die Prüfziffer oder eine TAN abgefragt. Trotzdem gibt es noch einige Anbieter im Netz, die diese Sicherheitsabfragen – auf eigenes Risiko hin – nicht verlangen.“ Wer im Geschäft an der Kasse zahlt, muss sich hingegen wenig Sorgen machen, weil die Karte in einem geringen Abstand von mindestens vier Zentimetern an das auslesefähige Gerät gehalten werden muss. Kriminelle müssten also sehr nah an das Opfer herantreten, um die Daten abzugreifen.

Dr. Julia Gerhards

Schutz vor möglichem Datendiebstahl

Wer seine funkfähigen Kredit- und EC-Karten vor illegalem Ausspähen schützen will, hat mehrere Möglichkeiten. Man kann beispielsweise alle Karten im Portemonnaie übereinander legen, was das Auslesen einzelner Karte erheblich erschwert. „Sie können Ihre Karten auch in einer speziellen Schutzhülle aufbewahren, mit der sich die Funkwellen abschirmen lassen“, empfiehlt Gerhards. In den Hüllen sind dünne Drähte eingearbeitet, welche die Funkwellen des NFC-Chips blockieren und damit das Auslesen verhindern. Solche Hüllen bieten manche Sparkassen und Banken kostenfrei an. Trotz aller Vorsichtsmaßnahmen rät die Expertin, regelmäßig alle Kontobewegungen und Kreditkartenabrechnungen zu prüfen, egal ob es sich bei den genutzten Karten um funkfähige handelt oder nicht. „Hat man den Verdacht, dass ein Missbrauch stattgefunden hat, sollte man das sofort melden. Für Zahlungen, die man nicht selbst getätigt hat, bekommt man sein Geld vollständig zurück“, so Julia Gerhards. Bei Diebstahl oder Verlust müssen Karten und Konten unverzüglich gesperrt werden. Die Rufnummer gibt es beim jeweiligen Kreditinstitut. Betroffene können sich alternativ auch an die zentrale Sperr-Hotline 116 116 wenden. Wurde eine gestohlene oder verlorene Karte vor der Sperrung bereits für Zahlungen missbraucht, müssen Verbraucher höchstens 50 Euro Ersatz leisten, erklärt Gerhards. „Und dies auch nur dann, wenn beim Bezahlvorgang eine so genannte ‚Zwei-Faktor-Authentifizierung‘ erfolgte, der Verbraucher also zum Beispiel zusätzlich zur Vorlage der funkfähigen Karte eine PIN eingeben musste.“

Sicherheitsrisiko Smartphone

Grundsätzlich hält die Verbraucherschutzexpertin das kontaktlose Bezahlen für genauso sicher wie herkömmliche Kartenzahlungen. Die Verbraucherzentrale Rheinland-Pfalz habe bislang noch keine Beschwerde erhalten, bei der die Kreditkartendaten durch das Auslesen des NFC-Chips illegal genutzt worden seien. Probleme sieht Gerhards hingegen bei Bezahlvorgängen, die mit dem Smartphone getätigt werden: „Hier besteht die Gefahr, dass Viren, Trojaner oder kriminelle Attacken den Zahlungsvorgang manipulieren.“ Hinter vermeintlich harmlosen Apps kann sich gefährliche Schadsoftware verbergen, die Passwörter ausspäht oder Kreditkarteninformationen ausliest. Wer sein Smartphone häufiger zum Bezahlen nutzt oder gar Online-Banking damit betreibt, sollte die Gerätesoftware möglichst auf dem aktuellsten Stand halten und automatische Updates nutzen. Bei allen Bezahlverfahren ist zudem eine regelmäßige Kontrolle der Geldbewegungen angeraten. Nur so fallen ungewollte Abbuchungen auf, die beim Zahlungsdienst umgehend reklamiert werden müssen.
AL (29.03.2019)

Folgende Artikel könnten Sie auch interessieren:

- Riskante Spiele-Apps
- Mehr Sicherheit beim Online-Banking
- Vorsicht beim App-Download!
- Moderne Informationstechnik im Einsatz
- Video: Internetkriminalität – So schütze ich mich!
- Phishing – so können Sie sich schützen

Alle Artikel dieser Kategorie

Weitere Infos zum Thema Internet und Mobil

Vorsicht bei billigen Angeboten

Fake-Shops bei Amazon

Immer wieder fallen Käufer auf so genannte „Fake-Shops“ bei Amazon...[mehr erfahren]

Soziale Kompetenz fehlt online und in der Realität

Ursachen und Formen von Cybermobbing

Beleidigungen, Ausgrenzungen, Schädigungen über virtuelle Kanäle –...[mehr erfahren]

Keine Rabatte mehr möglich

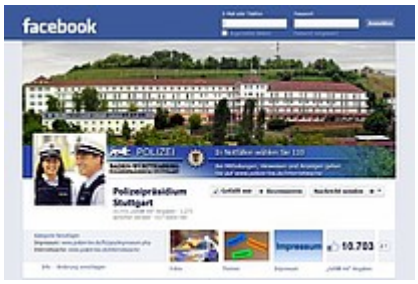
Medikamenten-Festpreise auch fürs Ausland

Immer mehr Menschen nutzen die Möglichkeit, Medikamente über das...[mehr erfahren]

Nutzung pornografischer Inhalte durch Jugendliche

„Hardcore“ ist keine Seltenheit mehr

Während man früher aufwändig nach Videos und Zeitschriften mit...[mehr erfahren]



Das Polizeipräsidium Stuttgart hat über 46.000 Facebook-Fans

Die Polizei auf Facebook und Twitter

Für die Polizeipräsidien sind Soziale Medien ein wichtiger Kanal, um...[mehr erfahren]
