

## **Vorsicht vor „Kartentricks“:**

### **So schützen Sie sich vor Betrug bei unbarem Zahlungsverkehr und Zahlungskartenbetrug.**

Das bargeldlose Bezahlen mit Kreditkarten, der ec-Karte, der Lastschrift oder im elektronischen Zahlungsverkehr ist heute eine selbstverständliche Bezahlmöglichkeit. Unbare Zahlungsmittel sind bequem in der Handhabung und können als sichere Zahlungsmittel eingesetzt werden. Allein in Deutschland sind zirka 112 Millionen Debit- und Kreditkarten ausgegeben.

Der unbare Zahlungsverkehr kann erfolgen:

- per Karte (ec-Karte, Geldkarte, Kreditkarte von VISA, Diners Club, American Express oder MasterCard),
- per Scheck (Reise-, Bar- bzw. Verrechnungsscheck),
- per Überweisung/Lastschrift  
oder
- per Datennetze (Telefon-, Home- und Internetbanking – auch als Online-Banking bezeichnet – mittels PC).

Nach dem es Ende der 1990er Jahre zu einem Anstieg der Fallzahlen kam, ist in den letzten Jahren eine deutliche Verringerung zu spüren.

Für das Jahr 2008 konnte ein Rückgang der erfassten Fälle um 7,4 Prozent gegenüber dem Jahr 2007 auf 66.842 Fälle festgestellt werden. Der ermittelte Schaden belief sich im Jahr 2008 auf 20,276 Millionen Euro und ist ebenfalls deutlich rückläufig. Ursächlich dafür sind beispielsweise die vermehrte Kontrolltätigkeit des Handels durch Verlangen des Ausweises und die Erfolge des Systems KUNO. Eine Statistik aus der PKS Bund (Quelle: BKA Wiesbaden) zum „Betrug mit unbaren Zahlungsmitteln“:

	<b>2008</b>	<b>2007</b>	<b>2006</b>	<b>2005</b>
<b>Erfasste Fälle insgesamt</b>	66.842	72.191	85.523	103.706
<b>Schaden insgesamt bei</b>	47 Mio	44 Mio	72 Mio	61,9 Mio

<b>vollendeten Fällen (in Euro)</b>				
<b>Aufgeklärte Fälle (in %)</b>	43,5	43,1	48,1	47,7

### **„Behalten Sie die Karten in der Hand!“**

Die Straftaten setzen meistens die Entwendung einer Kredit- bzw. ec-Karte voraus. Darum kommt es vor allem darauf an, ihren Verlust zu verhindern.

### **Die Tipps der Polizei:**

- Behandeln Sie Ihre ec- und Kreditkarten so sorgfältig wie Bargeld und tragen Sie diese dicht am Körper, verteilt in verschlossenen Innentaschen der Kleidung.
- Lassen Sie Zahlungskarten niemals in Büro-/Arbeitsräumen, Schwimmbädern, Krankenhäusern, Hotelzimmern, Kraftfahrzeugen etc. liegen – weder offen noch versteckt, auch nicht für kurze Zeit.
- Rechnen Sie insbesondere in Restaurants, Kaufhäusern, Bahnhöfen oder Flughäfen sowie auf Messen oder Ausstellungen mit Taschendieben.
- Überzeugen Sie sich regelmäßig, ob Sie Ihre Karte(n) noch besitzen.
- Bewahren Sie Kreditkarten-/Bankkartenbelege sorgfältig auf und werfen Sie diese nicht in den Papierkorb der Bank/des Geschäftes. Mit den Kontodaten aus dem Papierkorb ist Ihr Geld vor Tätern nicht mehr sicher. Vernichten Sie verschriebene Belege, u. U. auch den Durchschlag.
- Vergleichen Sie zeitnah Ihre Rechnungen mit Abbuchungen auf Ihrem Konto.
- Behalten Sie Ihre Karte stets im Auge.
- Stellen Sie sicher, dass Sie nach dem Bezahlen stets Ihre eigene ec- oder Kreditkarte zurückerhalten. Bestehen Sie darauf, dass verschriebene Kreditkartenbelege, u. U. auch der Durchschlag, sofort ungültig gemacht werden.
- Beachten Sie alle Auflagen, die Ihr Geld- oder Kreditkarteninstitut vertraglich mit Ihnen vereinbart hat. Lesen Sie auch das Kleingedruckte im Vertrag – vor allem die Abschnitte über die Haftung; diese legen fest, welche Sorgfaltspflichten Sie im Umgang mit Ihrer Zahlungskarte zu erfüllen haben.

- Lassen Sie Ihre Karte bei Verlust **sofort** für den weiteren Gebrauch sperren, auch wenn diese aus nicht nachvollziehbaren Gründen vom Geldautomaten einbehalten wird! Das Gerät könnte von Straftätern manipuliert sein.
- Beim Verlust anderer Karten empfehlen wir, unverzüglich das kontoführende Institut zu benachrichtigen. Manche Institute bieten hierzu einen eigenen Notruf-Service an.
- Erstellen Sie bei Verdacht auf eine Straftat sofort Anzeige bei der Polizei.

Die Telefonnummern der **Zentralen Sperrannahmedienste** lauten:

ec-Karten/Bankkarten	01805 021021
American Express	069 97977777
Eurocard/MasterCard	0800 8191040
Diners Club	01805 336695
VISA	0800 8149100
Zentraler Sperrnotruf	116 116

Bei den Kriminalpolizeilichen Beratungsstellen und bei jeder Polizeidienststelle erhalten Sie Broschüren und Faltblätter, wie z. B. „Wie schützen Sie Ihr Geld?“, „Vorsicht - „Karten-Tricks“!“ oder „Thema: Umgang mit unbaren Zahlungsmitteln; auch Ihr guter Name kann kopiert werden“.

### **Vorsicht beim Umgang mit der PIN!**

Vorsicht im Umgang mit der PIN ist vor allem an Geldautomaten und Kassen geboten. Mit folgenden Tipps vermindern Sie Ihr Risiko, beim Einsatz von „Plastikgeld“ Opfer von Straftaten zu werden:

- Üben Sie Sorgfalt bei der Verwendung Ihrer Kartendaten und PIN.
- Geben Sie Ihre PIN **nie** an Dritte weiter, nicht einmal Geldinstitute oder Kreditunternehmen kennen die PIN; weder Amtspersonen noch Mitarbeiter

von Geldinstituten werden nach Ihrer PIN fragen. Prägen Sie sich am besten Ihre PIN ein und vernichten Sie den PIN-Brief. Auf keinen Fall sollten Sie sich die PIN irgendwo notieren (schon gar nicht auf der Zahlungskarte, aber auch nicht im Adressbuch, getarnt als Telefonnummer o. Ä.).

- Beobachten Sie vor dem Geldabheben am Geldautomaten Ihr Umfeld genau. Achten Sie auf die äußere Beschaffenheit des Geldautomaten, melden Sie auffällige Veränderungen sofort an die Polizei!
- Lassen Sie sich bei der Eingabe der PIN am Geldautomaten oder im Handel am Kassensystem nicht beobachten. Bitten Sie aufdringliche Personen oder angebliche Helfer höflich, aber bestimmt, auf Distanz zu bleiben.
- Verdecken Sie die PIN-Eingabe, indem Sie die Hand oder Geldbörse als Sichtschutz dicht über die Tastatur halten.
- Geben Sie – selbst bei Aufforderung – die PIN niemals als Türöffner ein, auch nicht bei Kreditinstituten. Verständigen Sie in solchen Fällen sofort die Polizei!
- Befolgen Sie keine Hinweiszettel, die zur mehrmaligen Eingabe der PIN auffordern.
- Geben Sie beim Bezahlen nicht die PIN bekannt und achten Sie auf die Rückgabe der eigenen Zahlungskarte.
- Speichern Sie Ihre PIN, TAN oder sonstige Zugangscodes nicht auf dem PC.

## **Die Nutzung von Zahlungskarten im Internet**

Beim Bezahlen mit Kreditkarten(-daten) im Mail-, Phone- bzw. Internet-Ordner-Verfahren werden Waren oder Leistungen per Schreiben, Telefon, Fax oder über das Internet bestellt. Die Bezahlung erfolgt unter Angabe der Kreditkartennummer und der Gültigkeitsdauer.

Bei Internet-Transaktionen ist generell der Aspekt der Internet-Sicherheit im Auge zu behalten.

### **Die Tipps der Polizei:**

- Halten Sie Ihr Betriebssystem auf dem neuesten Stand und nutzen Sie entsprechende Update-Funktionen.
- Verwenden Sie aktuelle Virenschutzprogramme und eine aktuelle Firewall.
- Überprüfen Sie Browsereinstellungen, insbesondere hinsichtlich aktiver Inhalte (Näheres auf der Homepage für Sicherheit in der Informationstechnologie – [www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de)).
- Öffnen Sie keine Anhänge von unbekanntem Mails, die zur Eingabe von scheinbar gelöschten Benutzerdaten o. Ä. auffordern (Phishing-Mails) und folgen Sie auch nicht den dort angegebenen Links etc.
- Führen Sie die Transaktionen möglichst an Ihrem eigenen Rechner aus.
- Geben Sie Ihre Kreditkartennummer nur über Verbindungen weiter, die eine Verschlüsselung zwischen Ihrem Rechner und dem Empfänger gewährleisten (z. B. SSL-Standard).
- Speichern Sie Ihre PIN, TAN oder sonstige Zugangscodes nicht auf Ihrem PC.
- Bewahren Sie PIN und TAN getrennt voneinander auf.
- Verwenden Sie bei Passwörtern eine Kombination aus Buchstaben, Zahlen und Zeichen.
- Ändern Sie in regelmäßigen Abständen Ihr Passwort und verwenden Sie dieses nicht mehrfach.
- Kontrollieren Sie regelmäßig Ihre Umsätze auf dem Kontoauszug.

### **KUNO-Sperrsystem**

Mehr Sicherheit im unbaren Zahlungsverkehr wird durch ein neues computergestütztes System des Einzelhandels und der Polizei gegen den Missbrauch von gestohlenen ec-Karten erreicht.

Ziel ist, durch KUNO (Kriminalitätsbekämpfung im unbaren Zahlungsverkehr unter Nutzung nichtpolizeilicher Organisationsstrukturen) Betrugsfälle im kartengestützten Zahlungsverkehr zu reduzieren.

Bei Verlust der ec-Karte sollte man diese nicht nur bei der Bank sperren lassen, sondern auch bei der Polizei als gestohlen melden. Die Polizei meldet dann die Daten der abhanden gekommenen Karte (Bankleitzahl, Kontonummer und Kartenfolgenummer) dem Kooperationspartner des Einzelhandels. Von dort werden

diese Daten an die dem KUNO-Sperrsystem angeschlossenen Einzelhandelsgeschäfte weitergeleitet. So ist die Karte auch für das Lastschriftverfahren (Bezahlen mittels Karte plus Unterschrift) gesperrt.

### **Sicherheitsstandards**

Die Kreditwirtschaft hat auf die Ansprüche der Internet-Bankkunden, den Schutz der Daten und des Zahlungsverkehrs erhöhen, bislang mit folgenden Sicherheitsstandards reagiert:

#### **SSL-Verschlüsselung:**

Die Verbindung zwischen Privat- und Bankrechner erfolgt über einen Knoten im Internet. Die Daten gehen durch „einen sicheren Kanal“ an die Bank.

#### **HBCI-Standard (Homebanking Computer Interface):**

Auch hier ist die oben genannte Verbindung über einen Knoten im Internet aufgebaut. Die Daten gehen verschlüsselt und mit elektronischer Unterschrift an die Bank.

#### **SET (Secure Electronic Transaction):**

Bei SET wird die Direktbezahlung mit Kreditkarte in den virtuellen Raum übertragen, ohne dass der Kunde seine Kreditkartendaten angeben muss. Händler und Verkäufer weisen sich bei diesem von der Kreditwirtschaft entwickelten Verfahren durch Zertifikate aus, die miteinander abgeglichen werden.

Weitere Informationen erhalten Sie im Faltblatt Ihrer Polizei zum Thema Zahlungskartenbetrug „Vorsicht ‚Karten-Tricks‘!“ und im Internet unter [www.polizei-beratung.de/vorbeugung/internet](http://www.polizei-beratung.de/vorbeugung/internet) und [www.kartensicherheit.de](http://www.kartensicherheit.de)