



**THEMA** Zahlungskartenbetrug

## ***Vorsicht „Karten-Tricks“!***

**So schützen Sie sich vor dem Missbrauch Ihrer Zahlungskarte.**

**Wir wollen,  
dass Sie  
sicher leben.**



**Ihre Polizei**

Kompetent. Kostenlos. Neutral.



Das bargeldlose Bezahlen mit Kredit- und Debitkarte (früher auch als ec-Karte bezeichnet), per Lastschrift oder auch online ist heute eine Selbstverständlichkeit. Unbare Zahlungsmittel sind sicher und bequem.

Allerdings lauern auch hier Gefahren: Den weit verbreiteten Einsatz des „Plastikgeldes“ machen sich viele Täter zu eigen! Häufig gelangen die Täter durch Diebstahl (z. B. Taschendiebstahl) oder Einbruch (z. B. Diebstahl aus Kfz) in den Besitz der Zahlungskarte und damit auch der Daten der Zahlungskarte. Das unrechtmäßige Auslesen und Abspeichern der gesamten (Kreditkarten-) Magnetstreifendaten kann zur späteren Herstellung von Kartendubletten genutzt werden. Darüber hinaus können die Täter durch Ausspähen der PIN (z. B. bei der PIN-Verwendung am Geldautomat oder beim Bezahlen im Ladengeschäft) in deren Besitz kommen. Die aufgezeigten Situationen öffnen den Betrügern Tür und Tor. Achtung, auch hier können Ihre Daten ausgespäht werden: Zapfsäulenautomaten und Fahrkartenautomaten.

Die Täter können u. a.

- mit der Debitkarte und PIN im Handel bezahlen (electronic cash),
- mit der Debitkarte und gefälschter Unterschrift im Handel an der Kasse bezahlen (elektronisches Lastschriftverfahren – ELV),
- mit der Geldkarten-Funktion der Debitkarte bezahlen,
- mit der Kreditkarte im Handel bezahlen,
- mit gefälschten Debitkarten an ausländischen Geldautomaten Geld abheben oder
- mit Kreditkarten(-daten) im Mail-, Phone- bzw. Internet-Order-Verfahren bezahlen.



## SCHUTZ VOR KARTENVERLUST

### Tipps zur Vorsorge

Der größte Anteil der Straftaten setzt voraus, dass Ihre Karte entwendet wurde. Darum kommt es vor allem darauf an, den Verlust der Debit- bzw. Kreditkarte zu verhindern! Folgende Tipps sollten Sie beachten:

- Behandeln Sie Ihre Debit-/Kreditkarten **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. weder offen noch versteckt liegen, auch nicht für kurze Zeit.
- Rechnen Sie insbesondere in Restaurants, Kaufhäusern, Bahnhöfen oder Flughäfen sowie Messen oder Ausstellungen mit Taschendieben.
- Überzeugen Sie sich regelmäßig, ob Sie Ihre Karte(n) noch besitzen.
- Bewahren Sie Debit-/Kreditkartenbelege sorgfältig auf und werfen Sie diese nicht bspw. in den Papierkorb der Bank/des Geschäftes. Mit den Kontodaten aus dem Papierkorb ist Ihr Geld vor Tätern nicht mehr sicher.
- Vergleichen Sie zeitnah Ihre Rechnungen mit den Abbuchungen auf Ihrem Konto.
- Behalten Sie Ihre Karte stets im Auge.
- Stellen Sie sicher, dass Sie nach dem Bezahlen stets Ihre eigene Debit- oder Kreditkarte zurückerhalten. Bestehen Sie darauf, dass verschriebene Kartenbelege, unter Umständen auch das Durchschreibepapier, 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; sie legen fest, welche Sorgfaltspflichten Sie im Umgang mit Ihrer Zahlungskarte zu erfüllen haben.

## KARTENVERLUST

### Tipps für den Fall des Falles

Sollte Ihnen Ihre Karte – durch Diebstahl oder sonstigen Verlust – abhanden gekommen sein, ist es unbedingt erforderlich, Folgendes zu beachten:

- Lassen Sie Ihre Karte **sofort** für den weiteren Gebrauch **sperr**en, auch wenn diese aus nicht nachvollziehbaren Gründen vom Geldautomaten einbehalten wird! Das Gerät könnte von Straftätern manipuliert worden sein. Informieren Sie in diesem Fall auch umgehend den Geldautomatenaufsteller.
- Informieren Sie nach Sperrung Ihrer Karte zudem Ihr kontoführendes Institut
- **Bleiben Sie beim Geldausgabeautomaten**, auch wenn beispielsweise kein Geld ausgegeben wird. Lassen Sie sich nicht von vermeintlich „hilfsbereiten Fremden“ vom Automaten weg locken. Es könnte sich um einen Fall des sogenannten „Cash-Trapping“ handeln, dabei wird der Geldausgabeschacht, oftmals

mit aufgeklebten Vorsatzgeräten so manipuliert, dass beim Abhebevorgang die Geldscheine im Ausgabeschacht zurückgehalten werden.

- Verständigen Sie bei Verdacht auf eine Straftat sofort die Polizei!

Karten verloren oder gestohlen?  
Die Notruf-Nummer für jede Karte.  
**Sofort sperren unter:**

**SPERR-NOTRUF**  
**116 116**

Bitte vergessen Sie nicht, den Diebstahl Ihrer Debitkarte bei der Polizei zu melden, damit die Karte für das Lastschriftverfahren gesperrt wird.



[www.polizei-beratung.de](http://www.polizei-beratung.de)

Wir wollen,  
dass Sie  
sicher leben.



Ihre Polizei

[www.polizei-beratung.de](http://www.polizei-beratung.de)

**Zur Sperrung umseitig  
aufgeführte Daten  
bereithalten!**

Weitere Informationen unter:  
[www.servodata.de](http://www.servodata.de) oder  
[www.sperr-ev.de](http://www.sperr-ev.de)

Sofern sich Ihr Kartenherausgeber nicht dem **Sperr-Notruf 116 116** angeschlossen hat, verwenden Sie bitte folgende Rufnummern:

- **Debitkarte** (früher ec-Karte): **+49 - 1805 - 021 021<sup>1</sup>**
- **Mastercard** (nur Deutschland): **0800 - 819 1040<sup>2</sup>**  
- international (R-Gespräch): **+1 - 636 7227 111**
- **VISA-Card** (nur Deutschland): **0800 - 811 8440<sup>2</sup>**  
- international (R-Gespräch): **+1 - 410 581 9994**
- **American Express:** **+49 - 69 - 97 97 1000<sup>3</sup>**
- **Diners Club:** **+49 - 1805 - 07 07 04<sup>1</sup>**

<sup>1</sup> 14 Ct./Min. (inkl. USt.) aus dem dt. Festnetz, Mobilfunkhöchstpreis 42 Ct./Min. (inkl. USt.), abweichende Gebühren aus dem Ausland

<sup>2</sup> Kostenfrei aus dem dt. Festnetz, abweichende Gebühren aus dem Ausland und über Mobilfunk

<sup>3</sup> Gebühren der dt. Telekom innerhalb Deutschlands, abweichende Gebühren aus dem Ausland

Alle Angaben ohne Gewähr.



## UMGANG MIT DER PIN

### Verhalten an Geldautomaten, Kassen etc.

- Eine wichtige Voraussetzung für die Sicherheit im Umgang mit Zahlungskarten ist und bleibt die sorgfältige Handhabung der Kartendaten und der PIN. Der ordnungsgemäße und gewissenhafte Umgang mit Zahlungskarten ist der beste Garant für Sicherheit beim unbaren Zahlungsverkehr.
- Geben Sie Ihre PIN **NIE** an Dritte weiter; nicht einmal Geldinstitute oder Kreditkartenunternehmen kennen die PIN; weder Amtspersonen (z. B. Polizeibeamte) 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 die PIN irgendwo notieren (schon gar nicht auf der Zahlungskarte! Aber auch nicht im Adressbuch, getarnt als Telefonnummer o. Ä.).
- Beobachten Sie bereits vor dem Geldabheben am Geldautomaten Ihr Umfeld genau. Achten Sie auf die äußere Beschaffenheit des Geldautomaten, melden Sie auffällige Veränderungen sofort der Polizei! Seien Sie sich der Risikosituation immer bewusst!
- Achten Sie bei der Eingabe der PIN am Geldautomaten oder im Handel am Kassensystem stets darauf, dass niemand den Vorgang beobachten kann; bitten Sie aufdringliche Personen oder angebliche Helfer höflich aber bestimmt, auf Distanz zu bleiben.



HTTP://

- Verdecken Sie die PIN-Eingabe, indem Sie die Hand oder Geldbörse als Sichtschutz dicht über die Tastatur halten. Dies erschwert ein Ausspähen erheblich!
- Geben Sie – selbst bei Aufforderung – die PIN niemals an Türöffnern ein, auch nicht bei Geldinstituten. 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.

## **DIE NUTZUNG VON ZAHLUNGSKARTEN IM INTERNET**

### **Bezahlen mit Kreditkarten(-daten) im Mail-, Phone- bzw. Internet-Order-Verfahren**

Bei dieser Bezahlmöglichkeit werden Waren oder Leistungen per Schreiben, Telefon, Fax oder über das Internet bestellt. Die Bezahlung erfolgt unter Angabe der Kreditkartennummer und der Gültigkeitsdauer.

Die wachsende Zahl von Personen, die über einen Internet-Zugang verfügen und diesen auch zu finanziellen Transaktionen z. B. beim Online-Versandhandel einsetzen, machen sich auch Kriminelle zu Nutze. So unterschiedlich ihre Methoden sein mögen – ihr Ziel ist immer, an Zahlungskartendaten heranzukommen.



Der Schwerpunkt bei kriminellen Handlungen im Zusammenhang mit dieser Bezahlungsform verlagert sich, ausgehend von der immer häufigeren Nutzung dieses Mediums, in den Bereich der betrügerischen Einsätze von Zahlungskartendaten im Internet. Bei Internet-Transaktionen ist generell der Aspekt der Internet-Sicherheit im Auge zu behalten. **Beachten Sie bitte nachfolgende Tipps:**

- Halten Sie Ihr Betriebssystem auf dem neuesten Stand und nutzen Sie entsprechende Update-Funktionen.
- Verwenden Sie immer ein aktuelles Virenschutzprogramm und eine aktuelle Firewall.
- Überprüfen Sie die Browsereinstellungen, insbesondere hinsichtlich aktiver Inhalte (Näheres auf der Homepage des Bundesamtes für Sicherheit in der Informationstechnologie – [www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de)).
- Öffnen Sie keine Anhänge von unbekanntem Mail, 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 Transaktion möglichst am 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).



Sichere Seiten beginnen mit „https“ – ein kleines geschlossenes Vorhängeschlosssymbol in der Statuszeile Ihres Browsers kennzeichnet die sichere Verbindung.

Auch hier gilt: Es ist keine Situation denkbar, in der Ihre PIN berechtigterweise verlangt und daher von Ihnen preisgegeben werden muss.

Darüber hinaus kann zusätzlich die Angabe der Kartenprüfnummer gefordert werden, die auf der Kreditkarte selbst aufgedruckt, aber nicht im Magnetstreifen gespeichert ist.

Allgemein gilt: Versichern Sie sich, mit wem Sie es zu tun haben. Drucken Sie die Allgemeinen Geschäftsbedingungen und das Impressum (Adressenangabe, Telefonnummer) aus. Überprüfen Sie anhand der Angaben die Existenz des Internet-Unternehmens. Drucken Sie den kompletten Geschäftsvorgang aus. Beachten Sie bei Internet-Händlern mit Sitz im Ausland, insbesondere in Nicht-EU-Staaten, dass unser Rechtssystem möglicherweise keinen Zugriff hat. Wählen Sie ggf. andere Zahlungsmöglichkeiten aus (per Nachnahme, per Lastschrift, per Überweisung).

**Weitere Infos finden Sie im Internet unter:**

**[www.polizei-beratung.de/themen-und-tipps/betrug](http://www.polizei-beratung.de/themen-und-tipps/betrug)**

**[www.sperr-notruf.de](http://www.sperr-notruf.de)**

**[www.kartensicherheit.de](http://www.kartensicherheit.de)**



**Dieses Falblatt wurde ausgehändigt von:**

(05V)150.2012.08

**HERAUSGEBER:  
PROGRAMM POLIZEILICHE  
KRIMINALPRÄVENTION DER  
LÄNDER UND DES BUNDES**

Zentrale Geschäftsstelle  
Taubenheimstraße 85, 70372 Stuttgart

**Wir wollen,  
dass Sie  
sicher leben.**



**Ihre Polizei**

[www.polizei-beratung.de](http://www.polizei-beratung.de)