

## SICHERHEITSBEWUSSTER UMGANG MIT ZAHLUNGSKARTEN

Gestohlene, abhanden gekommene oder gefälschte girocards und Kreditkarten werden – häufig mehrfach – missbräuchlich verwendet, um in der Regel später leicht absetzbare Waren zu erlangen. Dadurch entstehen Jahr für Jahr hohe Schäden. Gerade im Bereich des elektronischen Lastschriftverfahrens (Beleg mit Unterschrift) gehen diese Schäden sehr häufig zu Lasten der betroffenen Unternehmen. Durch sicherheitsbewusstes Verhalten können Sie diese Schäden nachhaltig begrenzen oder – besser noch – von vornherein ganz ausschließen.

Täterinnen und Täter setzen gestohlene oder gefälschte Zahlungskarten vorzugsweise an zwei Typen von Kassen ein: an denen, die mit dem elektronischen Lastschriftverfahren arbeiten, oder an solchen, die bei Umsätzen unter der Genehmigungsgrenze – trotz ec-Cash-Verfahren mit Eingabe der PIN – nicht die Sperrsysteme der Kreditwirtschaft überprüfen. Gestohlene oder gefälschte Kreditkarten werden meistens an Kassen ohne Online-Autorisierung vorgelegt, wo nur mit Belegdruck gearbeitet wird.

### Empfehlungen zur Vorbeugung für Gewerbetreibende

- › Lassen Sie sich bei Kartenzahlungen den Personalausweis zeigen oder fragen Sie die Sperrdateien ab. Nur bei Stammkundschaft genügen Karte und Unterschrift!
- › Verwenden Sie bei Zahlungsvorgängen grundsätzlich das sichere ec-Cash-Verfahren mit Eingabe der PIN.
- › Sofern Sie das elektronische Lastschriftverfahren nutzen, sollten Sie sich dem KUNO-Verfahren des Handels anschließen oder sicherstellen, dass Ihr Netzbetreiber daran teilnimmt.
- › Halten Sie im Verdachtsfall Rücksprache mit dem Geldinstitut oder dem Kreditkartenunternehmen, lehnen Sie bei Unstimmigkeiten eine Kartenzahlung sicherheitshalber ab.
- › Rufen Sie bei offenkundigen Betrugsversuchen sofort die Polizei über die Notruf-Nr. 110.
- › Sichern Sie evtl. vorhandene Videoaufzeichnungen oder sonstige Beweismittel.
- › Legen Sie die Abläufe und Verantwortlichkeiten im Umgang mit unbaren Zahlungsmitteln insbesondere bei Unstimmigkeiten eindeutig fest.

- › Schulen Sie Ihr Personal entsprechend den Verhaltensempfehlungen der Polizei und legen Sie diese Tipps an ihren Kassen aus.

### Empfehlungen zur Vorbeugung für Kassenpersonal

- › Prüfen Sie bei Kartenzahlung, ob der auf der Karte angegebene Vorname (weiblich/männlich) zur Kundin oder zum Kunden passt.
- › Vergleichen Sie die Unterschriften von Zahlungsbeleg und Karte.
- › Lassen Sie sich im Zweifelsfall Ausweisdokumente mit Lichtbild (z. B. Personalausweis oder Führerschein) vorlegen. Notieren Sie die Ausweisdaten (auch Ausweisart und -nummer, ausstellende Behörde, Ort und Datum der Ausstellung).
- › Lehnen Sie bei Unstimmigkeiten die Kartenzahlung sicherheitshalber ab und schlagen Sie andere Zahlungsarten vor (Bargeld oder Einsatz anderer Karten).

### Empfehlungen bei Verdacht eines Betrugsversuchs

- › Bringen Sie sich nicht in Gefahr! Sie sind nicht berechtigt, Zahlungskarten oder Ausweisdokumente einzubehalten! Halten Sie niemals flüchtende Personen fest!
- › Informieren Sie Ihre Vorgesetzten und – soweit vorhanden – den Sicherheitsdienst.
- › Benachrichtigen Sie unverzüglich die Polizei und teilen Sie Ihre Wahrnehmungen mit.
- › Prägen Sie sich das Aussehen der Person ein (Alter, Größe, Haarfarbe, Sprache, Kleidung, besondere Merkmale) und merken Sie sich nach Möglichkeit auch weitere Einzelheiten: Begleitpersonen, Fluchtrichtung, Fahrzeug (Modell, Farbe, Kennzeichen).

Weitere Informationen finden Sie unter [www.polizei-beratung.de](http://www.polizei-beratung.de)

Mit freundlicher Empfehlung