Informationen Ihrer Polizei

ZAHLUNGSKARTENBETRUG

VORSICHT „KARTEN-TRICKS“

GEFAHREN BEIM BEZAHLEN MIT ZAHLUNGSKARTEN

Den weit verbreiteten Einsatz von Kredit- und Debitkarten nutzen viele Täter! Häufig gelangen sie beispielsweise durch Taschendiebstahl oder Einbruch (z. B. Autoaufbruch) in den Besitz der Karten. Das verbotene Auslesen und Abspeichern der gesamten Daten einer Zahlungskarte nutzen Täter zur späteren Herstellung von Kartendubletten (sogenanntes „Skimming"). Außerdem 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 Täter können u. a.:

- mit der Debitkarte und PIN im Handel bezahlen,
- mit der Debitkarte und gefälschter Unterschrift im Handel an der Kasse bezahlen (elektronisches Lastschriftverfahren – SEPA Lastschrift),
- mit der Geldkarten-Funktion der Debitkarte bezahlen,
- mit der Karte kontaktlos, je nach Anbieter, bis 25 Euro ohne PIN bezahlen,
- mit der Kreditkarte im Handel bezahlen,
- mit gefälschten Debitkarten an ausländischen Geldautomaten Geld abheben oder
- mit Kreditkarten(-daten) im Mail-, Phone- bzw. Internet-Bestell-Verfahren bezahlen.

© Rüdiger Kottmann

SKIMMING

Die Täter lesen die Magnetstreifendaten der Karten aus und übertragen diese auf Kartenrohlinge. Mit diesen heben die Täter dann im Ausland in Kombination mit der PIN Geld vom Konto der Opfer ab. Um in den Besitz der Daten zu kommen, installieren die Täter vor dem Karteneinschubschacht ein eigens hergestelltes Kartenlesegerät oder sogar eine vollständige Frontplatte. Diese Kartenleser sind optisch dem Modell der Geldautomaten angepasst (Farbe, Aufkleber) und so hergestellt, dass die eingeschobene Karte zum originalen Kartenleser weitertransportiert wird. So werden die Magnetstreifendaten ausgelesen und gespeichert, ohne dass die Bedienung des Geldautomaten beeinträchtigt und der Kunde dadurch misstrauisch wird. Die Eingabe der PIN wird mit einer Mini-Kamera gefilmt, die oft oberhalb der Tastatur in einer angeklebten Kameraleiste versteckt ist. Es kommen aber auch manipulierte Tastaturfelder zum Einsatz, die über die eigentliche Tastatur geklebt werden. Damit zeichnen die Täter die per Tastendruck eingegebene PIN auf.

TIPPS FÜR SICHERHEITSBEWUSSTES VERHALTEN

- Behandeln Sie Ihre Karten wie Bargeld und tragen Sie diese dicht am Körper verteilt in verschlossenen Innentaschen der Kleidung.
- Lassen Sie Karten niemals offen oder versteckt liegen, auch nicht für kurze Zeit. Taschendiebe lauern besonders gerne an belebten Orten.
- Überzeugen Sie sich regelmäßig, ob Sie Ihre Karte(n) noch besitzen.
- Bewahren Sie Kartenbelege sorgfältig auf und vergleichen Sie Ihre Rechnungen mit den Abbuchungen auf Ihrem Konto und Ihren Belegen.
- Stellen Sie sicher, dass Sie nach dem Bezahlen stets Ihre eigene Karte zurückerhalten. Bestehen Sie darauf, dass verschriebene Kartenbelege, unter Umständen auch das Durchschreibepapier, sofort ungültig gemacht werden.
- Beachten Sie die Auflagen, die Ihr Geld- oder Kreditkarteninstitut vertraglich mit Ihnen vereinbart hat. Achten Sie auf das Kleingedruckte im Vertrag – vor allem die Abschnitte über die Haftung. Dort steht, welche Pflichten Sie im Umgang mit Ihrer Zahlungskarte zu erfüllen haben.

© mystock/fotolia

KARTENVERLUST – WAS TUN?

- Lassen Sie Ihre Karte sofort unter **116 116** sperren, 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 den Geldautomatenaufsteller.
- Informieren Sie nach Sperrung Ihrer Karte Ihr kontoführendes Institut.
- Bleiben Sie beim Geldautomaten, auch wenn kein Geld ausgegeben wird. Lassen Sie sich nicht von vermeintlich „hilfsbereiten Fremden" weglocken. Es könnte sich um einen Fall des so genannten „Cash-Trapping" handeln. Hierbei wird der Geldausgabeschacht mit aufgeklebten Vorsatzgeräten so manipuliert, dass beim Abheben die Geldscheine im Schacht zurückgehalten werden.
- Verständigen Sie bei Verdacht auf eine Straftat sofort die Polizei unter **110**!

Damit Ihre Debitkarte auch für das elektronische Lastschriftverfahren (SEPA Lastschrift) gesperrt werden kann, für das nur eine Unterschrift benötigt wird, müssen Sie den Verlust der Polizei melden. Nur diese kann eine so genannte freiwillige KUNO-Sperrung bei den Handelsunternehmen veranlassen.

Diese Nummern sollten Sie sich notieren bzw. abspeichern:

Polizeinotruf **110**
Kostenlose Hotline der Bundespolizei **0800 6 888 000**
Zentraler Sperr-Notruf **116 116**
Individuelle Telefonnummer Ihrer Bank: _____
Ihre IBAN: _____
Ihre Kreditkartennummer(n): _____

UMGANG MIT DER PIN – RICHTIGES VERHALTEN AN GELDAUTOMATEN, KASSEN UND CO.

- Geben Sie Ihre PIN nie an Dritte weiter. Weder Geldinstitute noch Kreditkartenunternehmen kennen die PIN; weder Amtspersonen noch Mitarbeiter von Geldinstituten werden nach Ihrer PIN fragen. Prägen Sie sich Ihre PIN ein und vernichten Sie den PIN-Brief. Auf keinen Fall sollten Sie die PIN notieren (schon gar nicht auf der Zahlungskarte! Aber auch nicht im Adressbuch, getarnt als Telefonnummer).
- Achten Sie bereits vor dem Geldabheben auf Ihr Umfeld. Schauen Sie auf die Beschaffenheit des Geldautomaten, melden Sie Veränderungen sofort der Polizei unter **110**!
- Achten Sie bei der Eingabe der PIN stets darauf, dass Sie niemand beobachtet; bitten Sie aufdringliche Personen auf Distanz zu bleiben.
- Verdecken Sie die PIN-Eingabe, indem Sie die Hand oder Geldbörse als Sichtschutz über die Tastatur halten. Das erschwert ein Ausspähen erheblich!
- Geben Sie die PIN niemals an Türöffnern ein, auch nicht bei Geldinstituten. Verständigen Sie in solchen Fällen sofort die Polizei!

KONTAKTLOSES BEZAHLEN

Wenn auf Ihrer Karte dieses Wellensymbol  abgebildet ist, können Sie mit Ihrer Karte kontaktlos bezahlen, also durch Hinhalten der Karte an das Bezahlterminal. Insbesondere bei Beträgen bis 25 Euro, für die normalerweise keine PIN-Eingabe nötig ist, ist das Bezahlen mit rund 11 Sekunden mehr als doppelt so schnell als bei herkömmlichen Verfahren. Wenn Sie die Funktion deaktivieren möchten, wenden Sie sich bitte an Ihr Kreditinstitut.

ZAHLEN MIT SMARTPHONE

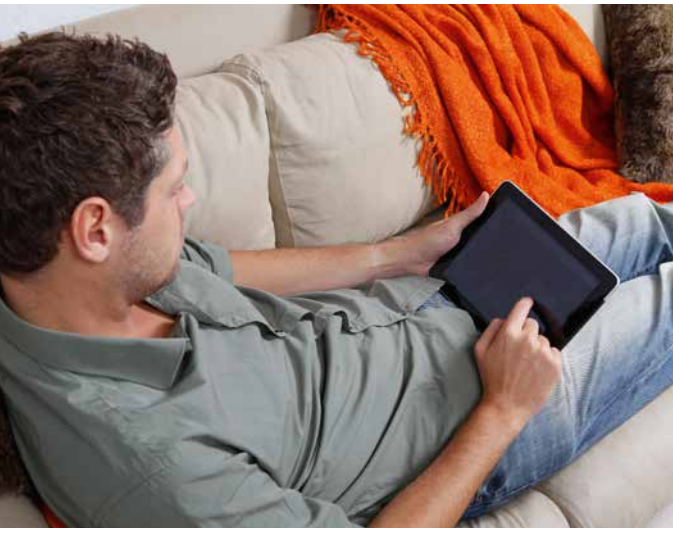
Vermehrt können Sie mit Ihrem Smartphone mittlerweile auch direkt an der Kasse bezahlen. Banken bieten Ihnen die kartengestützte Variante an. Hier wird in Ihrer virtuellen Geldbörse (englisch: „wallet“) Ihre Karte hinterlegt. Das kann je nach Bank auch eine eigene App der Bank sein oder Ihre Bank unterstützt Anwendungen von externen Anbietern der virtuellen Geldbörsen. Beachten Sie deshalb, dass Sie Ihr Smartphone ähnlich wie Ihren Computer sicher benutzen.

© pixdeluxe/istock

BEZAHLEN MIT KARTEN IM INTERNET

Kauf und Verkauf im Internet (z. B. beim Online-Shopping, Onlinebanking) machen sich auch Kriminelle zu Nutze. So unterschiedlich ihre Methoden auch sind – ihr Ziel ist immer, an Zahlungskartendaten heranzukommen. Dabei versuchen Täter insbesondere über betrügerische E-Mails (Phishing), Sicherheitslücken am Computer, Handy, Tablet oder Browser (Schadsoftware) an Ihre Daten zu gelangen. Bei der Eingabe sensibler Kartendaten bei Internettransaktionen sollten Sie auf Folgendes achten:

- Halten Sie Ihr Betriebssystem auf dem neuesten Stand und nutzen Sie entsprechende Update-Funktionen.
- Verwenden Sie immer ein aktuelles Virenschutzprogramm und eine Firewall.
- Überprüfen Sie die Browsereinstellungen auf aktive Inhalte (Näheres auf der Website des Bundesamtes für Sicherheit in der Informationstechnologie – **www.bsi-fuer-buerger.de**).
- Halten Sie sich nur auf vertrauenswürdigen und seriösen Internetseiten auf.
- Laden Sie nichts Riskantes herunter und achten Sie auf eine vertrauenswürdige Quelle.



© Wolfgang Schmidberger

- Öffnen Sie keine Anhänge und Links von unbekannten Mails, die zur Eingabe von scheinbar gelöschten Benutzerdaten o. Ä. auffordern (Phishing-Mails).
- Führen Sie das Bezahlen möglichst am eigenen Rechner und im eigenen Internetnetzwerk (keine öffentlichen Hotspots) aus.
- Nutzen Sie eine verschlüsselte Verbindung (z. B. SSL-Standard). Sichere Seiten beginnen mit „https“. Ein kleines geschlossenes Vorhängeschlosssymbol in der Statuszeile Ihres Browsers kennzeichnet die sichere Verbindung.
- Allgemein gilt: Gehen Sie vorsichtig mit Ihren sensiblen Daten im Internet und in sozialen Netzwerken um. Versichern Sie sich, mit wem Sie es zu tun haben. Werfen Sie einen Blick in die Allgemeinen Geschäftsbedingungen und das Impressum (Adressenangabe, Telefonnummer). Überprüfen Sie anhand der Angaben die Existenz des Internetunternehmens mit eigener Recherche im Internet.
- Bedenken Sie bei Internethändlern mit Sitz im Ausland, insbesondere in Nicht-EU-Staaten, dass unser Rechtssystem möglicherweise keinen Zugriff hat.
- Wählen Sie ggf. andere Zahlungsmöglichkeiten aus (per Nachname, per Lastschrift, per Rechnung).

© Tilmann Kübler

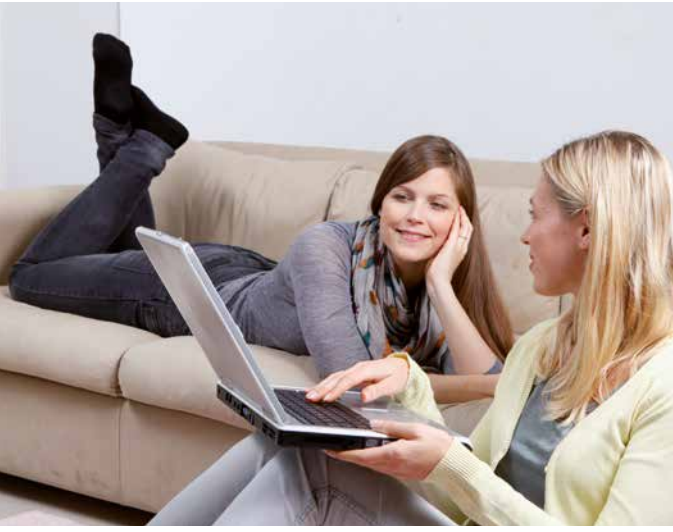
Weitere Infos finden Sie im Internet unter:

- **www.polizei-beratung.de/themen-und-tipps/betrug**
- **www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet**
- **www.bsi-fuer-buerger.de**
- **www.sperr-notruf.de**
- **www.kartensicherheit.de**

VERLUST DES NEUEN PERSONALAUSWEISES MIT ONLINE-AUSWEISFUNKTION – WAS TUN?

Wenn der Personalausweis gestohlen wurde oder abhandengekommen ist, muss die Online-Ausweisfunktion so schnell wie möglich gesperrt werden. Das geht im Bürgeramt und an sieben Tagen die Woche rund um die Uhr mit der gebührenfreien Rufnummer **116 116**. Aus dem Ausland steht der Sperrnotruf unter **+ 49-116 116** und **+ 49-30-40 50 40 50** (gebührenpflichtig) zur Verfügung. Zum Sperren der Online-Ausweisfunktion über den Sperrnotruf werden der Name, das Geburtsdatum und das Sperrkennwort abgefragt. Das Sperrkennwort steht im PIN-Brief. Bitte beachten: Auch wenn die Online-Ausweisfunktion über den Sperrnotruf gesperrt wurde, muss das Bürgeramt in jedem Fall über den Verlust des Ausweises informiert werden. Die Sperrung der Unterschriftsfunktion muss separat beim Anbieter des Signaturzertifikats erfolgen.

Weitere Infos finden Sie im Internet unter:
www.personalausweisportal.de



© Wolfgang Schmidberger

OSCAR CHARLIE

(08V)150.2019.05

EINE PUBLIKATION IHRER POLIZEI.

Weitere Infos finden Sie unter
www.polizei-beratung.de

Titelbild:
© Tilmann Kübler

Herausgeber:
Polizeiliche Kriminalprävention der Länder und des Bundes
Zentrale Geschäftsstelle
Taubenheimstraße 85
70372 Stuttgart

Wir wollen, dass Sie sicher leben.
Ihre Polizei