KREDITKARTE:

SO KÖNNEN SIE SICHER MIT IHRER KREDITKARTE EINKAUFEN – ONLINE UND OFFLINE!

CHECK24

INHALT

1. Allgemeine Informationen 03

2. Die Sicherheitsmerkmale 03

3. Sicher durch den Alltag 04

4. Sicher im Internet 05

HINWEIS: Trotz gewissenhafter Recherche kann die Richtigkeit und Aktualität der Angaben nicht garantiert werden.

KREDITKARTE:
SO KÖNNEN SIE SICHER MIT IHRER KREDITKARTE EINKAUFEN – ONLINE UND OFFLINE!

1. SICHER BEZAHLEN MIT DER KREDITKARTE

Die Zahlung per Kreditkarte ist praktisch und wohl deshalb auch so beliebt: International ist die Kreditkarte das Zahlungsmittel Nummer Eins im Onlinehandel. Die kleine Plastikkarte verfügt über eine große Anzahl von Sicherheitsmerkmalen, die Sie bestmöglich vor unberechtigten Zugriffen von außen schützen – egal, ob am Geldautomaten, im Supermarkt oder bei der Bezahlung im Internet. Warum auch nicht, schließlich steckt das kleine Bezahlerlein voller Vorteile und auch für Sicherheit ist gesorgt. Allerdings gibt es immer wieder Missbrauchsversuche.

Wir zeigen Ihnen, wieviel Technologie in der kleinen Karte steckt und mit welchen Sicherheitstipps Sie sich im Alltag und im Internet optimal schützen können.

2. SICHERHEITSMERKMALE

Die Kreditkarte ist dank modernster Technologien ein sicheres Zahlungsmittel. Wir geben Ihnen einen Überblick über die wichtigsten Sicherheitsmerkmale Ihrer Karte. Außerdem haben wir für Sie die besten Tipps für einen sicheren Umgang mit der Kreditkarte zusammengestellt.

Sicherheitsmerkmale auf der Vorderseite der Kreditkarte

1 EMV-Chip

Seit dem 1.1.2011 ist der EMV-Standard in Europa verpflichtend und alle seither ausgegebenen Karten sind damit ausgestattet. Dieser Chip weniger einfach ausgelesen oder dupliziert werden. Die im Chip gespeicherten Daten sind somit vor Fälschungen und Kopien geschützt.

2 Kartennummer-Index

Der Kartennummer-Index ist unter der Kreditkartennummer notiert und muss mit den ersten vier Stellen der geprägten Kartennummer übereinstimmen. Der Kartennummer-Index beginnt bei MasterCard-Kreditkarten in der Regel mit der Ziffer 5, bei Visa-Karten mit der Ziffer 4.

3 Hochprägung

Die Kreditkartennummer sowie der Name und das Gültigkeitsdatum sind bei Kreditkarten hochgeprägt. Eine Ausnahme stellen in der Regel Prepaid-Kreditkarten dar, die oftmals keine Hochprägung aufweisen. Nur Karten mit Hochprägung können an sogenannten Imprintern eingesetzt werden. Die Karten ohne Hochprägung sind in der Regel mit dem Hinweis „electronic use only“ versehen.

4 Sicherheitszeichen in ultraviolettem Licht

Dieses Sicherheitsmerkmal wird nur unter ultraviolettem Licht sichtbar. Bei MasterCard erscheinen unter ultraviolettem Licht beispielweise die Buchstaben M und C.

5 Hollogramm

Ein Hologramm ist eine zweidimensionale Abbildung, die ein dreidimensionales Bild zeigt. Eine Fälschung dieses Sicherheitsmerkmals ist sehr aufwendig und schwierig. Visa und MasterCard bedienen sich dabei unterschiedlicher Graphiken: Während das Hologramm bei Visa eine Taube darstellt, die am rechten Rand in der Mitte der Karte positioniert ist, zeigt das MasterCard-Hologramm zwei ineinander greifende Weltkugeln und das MasterCard-Logo.

Sicherheitsmerkmale auf der Rückseite der Kreditkarte

1 Unterschriftsstreifen

Der Unterschriftsstreifen ist gegen Manipulationen geschützt. Das chemische Papier des Unterschriftsstreifens ist oftmals mit einer Graphik oder dem Namen der Kreditkartengesellschaft versehen. Der Kreditkarteninhaber sollte die Karte sofort nach Erhalt unterschreiben.

2 Kartenprüfnummer

Bei der Kartenprüfnummer - auch als Kartenprüfziffer, CVC2 oder CVV2 bekannt – handelt es sich um die letzten drei Zahlen, die rechts im Unterschriftstreifen auf der Kreditkartenrückseite vermerkt sind. Diese Prüfnummer dient etwa beim Onlineshopping zur Kontrolle, ob dem Käufer die Karte physisch vorliegt. Die Prüfziffer kann nicht ausgelesen werden, da sie nicht auf dem Magnetstreifen oder dem Chip gespeichert ist. Somit wird durch die Abfrage der drei Ziffern die Sicherheit beim Onlineshopping erhöht.

Und zusätzlich: Das 3D-Secure Verfahren

Das 3D-Secure-Verfahren wird von vielen Banken angeboten und auf Kundenwunsch freigeschaltet. Die Sicherheit beim Onlineshopping wird durch den zusätzlichen Passwortschutz sowohl für Händler als auch für Kunden erhöht: Sobald der Kunde sich in einem Onlineshop im Bezahlvorgang befindet, stellt der Shop eine Anfrage an die Bank. Diese öffnet ein eigenes Browserfenster zur Identifizierung des Karteninhabers. Der Kunde gibt in diesem Fenster seine 3D PIN ein und autorisiert damit die Kartenzahlung. Nur, wenn die PIN korrekt eingegeben wurde und die Bank die Identität des Karteninhabers bestätigt hat, kann die Transaktion erfolgen und der Einkauf abgeschlossen werden. Der Vorgang gewährt somit zusätzliche Sicherheit, dauert dabei aber nur wenige Sekunden.

3. SICHER DURCH DEN ALLTAG

Allgemeine Tipps zur Kreditkarten Sicherheit

1. Der beste Tipp, um Kartenmissbrauch zu vermeiden: Nutzen Sie Ihren gesunden Menschenverstand!

2. Wenn jemand Sie auf Ihre Kreditkartendaten – egal ob persönlich oder im Internet – anspricht: werden Sie sofort hellhörig!

3. Die Bank würde Sie niemals nach ihrer PIN oder TAN fragen – weder per Post noch auf der Straße oder in einer E-Mail.

4. Wenn Sie sich nicht sicher sind: rufen Sie in Ihrer Bank an und holen Sie sich eine Rückversicherung. Lieber einmal zu viel gefragt, als einmal zu wenig!

5. Die Sperrhotline ist der letzte Rettungsring, wenn Sie die Karte verloren haben oder Betrüger Ihre Karte missbrauchen.

Die Nummer lautet 116 116.

Diese Punkte helfen Ihnen Ihre Kreditkarte offline vor Missbrauch zu schützen

- ☑ Die wichtigste Regel im Umgang mit der Kreditkarte ist die getrennte Aufbewahrung von Karte und Geheimnummer. Die PIN sollte beispielsweise niemals gemeinsam mit der Karte im Geldbeutel aufbewahrt werden und auch nicht auf oder in der Nähe der Karte notiert werden. Dies ist nicht nur relevant, um einen Betrug zu verhindern, sondern dies ist auch Voraussetzung dafür, dass die Bank für einen etwaigen entstandenen Schaden die Haftung übernimmt.

- ☑ Die PIN sollte zudem weder persönlich noch über E-Mails oder per Telefon an Dritte weitergegeben werden.

- ☑ Sofort nach Erhalt Ihrer neuen Kreditkarte sollten Sie diese auf dem dafür vorgesehenen Unterschriftsstreifen unterschreiben. Zahlen Sie beispielsweise in einem Ladengeschäft mit der Karte, wird die Unterschrift in Ihrem Ausweisdokument mit der Unterschrift auf der Kreditkarte verglichen.

- ☑ Wenn Sie Geld mit Ihrer Kreditkarte abheben, sollten Sie die PIN verdeckt eingeben und möglichst Geldautomaten wählen, die sich in der Bankfiliale und nicht im Außenbereich befinden. Automaten im Außenbereich können leichter von Betrügern präpariert werden. Zudem sollten Sie auf etwaige Unregelmäßigkeiten am Automaten achten.

- ☑ Prüfen Sie bei jeder Bezahlung, ob der auf dem Beleg angegebene Betrag korrekt ist. Erst, wenn Sie den Betrag kontrolliert haben, sollten Sie mit Ihrer Unterschrift die Zahlung bestätigen. Belege ohne angegebene Rechnungssumme sollten nicht unterschrieben werden.

- ☑ Kontrollieren Sie in regelmäßigen Abständen Ihre Kreditkartenabrechnung. Etwaige Betrugsfälle können so zeitnah aufgedeckt werden.

- ☑ Verwahren Sie Ihre Wertgegenstände diebstahlsicher. Tragen Sie beispielsweise Ihren Geldbeutel möglichst nicht in einer Außentasche Ihrer Jacke oder in der Gesäßtasche ihrer Hose.

- ☑ Informieren Sie sich über gängige Tricks von Betrügern, um dafür gewappnet zu sein. Beispielsweise fragt keine Bank an Türöffnern eine Geheimzahl ab.

- ☑ Notieren Sie sich die Notfall-Sperrnummer für Ihre Kreditkarte. So können Sie Ihre Karte sofort sperren lassen, falls Sie Unregelmäßigkeiten bemerken. Unter 116 116 erreichen Sie den allgemeinen Sperr-Notruf rund um die Uhr. Diese Nummer ist aus dem deutschen Festnetz oder Mobilfunknetz kostenlos, aus dem Ausland (unter +49 116 116) werden Gebühren fällig.

4. SICHER IM INTERNET

Und so können Sie auch im Internet unbesorgt mit Ihrer Kreditkarte zahlen

- ☑ Wenn Sie E-Mails erhalten, deren Absender Sie nicht kennen, klicken Sie in keinem Fall auf Links oder Anhänge. Sind Sie sich unsicher, können Sie die Mail im Zweifelsfall direkt in Ihrem Posteingang löschen – ohne sie zu öffnen. Denn in manchen Fällen können E-Mails sogenannte Script-Viren enthalten, die sich in HTML-Codes verstecken.

- ☑ Der Aufforderung bestimmte Programme herunterzuladen, sollten Sie nicht nachkommen. Es sei denn, Sie befinden sich auf der offiziellen Internet-Seite eines Unternehmens Ihres Vertrauens. Downloads sollten generell nie über Links in E-Mails gestartet werden.

- ☑ Versenden Sie keine vertraulichen Daten per E-Mail.

- ☑ Beim Online-Banking oder beim Einkauf im Internet sollten Sie sich vergewissern, dass Sie Ihre Daten nur über eine gesicherte Verbindung übermitteln. Diese sogenannte SSL-Verschlüsselung (Secure Socket Layer) erkennen Sie an der Adresszeile des Browser. Statt mit ://http beginnt die Adresszeile dann mit ://https. Zudem befindet sich neben der URL auf der linken Seite ein Schlosssymbol. Wenn dieses geschlossen ist, ist die Verbindung sicher. Durch ein Klicken auf das Schloss erhalten Sie zudem weitere Informationen über die Verbindung.

- ☑ Achten Sie in der Adresszeile nicht nur auf eine SSL-Verschlüsselung, sondern auch darauf, dass die URL Ihrer Bank oder des Onlineshops korrekt geschrieben wurde. Betrüger verwenden in manchen Fällen täuschend echt aussehende Fälschungen von Bankinternetseiten, um die Daten der Kunden abzugreifen. Die URL verrät dabei – beispielsweise durch Buchstabendreher – die Fälschung.

- ☑ Wählen Sie sichere Passwörter mit Großschreibungen und Sonderzeichen und verwenden Sie möglichst für jede Anwendung ein anderes Passwort.

- ☑ Wenn Ihre Bank diesen Service anbietet, sollten Sie beim Onlineshopping das sogenannte 3D-Secure Verfahren nutzen.

- ☑ Achten Sie beim Onlineshopping zudem auf den Einkauf in vertrauenswürdigen Shop. Diese erkennen Sie beispielsweise an bekannten Gütesiegeln – etwa dem TÜV-Zertifikat. Außerdem sollten Sie auch das Impressum kontrollieren oder – falls vorhanden – bereits bestehende Kundenbewertungen einsehen.

- ☑ Sie sollten Ihren Rechner mit Virenscannern und gegebenenfalls Firewalls vor Schadprogrammen wie Viren und Trojanern schützen. Die Virenscanner sollten immer aktuell gehalten werden, um den bestmöglichen Schutz zu garantieren.

Sie suchen nach der richtigen Kreditkarte? Dann nutzen Sie den **kostenlosen** & **unverbindlichen Kreditkarten Vergleich** von **CHECK24.**