

Informationen zur Sicherheit bei Internetzahlungen

Inhaltsverzeichnis

Einleitung	1
1 Sichere Kommunikation	1
1.1 Wie können Sie verdächtige Vorfälle oder Ähnliches melden?	1
1.2 Wie antwortet Ihnen der Lufthansa Miles & More Credit Card Service?	1
1.3 Wie setzt der Lufthansa Miles & More Credit Card Service Sie über betrügerische Transaktionen in Kenntnis oder warnt Sie vor Angriffen?	1
2 Schutz Ihrer Passwörter, Ihrer PIN und sonstiger vertraulicher Daten	2
3 Ihr Beitrag für sichere Internetzahlungen	2
3.1 Virens Scanner und Firewall	2
3.2 Das Sicherheitssystem Card Control	2
4 Risiken durch das Öffnen von Dateianhängen und Links in E-Mails	2
5 Nutzung der Original-Website des Online-Kartenkontos	3

Einleitung

Ihre Sicherheit steht bei der DKB AG an erster Stelle.

Deshalb sichern wir mit zahlreichen Funktionen Ihre Internetzahlungen und persönlichen Daten. Durch einfache Verhaltensregeln und den Schutz Ihres PCs, Tablets oder Mobiltelefons tragen auch Sie wirksam zur Sicherheit Ihrer Internetzahlungen bei.

1 Sichere Kommunikation

1.1 Wie können Sie verdächtige Vorfälle oder Ähnliches melden?

Wenn Sie verdächtige Vorgänge hinsichtlich Ihrer Kreditkarte oder unberechtigte Kartenverfügungen beobachten, bitten wir Sie, unverzüglich telefonischen Kontakt mit dem Lufthansa Miles & More Credit Card Service aufzunehmen.

Telefon & Notfallservice

Eine Nummer für alle Fragen und Anliegen. Wir unterstützen Sie bei technischen Fragen zum Online-Kartenkonto und helfen in Notfällen. Wenden Sie sich auch bei Verlust oder zum Sperren Ihrer Kreditkarte an den Lufthansa Miles & More Credit Card Service:

+49 69 667 888 700

Sie erreichen uns von Montag bis Freitag von 8:00 bis 20:00 Uhr. Den Notfallservice zur Sperrung Ihrer Karte erreichen Sie unter der gleichen Telefonnummer rund um die Uhr.

Postanschrift

Lufthansa Miles & More Credit Card Service
Postfach 2620
94016 Passau

Kartenemittentin

Deutsche Kreditbank AG
Taubenstr. 7– 9
10117 Berlin

1.2 Wie antwortet Ihnen der Lufthansa Miles & More Credit Card Service?

Weder die Deutsche Kreditbank AG (DKB AG) noch der Lufthansa Miles & More Credit Card Service oder Mastercard verwenden persönliche oder sicherheitsrelevante Konto- bzw. Kartendetails wie z. B. die Kartennummer oder die Kartenprüfnummer (CVC) in der Kommunikation mit Ihnen.

Zum Schutz der Kreditkartennummer verfügt die Lufthansa Miles & More Credit Card zusätzlich über eine Servicekartennummer. Diese wird in allen kartenbezogenen Services eingesetzt, sodass die Kreditkartennummer ausschließlich für Zahlungsvorgänge verwendet wird. Die Servicekartennummer finden Sie unterhalb des Namens auf Ihrer Kreditkarte.

Je nach Wunsch oder Dringlichkeit Ihrer Anfrage kontaktieren wir Sie per E-Mail unter dem Absender service@lufthansacard.de, in Ihrem Online-Kartenkonto, telefonisch oder schriftlich per Brief. Jede Nachricht im Namen von der DKB AG, der Miles & More GmbH oder Lufthansa, die in Bezug auf die sichere Nutzung der Internetzahlungsdienste der Kreditkarte über andere Wege versandt wird, ist nicht zuverlässig. Bitte kontaktieren Sie in Zweifelsfällen den Lufthansa Credit Card Service.

1.3 Wie setzt der Lufthansa Miles & More Credit Card Service Sie über betrügerische Transaktionen in Kenntnis oder warnt Sie vor Angriffen?

Über betrügerische Transaktionen werden Sie von unserer Präventionsabteilung telefonisch oder schriftlich informiert, ggf. im Rahmen eines notwendigen Kartenaustauschs.

Allgemeine aktuelle Sicherheitsinformationen finden Sie auf unserer Homepage unter miles-and-more-kreditkarte.com/sicherheit.

Mit den Card Control Funktionen Ihrer Kreditkarte bieten wir Ihnen außerdem unverzügliche Kontrolle und Steuerung Ihrer Kreditkartenumsätze (siehe Kap. 3.2).

2 Schutz Ihrer Passwörter, Ihrer PIN und sonstiger vertraulicher Daten

Sie haben dafür Sorge zu tragen, dass keine andere Person Kenntnis von Ihren Zugangsdaten und Ihrer PIN erhält. Insbesondere ist Folgendes zur Geheimhaltung der Zugangsdaten und der PIN zu beachten:

- Öffnen Sie alle Karten- und PIN-Briefe nur persönlich (der Lufthansa Miles & More Credit Card Service versendet alle Briefe ausschließlich an den jeweiligen Karteninhaber).
- Prägen Sie sich die PIN-Nummern ein und vernichten Sie anschließend die Briefe. Notieren Sie sich niemals die PIN, insbesondere nicht auf der Karte, in Notizbüchern oder in Ihrem Adressbuch, auch nicht als Telefonnummer getarnt.
- Im Rahmen einer Internetzahlung dürfen ausschließlich folgende Karteninformationen abgefragt werden:
 - a) Kreditkartennummer
 - b) Vorname und Name des Karteninhabers
 - c) Ablaufdatum der Karte
 - d) Kartenprüfnummer (CVC)
 - e) Evtl. TAN für Mastercard® SecureCode™
- Informieren Sie uns bitte umgehend, wenn Umschläge offen oder beschädigt sind oder Abdeckungen der PIN verletzt sind oder die PIN bei Öffnung des Briefes bereits sichtbar ist.
- Geben Sie niemals Karten, Passwörter und PIN außerhalb des Bezahlvorgangs an Dritte weiter. Kein Mitarbeiter des Lufthansa Miles & More Credit Card Service wird Sie jemals danach fragen, weder am Telefon noch per E-Mail.
- Es ist niemand berechtigt, Sie nach Passwörtern oder Ihrer PIN zu fragen, weder Amtspersonen wie Polizeibeamte noch Mitarbeiter von Kreditinstituten.
- Schirmen Sie bei der Eingabe Ihrer PIN die Tastatur so ab, dass Dritte Ihre PIN nicht ausspähen können. Fordern Sie aufdringliche Personen bzw. angebliche Helfer auf, Distanz zu halten.
- Speichern Sie Ihre Zugangsdaten nie elektronisch (z. B. auf Ihrem Handy oder Computer) ab.

3 Ihr Beitrag für sichere Internetzahlungen

3.1 Virens Scanner und Firewall

Setzen Sie immer einen aktuellen Virens Scanner ein, um Ihren Computer vor Viren, Trojanern und Würmern in empfangenen oder vorhandenen Daten zu schützen. Überprüfen Sie Ihren Computer laufend mit einer aktuellen Antivirensoftware wie z. B. „G Data InternetSecurity“. Nutzen Sie unbedingt die automatische Update-Funktion des Virenprogramms. Lassen Sie regelmäßig Ihren gesamten Datenbestand auf Ihrem Computer durch den Virens Scanner überprüfen.

Setzen Sie eine aktuelle Firewall ein, um unerwünschte Zugriffe aus dem Internet auf Ihren Computer und von Ihrem Computer ins Internet zu unterbinden. Nutzen Sie hierbei ebenfalls unbedingt die automatischen Update-Funktionen.

Beide Formen von Sicherheitssoftware sind auch in kostenlosen Versionen verfügbar. Achten Sie bei der Beschaffung auf vertrauenswürdige Quellen.

Falls Sie mobile Geräte nutzen, setzen Sie auch hier einen Antiviren-Scanner speziell für mobile Geräte ein und achten Sie darauf, dass dieser regelmäßig aktuelle Updates erhält.

3.2 Das Sicherheitssystem Card Control

Mit den Card Control Funktionen bieten wir Ihnen mehr Sicherheit und die Möglichkeit der unverzüglichen Kontrolle und Steuerung Ihrer Kreditkartenumsätze. Außerdem teilen wir Ihnen mit jeder Card Control Benachrichtigung Ihren aktuellen Verfügungsrahmen mit. Die individuellen Einstellungen nehmen Sie in Ihrem Online-Kartenkonto im Bereich Service – Meine Karten vor.

Card Control Benachrichtigungsservice

- Kostenlos und automatisch per E-Mail bei Umsätzen ab 500 Euro
- Kostenlos auf Wunsch per E-Mail bei Umsätzen ab 100 Euro
- Kostenlos per SMS für Umsätze ab 500 Euro. Für SMS-Benachrichtigungen über Umsätze ab 100 Euro fällt eine geringe SMS-Pauschale an.
- Mit der Benachrichtigungsfunktion erhalten Sie bei jeder Umsatzanfrage über den von Ihnen definierten Betrag und der jeweils ersten Umsatzanfrage nach einem Länderwechsel eine Benachrichtigung per SMS oder E-Mail. Bei Onlinezahlungen entfällt die Umsatzbenachrichtigung bei Länderwechsel.
- Optional im Inland und/oder Ausland auch über Beträge, die zur Reservierung dienen (z. B. beim Einchecken im Hotel), auch bei ausländischen Netzbetreibern.

Sollten Sie einen Umsatz bemerken, der nicht durch Sie veranlasst wurde, können Sie den Vorgang telefonisch bei uns überprüfen lassen: +49 69 667 888 800. So brauchen Sie nicht erst Ihre Kreditkartenabrechnung abzuwarten und sparen wertvolle Zeit.

Card Control Umsatzsteuerung

Folgende Einstellungen können Sie für den Einsatz Ihrer Lufthansa Miles & More Credit Card wählen:

- Länder, in denen (keine) Umsatzanfragen genehmigt werden sollen
- Ausschluss oder Begrenzung von Umsätzen per Internet und Telefon
- Ausschluss von Umsätzen im Einzelhandel
- Ausschluss von Abhebungen am Geldautomaten

4 Risiken durch das Öffnen von Dateianhängen und Links in E-Mails

Öffnen Sie zu keiner Zeit E-Mails oder Dateianhänge von Absendern, die Ihnen nicht bekannt sind. Achten Sie darauf, dass Sie den Spam-Filter in Ihrem E-Mail-Programm aktiviert haben.

Bei E-Mails gilt grundsätzlich: Weder die DKB AG noch Lufthansa, die Miles & More GmbH oder Mastercard fragen persönliche oder sicherheitsrelevante Konto- bzw. Kartendetails per E-Mail bei Ihnen ab. Sollte dies der Fall sein, handelt es sich mit großer Wahrscheinlichkeit um eine sogenannte Phishing-Mail, bei der versucht wird, an Ihre persönlichen Daten oder Passwörter zu gelangen. Sollten Sie vermuten, dass Sie eine betrügerische E-Mail empfangen haben, dann beachten Sie bitte Folgendes:

- Antworten Sie nicht und übermitteln Sie keinesfalls Ihre Daten.
- Öffnen Sie niemals Dateianhänge oder angegebene Hyperlinks zu Websites, wenn Sie den Absender nicht eindeutig als seriös identifizieren können, da sich sonst möglicherweise ein Trojaner auf Ihrem PC installiert.
- Bei E-Mails, in denen Sie aus Aktualisierungs- oder sonstigen Gründen zur Bereinigung oder Überprüfung Ihrer Kartendaten gebeten werden, benachrichtigen Sie uns bitte umgehend tele-

fonisch unter +49 69 667 888 700.

- Löschen Sie anschließend ggf. nach Absprache die E-Mail (auch aus dem Papierkorb).
- Sollten Sie bereits persönliche Daten weitergegeben haben, nehmen Sie bitte umgehend Kontakt zu uns auf. Überprüfen Sie Ihren Computer mit einer aktuellen Antivirensoftware.

5 Nutzung der Original-Website des Online-Kartenkontos

Achten Sie darauf, dass die technische Verbindung zum Online-Kartenkonto nur über die Internetseite der Lufthansa Miles & More Credit Card auf <https://www.miles-and-more-kreditkarte.com> oder <https://www.miles-and-more.kartenabrechnung.de> erfolgt.

Für den sicheren Datentransfer mit Ihnen nutzen wir eine SSL-Verschlüsselung, die den Missbrauch von Daten oder Datendiebstahl verhindert. SSL steht für Secure Socket Layer (dt.: sichere Sockelschicht) und wurde von der Firma Netscape und von RSA Data Security entwickelt. Der Browser stellt mittels des SSL-Protokolls eine gesicherte Verbindung her, verhindert ungewolltes Lesen oder Manipulieren der übertragenen Daten und stellt die eindeutige Identität einer Internetseite sicher. Dieses Verfahren wird von allen gängigen Browsern (z. B. Firefox, Internet Explorer, Safari oder Opera) unterstützt. Eine SSL-verschlüsselte Verbindung erkennen Sie unter anderem daran, dass in der Adressleiste Ihres Browsers der Link der Seite mit „https“ statt mit „http“ beginnt, bzw. am Schlosssymbol in der Adresszeile oder in der Fußzeile.

Anhand des geschlossenen Sicherheitsschlusses rechts neben der grünen Domainanzeige erkennen Sie, dass Ihre Daten verschlüsselt übertragen werden. Mit einem Klick auf das Schlosssymbol können Sie die Echtheit des Kommunikationspartners überprüfen. Ist das Schloss einmal geöffnet oder das **Zertifikat nicht aufgelistet**, sollten Sie keine sicherheitsrelevanten Daten eingeben. Sollte der grüne Bereich nicht grün dargestellt werden, wurde keine vertrauenswürdige Verbindung aufgebaut. Brechen Sie die Verbindung bitte sofort ab.