DKB Deutsche Kreditbank AG

Hinweise zur sicheren Nutzung des Internet-Banking und der Kreditkarten

Inhaltsverzeichnis

Einleitung

Ihre Sicherheit steht bei der DKB AG an erster Stelle.

Diese Kundeninformation gibt Ihnen einen Überblick über den sicheren Umgang mit Ihren persönlichen Daten und einfache Verhaltensregeln, die zur Sicherheit Ihrer Bankgeschäfte beitragen. Sie zeigt zudem, welche Leistungen die DKB für Ihre Sicherheit erbringt.

Ergänzt wird diese Broschüre durch die Allgemeinen Geschäftsbedingungen der DKB AG, die Girokartenbedingungen, die Kreditkarten-bedingungen für MasterCard und Visa Karten, die Bedingungen für Wertpapiergeschäfte, sowie die Bedingungen für DKB-Onlinebanking, die Bedingungen für Zahlungen mittels Lastschrift im Einzugsermächtigungsverfahren, die Bedingungen für den Überweisungsverkehr, Bedingungen für Zahlungen im SEPA-Firmen-Lastschriftverfahren und die Bedingungen für Zahlungen im SEPA-Basis-Lastschriftverfahren. Diese stehen im Internet auf www.DKB.de in der Form zur Verfügung, dass ein Download und eine Speicherung und/oder ein Ausdruck möglich sind.

Alle Angaben wurden sorgfältig ermittelt, für Richtigkeit und Vollständigkeit kann jedoch keine Gewähr übernommen werden.

1 Ihr Beitrag für sicheres Internet-Banking

Durch einfache Verhaltensregeln und den Schutz Ihres PCs, Tablets oder Mobiltelefons tragen Sie einfach und wirksam zur Sicherheit Ihrer Bankgeschäfte bei.

Achten Sie darauf, dass die technische Verbindung zum Onlinebanking der DKB AG nur über die Internetseite der DKB AG (www.DKB.de) erfolgt.

Stellen Sie sicher, dass keine andere Person Kenntnis oder Besitz von den personalisierten Sicherheitsmerkmalen und den Authentifizierungsinstrumenten (z. B. TAN oder Nutzungscode für die elektronische Signatur) erlangt. Jede Person, die die personalisierten Sicherheitsmerkmale kennt, hat die Möglichkeit, das Leistungsangebot des Onlinebankings einschließlich der dem Nutzer eingeräumten sonstigen Anwendungen missbräuchlich zu nutzen. So vermeiden Sie, dass z. B. Aufträge zu Lasten des Kontos/Depots erteilt werden.

Bei der DKB AG haben Sie die Möglichkeit Ihren Anmeldenamen und die PIN für Ihr Internet-Banking zu ändern. Erneuern Sie diese Zugangsdaten regelmäßig.

Folgendes bitten wir zur Geheimhaltung der personalisierten Sicherheitsmerkmale sowie der Authentifizierungsinstrumente zu beachten:

- Die personalisierten Sicherheitsmerkmale dürfen nicht elektronisch gespeichert werden.
- Die dem Nutzer zur Verfügung gestellten Authentifizierungsinstrumente (bspw. TAN) sind sicher und getrennt von den personalisierten Sicherheitsmerkmalen zu verwahren.
- Bei der Eingabe der personalisierten Sicherheitsmerkmale ist sicherzustellen, dass Dritte diese nicht ausspähen können.
- Der Nutzer muss jeweils nur eine TAN zur Autorisierung z. B. eines Auftrags, der Aufhebung einer Sperre oder zur Freischaltung einer neuen TAN-Liste verwenden.
- Personalisierte Sicherheitsmerkmale dürfen nicht außerhalb des Onlinebanking-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.
- Personalisierte Sicherheitsmerkmale dürfen nur auf den Internetseiten der DKB AG oder ihrer Kooperationspartner (z. B. SOFORT AG) gemäß Preis- und Leistungsverzeichnis der DKB AG oder den gesondert vereinbarten Internetseiten eingegeben werden.
- Das Gerät, mit dem eine TAN per SMS empfangen wird (z. B. Mobiltelefon), darf nicht für das Onlinebanking genutzt werden.

- Die Chipkarte mit Signaturfunktion ist nach Beendigung der Onlinebanking-Nutzung aus dem Lesegerät zu entnehmen und sicher und getrennt von der PIN zu verwahren.

Es kommt immer wieder vor, dass betrügerische Organisationen mittels sog. „Phishing-E-Mails“ versuchen Ihre persönlichen Daten auszuspähen. Beim Phishing wird versucht, über gefälschte E-Mails, Webseiten oder auch Kurznachrichten an Ihre persönlichen Daten wie z. B. Login-Daten oder Kreditkarteninformationen zu gelangen.

Hier gilt: Weder die DKB AG, noch Visa, MasterCard oder die Kooperationspartner der DKB fragen persönliche oder sicherheitsrelevante Konto- bzw. Kartendetails per E-Mail bei Ihnen ab.

Weitere Verhaltensregeln zum einfachen und wirksamen Schutz Ihrer Bankgeschäfte finden Sie unter https://www.DKB.de/kundenservice/sicherheit/.

2 Ihr Beitrag zum sicheren Umgang mit Karten

Durch einfache Regeln können Sie Ihren Sorgfalts- und Mitwirkungspflichten als Karteninhaber nachkommen:

(1) Unterschrift
Unterschreiben Sie als Karteninhaber nach Erhalt der Kreditkarte unverzüglich auf dem Unterschriftenfeld.

(2) Sorgfältige Aufbewahrung der Kreditkarte
Ihre Kreditkarte ist mit besonderer Sorgfalt aufzubewahren, um zu verhindern, dass sie abhanden kommt und missbräuchlich verwendet wird. Bewahren Sie diese nie unbeaufsichtigt – beispielsweise nicht im Fahrzeug – auf. Sorgen Sie dafür dass die Kartennummer, das Ablaufdatum und die rückseitig aufgetragene dreistellige Prüfziffer vor einem Zugriff von unberechtigten Dritten geschützt sind.

(3) Geheimhaltung der persönlichen Geheimzahl (PIN)
Der Karteninhaber hat dafür Sorge zu tragen, dass keine andere Person Kenntnis von seiner PIN erlangt und die PIN nie auf der Kreditkarte vermerkt oder in anderer Weise zusammen mit dieser aufbewahrt wird. Beachten Sie, dass jede Person, die die PIN kennt und in den Besitz der Kreditkarte kommt, die Möglichkeit hat, zusammen mit der PIN und Kreditkarte missbräuchliche Kartenverfügungen zu tätigen. Öffnen Sie alle Karten- und PIN-Briefe daher nur persönlich. Die DKB AG versendet alle Briefe ausschließlich an den jeweiligen Karteninhaber.

(4) Unterrichtungs- und Anzeigepflichten des Karteninhabers
Sobald Sie den Verlust, Diebstahl oder die missbräuchliche Verwendung Ihrer Kreditkarte, der Kartendaten oder der PIN feststellen oder einen entsprechenden Verdacht haben, nehmen Sie umgehend Kontakt mit uns auf (Sperranzeige).

(5) Sicher an Terminals und Automaten
Achten Sie auf die äußere Beschaffenheit von Terminal oder Automat und melden Sie auffällige Veränderungen sofort der Polizei. Schirmen Sie bei der Eingabe der PIN die Tastatur so ab, dass Dritte Ihre PIN nicht ausspähen können. Fordern Sie aufdringliche Personen bzw. angebliche Helfer auf, Distanz zu halten.

Weitere wichtige Verhaltensregeln zum sicheren Einsatz mit Karten finden Sie unter https://www.DKB.de/kundenservice/sicherheit/.

Sie haben eine Lufthansa Miles & More Kreditkarte?

Zur Anmeldung im Online-Kartenkonto Ihrer Miles & More Kreditkarte erhalten Sie einen Registrierungscode, um sich als berechtigter Nutzer des Online-Kartenkontos auszuweisen. Bei erstmaliger erfolgreicher Anmeldung zum Online-Kartenkonto wird Ihnen ein Benutzername angezeigt, den Sie jederzeit ändern können. Der Registrierungscode muss in ein persönliches Passwort geändert werden. Zur Autorisierung von Aufträgen ist die Eingabe einer einmalig gültigen Transaktionsnummer (TAN) erforderlich. Die TAN wird dem Karteninhaber jeweils per SMS an die von ihm in der Anmeldung zum SMS-TAN-Verfahren angegebene Mobilfunknummer übersandt.

3 Unsere Leistungen für Ihre Sicherheit

3.1 Für die Nutzung des Internet-Banking

Zur Abwicklung von Bankgeschäften mittels Onlinebanking erhalten Sie von der DKB AG personalisierte Sicherheitsmerkmale und Authentifizierungsinstrumente, um sich gegenüber der DKB AG als berechtigter Nutzer auszuweisen und Aufträge zu autorisieren.

Der Nutzer muss mittels Onlinebanking erteilte Aufträge (z. B. Überweisungen) zu deren Wirksamkeit mit dem personalisierten Sicherheitsmerkmal (TAN oder Nutzungscode für die elektronische Signatur) autorisieren und der DKB AG mittels Onlinebanking übermitteln. Die DKB AG bestätigt mittels Onlinebanking den Eingang des Auftrags.

Die DKB AG wird den Auftrag ausführen, wenn die notwendigen Ausführungsbedingungen erfüllt sind und kein Verdacht auf betrügerische Verwendung besteht. Sie werden über die Nichtausführung informiert.

Für das pushTAN-Verfahren benötigen Sie die DKB-pushTAN-App sowie ein Smartphone oder Tablet. Zur Nutzung des chipTAN-Verfahrens müssen Ihnen ein TAN-Generator und Ihre DKB-Girokarte vorliegen. Weitere Informationen zu beiden Verfahren finden sich unter www.DKB.de/TAN-Verfahren.

3.2 Für den Karteneinsatz

Allgemeines

Mit dem Einsatz Ihrer Giro- oder Kreditkarte erteilen Sie als Karteninhaber die Zustimmung bzw. Autorisierung zur Ausführung eines Zahlungsauftrages. Hierzu ist/sind entweder
- ein Beleg zu unterschreiben, auf den die Kartendaten übertragen wurden oder
- an Geldautomaten, bei Vertragsunternehmen sowie an automatisierten Kassen die PIN einzugeben oder
- die kontaktlose Bezahlfunktion Visa payWave/MasterCard PayPass zu nutzen, sofern diese Funktion auf der Kreditkarte vorhanden ist. Die Kreditkarte wird hierbei vor das Empfangsgerät des Vertragshändlers gehalten oder
- gegenüber Vertragsunternehmen die geforderten Kartendaten z. B. im Internet oder außerhalb dem Onlinebanking anzugeben. Dabei sind die gegebenenfalls von der DKB AG und/oder dem Vertragsunternehmen angebotenen besonderen Authentifizierungsverfahren zu nutzen.

Zahlungen im Internet

Mit der Eingabe Ihrer Kreditkartennummer im Internet bestätigen Sie Ihre Bereitschaft, die Kreditkarte auch für Zahlungen im Internet verwenden zu können.

Bei Nutzung Ihrer Kreditkarte dürfen Sie zur Autorisierung Ihres Zahlungsauftrages über elektronische Netze, wie z. B. das Internet, lediglich
- die Kartenmarke (Visa, MasterCard),
- den Namen des Karteninhabers,
- die Kartennummer,
- die Gültigkeitsdauer der Karte, und
- die rückseitig aufgetragene dreistellige Prüfziffer

angeben, **aber niemals die PIN**.

Die Kartenprüfnummer finden Sie auf der Rückseite Ihrer Karte im Unterschriftsfeld. Wir prüfen bei entsprechender Abfrage die Nummer im Rahmen Ihrer Internet-Zahlung und stellen fest, wenn diese bei einem Einkauf falsch eingegeben wird.

Von vielen Unternehmen wird die Nutzung eines zusätzlichen Sicherheitsverfahrens erwartet, um einen entsprechenden Umsatz zu authentifizieren. Wir bieten Ihnen für das Bezahlen Ihres Online-Einkaufs drei geprüfte Sicherheitsverfahren, die das persönliche Risiko auf ein Minimum reduzieren:
- Verified by VISA
- MasterCard® SecureCodeTM
- giropay

Bei Verified by Visa und MasterCard® SecureCode™ werden die Karteninhaberdaten durch ein individuelles Passwort geschützt. Solange nur Ihnen das Passwort bekannt ist, wird niemand sonst in der Lage sein, Ihre Karte bei den registrierten Online-Händlern einzusetzen. Beim Bezahlverfahren giropay nutzen Sie das sichere Internet-Banking der DKB.

Nach der Autorisierung können Sie den Zahlungsauftrag nicht mehr widerrufen. Soweit für die Autorisierung zusätzlich eine PIN oder die Unterschrift erforderlich ist, erfolgt die Autorisierung erst mit Karteneinsatz.

4 Sichere Nutzung der Hard- und Software

Sie haben sich stets Gewissheit über die Aktualität und Sicherheit der von Ihnen benutzten Technik und Software zu verschaffen und Risiken wie z. B. Computerviren oder Trojaner im Rahmen des Möglichen, z. B. durch die Installation und Aktualisierung eines handelsüblichen Virenschutzprogramms, einer Firewall und der regelmäßigen Sicherheits-Updates für den von Ihnen verwendeten Browser, auszuschließen.

Bei jedem Login in das Internet-Banking empfehlen wir Ihnen das Sicherheitszertifikat zu überprüfen, um sicherzustellen, dass Ihr Computer auch tatsächlich mit der DKB AG kommuniziert.

Prüfen Sie als Nutzer alle eingegebenen Daten auf Vollständigkeit und Richtigkeit. Soweit die DKB AG Ihnen als Nutzer Daten aus einem Onlinebanking-Auftrag wie z. B. Betrag und Kontonummer des Zahlungsempfängers im Kundensystem zur Bestätigung anzeigt, sind Sie verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

Weitere zu beachtende Sicherheitshinweise können Sie jederzeit über die Internetseiten der DKB AG unter folgendem Link abrufen: https://www.DKB.de/kundenservice/sicherheit/internet_banking.html.

5 Verlust oder Diebstahl von persönlichen Daten

Im Rahmen der Nutzung des Internet-Banking

Haben Sie den Verdacht, dass eine andere Person unberechtigt von Ihren personalisierten Sicherheitsmerkmalen oder von einem Authentifizierungsinstrument wie TAN oder von beidem Kenntnis erhalten hat oder besteht der Verdacht ihrer missbräuchlichen Nutzung, so sind Sie verpflichtet, unverzüglich die DKB AG hierüber zu unterrichten. Die DKB AG wird zunächst – zu Ihrer eigenen Sicherheit – Ihren Onlinebanking-Zugang sperren.

Zeigen Sie den Diebstahl oder Missbrauch unverzüglich bei der Polizei an.

Im Rahmen des Einsatzes von Giro- oder Kreditkarten

Stellen Sie als Karteninhaber den Verlust, Diebstahl oder die missbräuchliche Verwendung Ihrer Kreditkarte bzw. der Kartendaten fest, oder haben Sie den entsprechenden Verdacht, sind Sie verpflichtet, dies gegenüber der DKB AG umgehend anzuzeigen.

Stellen Sie beispielsweise eine nicht autorisierte oder fehlerhaft ausgeführte Kartenverfügung fest, haben Sie die DKB AG schnellstmöglich zu unterrichten und dabei die Details der beanstandeten Kreditkartenumsätze in Textform mitzuteilen. Sollte sich Ihre als verloren oder gestohlen gemeldete Kreditkarte wieder anfinden, darf diese nicht mehr eingesetzt werden.

Haben Sie den Verdacht, dass eine andere Person unberechtigt von Ihrem Passwort für das Online-Kartenkonto und/oder der auf das Mobiltelefon übersandten TAN Kenntnis erhalten hat, oder besteht der Verdacht einer missbräuchlichen Nutzung oder stellen Sie die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung Ihres Online-Kartenkontos oder einer TAN fest, so sind Sie verpflichtet, unverzüglich die DKB AG hierüber zu unterrichten. Die DKB AG wird – zu Ihrer eigenen Sicherheit – Ihre Kreditkarte sperren.

Zeigen Sie jeden Diebstahl oder Missbrauch unverzüglich bei der Polizei an.

6 Haftung hinsichtlich der Nutzung des Internetzahlungsdienstes

Als Internetzahlungsdienste gelten die Ausführung von Kartenzahlungen im Internet sowie die Durchführung von Überweisungen im Internet.

Wenn ein Umsatz nicht von Ihnen getätigt wurde, helfen wir gerne. Bitte beachten Sie hierbei folgende Regelungen hinsichtlich der Haftung:

6.1 Haftung bei nicht autorisierten und nicht oder fehlerhaft ausgeführten Onlinebanking-Verfügungen:

Die Haftung der DKB AG bei nicht autorisierten und nicht oder fehlerhaft ausgeführten Onlinebanking-Verfügungen richtet sich nach den für den jeweiligen Geschäftsvorfall vereinbarten Bedingungen (z. B. Bedingungen für den Überweisungsverkehr).

6.2 Haftung des Kunden bei missbräuchlicher Nutzung seines Authentifizierungsinstrumentes (z. B. TAN)

Im Rahmen der Nutzung des Internet-Banking

1. Haftung des Kunden für nicht autorisierte Zahlungsvorgänge vor der Verdachts- oder Sperranzeige

(1) Gesetzliche Bestimmungen (§ 675v Absatz 1 BGB) sehen eine verschuldensunabhängige Haftung des Kunden für Schäden bis zu einem Betrag von 150 Euro vor, wenn ein nicht autorisierter Zahlungsvorgang vor der Sperranzeige auf der Nutzung eines verlorengegangenen, gestohlenen oder sonst abhanden gekommenen Authentifizierungsinstruments beruht. Dies gilt auch für sonstige missbräuchliche Verwendungen eines Authentifizierungsinstruments, wenn der Nutzer die personalisierten Sicherheitsmerkmale nicht sicher aufbewahrt hat. Die DKB AG verzichtet allerdings auf eine Inanspruchnahme des Kunden, der ein Verbraucher ist, nach diesen gesetzlichen Bestimmungen.

Abweichungen zu dieser Regelung für Kunden, die keine Verbraucher sind, können in den Kreditkartenbedingungen für die DKB-VISA-Business-Card nachgelesen werden.

(2) Kommt es vor der Verdachts- oder Sperranzeige zu einer nicht autorisierten Verfügung und hat der Nutzer seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Kunde den hierdurch entstandenen Schaden in vollem Umfang, sofern nicht die Voraussetzungen des Absatzes 3 vorliegen. Grobe Fahrlässigkeit des Nutzers kann insbesondere vorliegen, wenn er
- den Verlust oder Diebstahl des Authentifizierungsinstruments oder die missbräuchliche Nutzung des Authentifizierungsinstruments
- oder des personalisierten Sicherheitsmerkmals der DKB AG nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat,
- das personalisierte Sicherheitsmerkmal elektronisch gespeichert hat,
- das personalisierte Sicherheitsmerkmal außerhalb des Onlinebanking-Verfahrens, beispielsweise per E-Mail, weitergegeben hat,
- das personalisierte Sicherheitsmerkmal einer anderen Person mitgeteilt und der Missbrauch dadurch verursacht wurde,
- das personalisierte Sicherheitsmerkmal auf dem Authentifizierungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (z. B. im Originalbrief, in dem es dem Nutzer mitgeteilt wurde),
- mehr als eine TAN zur Autorisierung eines Auftrags verwendet.

(3) Die DKB AG garantiert hiermit zugunsten des Kunden, der ein Verbraucher ist, die Übernahme des vollen Schadens. Detaillierte Bestimmungen/Informationen können den Bedingungen für das Onlinebanking entnommen werden.

2. Haftung der DKB AG ab der Verdachts- oder Sperranzeige

Sobald der DKB AG
- die Kenntniserlangung des personalisierten Sicherheitsmerkmals oder die Besitzerlangung des Authentifizierungsinstruments durch andere Personen oder
- der Verlust oder Diebstahl des Authentifizierungsinstruments der die missbräuchliche Nutzung des personalisierten Sicherheitsmerkmals oder des Authentifizierungsinstruments angezeigt wurde, übernimmt die DKB AG alle nach dem Zeitpunkt des Zugangs der Verdachts- oder Sperranzeige durch nicht vom Nutzer autorisierte Onlinebanking-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Nutzer in betrügerischer Absicht gehandelt hat.

3. Haftungsausschluss

Haftungsansprüche sind ausgeschlossen, wenn die einen Anspruch begründenden Umstände
- auf einem ungewöhnlichen und unvorhersehbaren Ereignis beruhen, auf das diejenige Partei, die sich auf dieses Ereignis beruft, keinen Einfluss hat, und dessen Folgen trotz Anwendung der gebotenen Sorgfalt von ihr nicht hätten vermieden werden können, oder
- von der DKB AG aufgrund einer gesetzlichen Verpflichtung herbeigeführt wurden.

DKB Deutsche Kreditbank AG

Im Rahmen des Einsatzes von Giro- oder Kreditkarten

1. Haftung des Karteninhabers bis zur Sperranzeige

Verlieren Sie Ihre Kreditkarte oder PIN oder wird Sie Ihnen gestohlen oder kommen Kreditkarte und/oder PIN Ihnen in sonstiger Weise abhanden und kommt es dadurch zu einer nicht durch Sie autorisierten Kartenverfügung, so haftet der Karteninhaber für Schäden, die bis zum Zeitpunkt der Sperranzeige verursacht werden, in Höhe von maximal 50 Euro, ohne dass es darauf ankommt, ob den Karteninhaber an dem Verlust oder Diebstahl ein Verschulden trifft. (Ausnahme: Vorsatz oder grobe Fahrlässigkeit)

Kommt es vor der Sperranzeige zu einer nicht autorisierten Kartenverfügung, ohne dass ein Verlust oder Diebstahl der Kreditkarte oder PIN vorliegt, haften Sie für die hierdurch entstandenen Schäden bis zu einem Betrag von maximal 50 Euro, wenn der Schaden darauf beruht, dass der Karteninhaber seine Pflicht zur sicheren Aufbewahrung der Kreditkarte oder PIN fahrlässig verletzt hat. (Ausnahme: Vorsatz oder grobe Fahrlässigkeit)

Kommt es vor der Sperranzeige zu einer nicht autorisierten Kartenverfügung und hat der Karteninhaber seine Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Karteninhaber den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Karteninhabers kann insbesondere dann vorliegen, wenn:

- er den Verlust, den Diebstahl oder die missbräuchliche Kartenverfügung der DKB AG schuldhaft nicht unverzüglich mitgeteilt hat,
- die PIN auf der Kreditkarte vermerkt oder zusammen mit der Kreditkarte verwahrt war oder
- die PIN einer anderen Person mitgeteilt und der Missbrauch dadurch verursacht wurde.

2. Haftung des Karteninhabers ab Sperranzeige

Sobald der DKB AG der Verlust oder Diebstahl der Kreditkarte, die missbräuchliche Verwendung oder eine sonstige nicht autorisierte Nutzung von Kreditkarte und/oder PIN angezeigt wurde, übernimmt die DKB AG alle danach durch Kartenverfügungen entstehenden Schäden. (Ausnahme: Vorsatz oder grobe Fahrlässigkeit)