DONNER & REUSCHEL

PRIVATBANK SEIT 1798

KUNDENINFORMATIONEN

SICHERHEIT IM ONLINE-BANKING

» Ihre Sicherheit liegt uns am Herzen. «

DONNER & REUSCHEL
PRIVATBANK SEIT 1798

INHALT (KLICK AUF EIN THEMA BRINGT SIE ZUR JEWEILIGEN SEITE)

IHRE SICHERHEIT – FÜR ALLE ONLINE-BANKING UND BROKERAGE-TRANSAKTIONEN

DONNER & REUSCHEL
Aktiengesellschaft

Friedrichstraße 18
80801 München

Ballindamm 27 / Hermannstraße 13,
20095 Hamburg

www.donner-reuschel.de
bankhaus@donner-reuschel.de

Telefon Hamburg: 040 30217-0
Telefon München: 089 2395-0

IHRE SICHERHEIT – FÜR ALLE ONLINE-BANKING UND BROKERAGE-TRANSAKTIONEN

Das Bankhaus DONNER & REUSCHEL setzt auf modernste Sicherheits- und Verschlüsselungsverfahren, damit die im Online-Banking übermittelten Daten nicht unberechtigt eingesehen, verändert oder missbraucht werden können. Das Verfahren mit Persönlicher Identifikationsnummer (PIN) und Transaktionsnummer (TAN) ist eine bewährte Methode, mit der Sie im Online-Banking Aufträge erteilen können. Mit dem PIN-TAN-Verfahren erledigen Sie Ihre Bankgeschäfte online direkt über unsere Website auf unserer Online-Banking-Plattform. Eine eigene Software brauchen Sie dafür nicht. Das TAN-Zweischritt-Verfahren bietet den derzeit zuverlässigsten Schutz gegen Betrugsversuche: Jede generierte Transaktionsnummer (TAN) ist nur für die aktuelle Online-Transaktion gültig. Sie ist für weitere Transaktionen unbrauchbar und damit für Betrüger wertlos. DONNER & REUSCHEL bietet Ihnen mehrere TAN-Verfahren, die Sie nach optionaler Freischaltung auch parallel verwenden können. Bei jeder Transaktion entscheiden Sie in der Transaktionsmaske, welches Verfahren Sie nutzen möchten.

VR-KENNUNG UND ALIAS:

Ihre persönliche Kennung erhalten Sie von der Bank ausschließlich auf dem Postweg. Sie ist eine individuelle Kennung, die nicht auf Konto- oder Depotauszügen kommuniziert wird. Dadurch wird die Sicherheit im Online-Banking weiter erhöht. Da die Kennung relativ lang ist, gibt es die Möglichkeit, sich einen individuellen Benutzernamen (Alias) zu vergeben und sich zukünftig mit diesem im Online-Banking anzumelden.

Für den Fall, dass ein unbefugter Dritter Kenntnis von Ihrem Alias erlangt hat, können Sie diesen im Online-Banking unter **Service → Zugangsdaten** ändern. Sollte ein unbefugter Dritter Kenntnis von Ihrer Kennung haben, können Sie schriftlich eine neue Kennung bei uns anfordern.

Aus Sicherheitsgründen empfehlen wir Ihnen die Wahl eines Alias, der Buchstaben, Ziffern und Sonderzeichen enthält und für Dritte nicht einfach herzuleiten ist.

Für die Vergabe eines Alias beachten Sie bitte folgende Bedingungen:

- Länge: 7 - 35 Stellen
- Unterscheidung bei der Groß- und Kleinschreibung
- Buchstaben A-Z und a-z
- Ziffern 0 - 9
- Sonderzeichen - ! % & / = ? * + , . ; : _ @
- Alias darf nicht mit VRK beginnen
- Leerzeichen (außer am Anfang und Ende des Alias)

Sollte Ihr vorgeschlagener Alias schon vergeben sein, erhalten Sie einen Hinweis dazu und können einen neuen Alias wählen.

PERSÖNLICHE IDENTIFIKATIONSNUMMER (PIN)

Die Online-Banking-PIN schützt zusammen mit der Kennung/dem Alias den Zugang zu Ihrem persönlichen Bereich im Online-Banking und wird bei der Erstanmeldung von Ihnen vergeben. Sie muss folgende Bedingungen erfüllen:

- Alphanumerische PIN
- Länge: 8-20 Stellen
- Unterscheidung bei der Groß- und Kleinschreibung
- Verwendung mindestens eines Großbuchstabens und einer Ziffer

Erlaubte Zeichen:

- Buchstaben A-Z und a-z
- Umlaute (ä, ö, ü, Ä, Ö, Ü)
- Ziffern (0-9)
- Sonderzeichen - ! % & / = ? * + , . ; : _ @

Wichtiger Hinweis:

Speichern Sie Ihre PIN niemals auf Ihrem Computer, schreiben Sie diese auch nirgendwo auf und geben Sie die PIN keinesfalls an Dritte weiter. Wenn Sie jedoch den Verdacht haben, Ihre PIN könnte Unbefugten bekannt geworden sein, so ändern Sie diese unverzüglich im Online-Banking nach dem Log-in unter:

Service → Zugangsdaten.

Sollten Sie nicht die Möglichkeit haben, die PIN zu ändern, veranlassen Sie eine Sperre Ihres Online-Banking-Zugangs.
(Hinweise hierzu sind unter dem Punkt **Sperrmöglichkeiten** bzw. **Notfallinformationen** aufgeführt).

INDIVIDUELLE START-PIN

Die individuelle Start-PIN ist eine 8-stellige Zahlenkombination zur erstmaligen Anmeldung im Online-Banking. Auch wenn Sie Ihre PIN einmal vergessen haben sollten, benötigen Sie für die Freischaltung des Online-Bankings eine Start-PIN. Diese Start-PIN wird Ihnen separat und ausschließlich auf dem Postweg mitgeteilt. Mit der Start-PIN, der VR-Kennung und einem freigeschalteten TAN-Verfahren können Sie sich über den Button „Erstanmeldung“ auf der Online-Banking-Startseite (wieder) freischalten.

TAN-VERFAHREN

DONNER & REUSCHEL bietet Ihnen folgende TAN-Verfahren an.

mobileTAN

Mit dem mobileTAN-Verfahren können Sie bequem Ihre Transaktionen durchführen. Die TAN wird Ihnen direkt auf Ihr Mobiltelefon gesandt. Hierzu ist es notwendig, dass Sie Ihre deutsche Mobiltelefonnummer bei DONNER & REUSCHEL registrieren. Für jede Transaktion erhalten Sie eine SMS mit einer einzelnen TAN und den Transaktionsdaten zum Abgleich Ihrer Eingabe. Auch die zeitlich begrenzte Gültigkeit der an- geforderten TAN dient der Sicherheit. Wenn Sie sich erfolgreich für das mobileTAN-Verfahren registriert haben, können Sie es auch parallel zum smart TAN-Verfahren nutzen. B Beim mobileTAN- Verfahren darf das Gerät, mit dem die TAN empfangen werden, nicht gleichzeitig für das Online-Banking genutzt werden, da andernfalls bei gezielten Angriffen alle nötigen Informationen und Funktionen auf demselben Gerät vereint sind. Für die Betriebssysteme iOS (Apple) und Google Android sind im Internet Apps zu finden, mit denen der Benutzer SMS-Nachrichten von seinem Mobiltelefon auf einen Computer weiterleiten kann. Bei der Benutzung solcher Apps wäre ein Trojaner in der Lage, auf diesem Computer im Hintergrund Überweisungen durchzuführen. Wir empfehlen Ihnen, diese Funktion nicht zu nutzen. Da die Zustellung von mobileTAN SMS außerhalb von Deutschland nicht garantiert werden kann, empfehlen wir Ihnen alternativ das pushTAN Verfahren zu nutzen. Bitte beachten Sie das mobileTAN Verfahren nicht parallel mit dem pushTAN Verfahren nutzen können.

smartTAN plus

Bei dem smartTAN plus-Verfahren werden Ihre Transaktionsnummern (TAN) über einen smartTAN Generator erzeugt. Dieses Verfahren ist in Verbindung mit Ihrer girocard schnell und ortsunabhängig einsetzbar. Die jeweils angeforderte TAN wird nur für den aktuellen Vorgang generiert und kann nicht für andere Transaktionen verwendet werden. Auch die zeitlich begrenzte Gültigkeit der angeforderten TAN sowie die Bestätigungspflicht einiger transaktionsbezogener Daten dient der Sicherheit. Sofern Sie noch keinen smartTAN Generator besitzen, können Sie diesen über DONNER & REUSCHEL beziehen.

Wichtig: Um das derzeitige smartTAN-Verfahren nutzen zu können, benötigen Sie einen smartTAN Generator mit HHD-Spezifikation 1.4. Für Fragen hierzu stehen wir Ihnen gern beratend zur Verfügung.

Hinweis:
Wir weisen darauf hin, dass die girocard immer getrennt von der Online-Banking-PIN verwahrt werden sollte. Bitte bewahren Sie auch Ihre girocard und den TAN Generator getrennt voneinander auf. Dadurch reduzieren Sie das Missbrauchsrisiko erheblich.

pushTAN mit my-SecureSIGN

Mit dem push-TAN-Verfahren my-SecureSIGN empfangen Sie Transaktionsnummern (TAN) jederzeit sicher und bequem auf Ihrem Smartphone oder Tablet. Die TAN-Benachrichtigungen sind vergleichbar mit dem mobileTAN-Verfahren. Sie werden jedoch nicht per SMS versandt, sondern in der my-SecureSIGN-App angezeigt.

Wichtig:
Um das pushTAN Verfahren zu nutzen benötigen Sie ein Smartphone oder Tablet, auf dem die App installiert ist sowie eine Registrierung in der App.

Von mobileTAN auf pushTAN umstellen:

Sollten Sie bereits jetzt mobileTAN-Verfahren nutzen, so wird das mobileTAN-Verfahren automatisch deaktiviert, sobald Sie sich für my-SecureSIGN freischalten lassen. Statt einer SMS erhalten Sie die TAN nach der Umstellung ausschließlich via push-Nachricht über die my-SecureSIGN App.

Nutzung von smartTAN und pushTAN:

Wenn Sie Ihre TAN aktuell mittels TAN-Generator generieren, ist die Nutzung beider Verfahren möglich. Sobald die Freischaltung für my-SecureSIGN erfolgt ist, können Sie sich aussuchen, ob Sie die TAN per push-Nachricht über die App erhalten möchten oder wie bisher den TAN-Generator benutzen.

Sicherheit:
Bitte prüfen Sie immer in der my-SecureSIGN App die Transaktionsdaten auf Richtigkeit, wie zum Beispiel den Betrag und die IBAN des Empfängers. Die my-SecureSIGN App verwendet Sicherheitskomponenten, durch die Angriffe deutlich erschwert werden. Bitte bedenken Sie, dass wegen eines möglichen Befalls, beispielsweise durch einen Trojaner, die gleichzeitige Verwendung des Webbankings oder einer Banking App und der my-SecureSIGN App auf dem gleichen Gerät ein höheres Risiko darstellt, als die Nutzung zweier verschiedener bzw. voneinander getrennter Geräte. Für Ihre Sicherheit empfehlen wir Ihnen die App-Passwörter nicht zu speichern.

Für Fragen stehen wir Ihnen beratend zur Verfügung.

TRANSAKTIONEN ÜBER BANKING SOFTWARE (FINTS/HBCI)

Nutzen Sie eine Banking-Software (wie z. B. windata professional), gewährleistet der HBCI-Standard (Homebanking Computer Interface) eine hohe Übertragungssicherheit für Banktransaktionen per Internetverbindung über PIN/TAN oder Chip-Karte. HBCI wurde als Standard zwischen allen deutschen Kreditinstituten vereinbart und verwendet bei der Übermittlung von Daten ein allgemein anerkanntes und leistungsfähiges Signatur- und Verschlüsselungsverfahren, damit die Datenübermittlung im Internet abgesichert ist. Beim Online-Banking nach FinTS/HBCI-Standard werden die Zahlungsdaten offline erfasst und erst danach, wenn sie an die Bank übertragen werden sollen, online abgesendet.

FinTS/HBCI mit PIN und TAN

Bei dieser Variante können Sie zwischen den freigeschalteten TAN-Verfahren wählen.

Empfehlung:
Bitte speichern Sie Ihre persönliche PIN nicht auf dem Endgerät, mit dem Sie Ihre Banking-Software nutzen, da eine Schadsoftware diese auslesen könnte.

FinTS/HBCI mit elektronischer Signatur

Zu diesem Verfahren werden die Transaktionen durch eine digitale Signatur gegen unautorisierte Änderungen geschützt.

HBCI mit Chipkarte
Zur Nutzung dieses Verfahrens benötigen Sie eine HBCI/FinTS-Chipkarte, eine Finanz-Software sowie ein kompatibles Chipkartenlesegerät (Secoder), das mit Ihrem Computer verbunden wird. Zusammen mit der Chipkarte werden PIN und PUK zur Verfügung gestellt. Die PIN dient zur Freigabe von Transaktionen, die PUK zur Entsperrung bzw. Änderung der PIN. In Verbindung mit dem Kartenlesegerät und der PIN wird eine digitale Signatur erstellt und der Vorgang sicher verschlüsselt an die Bank übertragen.

Wir empfehlen Ihnen dringend:
Speichern Sie die elektronische Signaturdatei nicht auf einem Endgerät (z.B. Festplatte des Computers). Stellen Sie diese immer nur zum jeweiligen Vorgang über ein externes Medium bereit (z.B. über einen USB-Stick). Des Weiteren raten wir davon ab, die PIN bzw. das Passwort zur elektronischen Signaturdatei dauerhaft auf dem Endgerät zu speichern, da Betrüger diese unter Umständen über eine Schadsoftware auslesen könnten.

» **Weitere Informationen über FinTS/HBCI** finden Sie unter: http://www.hbci-zka.de/

DIE SICHERHEIT IHRER KARTENZAHLUNGEN

Sichere Online-Zahlungen mit 3D Secure

Die Sicherheitsverfahren **Mastercard® Secure Code™** und **Verified by Visa** sind ein von Mastercard® und Visa entwickelter Sicherheitsstandard für Kreditkartenzahlungen, der die Gefahr des Kartenmissbrauchs durch Dritte bei Zahlungen im Internet erheblich reduziert.

Sobald Sie Ihre DONNER & REUSCHEL Kreditkarte über unsere Internet-Seite https://www.donner-reuschel.de/unsere-angebote/service/3d-secure.html für 3D Secure registriert und freigeschaltet haben, profitieren Sie beim Online-Einkauf von dem zusätzlichen Schutz dieses Verfahrens. Immer mehr Händler unterstützen die Absicherung der Kauftransaktion über 3D Secure bereits in ihren Online-Shops. Als registrierter Kreditkarteninhaber können Sie zwischen den Verfahren eComTAN-App und SMS mit zusätzlicher Sicherheitsfrage wählen. Während des Online-Bezahlvorgangs mit Ihrer Kreditkarte erhalten Sie auf Ihrem Mobiltelefon eine Transaktionsnummer (E-Commerce-TAN) via Push-Nachricht oder SMS. Im Online-Shop des teilnehmenden Händlers wird Ihnen eine Eingabeseite angezeigt, auf der Sie Ihre erhaltene TAN eingeben. Während der Transaktion wird die Richtigkeit der Daten automatisch geprüft. Dieser Vorgang läuft direkt über den Server unseres Dienstleisters. Stimmen die Daten mit denen des von Ihnen beabsichtigten Kaufs überein, geben Sie die TAN in die Freigabemaske ein. Bei Nutzung des SMS-Verfahrens werden Sie außerdem gebeten, Ihre hinterlegte Sicherheitsfrage zu beantworten. Die Zahlung wird nur nach korrekter Eingabe Ihrer Sicherheitsmerkmale ausgeführt. Sollte die Nachricht mit der Bestätigung nicht die erwarteten Transaktionsdaten enthalten, geben Sie die E-Commerce-TAN nicht ein, sondern wenden Sie sich an unseren 24 Stunden am Tag erreichbaren 3D Secure-Service unter der Telefonnummer 0721 1209-66001, Auswahl 3.

Wir empfehlen Ihnen die Verwendung dieser Sicherheitsmechanismen sehr, da hiermit die Sicherheit von Kreditkarten-Zahlungen im Internet deutlich erhöht wird. Registrieren Sie sich nur einmalig mit Ihrer Mobiltelefonnummer oder entscheiden Sie sich für die eComTAN-App, um von dem hohen Sicherheitsniveau zu profitieren. So können Sie sicher sein, dass nur Sie Ihre Kreditkarte bei den teilnehmenden Händlern einsetzen. Ein Missbrauch Ihrer Kreditkarten-Daten kann so durch die Übermittlung der zur Freigabe erforderlichen E-Commerce-TAN verhindert werden.

» **Weitere Informationen zu 3D Secure** finden Sie auf unserer Website:

» **Weitere Informationen zu 3D Secure** finden Sie auf unserer Website:
https://www.donner-reuschel.de/unsere-angebote/service/3d-secure.html

» Bei **Fragen zur Aktivierung** unterstützt Sie die Service-Hotline unseres Dienstleisters:
Telefon 0721 1209 66 001 (Auswahl 3).

Sicherheitshinweis zu 3D Secure:

Per E-Mail oder Telefon wird weder DONNER & REUSCHEL noch ein Dienstleister wie Mastercard® oder VisaCard Sie jemals nach Ihren Mastercard® SecureCode™ / Verified by Visa Daten fragen oder Sie zur Registrierung bzw. Freischaltung Ihrer Karte auffordern.

ALLGEMEINE SICHERHEITSHINWEISE – DARAUF SOLLTEN SIE ACHTEN

Beachten Sie bitte:
Das Bankhaus DONNER & REUSCHEL wird Sie nie telefonisch, per E-Mail, Fax oder SMS nach Zugangsdaten, Passwörtern, PIN, TAN oder Kreditkartennummern fragen. Wir fordern Sie auch nicht auf, Links in E-Mails zu folgen oder Überweisungen zu Testzwecken auszuführen. Ignorieren Sie solche Aufforderungen, Nachrichten oder Links. Informationen, die Sie über Ihre Postbox von uns erhalten, sind sicher!

Phishing

Bitte beachten Sie, dass weltweit zunehmend Angriffe über Phishing-E-Mails verzeichnet werden. Hierbei handelt es sich um E-Mails von Trickbetrügern, mit denen die Empfänger aufgefordert werden, über ein Online-Formular persönliche und geheime Kundendaten – etwa Kontonummer, VR-Kennung, Bank-ID, PIN und TAN oder auch Kreditkarteninformationen – einzugeben. Phishing-E-Mails sind durch das professionelle Layout und die inzwischen auch sprachlich sehr gute Aufbereitung häufig täuschend echt und selbst für Experten oft nicht auf den ersten Blick zu erkennen. Die in den Phishing-E-Mails enthaltenen Links (Verknüpfungen) führen zu einer vermeintlichen Bank-Webseite, hinter der sich jedoch tatsächlich betrügerische bankfremde Webseiten verbergen.

„Trojanisches Pferd“ (auch: „Trojaner“)

Ein „Trojaner“ ist oft als nützliches Computerprogramm (bspw. zur Performance-Optimierung Ihres Computers) getarnt, das Sie im Internet kostenlos herunterladen können, welches dann aber auf Ihrem Computer Schaden anrichtet. Das Ziel vieler Trojaner ist das Ausspähen sensibler Daten wie z. B. Passwörter, PIN, TAN und das Versenden dieser Daten an die Betrüger. Über eine spezielle Trojaner-Variante (sogenannte Backdoor-Trojaner) kann ein Betrüger auf fremde Computer zugreifen und die Fernkontrolle über alle Funktionen übernehmen. So können Betrüger auch Ihre Tastatureingaben (bspw. Kennung und Passwort) beobachten und selbst verwenden.

Trojaner werden auch auf mobilen Endgeräten (Smartphones, Tablets) verstärkt festgestellt. Sie versuchen, mobile TANs abzugreifen, um das Bankkonto des Besitzers zu leeren. Die Trojaner sind insbesondere bei Geräten mit dem Betriebssystem Android festzustellen, da dort durch die Besitzer der Download von Software aus Drittquellen als Option erlaubt wird. Meist verbergen sie sich hinter vermeintlich nützlichen Programmen/Apps oder werden unter einem Vorwand unbemerkt implementiert (z.B. als notwendiges Update).

Tastatureingaben-Aufzeichnung (engl. „Keylogger“)

Ein Keylogger kann eine Hard- oder Software sein, die Tastatureingaben des Benutzers an einem Computer mitprotokolliert. Die erlangten Daten werden automatisch an den Betrüger übermittelt. Wir empfehlen Ihnen in diesem Zusammenhang, grundsätzlich keine Banking-Transaktionen oder Kartenzahlungen auf öffentlichen Rechner (bspw. Internet-Cafe) durchzuführen.

SICHERHEITSMASSNAHMEN – WIE KÖNNEN SIE IHRE SYSTEME SCHÜTZEN?

Technische Voraussetzungen

Das DONNER & REUSCHEL Online-Banking unterstützt die gängigsten Internet-Browser, wie z.B.

- **Microsoft Internet Explorer und Edge**
- **Mozilla Firefox**
- **Safari**
- **Google Chrome**

Bitte beachten Sie, dass Ihr Browser zur Nutzung des Online-Bankings temporäre Cookies zulassen und JavaScript aktiviert sein muss.

Antivirussoftware und Firewall

Zum Schutz Ihres Systems empfehlen wir Ihnen grundsätzlich den Einsatz und die Aktivierung eines Antivirenprogramms und einer Firewall. Zusätzlich können Sie Ihr System durch weitere Sicherheitsprogramme wie z. B. Anti-Spyware-Programme schützen. Alle Programme sollten immer auf dem aktuellsten Software-Stand gehalten werden.

Downloads

Eine besondere Gefahr, Computer und mobile Geräte, wie Smartphones und Tablets, mit Viren oder anderen Schadprogrammen zu infizieren, besteht bei Downloads aus dem Internet. Zu Ihrer Sicherheit empfehlen wir, ausschließlich Programme, Apps und Dateien aus sicheren und vertrauenswürdigen Quellen herunterzuladen.

E-Mail-Anhänge

Öffnen Sie keinesfalls E-Mail-Anhänge von unbekannten Absendern, aber auch bei bekannten Absendern sollten Sie vorsichtig sein. Wir empfehlen zur Sicherheit, alle E-Mail-Anhänge vor dem Öffnen mit Ihrer Antivirensoftware auf Viren zu prüfen. Hierzu ist, abhängig von der verwendeten Software, ggf. ein Zwischenspeichern der Anhänge notwendig.

Aktualisierungen (Updates)

Wir empfehlen Ihnen dringend die regelmäßige Aktualisierung Ihres Betriebssystems, Internet-Browsers und Ihrer Sicherheitssoftware wie z.B. Virenscanner, Firewall, Anti-Spyware etc. Verfügbare Aktualisierungen sollten so zeitnah wie möglich nach ihrer Bereitstellung installiert werden. Unterstützend gibt es zudem kostenlose Software, die nach Updates schaut und diese bis auf wenige Ausnahmen automatisch installiert.

Drahtlosverbindungen schützen

Sichern Sie Ihre drahtlose (Funk-)Netzwerkverbindung zuhause durch die derzeit höchste Sicherheitsstufe WPA2 und mit einem komplex gestalteten Passwort zum Aufbau der WLAN-Verbindungen. Ändern Sie in jedem Fall das mitgelieferte Standardpasswort Ihres WLAN-Routers in ein individuelles Passwort. Nutzen Sie Online-Banking-Funktionen nie in öffentlichen, unverschlüsselten Netzen (bspw. kostenlose unverschlüsselte WLANs an Flughäfen). Sämtliche Eingaben – wie zum Beispiel Ihre Benutzerkennung und Ihre PIN beim Online-Banking – lassen sich im Klartext von Dritten mitlesen!

Überprüfung der SSL-Verschlüsselung

DONNER & REUSCHEL setzt zur zusätzlichen Sicherung des Online-Bankings vor dem Hintergrund von Phishing-Angriffen ein EV (Extended-Validation)-SSL- Zertifikat ein, dessen Ausgabe an strenge Vergabekriterien gebunden ist und die derzeit stärkste Validierung von Webseiten darstellt.

In der Adresszeile des Browsers wird zusätzlich ein Feld angezeigt, in dem Zertifikats- und Domaininhaber im Wechsel mit der Zertifizierungsstelle eingeblendet werden. Zudem wird je nach verwendetem Browser die komplette Adresszeile oder ein Teil davon grün eingefärbt (sog. „Greenbar"). Prüfen Sie die Adresszeile dahingehend und stellen Sie so vor der Anmeldung zum Online-Banking sicher, dass Sie sich auf den gesicherten Online-Banking-Seiten der DONNER & REUSCHEL Aktiengesellschaft befinden. Nehmen Sie Hinweise auf etwaige Zertifikatsprobleme auf der Website ernst und führen Sie kein Online-Banking durch, falls eine solche Meldung erscheint. Es könnte sich um eine gefälschte Webseite handeln, die zwar wie die originale DONNER & REUSCHEL Webseite aussieht, aber von Betrügern geführt wird. Geben Sie keinesfalls Ihre VR-Kennung/ Alias oder Ihre PIN ein. Während der gesamten Zeit, in der Sie unser Online-Banking nutzen, muss in der Adresszeile Ihres Internetbrowsers https://banking.donner-reuschel.de angezeigt werden. Das SSL-Protokoll (Secure Socket Layer) verhindert, dass Daten von anderen gelesen oder manipuliert werden können. Die Erweiterung „s" in „https" weist hierbei auf eine mit SSL verschlüsselte Übertragung hin. Bitte achten Sie darauf, dass in Ihrem Internet-Browser das entsprechende Symbol – ein Vorhängeschloss – erscheint. Beenden Sie unverzüglich die Internetverbindung und schließen Sie Ihren Browser, falls eine der vorgenannten Bedingungen nicht zutrifft.

Getrennte, sichere Aufbewahrung von PIN und girocard

Teilen Sie grundsätzlich niemandem Ihre PIN für Ihre girocard mit. Vermeiden Sie es, die PIN schriftlich zu notieren. Falls Sie die PIN dennoch schriftlich festhalten möchten, bewahren Sie diese Unterlage nicht zusammen mit Ihrer girocard auf, mit der Sie über den smartTAN-Generator TANs erzeugen. Speichern Sie Ihre PIN unter keinen Umständen auf Ihrem Computer.

Regelmäßige PIN-Änderung für das Online-Banking

Bitte ändern Sie Ihre PIN für das Online-Banking regelmäßig. Diese Vorsichtsmaßnahme erschwert unberechtigten Personen den Online-Zugang zu Ihren Konten und Depots bei DONNER & REUSCHEL. Dabei sollten Sie keine leichten Zahlenkombinationen wie z. B. Geburtsdaten oder Telefonnummern nutzen. Verwenden Sie nur sichere und jeweils unterschiedliche Passwörter.

Persönliche Daten schützen

Schützen Sie Ihre reale und digitale Identität. Hierzu gehört ein starker Schutz Ihrer E-Mail-Konten (komplexe, ausreichend lange Passwörter verwenden, zyklisch wechseln) sowie eine ausreichende Zurückhaltung bei der Angabe von persönlichen Daten im Internet.

Mobilfunkverträge schützen

Sichern Sie alle Änderungen an Mobilfunkverträgen durch eine Passwortvergabe ab. Mobilfunkverträge, die durch ihre Nutzer nicht mit einem Passwort gegen telefonische Änderungen geschützt sind, wurden zum Ziel von betrügerischen Angriffen. Betrüger können mit Angabe von Name, Adresse und Geburtsdatum des Opfers beim Mobilfunkanbieter die Zusendung einer neuen SIM-Karte veranlassen und so Zugriff auf die SMS mit der TAN des Kontoinhabers erhalten. In Verbindung mit einer Schadsoftware (wie z. B. der Trojaner ZEUS), die auf dem Computer eingeschleust wurde, kann der Betrüger Überweisungen durchführen.

Online-Limit einrichten

Sie können bei uns ein an Ihre Bedürfnisse angepasstes Online-Limit festlegen. Wir empfehlen Ihnen, diese Möglichkeit zu nutzen, da ein individualisiertes Online-Limit zusätzliche Sicherheit im Online-Banking bietet. Gerne zeigen wir Ihnen die verschiedenen Möglichkeiten auf. Bitte wenden Sie sich hierzu an Ihren Berater.

IHRE SPERRMÖGLICHKEITEN FÜR DAS ONLINE-BANKING

Sollten Sie den Verdacht haben, dass unberechtigte Personen Kenntnis von Ihrer PIN haben bzw. in den Besitz Ihrer girocard gekommen sind, veranlassen Sie bitte eine Sperre Ihrer Karte und Ihres Online-Banking-Zugangs. Die Sperre kann anschließend nur über die Bank aufgehoben werden.

Im Bereich Online-Banking stehen Ihnen im Bereich Service/Sperren **folgende Sperrmöglichkeiten zur Verfügung:**

SB-Kontosperre

Die Sperre bezieht sich auf Verfügungen und Auskünfte an den SB-Terminals, Online-Banking, PC-Zahlungsverkehrsprogramme und Telefon-Banking. Wenn Sie als Kontoinhaber den SB-Service sperren, wird der Zugriff auf das Konto auch für sämtliche SB-Berechtigte gesperrt. Wenn Sie als Bevollmächtigter die Sperre veranlassen, bezieht sich diese nur auf Ihren eigenen Kontenzugriff. Die Sperre kann nur durch die Bank aufgehoben werden.

SB-Verfügungssperre

Nach Einrichtung einer SB-Verfügungssperre kann der Kontoberechtigte für das ausgewählte Konto keine Verfügung mehr tätigen. Wenn der Kontoinhaber sich selbst sperrt, sind sämtliche SB-Berechtigte dieses Kontos ebenfalls für SB-Verfügungen gesperrt. Die Berechtigung für SB-Auskünfte bleibt in jedem Fall bestehen. Der Kontoinhaber kann die Sperre eines Bevollmächtigten wieder aufheben. Eine Sperre des Kontoinhabers kann nur die Bank aufheben. Ihre Online-Banking-Sitzung wird nach Durchführung der Sperre automatisch abgemeldet.

SB-Zugangssperre

Diese Sperre bezieht sich auf Verfügungen und Auskünfte des angemeldeten Nutzers im Online-Banking, in den Zahlungsverkehrsprogrammen und im Telefon-Banking. Die Funktionen am SB-Terminal können weiter genutzt werden. Andere SB-Berechtigte haben weiter Zugriff auf Ihre Konten. Die SB-Zugangssperre kann nur durch die Bank wieder aufgehoben werden. Ihre Online-Banking-Sitzung wird nach Durchführung der Sperre automatisch abgemeldet.

SPERREN IM ONLINE-BANKING

Um unberechtigten Zugriff auf Ihr Online-Banking zu vermeiden, werden besondere Sicherheitsvorkehrungen getroffen. Unter bestimmten Umständen wird hierfür automatisch eine Sperre in Ihrem Online-Banking hinterlegt.

Sperre der PIN bzw. TAN im Online-Banking

Der Online-Banking-Zugang wird aus Sicherheitsgründen gesperrt, wenn dreimal eine falsche PIN eingegeben wurde. Wird dreimal eine falsche TAN eingegeben, wird nur die Möglichkeit zur Übermittlung von TAN-pflichtigen Aufträgen gesperrt. Für eine Entsperrung von Zugangsdaten benötigen wir einen schriftlichen Auftrag von Ihnen. Sollte die angegebene Grenze noch nicht erreicht sein, wird der jeweilige Fehlerzähler nach Eingabe der richtigen PIN oder einer TAN wieder auf 0 zurückgesetzt.

FinTS/HBCI - Sperre der PIN bzw. TAN

Auch hier wird der FinTS/HBCI-Zugang aus Sicherheitsgründen gesperrt, wenn dreimal eine falsche PIN eingegeben wurde. Hier gelten die gleichen Voraussetzungen wie beim Online-Banking mit PIN und TAN. Eine Entsperrung der Zugangsdaten erfolgt erst nach Eingang Ihres schriftlichen Auftrages.

FinTS/HBCI – Sperre der Signaturdatei

Zum Sperren und Entsperren Ihrer Signatur- bzw. Schlüsseldatei wenden Sie sich bitte an Ihren Berater.

FinTS/HBCI – Sperre der Chipkarte

Die FinTS/HBCI PIN der Chipkarte wird nach drei Fehlversuchen gesperrt. Sie kann über eine PUK, die Sie mit Ihren Zugangsdaten erhalten haben, entsperrt werden. Wird die PUK dreimal falsch eingegeben, wird der FinTS/HBCI-Zugang Ihrer Karte endgültig gesperrt. Es muss eine neue HBCI-FinTS-Chipkarte samt neuen Zugangsdaten beantragt werden.

Beachten Sie bitte auch die Hinweise zu Sperren unter den Notfallinformationen.

ENTSPERREN IHRES ONLINE-BANKING-ZUGANGS

Ist Ihr Zugang gesperrt und Ihnen die PIN noch bekannt, kann eine Entsperrung durch Ihren Berater oder durch einen schriftlichen Auftrag zur Entsperrung der PIN erfolgen. Nach erfolgter Entsperrung können Sie in diesem Fall das Online-Banking sofort wieder nutzen. Falls Ihr Online-Banking-Zugang gesperrt und Ihnen die PIN nicht bekannt ist, wenden Sie sich bitte an Ihren Berater oder erteilen Sie uns einen schriftlichen Auftrag zur Erstellung einer neuen PIN. Wir werden Ihnen dann eine Start-PIN auf dem Postweg zukommen lassen. Bitte beachten Sie, dass Ihre alte PIN damit sofort die Gültigkeit verliert und nicht mehr genutzt werden kann.

NOTFALLINFORMATIONEN

Meldung eines Manipulations-Verdachts

Sollten Sie den Verdacht haben, dass Zahlungen manipuliert wurden oder sollten Sie verdächtige Anomalien während einer Transaktion feststellen, verständigen Sie bitte sofort Ihren Berater und sperren Sie ggf. Ihren Zugang, wie unter Konto-/Zugangssperre beschrieben. Aktuelle Hinweise zu möglichen Sicherheitsrisiken im Online-Banking (z. B. Phishing-E-Mails) finden Sie auf unserer Online-Banking-Webseite: https://banking.donner-reuschel.de.

Karte sperren

Telefon:
Bei Verlust oder Diebstahl Ihrer Karte (girocard, HBCI/Fin/TS-Chipkarte, Mastercard, VISA Card) rund um die Uhr unter der zentralen Telefonnummer:

116 116 (in Deutschland gebührenfrei),
0049 116 116 (außerhalb Deutschlands gebührenpflichtig)

Online (nur girocard):
1. Im Online-Banking anmelden
2. Öffnen Sie bitte ***Service***
3. Wählen Sie den Bereich ***Sperren***
4. Nehmen Sie unter ***Kartensperren*** die entsprechende Kartensperre vor.

Konto-/ Zugangssperre

Telefon:
Sollten Sie Ihre Zugangsdaten zum Online-Banking nicht zur Hand haben, so können Sie die Sperre rund um die Uhr unter der zentralen Telefonnummer beauftragen: 116 116 (in Deutschland gebührenfrei), 0049 116 116 (außerhalb Deutschlands gebührenpflichtig)

Online:
1. Im Online-Banking anmelden
2. Öffnen Sie bitte ***Service***
3. Wählen Sie den Bereich ***Sperren***
4. Richten Sie je nach Ihrer Situation eine SB-Kontosperre, -Verfügungssperre (sofern auch Bevollmächtigte Zugriff auf Ihr Konto haben) oder -Zugangssperre ein.

Weitere Informationen für Ihre Sicherheit:

» Für Sicherheit in der Informationstechnik für Bürger:
www.bsi-fuer-buerger.de Bundesamt

» Sicherheitsportal mit Hintergrundinformationen:
www.heise.de/security

Hinweis:

Dieses Dokument enthält Links zu externen Websites Dritter, auf deren Inhalte wir keinen Einfluss haben. Deshalb können wir für diese fremden Inhalte auch keine Gewähr übernehmen. Für die Inhalte der verlinkten Seiten ist stets der jeweilige Anbieter oder Betreiber der Seiten verantwortlich. Die verlinkten Seiten wurden zum Zeitpunkt der Verlinkung auf mögliche Rechtsverstöße überprüft. Rechtswidrige Inhalte waren zum Zeitpunkt der Verlinkung nicht erkennbar. Eine permanente inhaltliche Kontrolle der verlinkten Seiten ist jedoch ohne konkrete Anhaltspunkte einer Rechtsverletzung nicht zumutbar. Bei Bekanntwerden von Rechtsverletzungen werden wir derartige Links umgehend entfernen.

DONNER & REUSCHEL
PRIVATBANK SEIT 1798

Die Privatbank der SIGNAL IDUNA Gruppe

DONNER & REUSCHEL
Aktiengesellschaft

Friedrichstraße 18
80801 München

Ballindamm 27 / Hermannstraße 13,
20095 Hamburg

www.donner-reuschel.de
bankhaus@donner-reuschel.de

Telefon Hamburg: 040 30217-0
Telefon München: 089 2395-0