

Sicherheitshinweise

Schutz des Zugangs durch PIN und TAN:

Die Sicherheit Ihrer Daten beim Online-Banking wird durch das bewährte PIN/TAN-Verfahren gewährleistet. Die PIN (Ihre fünfstellige "Persönliche Identifikations-Nummer") und die TAN (Ihre sechsstellige "Transaktions-Nummer") erhalten Sie kostenlos bei uns.

Nur bei Eingabe der richtigen PIN ist überhaupt eine erfolgreiche Anmeldung zum Online-Banking möglich. Genau wie beim Geldautomaten verhindern wir Missbrauch oder unbefugte Zugriffe: wird die PIN dreimal falsch eingegeben, wird der Online-Zugang zum Konto aus Sicherheitsgründen automatisch gesperrt. Außerdem muss jeder einzelne Auftrag durch Eingabe des zweiten Sicherheitscodes, der TAN, ausdrücklich autorisiert werden. Jede TAN kann nur einmal verwendet werden, nach Gebrauch verliert diese automatisch ihre Gültigkeit. Eine dreimalige Falscheingabe bewirkt die Sperrung des TAN-Bogens. Diese Sperrung kann nicht aufgelöst werden - Sie erhalten aber automatisch von uns eine neue Liste.

Sichere Übertragung der Anwendung:

Zur sicheren Datenübertragung werden alle HTML-Seiten mittels SSL (Secure Socket Layer) verschlüsselt. Dadurch ist sichergestellt, dass niemand unberechtigt die gesendeten Daten lesen oder manipulieren kann. Um den aktuellen Sicherheitsstandards Rechnung zu tragen, lassen wir nur noch die SSL-Version 3.0 zu. Daher müssen Sie in den Sicherheitseinstellungen Ihres Browsers unbedingt SSL 3.0 aktiviert haben.

Das können Sie tun

Umgang mit PIN und TAN:

Halten Sie Ihre PIN und TAN geheim. Teilen Sie diese Legitimationsdaten niemandem mit, auch nicht Ihrem Berater!

Speichern Sie unter keinen Umständen PIN und TAN auf Ihrem Computer - dort können Sie nämlich übers Internet "ausgespäht" werden!

Ändern Sie Ihre PIN in regelmäßigen Abständen:

Wenn Sie annehmen, dass Unbefugte Kenntnis von Ihrer PIN und Ihren TAN erlangt haben, lassen Sie Ihr Konto umgehend durch unsere Hotline (07 11) 21 48-4 44 für das Online-Banking sperren!

Die Änderung oder Sperre der PIN und die Sperre der TANs können Sie auch selbst in der Online-Banking-Anwendung vornehmen.

Bewahren Sie PIN und TAN unbedingt getrennt voneinander an einem sicheren Ort auf.

Beachtung des SSL-Symbols während der Ausführung:

Während der gesamten Ausführung der Anwendung muss das Sicherheitssymbol Ihres Browsers geschlossen dargestellt werden. Sie erkennen es in der Ecke rechts unten im Browserfenster: Dort wird dann ein geschlossenes Vorhängeschloss oder ein nicht durchgebrochener Schlüssel angezeigt.

Viren:

Überprüfen Sie Ihren Computer in regelmäßigen Abständen mit Hilfe eines Virensuchprogramms. Verwenden Sie keine Programme eines unbekanntem Anbieters. Aktualisieren Sie Ihr Virensuchprogramm regelmäßig.

Fremde Computer:

Loggen Sie sich nie von einem unbekanntem Computer aus in die Bank ein. Besonders Internetcafés bieten oft keine sichere Plattform für Online-Banking.

Software:

Installieren Sie niemals Software aus unbekannter Quelle auf dem eigenen Computer. Seien Sie sich klar darüber, dass Sie jedem Programmierer, dessen Software Sie installieren, Ihr volles Vertrauen aussprechen.

Löschen:

Falls Sie den Computer mit unbekanntem Personen teilen, sollten Sie nach dem Online-Banking den Zwischenspeicher (Browser-Cache) löschen. Im Internet Explorer geht das über Extras>Internetoptionen>Allgemein>Temporäre Internetdateien>Dateien löschen, bei Netscape über Bearbeiten>Einstellungen>Erweitert>Cache>Speicher-Cache löschen>Festplatten-Cache löschen.

Prüfen:

Nehmen Sie sich regelmäßig Zeit, die Online-Kontoauszüge zu überprüfen. So kommen Sie Missbrauch und anderen Unregelmäßigkeiten schnell auf die Spur. Sie können auch zur Erhöhung der Sicherheit eine Höchstgrenze für Überweisungen vereinbaren.