

# Online-Banking Sicherheits- und Ersteinstiegshinweise

Stand: September 2009

## Ansprechpartner

Kerstin Sündermann	03991 / 178 266
Hans-Jürgen Otto	03991 / 178 231
Mario Köhler	03991 / 178 240

## Sicherheitshinweise

- Teilen Sie Ihre Zugangsdaten/Passwörter niemals einer anderen Person mit!
- Speichern Sie Ihre Zugangsdaten nicht auf dem PC ab!
- Sollte sich eine andere Person Zugriff zu Ihren Zugangsdaten verschafft haben, sperren Sie Ihr Konto über das Internet-Banking oder wenden Sie sich telefonisch an uns!
- Schützen Sie Ihren PC vor Angriffe von außen mit einer stets aktuellen Antiviren-Software und einer Firewall!
- Reagieren Sie niemals auf Emails, die Sie aus Gründen wie Datenaktualisierung etc. auffordern, Zugangsdaten preiszugeben! Es handelt sich in diesen Fällen um sogenannte Phishing-Mails, die in der Regel mit dem Absender einer Bank versehen sind. Die tatsächlichen Absender derartiger Emails verfolgen das Ziel, Ihre Online-Banking-Zugangsdaten zu erlangen, um diese missbräuchlich zu verwenden. Bitte beachten Sie, dass wir Sie niemals per Email oder per Telefon auffordern werden, Zugangsdaten preiszugeben.
- Starten Sie das Internet-Banking nur über unsere Homepage <http://www.raiba-seenplatte.de>!

Ausführliche Informationen zum Thema Sicherheit im Internet finden Sie ab der Seite 3.

## Ersteinstieg Online-Banking über eine Software

Sofern Sie das Online-Banking über eine Software wie StarMoney, Quicken, T-Online etc. nutzen, stehen Ihnen die Sicherheitsverfahren HBCI mit Chipkarte und Kartenleser, HBCI mit Datei und PIN/TAN zur Verfügung. Der Ersteinstieg ist von Software zu Software unterschiedlich. Wenden Sie sich bitte bei Fragen zur Software- und Kontoeinrichtung an den Softwarehersteller. Haben Sie die Software StarMoney von uns erhalten, stehen wir Ihnen bei Fragen selbstverständlich gerne zur Verfügung.

Der Einsatz des Sicherheitsverfahrens PIN/TAN setzt vor der Kontoeinrichtung in der jeweiligen Software die Freischaltung des Kontos im Internet-Banking voraus. Folgen Sie in diesem Fall bitte den anschließenden Hinweisen zum Ersteinstieg im Internet-Banking.

## Ersteinstieg Internet-Banking

Rufen Sie zunächst unsere Internetadresse <http://www.raiba-seenplatte.de> auf. Wählen Sie anschließend den Punkt **Online-Banking "Zum Konto-Login"**. Das Internet-Banking wird nun gestartet.

Geben Sie in der Anmeldemaske Ihre Kontonummer ein. Klicken Sie anschließend auf "Weiter" (das Feld PIN bitte bei der Erstanmeldung frei lassen).

Sie befinden sich jetzt auf der Seite "PIN-Vergabe / Ersteinstieg". Geben Sie zunächst Ihre persönliche Kundennummer ein. Sollte diese Ihnen nicht bekannt sein, wenden Sie sich bitte an Ihren Kundenberater oder Ihre Filiale.

### **PIN-Wechsel/Ersteinstieg notwendig**

Um unberechtigte Zugriffe auf Ihre Selbstbedienungskonten auszuschließen, vergeben Sie bitte eine von Ihnen frei wählbare 5-stellige PIN. Es werden Buchstaben und Ziffern akzeptiert.

Diese PIN gilt für sämtliche SB-Konten, bei denen Sie Kontoinhaber oder Bevollmächtigter sind.

PIN = persönliche Identifikationsnummer

Bitte geben Sie zusätzlich Ihre Kundennummer an.

Kundennummer

Bitte geben Sie die neue PIN ein:

Bitte wiederholen Sie die neue PIN zur Kontrolle:

[▶ Weiter](#)   [▶ Zurück](#)

Anschließend werden Sie aufgefordert eine frei wählbare 5-stellige PIN (Ziffern oder Buchstaben) einzugeben. Um Fehler zu vermeiden, wiederholen Sie im nächsten Feld die PIN-Eingabe und klicken dann auf "Weiter".

Der Vorgang muss mit einer Transaktionsnummer (TAN) abgeschlossen werden. Hierzu wählen Sie nach entsprechender Aufforderung das von Ihnen gewünschte TAN-Verfahren. Die TAN ist ein 6-stelliger, numerischer Sicherheitscode, der als digitale Unterschrift fungiert und unter anderem der Absicherung von Überweisungen dient.

[Home](#) | [Demo](#) | [Hilfe](#) | [Kontakt](#)

InternetBanking  
Auswahl des TAN-Verfahrens

### **PIN-Wechsel/Ersteinstieg notwendig**

Bitte wählen Sie das gewünschte TAN-Verfahren.

- Sm@rtTAN plus
- Sm@rtTAN optic
- mobileTAN

[? Hilfe](#)   [▶ Weiter](#)

### **Sm@rtTAN plus**

Für die TAN-Erzeugung führen Sie zunächst die entsprechende VR-BankCard in den TAN-Generator und drücken Sie die Taste "TAN". Sie werden aufgefordert einen Code einzugeben, der Ihnen in der Internet-Banking-Maske angezeigt wird. Bestätigen Sie den Vorgang anschließend zweimal mit OK. Die TAN erscheint nun auf dem Display des TAN-Generators. Diese TAN geben Sie in die Internet-Banking-Anwendung ein und gehen auf "Weiter". Sie befinden sich nun auf der Inhaltsübersicht des Internet-Bankings.

### **Sm@rtTAN optic**

Über eine optische Schnittstelle auf der Rückseite des TAN-Generators werden die notwendigen Daten vom Monitor Ihres PC direkt zum Sm@rt-TAN optic TAN-Generator übertragen. Führen Sie die entsprechende VR-BankCard in den TAN-Generator und drücken Sie die Taste "F". Halten Sie dabei das Gerät an die animierte Grafik Ihres Monitors. Bitte beachten Sie unbedingt die Positionierungspfeile. Auf dem Display des TAN-Generators erscheint der Hinweis "Allgemeiner Bankauftrag". Drücken Sie die "OK" Taste des TAN Generators. Die TAN erscheint nun auf dem Display des TAN-Generators. Diese TAN geben Sie in die Internet-Banking-Anwendung ein und gehen auf "Weiter". Sie befinden sich nun auf der Inhaltsübersicht des Internet-Bankings.

### **mobile TAN**

Nutzen Sie das Verfahren mobile TAN, wird Ihnen die TAN per SMS an Ihre bei uns hinterlegte Handy-Nummer gesendet. Diese TAN geben Sie in die Internet-Banking-Anwendung ein und gehen auf "Weiter". Sie befinden sich nun auf der Inhaltsübersicht des Internet-Bankings.

## **Ausführliche Sicherheitshinweise zum Internet-Banking**

Das Internet hat sich zu einem selbstverständlichen Medium entwickelt, dessen Bedeutung stetig zunimmt. Neben den positiven Möglichkeiten des Internets ergeben sich jedoch auch eine Reihe von Sicherheitsrisiken, denen durch geeignete Maßnahmen entgegengewirkt werden muss.

Für die Sicherheit des Internet-Bankings ist neben der Vielzahl von Sicherheitsvorkehrungen, die durch Volks- und Raiffeisenbanken und IT-Dienstleister der Banken eingeleitet wurden, die Sicherheit des Internetnutzer-PCs sowie die Sensibilisierung der Internet-Banking-Nutzer von hoher Bedeutung.

Gerade aktuelle Angriffszenarien zielen immer öfter nicht nur auf die Ausnutzung von System- und Anwendungsschwachstellen und nutzen gezielt bestimmte Verhaltensmuster der Anwender. Durch den sensiblen Umgang mit den gegebenen technischen Möglichkeiten lassen sich jedoch die meisten Angriffe abwehren.

Folgende Punkte sind von wesentlicher Bedeutung:

[Sicherheit am Internet-PC](#)

[Prüfung der Authentizität des Online-Angebots](#)

[Generelle Verhaltensregeln](#)

## **Sicherheit am Internet-PC**

Der vertrauenswürdige Zustand Ihres PCs ist die Voraussetzung für sicheres Internet-Banking. Um die Sicherheit Ihres PCs zu gewährleisten, sind folgende Maßnahmen von wesentlicher Bedeutung:

Nutzen und installieren Sie nur Software aus vertrauenswürdigen Quellen.

Überlegen Sie immer, ob Sie eine Software wirklich brauchen und ob Sie dem Anbieter (Hersteller und Download-Quelle) wirklich vertrauen. Generell sollten Sie keine Dateien von unbekanntem Servern bzw. E-Mail-Anhänge unbekanntem Ursprungs öffnen, herunterladen oder ausführen. Sollte dies jedoch erforderlich sein, so ist zumindest eine Überprüfung der Dateien mit einem aktuellen Virens Scanner sinnvoll.

Schutz vor Viren, Würmern und "Trojanischen Pferden"

Einmal auf Ihrem System installierte Viren, Würmer oder "Trojanische Pferde" haben auf Ihrem System weitreichende Möglichkeiten. Sobald eine solche Schadsoftware auf Ihrem System installiert wurde, kann der Schutz Ihrer Daten und die korrekte Funktion von Betriebssystem und Anwendungen prinzipiell nicht mehr gewährleistet werden.

Um eine optimale Abwehr von Schadsoftware zu erreichen, ist die Installation eines Virens Scanner und einer Personal Firewall erforderlich bzw. sinnvoll. Wesentlich für die Wirksamkeit dieser Komponenten ist zudem eine regelmäßige Aktualisierung (mind. 1-mal pro Woche).

Sicherheitsaktualisierungen für Betriebssystem und Browser:

Zum Teil nutzen Angreifer und Schadprogramme Sicherheitslücken im Betriebssystem und Programmen wie dem Browser, um sich unbemerkt in Ihrem PC einzunisten. Um das Angriffspotential über offene Schwachstellen zu minimieren, sollten Aktualisierungen für Betriebssysteme, Browser und Sicherheitskomponenten (wie Personal Firewall oder Virens Scanner) umgehend installiert werden. Die meisten Programme bieten für diesen Zweck automatische Update-Funktionen, die in regelmäßigen Abständen auf den Herstellerseiten nach Aktualisierungen der Produkte suchen und diese ggf. installieren.

Auf folgenden Seiten finden Sie weiterführende Informationen zur Sicherheit im Internet:

[www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de)

[www.sicherheit-im-internet.de](http://www.sicherheit-im-internet.de)

## **Prüfung der Authentizität des Online-Angebots**

Die Authentifizierung ist der Nachweis eines Kommunikationspartners, dass er tatsächlich derjenige ist, für den er sich ausgibt. Die Authentizität wird beim Internet-Banking durch Einsatz des SSL-Protokolls gewährleistet. Hierbei wird über ein Zertifikat die Authentizität des Anbieters bestätigt. Eine erste und einfache Möglichkeit der Prüfung ist zudem anhand der angezeigten Internet-Adresse (URL) im Browser möglich.

Prüfen der Internet-Adresse:

Als Anwender sollten Sie darauf achten, dass Sie die korrekte Adresse (URL) für das Internet-Banking kennen. Bei jeder Internet-Banking Sitzung sollten Sie die im Browser angezeigte URL auf Plausibilität prüfen. Jede unbekannte Internet-Adresse kann als nicht vertrauenswürdig eingestuft werden. Geben Sie bei fremden Adressen niemals persönliche Informationen und/oder Ihre Internet-Banking-Zugangsdaten ein.

Der Zugang zum Internet-Banking sollte immer über die offizielle Homepage Ihrer Bank gestartet werden. Auf keinen Fall sollten Sie Links zum Internet-Banking verwenden, die über Web-Seiten oder E-Mails anderer Anbieter zur Verfügung gestellt werden.