

## **Online-Banking Sicherheits- und Ersteinstiegshinweise**

Stand: August 2008

### **Ansprechpartner**

Steffen Friedrich	0395 / 5585 577
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 Diskette 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**

Das Internet-Banking können Sie ausschließlich mit dem Sicherheitsverfahren PIN/TAN nutzen. Die PIN ist ein alphanumerischer Sicherheitscode, welchen Sie jederzeit ändern können. Erst nach Eingabe Ihrer Kontonummer und der PIN kann am Online-Banking teilgenommen werden. Die TAN ist ein 6-stelliger, numerischer Sicherheitscode, der als digitale Unterschrift fungiert und unter anderem der Absicherung von Überweisungen dient. Mit Ihrer ec-Karte und dem Sm@rtTAN plus-Kartenleser können Sie per Knopfdruck TAN's generieren. Beachten Sie hierzu bitte die Bedienungsanleitung zum Sm@rtTAN plus-Kartenleser.

Rufen Sie zunächst unsere Internetadresse <http://www.raiba-seenplatte.de> auf. Wählen Sie anschließend den Punkt **Online-Banking**. 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 Kundennummer \_\_\_\_\_ ein. Anschließend werden Sie aufgefordert eine freiwählbare 5-stellige PIN (Ziffern oder Buchstaben) einzugeben. Um Fehler zu vermeiden, wiederholen Sie im nächsten Feld die PIN-Eingabe. In das Feld "TAN" tragen Sie bitte eine TAN (sechsstellige Nummer) ein und klicken anschließend auf "Weiter". Nachfolgend finden Sie Erläuterungen zur Erzeugung der TAN.

### **Sm@rtTAN plus**

Sofern Sie für die TAN-Erzeugung einen Kartenleser verwenden, müssen Sie für die TAN-Erzeugung die entsprechende ec-Karte in das Lesegerät stecken. Danach 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.

### **mobile TAN**

Nutzen Sie das Verfahren mobile TAN, wird Ihnen die TAN per SMS an Ihre bei uns hinterlegte Handy-Nummer gesendet. Sie befinden sich nun auf der Inhaltsübersicht des Internet-Bankings.

InternetBanking  
PIN-Vergabe / Ersteinstieg

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

Um unberechtigte Zugriffe auf Ihre Selbstbedienungskonten auszuschließen, vergeben Sie bitte eine von Ihnen freiwählbare 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:

TAN

## **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 Angriffsszenarien 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 Ursprung 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.

## Bedeutung und Kontrolle der wesentlichen Bestandteile der Internet-Adresse (URL) des Internet-Bankings der Volks- und Raiffeisenbanken bei der GAD eG

Die Adresse des Internet-Bankings beginnt immer mit: [https://internetbanking.gad.de/...](https://internetbanking.gad.de/)

https:// - Kommunikation über das SSL-Protokoll (Verschlüsselte Kommunikation mit Authentizitätsnachweis des Anbieters) gad.de - Internet-Domain des IT-Dienstleisters für Volks- und Raiffeisenbanken (GAD eG) internetbanking - Name der Internet-Banking-Systeme bei gad.de

Die Adresse des Internet-Brokerage beginnt immer mit: [http://www.brokerage.vr-networld.de/...](http://www.brokerage.vr-networld.de/)

http:// - Kommunikation über das HTTP-Protokoll. Ab der Anmeldung wird für die Kommunikation das verschlüsselte HTTPS-Protokoll verwendet.

vr-networld.de - Internet Domain des Finanzportals der Volks- und Raiffeisenbanken

www.brokerage - symbolischer Ort des Service „Brokerage“

Diese Bestandteile der URL müssen immer übereinstimmen.

### Zertifikatsprüfung

Die SSL-Verbindung garantiert Ihnen, dass eine verschlüsselte Kommunikation mit der GAD eG, dem IT-Dienstleister Ihrer Volks- und Raiffeisenbank, stattfindet. SSL-Zertifikate enthalten hierfür generell den öffentlichen Schlüssel des Anbieters, sowie Angaben zur eindeutigen Identifikation.

Das SSL-Zertifikat zum InternetBanking ist auf den IT-Dienstleister der Volks- und Raiffeisenbanken ausgestellt (Besitzer/Antragsteller).

Hierbei handelt es sich um die GAD eG mit Sitz in Münster.

Niemals sollte ein Zertifikat eines anderen Anbieters im Rahmen einer Internet-Banking- Sitzung akzeptiert werden. Manuelle Bestätigungen des Zertifikats sind zudem beim Internet-Banking der GAD eG nicht erforderlich, da hierbei ein Zertifikat einer vertrauenswürdigen Zertifizierungsstelle zum Einsatz kommt.

Potentielle Angreifer nutzen i.d.R. eigenerstellte Zertifikate, welche vom Browser nur mit Bestätigung des Benutzers akzeptiert werden, da dieser die Authentizität nicht zweifelsfrei feststellen kann.

Bei Zertifikatsfragen des Browsers ist daher Vorsicht geboten, bevor fremde Zertifikate akzeptiert bzw. als vertrauenswürdig eingestuft werden.

Das Zertifikat des Anbieters sowie Angaben zur Stärke der Verschlüsselung Ihrer SSL-Sitzung können Sie überprüfen, indem Sie einen Doppelklick auf das Symbol "Vorhängeschloss" in der Statuszeile des Browsers durchführen.

### Zertifizierungsstelle

Die Zertifizierungsstelle ist eine international anerkannte, unabhängige und vertrauenswürdige Instanz, die Zertifikate ausstellt. Bei der Zertifikatsausstellung ist ein spezieller Authentizitätsnachweis erforderlich, so dass später über das ausgestellte Zertifikat eine Authentizitätsprüfung möglich ist.

Das Internet-Banking der GAD eG verwendet "VeriSign" als Zertifizierungsstelle.

## **Generelle Verhaltensregeln**

### Geheimhaltung von PIN und TAN

PIN und TANs dürfen nur im gesicherten Internet-Banking Angebot verwendet werden. Niemals dürfen PIN und TAN per E-Mail übertragen oder auf anderem Wege Dritten anvertraut werden.

Achten Sie darauf, dass Ihnen bei der Eingabe von PIN und TAN niemand "über die Schulter sieht" und speichern Sie nie Ihre PIN und TAN auf der Festplatte oder anderen Speichermedien Ihres PCs. Deaktivieren Sie hierzu auch die automatische Passwort-Speicherung Ihres Browsers.

### Änderung der PIN und Sperrung von TAN-Bögen bei Verdacht der Kompromittierung

Sollten Sie versehentlich eine zweifelhafte Internet-Seite besucht und Ihre Daten preisgegeben haben, empfehlen wir Ihnen, die PIN zu ändern bzw. die TAN-Liste zu sperren. Beides kann im Internet-Banking Angebot der Volks- und Raiffeisenbanken durchgeführt werden. Wenden Sie sich bei Problemen umgehend an Ihre Bank.

### Prüfung der SSL-Verbindung

Die Stärke der Verschlüsselung Ihrer SSL-Sitzung sowie das Zertifikat des Anbieters können Sie überprüfen, indem Sie einen Doppelklick auf dem Symbol "Vorhängeschloss" in der Statuszeile des Browsers durchführen.

Nutzen Sie Internet-Banking nur über die gesicherten SSL-Verbindungen zum Rechenzentrum der GAD eG.

Achten Sie auf die Korrektheit der Internet-Banking-Adresse (URL).

Rufen Sie das Internet-Banking ausschließlich über die Homepage der Raiffeisenbank Mecklenburger Seenplatte eG auf.