

# Online-Banking

**Bankgeschäfte erledigen  
einfach & sicher  
rundum die Uhr von überall**



## Herzlich Willkommen

Homebanking ermöglicht den Zugang zur Bank rund um die Uhr und an sieben Tagen in der Woche. Schon seit vielen Jahren bieten wir unseren Kunden diese Möglichkeit der Online-Kontenverwaltung an.

Über unsere Homepage [www.steyler-bank.de](http://www.steyler-bank.de) und die App „Mybanking“ steht Ihnen unser Kundenzugang zur Verfügung, über welchen Sie zahlreiche Bankgeschäfte einfach von zu Hause aus erledigen können.

Auf den folgenden Seiten erfahren Sie, wie Sie sich für die Nutzung des Online-Banking anmelden. Außerdem enthält diese Broschüre Informationen über die verwendeten Zwei-Schritt-TAN-Verfahren (Sm@rt-TANoptic und SecureGo Plus) sowie eine kurze Einweisung in die Online-Filiale und die Ihnen zur Verfügung gestellten Leistungsmerkmale. Abschließend geben wir Ihnen nützliche Tipps für Ihre Sicherheit im Umgang mit dem Online-Banking.

---

## Was tun bei Verlust oder Diebstahl Ihrer Karten?

### Giro- oder Kreditkarte sperren

Sie haben Ihre Karte verloren oder sie wurde gestohlen? Dann sollten Sie Ihre Karte so schnell wie möglich sperren lassen. Der zentrale Sperrenannahme-Dienst ist täglich rund um die Uhr erreichbar. Die Aufnahme Ihrer Angaben erfolgt grundsätzlich durch einen Sprachcomputer.

#### **Girokarte sperren: +49 (0)1805 - 021 021**

(14 Ct./min. (inkl. USt.) aus dem deutschen Festnetz, Mobilfunkhöchstpreis 42 Ct./min (inkl. USt.), abweichende Gebühren aus dem Ausland)

#### **Kreditkarte sperren: +49 (0)721/1209-66001**

## Was tun bei Diebstahl Ihrer Authentifizierungsdaten?

### Online-Banking sperren

Sperren Sie Ihren Zugang zum Online-Banking, wenn Sie den Verdacht haben, dass Dritte im Besitz Ihrer PIN sind oder sich Ihr Browser merkwürdig verhält. Eine Sperrung können Sie bei uns vornehmen oder durch die dreimalige Eingabe einer falschen PIN beim Anmelden bewirken.

Oder Sie rufen die von der Bank angegebene Sperr-Notrufnummer an.

#### **Online-Zugang sperren: +49 (0)1805 - 021 021**

# 1. TAN-Verfahren aktivieren

Sicherheit steht beim Online-Banking an erster Stelle. Zum Schutz Ihres Kontos vor unberechtigten Zugriffen gibt es das PIN-/TAN-Verfahren. Die PIN ist Ihre **P**ersönliche **I**dentifikations-**N**ummer, mit der Sie sich beim Online-Banking identifizieren. Die TAN ersetzt bei Online-Verfügungen Ihre Unterschrift.

Jede TAN kann nur einmalig verwendet werden. Ihre PIN und Ihre TAN sind für alle Konten gültig, für die Sie verfügungsberechtigt sind.

## Mehr Sicherheit beim Online-Banking

Leider sind die heimischen PCs ebenso wie Smartphones oder Tablets in der heutigen Zeit zunehmend der Gefahr des Ausspähens durch Betrüger („Hacker“) ausgesetzt. Auch aktuelle Schutzprogramme können dies nicht immer verhindern. Um dem entgegenzuwirken, wird mit dem Zwei-Schritt-TAN-Verfahren das Online-Banking gegen Angriffe abgeschottet, sodass kein Missbrauch mehr möglich ist. Das funktioniert so:

### 1) Trennung der Übertragungswege:

Überweisungserfassung und Übermittlung der Transaktionsnummer erfolgen auf unterschiedlichen Wegen.

### 2) TAN-Bindung:

Jeder Auftrag hat eine eigene Transaktionsnummer (TAN). Für das Zwei-Schritt-TAN-Verfahren bieten wir Ihnen folgende Möglichkeiten:

- SecureGo plus-App (mit Smartphone oder Tablet)
- Sm@rt-TAN optic (mit Girocard und Lesegerät)

## TAN-App SecureGo plus

- 1 SecureGo plus im App-Store Ihres Anbieters herunterladen. Anwendung starten und App-Kennwort festlegen.
- 2 Bankverbindung freischalten
- 3 Per Post erhalten Sie Ihren Freischaltcode, den Sie bitte in der App eingeben.
- 4 Start-PIN für das Online-Banking in eine individuelle PIN ändern
- 5 Online-Zugang ist vollständig eingerichtet

Eine ausführliche Anleitung finden Sie auf [Seite 6](#).

## Sm@rt-TAN optic - So geht's

Um eine Sm@rtTAN optic zu erzeugen, benötigen Sie ein spezielles Kartenlesegerät, das Sie bei uns kostenpflichtig bestellen können. In dieses Gerät stecken Sie Ihre Steyler Bank-Girocard. Sie können das Gerät übrigens nicht nur für Ihr Konto bei der Steyler Ethik Bank nutzen, sondern für alle Konten von Volks- und Raiffeisenbanken in Deutschland.

- 1 Sie melden sich für das Online-Banking an, füllen den Überweisungsauftrag aus und drücken auf **Ausführen**. (Hinweise zur Erstanmeldung im Online-Banking finden Sie Seite 4.)
- 2 Stecken Sie Ihre Girocard mit dem Chip voran in den TAN-Generator und drücken Sie „F“.
- 3 Halten Sie den TAN-Generator an die animierte Grafik. Dabei müssen die Markierungen (Dreiecke) der Grafik mit denen auf Ihrem TAN-Generator übereinstimmen.
- 4 Prüfen Sie die Anzeige auf dem Leserdisplay und bestätigen Sie mit **OK**.
- 5 Das Gerät generiert nun für Sie eine TAN, die nur für diesen Auftrag gilt.
- 6 Jetzt werden Ihnen die Details zu Ihrem Auftrag noch einmal auf dem TAN-Generator gezeigt. Prüfen Sie die einzelnen Angaben (Empfänger-IBAN und Betrag) und bestätigen Sie diese jeweils mit **OK**.
- 7 **Bitte beachten:** Überprüfen Sie die Anzeige des TAN-Generators immer anhand der Original-Transaktions-Daten - z.B. einer Rechnung.
- 8 Nun geben Sie die TAN am PC ein und senden diese ab. Damit ist die Transaktion beendet.

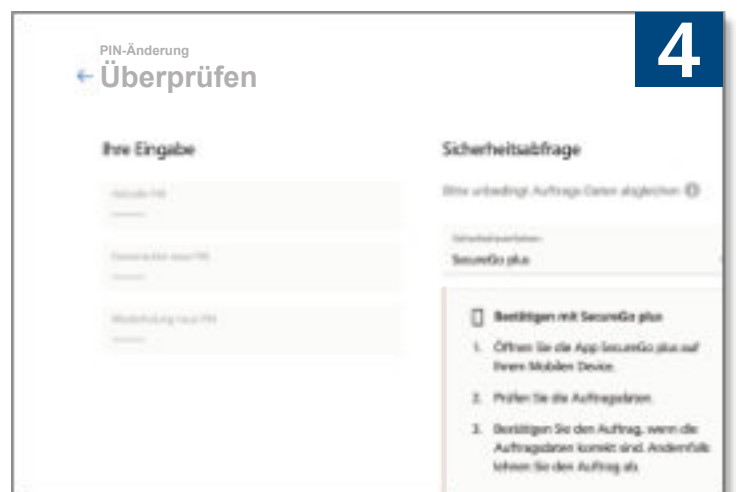
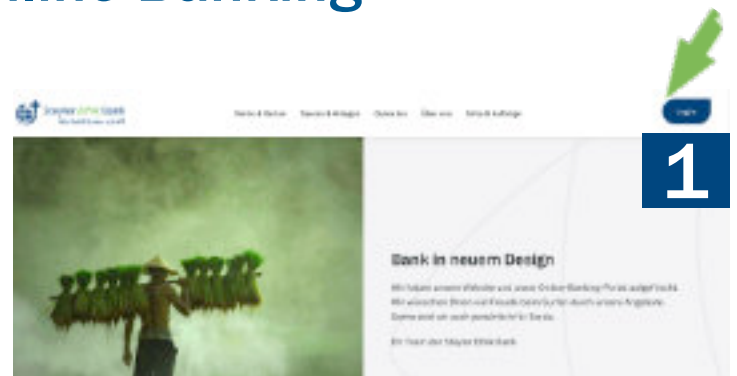
## Übrigens:

Um die Sicherheit des Online-Bankings zu erhöhen, wird bei der Anmeldung alle 90 Tage zusätzlich zum Passwort auch eine aktuelle TAN abgefragt.

## 2. Erstanmeldung zum Online-Banking

In Schritt 1 haben Sie bereits das TAN-Verfahren aktiviert und sich für eine von zwei Varianten entschieden. Um die Vorteile des Online-Bankings nutzen zu können, benötigen Sie zudem Ihre Steyler-Kennung. Diese können Sie kostenlos bei Ihrem Berater beantragen. Daraufhin erhalten Sie für die Erstlegitimation per Post eine individuelle, nicht reproduzierbare Start-PIN.

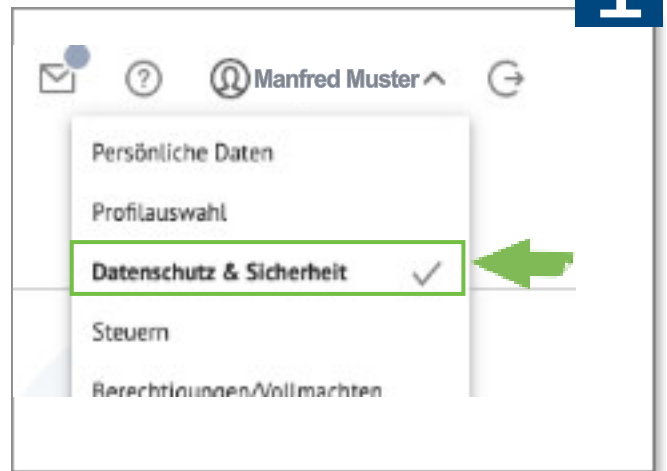
- 1 Zur Anmeldung im Online-Banking-System rufen Sie bitte zunächst die Internetseite der Steyler Ethik Bank unter [www.steyler-bank.de](http://www.steyler-bank.de) auf. Klicken Sie oben rechts auf **Login**.
- 2 Sie gelangen nun zur Anmeldungsmaske. Dort geben Sie Ihre Steyler-Kennung und die Start-PIN ein, die Sie per Post erhalten haben. Bestätigen Sie die Daten, indem Sie auf **Anmelden** klicken.
- 3 Bei der Erstanmeldung gelangen Sie automatisch zur Maske **PIN-Änderung**. Tragen Sie im oberen Feld zunächst die **Start-PIN** ein. Die selbstgewählte neue PIN, geben Sie in die zweite Zeile ein. In der dritten Zeile wiederholen Sie diese, um Tippfehler zu vermeiden. Klicken Sie auf **„Eingabe prüfen“**.
- 4 Nachdem Sie auf „Eingaben prüfen“ geklickt haben, meldet sich Ihre SecureGo plus App auf Ihrem Smartphone. Öffnen Sie die SecureGo plus App. Gehen Sie auf **„Freigeben“** um die Erst-PIN-Änderung abzuschließen.



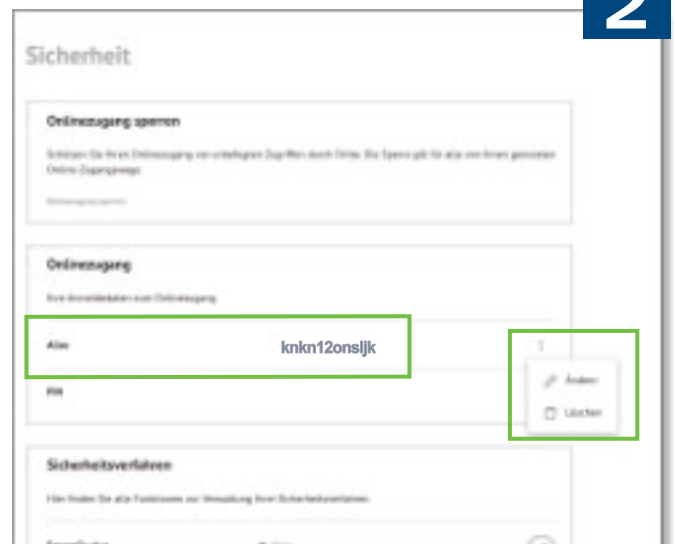
### 3. Änderung Steyler Kennung/Alias

**1** Nachdem Sie sich erfolgreich beim Online-Banking angemeldet haben, sollten Sie nun noch Ihre Steyler Kennung/Alias anpassen. Die Kennung, die Sie per Post erhalten haben besteht aus einer zufälligen Zahlenfolge und lässt sich daher nicht gut merken. Doch das ist kein Problem, denn Sie können sich Ihr eigenes Kennwort (Alias) erstellen.

Hierzu klicken Sie auf Ihren Namen, den Sie am rechten Rande der oberen Navigationsleiste finden. Aus dem Menue, das sich dann öffnet, wählen Sie den Unterpunkt **Datenschutz & Sicherheit**.



**2** Es öffnet sich das Fenster „Sicherheit“. Hier klicken Sie auf bei **Alias** auf die **3 Punkte** und dann auf **Ändern**. Jetzt können Sie sich eine neue Kennung vergeben. Bestätigt wird das Ganze über eine TAN, die Sie über Ihre Secure-Go Plus App erhalten.





## SecureGo plus

Die App einfach aktivieren und nutzen.

Gehen Sie beim Onlinebanking auf Nummer sicher – und machen Sie es sich noch bequemer, denn mit der neuen SecureGo plus App geben Sie Transaktionen ganz einfach frei.

### So aktivieren Sie SecureGo plus

1. Installieren Sie die SecureGo plus App auf Ihrem Smartphone. Sie erhalten SecureGo plus sowohl im Apple App Store als auch im Google Play Store:

Jetzt QR-Code scannen und SecureGo plus installieren.



iOS



Android

2. Legen Sie einen individuellen Freigabe-Code fest und bestätigen Sie diesen. Mit dem Code können Sie künftig Transaktionen freigeben.



3. Wählen Sie nun im Menü „Bankverbindungen“ und scannen Sie anschließend den Aktivierungscode im Anschreiben oder geben Sie ihn ein. Die Aktivierung ist damit abgeschlossen!



### Und so nutzen Sie SecureGo plus

1. Geben Sie Ihre Transaktion wie gewohnt im OnlineBanking ein. Sie erhalten automatisch eine Push-Nachricht auf Ihrem mobilen Endgerät.



3. Bestätigen Sie die Transaktion mit Ihrem individuellen Freigabe-Code, Ihrem Fingerabdruck oder der Gesichtserkennung Ihres mobilen Endgeräts. Alternativ geben Sie die angezeigte TAN für diese Transaktion in Ihrem OnlineBanking ein.



2. Starten Sie die App SecureGo plus, indem Sie das App-Icon oder die Push-Nachricht auf Ihrem mobilen Endgerät antippen. Prüfen Sie die Transaktionsdaten.



4. Sie erhalten sowohl im OnlineBanking als auch in der SecureGo plus App den Hinweis, dass die Transaktion erfolgreich ausgeführt wurde.



#### Noch Fragen?

Haben Sie Fragen zur Einrichtung oder Nutzung der App? Wir stehen Ihnen für Rückfragen gerne zur Verfügung.

#### Wichtiger Hinweis:

Um SecureGo plus optimal nutzen zu können empfehlen wir die Aktivierung von Push-Nachrichten für diese App.

## Tipps für Ihre Sicherheit

Das Internet stellt viele Möglichkeiten zur Verfügung. Es ist immer und nahezu überall verfügbar. Da liegt es nahe, auch die persönlichen Bankgeschäfte online zu erledigen.

Im weltweiten Netz tätigen Sie zum Beispiel einfach und bequem Ihre Überweisungen oder rufen zu jeder Tageszeit Ihren Kontostand ab. Aber das Internet birgt auch Gefahren. Vermehrt warnen Experten und Medien vor Risiken wie z. B. Phishing-Attacken, neuen Viren und Würmern. Trotzdem können Sie die Vorzüge des Online-Bankings gesichert nutzen, wenn Sie diese Gefahren kennen und wissen, wie Sie die Abwehr Ihres Computers, Tablets oder Smartphones stärken.

Wir helfen Ihnen gerne und zeigen einige Möglichkeiten auf, wie Sie sich ganz einfach und wirkungsvoll vor unerwünschten Zugriffen schützen.

- Folgen Sie niemals Aufforderungen in E-Mails oder Dialogfenstern, die – aus welchem Grund auch immer – nach Ihrer PIN oder TAN fragen. Seriöse Internetanbieter fragen niemals nach sicherheitsrelevanten Daten. Verwenden Sie auch keine Links aus E-Mails.
- Geben Sie die Webadresse Ihrer Bank immer von Hand ein, niemals über den Link in einer E-Mail.
- Moderne Betriebssysteme machen es Ihnen leicht. Nutzen Sie die automatischen Updates und stellen Sie die Sicherheitsoptionen Ihres Browsers mindestens auf mittel.
- Speichern Sie keine persönlichen Zugangsdaten auf Ihrem Computer.
- Benutzen Sie möglichst immer Ihren eigenen Computer, denn fremde Rechner können Sicherheitslücken aufweisen.
- Starten Sie den Browser neu, bevor Sie das Online-Banking aufrufen.
- Prüfen Sie das Vorhängeschloss der gesicherten https-Internetseite. Kennen Sie den Eigentümer oder den Zertifikatsaussteller nicht, brechen Sie die Sitzung ab.
- Gleichen Sie Ihre Kontoumsätze vor und nach jeder Transaktion ab.
- Fragen Sie sich immer, wann eine Dateneingabe sinnvoll ist.
- Öffnen Sie keine E-Mail-Anhänge, wenn Sie diese nicht angefordert haben.
- Beachten Sie die aktuellen Sicherheitshinweise und Warnmeldungen Ihrer Bank.
- Ändern Sie regelmäßig Ihre PIN.
- Verwenden Sie für Ihre PIN keine leicht nachvollziehbaren Zahlen- oder Buchstabenkombinationen (z. B. Geburtsdaten oder Namen).
- Prüfen Sie die Anzeige im Leser vor der Benutzung der erzeugten TAN. Diese Daten entsprechen genau der Aktion, die von der Bank nach Ihrer Freigabe ausgeführt wird. Schützen Sie Ihren PC mit einer aktuellen Antivirensoftware und einer Firewall.
- Sperren Sie Ihren Zugang zum Online-Banking, wenn Sie den Verdacht haben, dass Dritte im Besitz Ihrer PIN sind oder sich Ihr Browser merkwürdig verhält. Eine Sperrung können Sie bei uns vornehmen oder durch die dreimalige Eingabe einer falschen PIN beim Anmelden bewirken. Oder Sie rufen die von der Bank angegebene Sperr-Notrufnummer **116 116** an.

### Weitere Informationen

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

(Stand der Broschüre: 29. April 2022)