Volksbank Eifel eG

Hinweise zum Ersteinstieg beim Online-Banking (eBanking)
mit dem TAN-Verfahren VR-SecureGo

Sehr geehrte Kundin, sehr geehrter Kunde,

Sie haben sich für eBanking entschieden. Verschiedene Aktionen im eBanking wie Passwort-Änderungen oder Überweisungen müssen mit einer Transaktionsnummer (TAN) bestätigt werden. Aus diesem Grund ist eine aktivierte App VR-SecureGo zu deren Erzeugung Grundvoraussetzung.

Bitte gehen Sie nach folgender **Anleitung** vor:

Sie erhalten drei Briefe:

Brief 1:
- **Vertragsunterlagen Online-Banking (eBanking) mit Ihrem VR-Netkey**
  (Bankausfertigung bitte unterschrieben zurücksenden)

Brief 2:
- **Ihre Start-PIN** für die Anmeldung im **eBanking**

Brief 3 (nach Durchführung der Punkte 1 – 4 im ersten Schritt):
- **Freischaltcode** für Ihr gewähltes TAN-Verfahren: **TAN-App VR-SecureGo**

Erster Schritt: Aktivierung der TAN-App VR-SecureGo

1. Bitte laden Sie die neue App im Appstore bzw. Playstore auf Ihr Smartphone oder Tablet herunter.

Die Installation ist auch mittels hier abgebildetem QR-Code möglich:

QR-Code zum Download für iOS

QR-Code zum Download für Android

Öffnen Sie die neu installierte TAN-App VR-SecureGo auf Ihrem Smartphone oder Tablet. Je nach Betriebssystem werden bei der Installation Ihre Zustimmung zum Erhalt von Mitteilungen (Push-Nachricht) und der Zugriff auf die Kamera vorausgesetzt.

2. Geben Sie die Bankleitzahl der Volksbank Eifel eG **586 601 01** sowie den neuen **VR-NetKey** (**Brief 1**) ein.

3. Vergeben Sie sich jetzt ein **Anmeldekennwort**, das bei jedem Start der App eingegeben werden muss (später ist auch Touch ID möglich), und drücken Sie anschließend auf **Sichern**.

Das **Anmeldekennwort** muss mindestens 1 Großbuchstaben, 1 Kleinbuchstaben und 1 Ziffer enthalten sowie aus mindestens 8 Zeichen bestehen. Sonderzeichen können genutzt werden, jedoch keine Leerzeichen.

4. Stimmen Sie den Sonderbedingungen zu und tippen Sie auf "App registrieren". Dadurch wird die sicherheitstechnische Bindung zwischen Ihrem Smartphone oder Tablet, der VR-SecureGo-App und Ihrem VR-NetKey hergestellt. Falls Sie an dieser Stelle auf "Abmelden" tippen, bricht der Registrierungsprozess ab und Ihr Anmeldekennwort wird nicht gespeichert. Beim nächsten Aufruf der VR-SecureGo-App müssen Sie dann den gesamten Prozess wiederholen.

5. Ihren persönlichen Freischaltcode erhalten Sie dann per Post (Brief 3).

Achtung: Der Registrierungsprozess unterliegt höchsten Sicherheitsbedingungen. Ihren persönlichen Freischaltcode senden wir Ihnen innerhalb von 2 Tagen mit Brief 3 auf dem Postweg an die bei uns hinterlegte Adresse. Sobald der Brief vorliegt, können Sie entsprechend fortfahren.

Geben Sie den Freischaltcode bitte in der VR-SecureGo-App ein. Sie können Ihren Freischaltcode dafür entweder scannen oder manuell eingeben. Hinweis für Nutzer von iOS: Der Scan funktioniert nur, wenn Sie der VR-SecureGo-App Zugriff auf Ihre Kamera erlaubt haben.

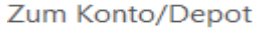
6. Nachdem Sie Ihren persönlichen **Freischaltcode eingegeben** haben, können Sie nun die App VR-SecureGo für TAN-pflichtige Transaktionen nutzen.

Weitere Informationen zur App erhalten Sie unter https://www.volksbank-eifel.de/banking-service/banking-brokerage/onlinebanking/tan-app.html

Zweiter Schritt: Erstanmeldung im eBanking

Jetzt kann die Erstanmeldung für das eBanking über unsere Internetseite, entweder am PC oder Tablet/Smartphone durchgeführt werden. Die folgende Anleitung beschreibt die Anmeldung am PC, am Tablet/Smartphone sind die Bezeichnungen teilweise leicht abweichend.

1. Rufen Sie bitte im Internet unsere Homepage **www.volksbank-eifel.de** auf.

2. Wählen Sie bitte den Button  oben rechts und dann 

3. Es öffnet sich ein neues Fenster, in dem Sie nach Ihrem **VR-Netkey (Brief 1)** und der PIN gefragt werden. Geben Sie bitte die erhaltene **Start-PIN (Brief 2)** ein und klicken auf 

4. Ihre **Start-PIN** müssen Sie zwingend ändern. Sie erhalten nun in Ihre **TAN-App VR-SecureGo** eine Push-Nachricht von unserem Rechenzentrum, in der die 6-stellige Transaktionsnummer (TAN) zur Bestätigung der PIN-Vergabe enthalten ist.

5. Die TAN geben Sie bitte in dem dafür vorgesehenen Feld ein und klicken auf 

6. Um weitere Anmeldungen zu vereinfachen, haben Sie die Möglichkeit, sich anstelle des **VR-Netkeys** einen Anmeldenamen/Alias zu vergeben. Klicken Sie dazu bitte oben auf den Reiter  und hierunter auf 

So funktioniert eBanking mit VR-SecureGo:

1. Sie erfassen Ihre Transaktion wie gewohnt. Beim Schritt „Eingabe prüfen" wird automatisch eine TAN angefordert.

2. Öffnen Sie die VR-SecureGo-App auf Ihrem Smartphone und melden Sie sich an. Sie können die App auch über das Antippen der Push-Nachricht aufrufen.

3. Prüfen Sie in der App, ob die Transaktionsdaten (z.B. Betrag und Empfänger-IBAN) korrekt sind.

4. Sind die übermittelten Daten richtig, geben Sie die TAN im eBanking ein. Sie gilt nur für diese Transaktion.

5. Sie erhalten eine Bestätigung für die erfolgreiche Ausführung der Transaktion.

Bei Fragen stehen wir Ihnen natürlich gerne zur Verfügung.
Senden Sie uns eine E-Mail an info@volksbank-eifel.de oder rufen Sie uns unter 06561 63-0 an.
Wir helfen Ihnen gerne weiter!
Unten stehend haben wir Ihnen einige Informationen zur Sicherheit im eBanking zusammengestellt.
Mit freundlichen Grüßen
Ihre Volksbank Eifel eG

Worauf sollten Sie beim Online-Banking (eBanking) achten?

Wenn Sie einige Grundregeln beachten, lässt sich die Sicherheit des Online-Bankings deutlich verbessern – auch wenn es niemals einen vollkommenen Schutz geben wird. Diese Checkliste gibt Ihnen einen Überblick über die wichtigsten Schutzmaßnahmen.

1. Zugangsdaten
Wenn Sie Ihre Zugangsdaten nicht angemessen schützen, können diese schnell in die Hände von Kriminellen geraten. Diese können sie zu hohen Abhebungen missbrauchen. Zu einem angemessenen Schutz gehört auch, dass Sie extrem vorsichtig bei der Weitergabe von Bankdaten sein sollten:

- Bewahren Sie Ihre Zugangsdaten an einem sicheren Ort auf, so dass diese nicht gestohlen oder kopiert werden können.
- Geben Sie niemals Ihre Bankdaten oder TANs im Internet weiter (z.B. in sozialen Netzwerken).
- Nutzen Sie Ihre Bankdaten nur auf der Banking-Plattform Ihres Online-Banking-Anbieters oder in vertrauenswürdigen Online-Shops.
- Speichern Sie keine Bankdaten auf Ihrem PC oder auf Ihrem Handy/ Smartphone.
- Wechseln Sie in regelmäßigen Abständen ihr Kennwort für den Zugang zum Online-Banking.
- Reagieren Sie nicht auf Phishing-Mails. Ihre Bank fordert Sie niemals per E-Mail oder Telefon dazu auf, vertrauliche Daten bekannt zu geben.

2. Verschlüsselung
Wenn Transaktionen nicht über das https-Protokoll übertragen werden, werden die Informationen nicht verschlüsselt und können gegebenenfalls im Internet ausgelesen werden.

- Achten Sie darauf, dass bei der Übertragung der Daten die Kommunikation verschlüsselt wird. Dies können Sie an der Verwendung des https-Protokolls erkennen.
- Verschlüsseln Sie Ihre WLAN-Verbindung

3. Überweisungslimit
Durch das Festsetzen eines Höchstbetrags für Überweisungen können Sie verhindern, dass bei Verlust oder Diebstahl Ihrer Zugangsdaten sehr hohe Summen von Ihrem Konto abgebucht werden.
Legen Sie mit Ihrer Bank ein Limit für tägliche Geldbewegungen fest.

4. Webseite des Online-Banking-Anbieters
Betrüger können Webseiten erstellen, die der Ihrer Bank täuschend ähnlich sehen. Geben Sie dort Ihre Bankdaten ein, landen diese direkt bei den Online-Kriminellen.

- Überprüfen Sie regelmäßig die Seite des Online-Banking auf auffällige Veränderungen. Wenn Sie beim Login nach einer TAN gefragt werden, befinden Sie sich mit Sicherheit auf einer gefälschten Seite.
- Geben Sie die Internetadresse Ihrer Bank bei jedem Aufruf erneut über die Tastatur ein.
- Überprüfen Sie das Zertifikat, das unser Online-Banking zur Verifizierung der Webseite anbietet.

5. Eigenes Gerät
Wer Bankgeschäfte im Internetcafé abwickelt, riskiert, dass Kriminelle diese Informationen im Cache auslesen.

- Betreiben Sie Online-Banking – soweit möglich – nur von eigenen Geräten aus.

6. Sichere Kommunikationswege
Die sichere Kundenkommunikation (insbesondere über potentielle Risiken und sicherheitsrelevante Änderungen in Zahlungsverkehrs-Verfahren oder zum Online-Banking) erfolgt durch uns über folgende Kanäle:

Elektronisch: als Information in Ihren elektronischen Postkorb des Online-Bankings oder über den Kontoauszugsdrucker.
Schriftlich: Per Brief.
Persönlich: Im Beratungsgespräch mit dem Kunden.

Wir werden Sie nicht telefonisch oder per Mail auffordern, Überweisungen zu tätigen oder Ihre Zugangsdaten wie TAN oder PIN bekannt zu geben. Sollten Sie solche Aufforderungen erhalten, setzen Sie sich persönlich mit uns in Verbindung (Tel: 06561 63-0).

Wenn Sie alle Kriterien überprüft und abgehakt haben, sind Sie einem sicheren Online-Banking schon einen Schritt näher gekommen. Sollte Ihnen beim Online-Banking etwas verdächtig vorkommen, sperren Sie den Zugang bei Ihrer Bank. Schauen Sie am besten regelmäßig auf die Checkliste und rufen sich die Tipps in Erinnerung! Beachten Sie auch die Warnmeldungen des Bürger-CERT (www.buerger-cert.de) oder anderer Warndienste. Dort wird auf Schwachstellen und Angriffe auf Online-Banking-Anbieter hingewiesen. Weitere Informationen finden Sie auf www.bsi-fuer-buerger.de/Onlinebanking. Anmerkungen senden Sie bitte an fragen@bsi-fuer-buerger.de . Betreiben Sie Online-Banking – soweit möglich – nur von eigenen Geräten aus. Überprüfen Sie regelmäßig die Seite Ihres Online-Banking-Anbieters auf auffällige Veränderungen. Wenn Sie beim Login nach einer TAN gefragt werden, befinden Sie sich mit Sicherheit auf einer gefälschten Seite. Geben Sie die Internetadresse Ihrer Bank bei jedem Aufruf erneut über die Tastatur ein. Überprüfen Sie das Zertifikat, das Ihr Online-Banking-Anbieter zur Verifizierung der Webseite anbietet.