Volksbank Eifel eG

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

Herzlich willkommen

Sehr geehrte Kundin, sehr geehrter Kunde,

Sie haben sich für unser eBanking entschieden. Unsere Schritt-für-Schritt-Anleitung soll Sie bestmöglich bei der Erstanmeldung im eBanking unterstützen.

Wenn Sie das eBanking der Volksbank Eifel mit dem TAN-Verfahren VR SecureGo plus nutzen möchten, benötigen Sie ein Smartphone (Betriebssystem Android oder iOS) und die Smartphone-App VR SecureGo plus, um verschiedene Aktionen im eBanking mit einer TAN bestätigen zu können. Vor Nutzung des eBankings, wird das TAN-Verfahren eingerichtet.

Die in dieser Anleitung verwendeten Fachbegriffe können Sie ab Seite 6 mit einer kurzen Definition nachlesen.

Schritt 1: Sie erhalten Post

Nachdem Sie die Freischaltung für das eBanking beantragt haben, erhalten Sie Ihre persönlichen Zugangsdaten per Post. Zu Ihrer Sicherheit werden die Zugangsdaten zeitlich verzögert in Einzelbriefen versendet. In der Regel werden die Briefe innerhalb von 2-4 Tagen zugestellt.

Warten Sie mit der Einrichtung, bis Ihnen alle drei Briefe vorliegen!

Brief 1: Vertragsunterlagen Online-Banking (eBanking) mit Ihrem VR-Netkey (Die Bankausfertigung senden Sie bitte unterschrieben an uns zurück)

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

Brief 3: Ihr Aktivierungscode für Ihr gewähltes TAN-Verfahren TAN-App VR SecureGo plus

Schritt 2: Laden Sie die VR-SecureGo plus App auf Ihr Smartphone/Tablet herunter

Bitte nehmen Sie Ihr Smartphone zur Hand und laden Sie sich die VR SecureGo plus App im Appstore für alle Apple-Geräte oder im Playstore für alle Android-Geräte herunter oder scannen Sie den hier abgebildeten QR-Code.

Mit dieser App werden TANs erstellt, die Sie für verschiedene Aktionen im eBanking, zum Beispiel zur Bestätigung von Überweisungen und Daueraufträgen benötigen. Dadurch wird die Sicherheit des Online-Bankings enorm erhöht!

im Apple App Store (iOS)

SecureGo plus

im Google PlayStore (Android)

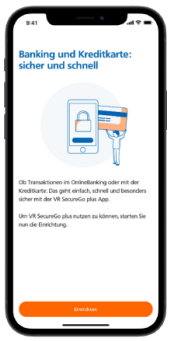
SecureGo plus

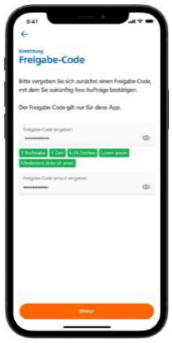
Schritt 3: Richten Sie die VR SecureGo plus App ein

Öffnen Sie die App VR SecureGo plus auf Ihrem Smartphone oder Tablet.

- Starten Sie über den Button „Einrichten".
- Die App bittet Sie um Erlaubnis, die Standortdaten des Smartphones auszulesen. Dies dient dazu, Betrugsversuche noch besser erkennen zu können.
- Die App zeigt Ihnen die Möglichkeit zum Erhalt von Push-Nachrichten an.
- Sie müssen nun einen Freigabe-Code eingeben. Diesen Code vergeben Sie sich selbst.
- Tipp: Unter den Feldern zum Freischalt-Code können Sie die biometrische Erkennung aktivieren. Wir empfehlen Ihnen, dies zu tun. Damit wird die Nutzung der App für Sie viel bequemer.

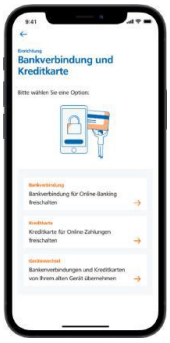
  Der Code muss zwischen 8-25 Zeichen lang sein und folgende Voraussetzungen erfüllen:
  1 Zahl
  1 Großbuchstabe
  1 Kleinbuchstabe





- Wählen Sie nun den Menüpunkt „Bankverbindung für Online-Banking freischalten“.
- Die App fordert Sie nun auf, den Zugriff auf Ihre Kamera zu gewähren.
- Scannen Sie nun den Aktivierungscode (QR-Code), den Sie mit unserem dritten Schreiben erhalten haben.
- Sofern Sie dem Zugriff auf die Kamera nicht zugestimmt haben, müssen Sie den Aktivierungscode manuell erfassen.

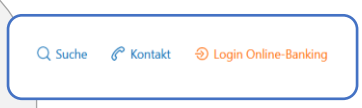
Herzlichen Glückwunsch! Sie haben sich nun erfolgreich für die Nutzung von VR SecureGo plus freigeschaltet.

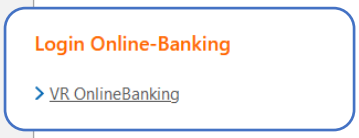


Schritt 4: Melden Sie sich zum ersten Mal im OnlineBanking an

Anmeldung über PC/Laptop

- Gehen Sie auf unsere Homepage www.volksbank-eifel.de und klicken sie oben rechts auf „Login Online-Banking"
- Klicken Sie dann auf "VR OnlineBanking"
- Nach der Anmeldung klicken Sie rechts oben auf Ihren Namen und öffnen das Fenster „Datenschutz & Sicherheit“ -> Onlinezugang





Anmeldung über die VR Banking App

- Bitte nehmen Sie Ihr Smartphone zur Hand und laden Sie sich die VR Banking App im Appstore für alle Apple-Geräte oder im Playstore für Android-Geräte herunter oder scannen Sie den hier abgebildeten QR-Code.
- Klicken Sie dann auf "Weiter", Sie werden zum Anmeldebildschirm geleitet.
- Geben Sie jetzt Ihr individuelles Anmeldekennwort ein, das bei jedem Start der App eingegeben werden muss (später ist auch Touch-ID/Fingerprint, bzw. Face-ID/Gesichtserkennung möglich).
  Das Anmeldekennwort muss mindestens 5 Zeichen enthalten. Sie erreichen eine erhöhte Sicherheit, wenn Sie Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen verwenden.
  Geben Sie nun Ihr Kennwort unter „Anmeldekennwort wiederholen“ ein zweites Mal zur Sicherheitsüberprüfung ein und tippen Sie auf „Weiter“.
- Als Nächstes geben Sie bitte die Bankleitzahl 58660101 ein.
- Weiter geht’s mit der **PIN-Änderung**

im Apple App Store (iOS)

im Google PlayStore (Android)

PIN-Änderung

- Geben Sie nun Ihren VR-NetKey (die 10-stellige Nummer) und Ihre Start-PIN ein - beides haben Sie per Post in zwei getrennten Briefen von uns bereits erhalten (Brief 1 und Brief 2) und klicken auf „Login“, bzw. „Anmelden“
- Ihre Start-PIN müssen Sie nun in eine selbstgewählte PIN ändern.
  Geben Sie im ersten Feld erneut Ihre Start-PIN ein.
- Geben Sie im zweiten Feld nun die von Ihnen gewählte neue PIN ein. Die PIN muss mindestens entweder rein numerisch sein oder mind.
  - 1 Großbuchstaben und 1 Ziffer enthalten.

  Erlaubter Zeichensatz:
  - Buchstaben: A-Z und a-z, inkl. Umlaute und ß
  - Ziffern: 0-9
  - Sonderzeichen: @ ! % & / = ? * + ; : , . _ -
- Geben Sie in das dritte Feld zur Bestätigung nochmals die von Ihnen gewählte neue PIN ein.
- Gehen Sie auf "Eingaben prüfen". An dieser Stelle senden wir Ihnen einen Auftrag in die VR SecureGo plus App zur Bestätigung.
- Öffnen Sie die VR SecureGo plus App auf Ihrem Smartphone.
- In der App erscheint nun der aktuelle Auftrag. Bitte prüfen Sie die in der App angezeigten Daten auf Richtigkeit und bestätigen Sie durch Eingabe des Anmeldekennworts den Vorgang.

Herzlichen Glückwunsch! Sie haben sich nun erfolgreich für das OnlineBanking freigeschaltet.
Schauen Sie sich in Ruhe um und lernen Sie Ihr neues OnlineBanking kennen.

Einen einfacheren Einstieg ins OnlineBanking bietet die Möglichkeit, anstelle des VR-NetKeys einen Anmeldenamen/Alias zu vergeben. Klicken Sie dazu bitte im OnlineBanking oben rechts auf Ihren Namen und öffnen das Fenster „Datenschutz & Sicherheit“ -> Onlinezugang

Schritt 5: Loggen Sie sich aus dem OnlineBanking aus

Es gibt zwei Möglichkeiten das OnlineBanking wieder zu verlassen.

- Wenn Sie alles erledigt haben und das OnlineBanking verlassen möchten, dann klicken Sie einfach oben rechts auf den Button "Abmelden".
- Wenn Sie länger als 5 Minuten inaktiv sind, dann führt das OnlineBanking einen automatischen Logout durch und meldet Sie aus dem OnlineBanking ab - diese Funktion dient Ihrer Sicherheit.

Wir wünschen Ihnen gutes Gelingen mit dem OnlineBanking Ihrer Volksbank Eifel eG!

So funktioniert OnlineBanking mit der VR SecureGo plus App

- Sie erfassen Ihre Transaktion im OnlineBanking. Beim Schritt „Eingabe prüfen" wird automatisch eine TAN angefordert.
- Öffnen Sie die VR SecureGo plus App auf Ihrem Smartphone. Sie können die App auch über das Antippen der Push-Nachricht aufrufen.
- Prüfen Sie in der App, ob die Transaktionsdaten (z.B. Betrag und Empfänger-IBAN) korrekt sind.
- Sind die übermittelten Daten richtig, bestätigen Sie den Vorgang und geben das Anmeldekennwort ein. Die TAN wird automatisch übertragen. Sie gilt nur für diese Transaktion.
- Sie erhalten eine Bestätigung für die erfolgreiche Ausführung der Transaktion.

Bei Fragen stehen wir Ihnen sehr gerne zur Verfügung.
Senden Sie uns eine E-Mail an info@volksbank-eifel.de oder
rufen Sie uns unter 06561 63-0 von Montag bis Freitag in der Zeit von 7:00 bis 19:00 Uhr an.
Wir helfen Ihnen sehr gerne weiter!

Untenstehend haben wir Ihnen Fachbegriffe zum Nachlesen und einige Informationen zur Sicherheit im OnlineBanking zusammengestellt.

Fachbegriffe

Alias: Der Alias-Name ist ein Benutzername, meist die Kurzform eines Namens oder ein Spitzname, der von Ihnen selbst vergeben wird und anstelle des schwer zu merkenden VR-Netkeys benutzt werden kann. Er wird dem persönlichen VR-Netkey zugeordnet und vereinfacht die Anmeldung.

App ID: Die App ID ist ein technischer Parameter, der eine eindeutige Identifikation ermöglicht.

Appstore/Playstore: Bezeichnung für eine internet-basierte digitale Vertriebsplattform für Anwendungssoftware. Hier wird Benutzern von Smartphones und Tablets ermöglicht, Software (Apps) aus einem Katalog herauszusuchen und herunterzuladen.

PIN: Das ist die Persönliche Identifikationsnummer, eine Geheimzahl, mit der man sich gegenüber einer Maschine authentisieren kann. Die PIN gilt als Schutz vor unberechtigter Nutzung und sollte nur dem jeweiligen Nutzer bekannt sein. Nach der ersten Anmeldung im eBanking werden Sie aufgefordert, diese Start-PIN zu ändern. Wir empfehlen Ihnen die Änderung in eine nur Ihnen bekannte PIN.

Push-Nachrichten: Das sind Nachrichten, die direkt auf dem Smartphone-Bildschirm erscheinen. Man hat durch Antippen dieser Nachricht direkten Zugriff auf die App, ohne diese erst im Menü öffnen zu müssen.

QR-Code: Das ist ein zweidimensionaler Code, der verschlüsselte Daten enthält. Scannen Sie z. B. den o. a. QR-Code, werden Sie direkt zum Herunterladen der VR SecureGo plus App im Appstore bzw. Playstore weitergeleitet.

TAN: TAN steht für Transaktionsnummer. Es handelt sich hier um eine sechsstellige Zahl, die als einmaliges Kennwort für eine Transaktion im eBanking genutzt wird. Ohne gültige TAN wird der Auftrag nicht ausgeführt. Da die Bank die Identität des Kunden nicht selbst über das Internet prüfen kann, muss der Kunde sich mit der TAN „ausweisen".

TAN-Verfahren: Um eine TAN erstellen zu können, bieten wir verschiedene Verfahren an: Die TAN-App VR SecureGo plus, hier wird die TAN auf dem Smartphone oder Tablet in der TAN-App empfangen oder das Sm@rt-TAN-Verfahren, hier erfolgt die Erstellung der TAN mit einem Lesegerät.

Touch-ID: Über die "Touch-ID" (iOS) bzw. den "Fingerprint" (Android) erfolgt die Anmeldung in der VR-SecureGO-App mittels Fingerabdruck anstatt des bisherigen Anmeldekennworts. Die Nutzung ist derzeit für iPhone- bzw. iPad-Nutzer (ab iPhone 5s / iPad Air2) und unter Android (ab Version 6) möglich. Ihr Anmeldekennwort bzw. Ihr Fingerabdruck wird verschlüsselt ausschließlich auf Ihrem Smartphone bzw. Tablet abgespeichert. Bitte verwenden Sie daher nur Ihren eigenen Fingerabdruck. Bei Verlust Ihres Smartphones oder Ihres Tablets informieren Sie bitte unverzüglich Ihre Volksbank Eifel eG. Aus Sicherheitsgründen empfehlen wir, die Touch-ID bzw. den Fingerprint nicht gleichzeitig für die VR Banking App und die TAN-App VR SecureGo plus zu nutzen.

Transaktionen: Hierunter versteht man vorwiegend Bezahlvorgänge, aber auch weitere Aufträge, die im OnlineBanking getätigt werden.

VR-Netkey: Der VR-Netkey ist Ihr persönlicher Benutzername für den Online-Zugang zu allen Konten, für die Sie verfügungsberechtigt sind.

Worauf sollten Sie beim OnlineBanking achten?

Wenn Sie einige Grundregeln beachten, lässt sich die Sicherheit des OnlineBankings 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 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.

4. Kontobewegungen

Überprüfen Sie in regelmäßigen Abständen die Bewegungen Ihres Kontos.

5. Webseite des Online-Banking-Anbieters

Betrüger können Webseiten erstellen, die dem Original täuschend ähnlich sehen. Geben Sie dort Ihre Bankdaten ein, landen diese direkt bei den Online-Kriminellen.

- Gehen Sie stets kritisch mit Veränderungen in Ihrem Online-Banking um.
- Geben Sie die Internetadresse Ihrer Bank bei jedem Aufruf erneut über die Tastatur ein. Überprüfen Sie das Zertifikat, das wir Ihnen zur Verifizierung der Webseite anbieten.

6. Eigenes Gerät

Wer Bankgeschäfte im Internetcafé abwickelt, riskiert, dass Kriminelle diese Informationen im Cache (Zwischenspeicher) auslesen. Der Cache ist ein Puffer-Speicher, in dem Daten für ein schnelleres erneutes Zugreifen zwischengespeichert sind.

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

Wenn Sie alle Kriterien berücksichtigen, sind Sie einem sicheren Online-Banking schon einen Schritt näher gekommen. Sollte Ihnen beim OnlineBanking etwas verdächtig vorkommen, informieren Sie uns umgehend unter 06561 63-0. Unser KundenServiceCenter ist Montag bis Freitag von 7:00 - 19:00 Uhr für Sie erreichbar. Schauen Sie am besten regelmäßig auf diese Checkliste und rufen sich die Tipps in Erinnerung.