Volksbank Eifel eG

Hinweise zum Ersteinstieg beim eBanking mit dem Sm@rt-TAN photo-Verfahren

1. Nachdem Sie den Brief mit der Start-PIN erhalten haben, rufen Sie bitte im Internet unsere Homepage **www.volksbank-eifel.de** auf.

2. Wählen Sie bitte den Button Login rechts oben und dann Zum Konto/Depot

3. Es öffnet sich ein neues Fenster, in dem Sie nach Ihren **VR-NetKey** (diesen entnehmen Sie bitte dem separat beigefügten Schreiben) und der **PIN** gefragt werden. Als PIN geben Sie bitte die **erhaltene Start-PIN** ein und klicken auf Anmelden

4. Jetzt werden Sie aufgefordert, Ihre vorgegebene Start-PIN in eine **persönliche PIN** zu ändern. Geben Sie zunächst bei „Aktuelle PIN" die Start-PIN ein, die Sie mit der Post erhalten haben. Anschließend vergeben Sie sich eine neue PIN und bestätigen diese im Feld „Wiederholung neue PIN". Nach erfolgter Eingabe klicken Sie bitte auf den Button „Eingaben prüfen".

5. Beim Sm@rt-TAN photo-Verfahren klicken Sie bitte auf TAN-Eingabe durch Farbcode-Erkennung (Sm@rt-TAN photo) nun erscheint ein stehendes Bild (Farbcode-Grafik, ähnlich eines QR-Codes) auf Ihrem Bildschirm.

6. Schieben Sie Ihre Bankkarte oben in den TAN-Generator und drücken die Taste "Scan" (**rechte schwarze Taste**). Halten Sie den TAN-Generator so vor die Farbcode-Grafik, dass der Farbcode in der Anzeige vollständig zu sehen ist. Prüfen Sie die Anzeige auf dem Display Ihres TAN-Generators und drücken Sie "OK".

7. Im Display werden jetzt Kontrolldaten angezeigt. Prüfen Sie bitte diese Daten und bestätigen sie jeweils mit der OK-Taste, bis Ihre Transaktionsnummer (TAN) erscheint.

8. Abschließend bestätigen Sie die Änderung Ihrer PIN, indem Sie die erhaltene TAN in dem dafür vorgesehenen Feld eingeben und auf > Weiter klicken.

9. 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 Service und dann auf Alias

Bei weiteren 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!
Auf der Rückseite haben wir Ihnen einige Informationen zur Sicherheit im Online-Banking 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 und Ihre TAN-Listen 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.
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.