Sicherheit im Onlinebanking

Spar- und Kreditbank des Bundes Freier evangelischer Gemeinden eG

Mit dieser Kundeninformation möchten wir Ihnen einige Tipps zum sicheren Online-Banking geben.

Hotline

Bei Fragen stehen wir Ihnen telefonisch unter 02302/93030-19 oder per Mail über die Adresse info@skbwitten.de zur Verfügung.

Mit uns kommunizieren

Sensible Daten werden von uns nur über sichere Kommunikationswege übermittelt. Hierfür nutzen wir folgende Kanäle:

- Persönlich in unseren Bankräumen
- Per Briefzustellung
- Der elektronische Postkorb im Internetbanking
- Via papierhaften Kontoauszug
- Per Fax

Einloggen

Das Login zum Internetbanking finden Sie auf unserer Internetseite www.skbwitten.de oben rechts. Bitte gehen Sie nicht über Schaltflächen, z. B. in einer E-Mail (Phishing), in das Internetbanking. Wenn Sie die Internetseite als Lesezeichen oder Favoriten anlegen, können Sie die Seite schnell erreichen.

Virenschutz & Firewall

Zu Ihrer Sicherheit sollte Ihr Computer immer über einen aktuellen Virenschutz und eine Firewall verfügen. Sie sollten nur ein aktuelles Betriebssystem auf Ihrem Computer einsetzen.

Konto sperren

Sollten Sie der Meinung sein, dass jemand anderes Zugriff zu Ihrem Konto erhalten hat, können Sie das Konto jederzeit durch absichtliche Eingabe von falschen PIN-Nummern sperren. Es erscheint nach drei Fehlversuchen der Hinweis „Konto gesperrt“. Alternativ können Sie auch Ihren Berater anrufen oder die zentrale Sperrhotline 116 116 nutzen.

PIN & TAN zurücksetzen

Sollte Ihr Konto gesperrt sein, können Sie über den Kundenauftrag „PIN-TAN Rücksetzung“ die Zusendung einer neuen Start-PIN beauftragen. Zu Ihrer Sicherheit geht dies nur mit dem von Ihnen unterschriebenen Kundenauftrag. Den Vordruck finden Sie auf unserer Internetseite unter „Downloads“.

Limit temporär ändern

Mit dem Onlinebankingvertrag wurde ein Verfügungslimit vereinbart, welches Sie jederzeit temporär ändern lassen können. Zu Ihrer Sicherheit sollte der Betrag nur so hoch sein, wie Sie für gewöhnlich überweisen. Die Änderung erfolgt mittels unterschriebenen Kundenauftrag „Limitänderung“ (den Vordruck finden Sie auf unserer Internetseite unter „Downloads“) oder durch Nachricht über den elektronischen Postkorb.

Phishing

Immer wieder werden E-Mails versendet, die aussehen, als kämen sie von einer Bank. Wir würden Sie nie per E-Mail auffordern, auf Ihre Onlinebankingseite zu gehen oder sensible Daten preiszugeben. E-Mails stellen keine sichere Kommunikation dar.