

Sicherheitshinweise für die BKB-Online-Banking-Nutzung

E-Banking-Systeme von Banken werden nicht nur von den Kunden für eine ordnungsgemäße Auftragsübermittlung und den Abruf von Kontoinformationen genutzt, sondern auch unberechtigte Dritte versuchen vielfach, unberechtigt und aus betrügerischer Absicht einen Zugang zu erhalten. Vor diesem Hintergrund sollten Sie sich schützen und folgende Sicherheitshinweise für die BKB-Online-Banking-Nutzung dringend beachten:

1. Ihr PC

- Halten Sie das Betriebssystem auf Ihrem PC stets auf dem neuesten Stand, indem Sie die laufenden Aktualisierungen, u. a. zwecks Schließen von festgestellten Sicherheitslücken, manuell oder besser automatisiert regelmäßig installieren.
- Aktivieren Sie grundsätzlich die „Firewall“ in Ihrem Betriebssystem. Hierdurch werden alle aus- und eingehenden Verbindungen überwacht und ungewöhnliche Situationen angezeigt.
- Für den Zugang zum Internet ist die Benutzung eines „Browsers“ erforderlich. Nutzen Sie ausschließlich einen vertrauenswürdigen Browser, stets in der neuesten Version durch regelmäßige Aktualisierung, und aktivieren Sie die Sicherheitseinstellungen.
Einen Browser ohne Sicherheitseinstellungen sollten Sie bei der BKB-Online-Banking-Nutzung nicht benutzen.
- Schließen Sie Browserfenster nach der Abmeldung aus dem BKB-Online-Banking und löschen Sie regelmäßig die Browserdaten (Cookies, Verlauf, Cache) auf Ihrem PC.
- Die Nutzung eines regelmäßig aktualisierten Virenschanners ist unverzichtbar, um sich vor schädlicher Software (z. B. Viren und Trojaner) zu schützen. Lassen Sie den eingesetzten Virenschanner am besten automatisiert aktualisieren und führen Sie regelmäßig eine Überprüfung des Datenbestands Ihres PCs auf Virenbefall durch.
- Stellen Sie sicher, dass bei einer Datenübertragung über ein WLAN (lokales Funknetz) die Verschlüsselung aktiviert ist, verzichten Sie grundsätzlich auf eine E-Banking-Nutzung über öffentliche „Hotspots“ und deaktivieren Sie das „Bluetooth“ während der E-Banking-Nutzung.
- Wenn Ihnen Unstimmigkeiten bei Ihren Arbeiten im BKB-Online-Banking auffallen, sollten Sie die Arbeiten sofort abbrechen und uns unverzüglich darüber informieren. Dies gilt auch, wenn Sie feststellen, dass Ihr PC von einer schädlichen Software befallen ist.

Wir weisen darauf hin, dass wir keine Verantwortung für die von Ihnen eingesetzte Technik für die E-Banking-Nutzung übernehmen können.

2. Zugangsdaten

Für die Anmeldung im BKB-Online-Banking ist die Erfassung einer Kundennummer, Teilnehmernummer und eines persönlichen PINs erforderlich. Ihre Kundennummer und Teilnehmernummer werden Ihnen von der BKB Bank zur Verfügung gestellt und können von Ihnen nicht geändert werden. Die PIN ist von Ihnen selbst zu bestimmen.

Bitte beachten Sie hierzu die folgenden Empfehlungen:

- Achten Sie bei der Auswahl der PIN auf eine hohe Sicherheit (Kombination aus Buchstaben, Groß- und Kleinschreibung und Zahlen) und verzichten Sie auf eine einfache PIN (z. B. Geburtsdatum, Namen, Telefon-Nummern etc.)
- Verzichteten Sie darauf, die PIN und die Anmeldedaten auf Ihrem PC zu speichern und geben Sie diese Daten auf keinen Fall einem Dritten bekannt, auch nicht einem Ansprechpartner bei der BKB-Bank.
- Die PIN sollte von Ihnen in regelmäßigen Abständen geändert werden. Bei einem Verdacht, dass Dritte Kenntnis über die PIN erhalten haben könnten, sollte eine Änderung unverzüglich vorgenommen werden.
- Verwenden Sie Ihre PIN für das BKB-Online-Banking nicht gleichzeitig auch für sonstige Anmeldungen im Internet (z. B. E-Mail).

Für die Autorisierung von E-Banking-Vorgängen ist die Erfassung einer TAN erforderlich.

Im BKB-Online-Banking erfolgt die Bereitstellung der TANs über papierhafte TAN-Listen und alternativ über TAN-Generator mit Signaturkarte.

Bitte beachten Sie hierzu folgende Hinweise:

- Bewahren Sie die Ihnen zur Verfügung gestellten TAN-Listen und den TAN-Generator/die Signaturkarte sicher (ggfs. auch unter Verschluss) und stets getrennt von der PIN auf.
- Hinterlegen Sie Ihre TAN-Listen, gescannt oder manuell erfasst, niemals auf Ihrem PC oder Ihrem Smartphone und nutzen Sie ausschließlich die zur Verfügung gestellte Papier-Version.
- Überprüfen Sie bei der Aufforderung zur TAN-Angabe nochmals die Auftragsdaten. Stellen Sie Abweichungen von Ihren Erfassungen fest, brechen Sie den Vorgang bitte sofort ab und informieren Sie uns unverzüglich.

Wir weisen darauf hin, dass die BKB Bank Sie niemals auffordern wird, Ihre Zugangs- und Autorisierungsdaten (PIN und TAN) bekannt zu geben. Informieren Sie uns bitte unverzüglich, wenn Sie solch eine Anfrage telefonisch oder per E-Mail erhalten sollten und verweigern Sie stets eine Bekanntgabe.

3. Ergänzende Maßnahmen

- Begrenzen Sie Ihr Limit für Überweisungsausführungen auf die für Sie notwendige Höhe. Sollte das von Ihnen gewählte Limit in Einzelfällen nicht ausreichen, können Sie eine zeitlich begrenzte Erhöhung über Ihren zuständigen Betreuer veranlassen.
- Führen Sie regelmäßig eine Kontrolle der Umsätze auf Ihrem Konto durch. Beschränken Sie Ihre Kontrolle nicht nur auf Beträge, sondern überprüfen Sie stets auch die sonstigen Umsatz-Angaben.
- Überprüfen Sie bei Ihrer Anmeldung im BKB-Online-Banking, dass Ihnen die Internet-Adresse <https://www.bv-activebanking.de/kbc-bank/loginFormAction.do> angezeigt wird.
- Pflegen Sie einen sehr vorsichtigen Umgang mit E-Mails von Ihnen unbekanntem Absendern und vermeiden Sie grundsätzlich, beigefügte Anhänge in diesen E-Mails zu öffnen. Über das Öffnen der Anhänge kann schädliche Software auf Ihren PC gelangen. Wir empfehlen, E-Mails von unbekanntem Absendern generell zu löschen.
- Installieren Sie auf Ihrem PC ausschließlich Software von vertrauenswürdigen Anbietern. Von der BKB Bank werden Sie nicht aufgefordert werden, Software oder Apps zu installieren. Halten Sie bei solch einer Anfrage vor einer Ausführung stets Rückfrage bei uns.
- Besteht Ihrerseits der Verdacht, dass Ihre Tätigkeiten im BKB-Online-Banking nicht wie von Ihnen gewohnt ablaufen oder stellen Sie ggf. andere/geänderte optische Darstellungen fest, brechen Sie den Vorgang bitte sofort ab und informieren Sie uns unverzüglich. Wir werden den Zugang sofort sperren, um eventuelle Schäden zu vermeiden.

Wir bedanken uns bei Ihnen für die Beachtung der Sicherheitshinweise im BKB-Online-Banking. Seien Sie bei Ihren Tätigkeiten im BKB-Online-Banking stets wachsam und kritisch. Nur dadurch können betrügerische Handlungen im E-Banking durch unberechtigte Dritte vermieden werden.