

---

# Was Sie selbst zur Sicherheit beitragen können

## BTV Tipps:

Phishing nutzt wie die meisten Trickbetrügereien eine Kombination aus technischen und menschlichen Schwächen. Doch mit einer gesunden Portion Misstrauen und den folgenden Verhaltensregeln können Sie sich effektiv gegen Betrüger schützen.

- Geheimhaltung der PIN: gehen Sie mit Ihrer BTV ONLINE-Banking PIN mit der gleichen Sorgfalt um, wie Sie dies mit Ihrem Bankomat-PIN tun.
- Geheimhaltung der TAN-Codes: verwahren Sie Ihren TAN-Generator und Ihre Chipkarte immer an einem sicheren Ort.
- Sperren Sie Ihren Zugang zum ONLINE-Banking, sobald Sie den Verdacht haben, dass ein Dritter im Besitz Ihrer PIN oder TAN ist.
- Vereinbaren Sie ein Tageslimit für Onlineüberweisungen. So kann möglicher Schaden von vornherein begrenzt werden.
- Verlassen Sie die BTV ONLINE-Banking-Anwendung stets durch Klick auf den link „Abmelden“. Dadurch wird die sichere Verbindung mit dem Server sofort beendet. Zu Ihrer Sicherheit erfolgt eine automatische Abmeldung vom BTV ONLINE-Banking, falls über eine längere Zeit kein Funktionsaufruf oder sonstige Eingaben erfolgen. Sie kommen zur Eingabemaske zurück und müssen für einen neuerlichen Einstieg wieder Ihre Identifikationsmerkmale eingeben.
- Änderung Ihrer PIN: falls Sie den Verdacht haben, dass jemand Ihre PIN in Erfahrung gebracht haben könnte, ändern Sie sofort Ihre PIN im BTV ONLINE-Banking.
- Es wird Ihnen empfohlen weder PIN noch ONLINE-Banking-Nummer in irgendeiner Software abzuspeichern, da dies ein Sicherheitsrisiko darstellen würde.
- Regelmäßige Updates gewährleisten, dass die Sicherheitsvorkehrungen von Internetbrowser und Betriebssystem immer auf dem neuesten Stand sind. Dazu sollten auch die sogenannten Patches oder Bug-Fixes, mit denen die Hersteller regelmäßige Sicherheitslücken schließen, unverzüglich installiert werden.
- Auch der Browser kann mit entsprechenden Einstellungen vor fremden Zugriff gesichert werden. Dabei sollten etwa die Ausführung von Active-X-Inhalten unterbunden und Java-Anwendungen nur nach Rückfrage gestattet werden.
- Ein Virens Scanner, der regelmäßig aktualisiert werden muss, kann den Rechner vor Angriffen durch Hacker schützen. Eine persönliche Firewall überwacht zudem den ein- und ausgehenden Netzverkehr und verhindert unbefugte Zugriffe von außen.
- Seriöse Internet-Anbieter fragen niemals nach sicherheitsrelevanten Daten! Antworten Sie deshalb grundsätzlich nicht auf E-Mails, bei denen – aus welchem Grund auch immer – nach Ihrer PIN oder TAN gefragt wird.
- Verwenden Sie keine Links aus Mail-Adressen, um Ihr ONLINE-Banking aufzurufen. Geben Sie die Adresszeile stets von Hand ein. Oder benutzen Sie Bookmarks, die Sie selbst angelegt haben.
- Prüfen Sie, ob die angezeigte Internet- Adresse mit der zertifizierten Adresse Ihrer Bank übereinstimmt (Doppelklick auf das VeriSign-Symbol). Bei Abweichungen den Vorgang sofort abbrechen und die Bank benachrichtigen.