Was tun im Falle eines Missbrauchs?

Sperren Sie Ihren Online-Banking-Zugang, sobald Sie glauben, dass ein **Dritter Ihre PIN oder TAN erlangt hat.**
Wichtig: Wenn Sie eine betrügerische Überweisung feststellen, sollten Sie Ihren Online-Banking-Zugang ebenfalls sperren und sich unverzüglich (außerhalb unserer Geschäftszeiten am nächsten Bankgeschäftstag ab 8:00 Uhr) mit Ihrer kontoführenden Geschäftsstelle in Verbindung setzen und veranlassen Sie einen Überweisungsrückruf.

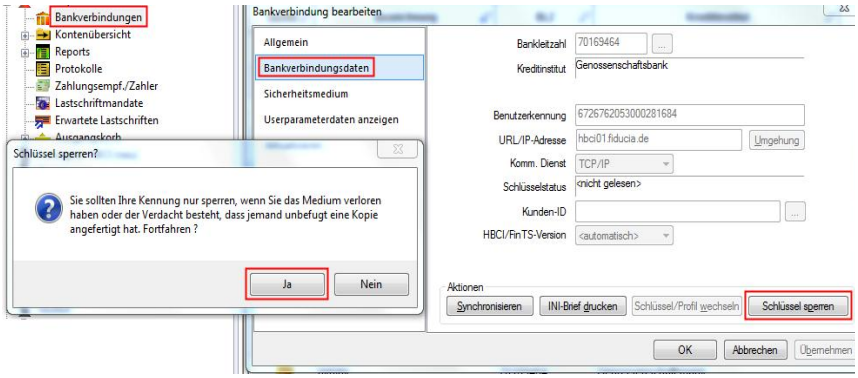
Sperren des Online-Banking-Zugangs – PIN / TAN (Internetseite)

Im Online-Banking unter „Service“, Online-Zugang sperren“ (siehe Bild)

oder durch **neunmalige Falscheingabe der PIN in der Anmeldemaske.**

Hinweis: Nach dreimaliger Falscheingabe ist **nur** die PIN gesperrt. Mit der PIN und einer TAN, kann der Account wieder entsperrt werden.

Sperren des Online-Banking-Zugangs – HBCI mit Schlüsseldatei und Zahlungsverkehrssoftware / VR-Networld-Software:



In der VR-Networld-Software:
1. Wählen Sie in der Baumstruktur Ihre **Bankverbindung**;
2. **Bankverbindungsdaten**
3. **„Schlüssel sperren“**.
4. **„Schlüssel sperren?“** mit **„Ja“ bestätigen.**

Bei Einsatz eines anderen Zahlungsverkehrsprogramms informieren Sie sich bitte beim Hersteller der Software, ob bzw. wie der Online-Zugang im Programm gesperrt wird.

Eine Sperrung des Online-Zugangs über VR-NetKey oder HBCI ist auch durch uns unter folgenden Telefonnummern möglich:

- **Bank:** **089 86303-251 oder -271** (Mo. bis Fr. 8:00 bis 16:00 Uhr; Do. bis 17:30 Uhr)
- **Zentrale Sperrhotline:** **116 116** (24/7; innerhalb Deutschlands gebührenfrei)
- **Hotline für Fragen zum Thema Sicherheit: 0800 5053111** (außerhalb unserer Geschäftszeiten, 8:00 bis 24:00 Uhr)