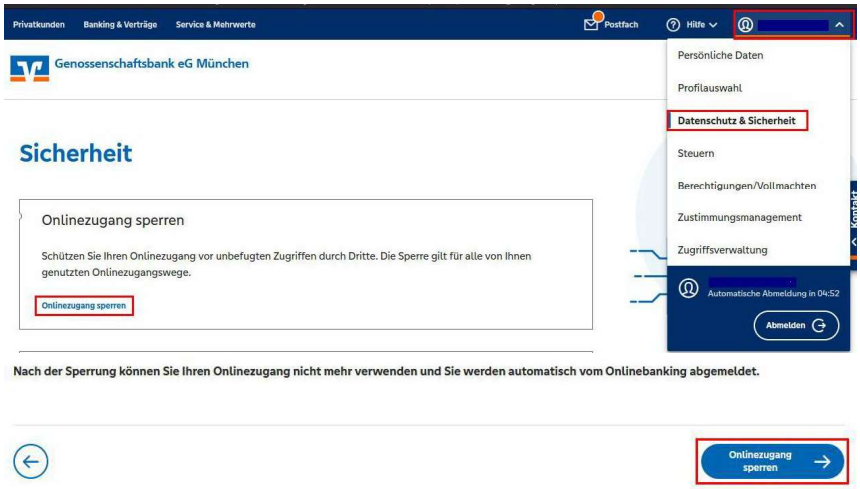
Was tun im Falle eines Missbrauchs?

Sperren Sie Ihren Online-Banking-Zugang, sofern Sie glauben, dass ein **dritte Person Kenntnis über Ihre Zugangsdaten erlangt hat.**
Wichtig: Wenn Sie eine betrügerische Überweisung feststellen, sollten Sie Ihren Online-Banking-Zugang ebenfalls sperren (außerhalb der Öffnungszeiten über die Allgemeine Sperrrufnummer 116 116) und sich unverzüglich (außerhalb unserer Geschäftszeiten am nächsten Bankgeschäftstag ab 9:00 Uhr) mit Ihrer kontoführenden Geschäftsstelle in Verbindung setzen und veranlassen Sie einen Überweisungsrückruf.

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

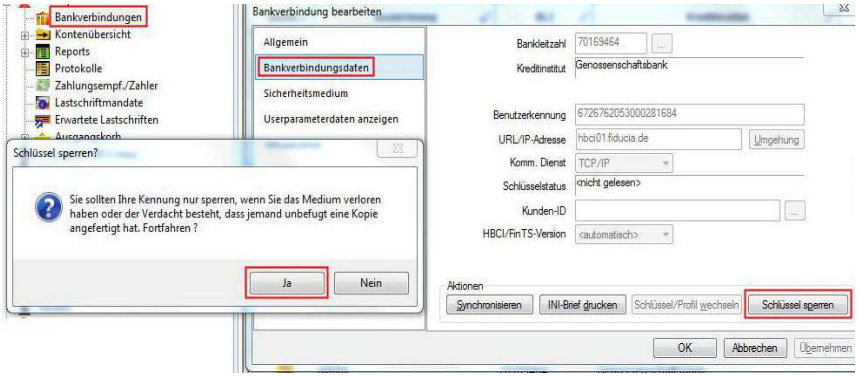


In VR OnlineBanking nach der Anmeldung in der rechten oberen Ecke das Menü öffnen, danach auf „Datenschutz & Sicherheit und dann auf „Onlinebanking sperren“ (siehe Bild). Auf der Folgeseite bestätigen Sie die Eingabe bitte nochmal.

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 werden kann.

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

- **Bank (IT-Abteilung):** **089 86303-0** während den Öffnungszeiten (siehe Homepage)
- **Zentrale Sperrhotline:** **116 116** (24/7; innerhalb Deutschlands gebührenfrei)