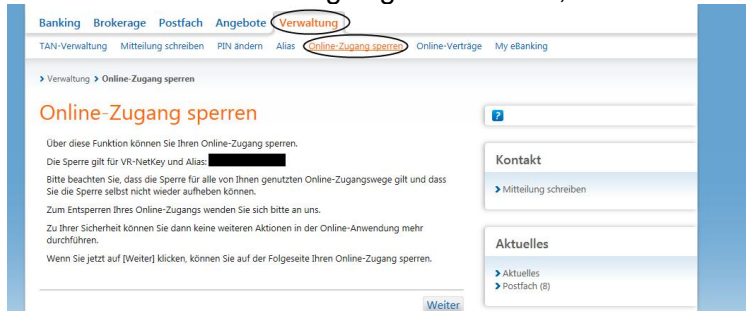


Was tun im Falle eines Missbrauchs?

Sperren Sie Ihren Online-Banking-Zugang, sobald Sie glauben, dass ein Dritter Ihre PIN oder TAN erlangt hat. Sobald Überweisungen in Ihren Kontobewegungen aufgeführt werden, die Sie nicht getätigt haben, sollten Sie ebenfalls Ihren Online-Banking-Zugang sperren.

Dies geht am schnellsten direkt über Ihren Online-Banking-Zugang unter der Rubrik „Verwaltung“ und dem Menüpunkt „Online-Zugang sperren“ (siehe Bild) oder durch neunmalige falsche Eingabe Ihrer PIN bei der Online-Banking-Anmeldung.

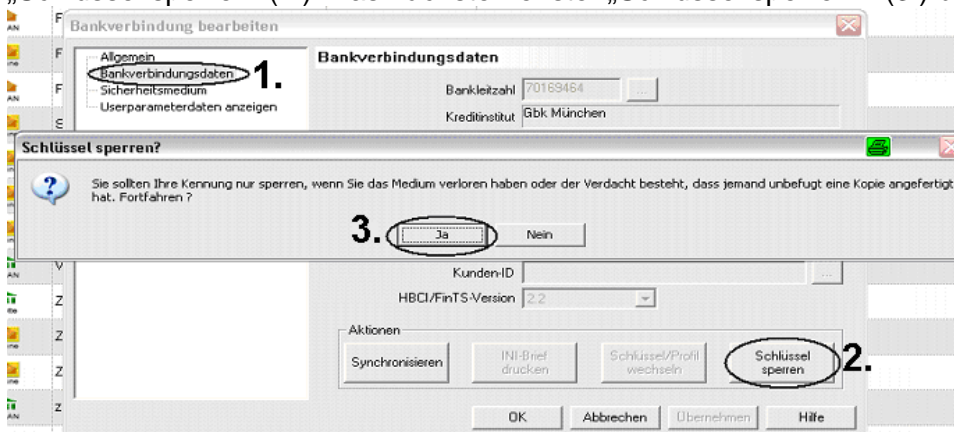
Bereits nach dreimaliger Falscheingabe ist zwar die PIN gesperrt, falls der Kriminelle jedoch die korrekte PIN sowie eine gültige TAN kennt, ist er in der Lage den Zugang wieder zu entsperren.



Wichtiger Hinweis für Teilnehmer unseres weiteren Online-Zahlungsverkehrs-Verfahrens „HBCI mit Schlüsseldatei“ und Zahlungsverkehrssoftware:

Die Sperre des HBCI-Schlüssels kann entweder durch die Bank erfolgen oder direkt in der Zahlungsverkehrssoftware rund um die Uhr selbst durchgeführt werden. Beim Einsatz von VR-Networld-Software gehen Sie bitte wie folgt vor:

Wählen Sie in der Baumstruktur Ihre Bankverbindung aus und öffnen Sie diese. Im folgenden Fenster wählen Sie „Bankverbindungsdaten“ (1.) und klicken Sie auf die Schaltfläche „Schlüssel sperren“ (2.). Das nächste Fenster „Schlüssel sperren?“ (3.) bestätigen Sie mit „Ja“.



Bei Einsatz anderer Zahlungsverkehrsprogramme informieren Sie sich bitte beim Hersteller beziehungsweise beim Herausgeber der Software, ob der Online-Zugang im Programm gesperrt werden kann und was hierbei zu beachten ist.

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

Bank: 089 / 86 303 -251 oder -271 (Mo. bis Fr. 8:00 bis 16:00 Uhr; Do. bis 17:30 Uhr)

Weitere Hotlines: 116 116 (außerhalb unserer Geschäftszeiten; innerhalb Deutschlands gebührenfrei)

Hotline für Fragen zum Thema Sicherheit:

0800 / 505 3111 (außerhalb unserer Geschäftszeiten, 8:00 bis 24:00 Uhr)

Wichtig:

Für den Fall, dass Sie eine betrügerische Überweisung feststellen, setzen Sie sich unverzüglich (außerhalb unserer Geschäftszeiten am nächsten Bankgeschäftstag ab 8:00 Uhr) mit Ihrer kontoführenden Geschäftsstelle in Verbindung und veranlassen Sie einen Überweisungsrückruf.