M. M. WARBURG & CO
1798

Allgemeine Sicherheitshinweise für Zahlungen im Internet

- Stellen Sie sicher, dass Ihr PC oder Ihr Smartphone durch aktuelle Firewalls und Antivirenprogramme ausreichend geschützt ist. Aktualisieren Sie Ihre Software regelmäßig und führen Sie wöchentlich einen Suchlauf durch. Eine veränderte Anzeige Ihrer Programme auf Ihrem PC kann ein Hinweis auf eine vorhandene Schadsoftware sein.

- Weitere Sicherheitshinweise sowie aktuelle Warnungen vom Bundesamt für Sicherheit in der Informationstechnik finden Sie unter www.bsi-fuer-buerger.de.

- Geben Sie unsere Internetadresse für das Online-Banking immer direkt in Ihrem Browser ein. Verwenden Sie keine Bookmarks oder Favoriten und folgen Sie keinen Weblinks. Die Verbindung muss immer über eine sichere Verbindung erfolgen. Achten Sie daher darauf, dass die Internetadresse immer mit den Buchstaben „https://“ beginnt.

- Unsere Mitarbeiter oder Mitarbeiter unserer Partner (z. B. MasterCard) werden Sie niemals per E-Mail oder telefonisch nach Ihren vertraulichen Daten wie zum Beispiel Ihrer Kreditkartennummer, Ihrer PIN oder einer TAN fragen. Geben Sie diese nicht an unberechtigte Dritte weiter.

- Nutzen Sie für das Online-Banking möglichst nur unsere Web-Anwendung oder eine sichere HBCI-Software.

- Bitte beachten Sie, dass Sie beim Anmelden zum Online-Banking nur Ihre Kundennummer und Ihren persönlichen PIN eingeben müssen. Falls Sie aufgefordert werden weitere persönliche Daten einzugeben, tun Sie dies nicht und informieren Sie uns umgehend.

- Nutzen Sie nur starke Passwörter die schwer zu knacken sind. Besonders sicher sind willkürliche Kombinationen aus Zahlen, Buchstaben und Sonderzeichen. Wiederholungen, bekannte Namen, Geburtsdaten und Zahlenreihen sind als Passwort ungeeignet. Vermerken Sie Ihr Passwort niemals auf Ihrer Festplatte, im Adressbuch oder im Telefonverzeichnis.

- Sollten Sie den Verdacht haben, dass unberechtigte Dritte Kenntnis über Ihre Zugangsdaten haben oder im Besitz einer gültigen TAN sind, muss das Online-Banking oder Ihre Kreditkarte sofort gesperrt werden. Das Online-Banking können Sie direkt über die Anwendung unter dem Reiter Verwaltung, durch 3 x falsche PIN-Eingaben oder über die unten genannte Sperrhotline sperren. Die Kreditkarte können Sie über die Sperrhotline +49 116 116 sperren.

- Nutzen Sie für Transaktionen im Internet keinen öffentlichen Computer oder WLAN‘s, da Sie keine Informationen über die Sicherheitsvorkehrungen haben.

- Sobald Sie sich auf einer Internetseite anmelden, melden Sie sich vor dem Verlassen der Seite wieder ab. Nur dadurch wird die Datenverbindung zur Internetseite zuverlässig getrennt.

12129 Version 01.18

M. M. WARBURG & CO
1798

Sicherheitshinweise für das mobile TAN Verfahren

- Die Zusendung der TAN per SMS ist ein wichtiger Sicherheitsbestandteil für die Nutzung Ihres Online-Bankings. Sollten Sie Ihr Mobiltelefon verloren haben, benachrichtigen Sie uns umgehend unter der unten aufgeführten Sperrhotline! Wir veranlassen eine sofortige Sperre Ihres Zuganges zum Online-Banking.

- Geben Sie niemals Ihre Mobiltelefonnummer in ein Webformular ein. Die Bank möchte niemals Ihre Mobilfunknummer über ein Webformular bestätigt haben oder wird eine Änderung über ein Webformular vornehmen.

- Sofern Sie aufgefordert werden, im Zusammenhang mit dem Online-Banking, ein Sicherheitszertifikat auf Ihr Mobilfunktelefon zu laden, führen Sie dieses nicht aus und informieren Sie uns umgehend. Für die Nutzung der mobilen TAN ist weder ein Zertifikat noch eine zusätzliche Anwendung nötig.

- Ein wichtiges Sicherheitsmerkmal für die Nutzung des mobilen TAN-Verfahrens ist die Trennung der Übertragungswege der Online-Banking-Anwendung sowie der Übermittlung der TAN. Wird die Trennung durch die Nutzung der Anwendung auf dem Mobiltelefon aufgehoben, ist dieser Schutz nicht mehr gewährleistet. Daher sollte das Gerät, mit dem die TAN empfangen werden, nicht gleichzeitig für das Online-Banking genutzt werden.

- Prüfen Sie beim mobilen TAN-Verfahren stets sorgfältig die Richtigkeit der im Display des Geräts angezeigten Daten mit den Angaben zur eingegebenen Transaktion. Verwenden Sie die angezeigte TAN nur, wenn die Daten übereinstimmen.

Sicherheitshinweise für den TAN-Generator

- Der TAN-Generator ist ein wichtiger Sicherheitsbestandteil für die Nutzung Ihres Online-Bankings. Bitte achten Sie darauf, dass das Gerät nicht in die Hände Unberechtigter gelangt.

- Sollten Sie Ihren TAN-Generator einmal verlegt oder verloren haben, benachrichtigen Sie uns umgehend unter der unten aufgeführten Sperrhotline! Wir veranlassen eine sofortige Sperre Ihres Zuganges zum Online-Banking.

SPERRHOTLINE

National (kostenfrei) Tel. 0800 588 78 25

International und aus dem Mobilfunknetz Tel. +49 201 3101-102

12129 Version 01.18