BANKHAUS HAFNER
Privatbank seit 1914

SICHERHEITSHINWEISE für das Online-Banking

In diesem Dokument erhalten Sie wichtige Sicherheitshinweise, die unbedingt eingehalten werden sollten:

Sicherheitsrelevante Themen

- Browser-Software / Betriebssystem
- Anti-Virus-Maßnahmen / Firewall
- SSL-Protokoll
- Abmelden / Automatische Zeitüberwachung
- Benutzerautorisierung durch PIN / TAN (Freigabe)
- Geheimhaltung
- Zugangswege

Browser-Software / Betriebssystem

Bitte setzen Sie für die Online-Anwendungen nur vom jeweiligen Hersteller freigegebene Versionen eines Internet-Browsers ein, z. B.

- Mozilla Firefox
- Microsoft Edge
- Apple Safari
- Google Chrome

Anti-Virus-Maßnahmen / Firewall

Achten Sie darauf, dass Sie die eingesetzte Browser-Software aus vertrauenswürdigen Quellen bezogen haben, so dass sichergestellt ist, dass es sich um unveränderte Originalsoftware handelt. Nutzen Sie zudem die aktuelle Version des Internet-Browsers. Nur die jeweils aktuellen Versionen der gängigen Browser können die bestmögliche Sicherheit gewährleisten. Zudem bieten Hersteller von Betriebssystemen stets neue Updates an. Informieren Sie sich deshalb regelmäßig über die neuesten Entwicklungen und halten Sie Ihr Betriebssystem durch Updates auf dem jeweils aktuellen Stand. Weitere nützliche Tipps zum Thema ‘Sicherheit im Internet' finden Sie auch unter https://www.bsi-fuer-buerger.de/.

SSL-Protokoll

Grundlage der sicheren Internet-Verbindung ist die Verwendung des SSL-Protokolls für die Übertragung der Daten. Das Bestehen einer sicheren SSL-Verbindung wird Ihnen durch ein geschlossenes Schloss-Symbol angezeigt. Bitte achten Sie darauf, dass während der gesamten Verbindungsdauer mit unserer Online-Anwendung dieses Symbol ununterbrochen dargestellt wird. Durch einen Klick auf das jeweilige Symbol werden Ihnen weitere Informationen angezeigt Die Darstellung ist abhängig von der von Ihnen eingesetzten Browserversion.

BANKHAUS HAFNER
Privatbank seit 1914

Abmelden / Automatische Zeitüberwachung

Um die Online-Anwendung ordnungsgemäß zu beenden, wählen Sie bitte immer die Schaltfläche "Abmelden" rechts oben neben Ihrem Namen. Wenn Sie einmal vergessen haben sollten, die Anwendung zu beenden, oder längere Zeit Ihren Rechner unbeaufsichtigt lassen, bricht die automatische Zeitbeschränkung das Programm ab, sobald im festgelegten Zeitraum keine Eingabe erfolgt.

Benutzerautorisierung durch PIN / TAN (Freigabe)

Zur Identifikation gegenüber unserem Online-Anwendungsrechner benötigen Sie von uns zu Ihrer Zugangskennung (Online-Zugang) eine PIN und TANs. Die PIN ist nur Ihnen bekannt und Sie erhalten diese in einem verschlossenen Umschlag. Die TANs sind ebenfalls nur Ihnen bekannt. Sie erhalten diese, abhängig davon, welches Verfahren bei Ihnen eingesetzt wird, in folgender Form:

- als SecureGo plus -TAN (Freigabe) in Ihrer SecureGo plus -App oder
- oder als Sm@rt-TAN plus auf Ihrem TAN-Generator

Alle Vorgänge im Online-Banking, die zu einem Geschäftsvorgang führen, wie z. B. Überweisungen, werden zusätzlich noch durch die Eingabe einerTAN (Transaktionsnummer) oder durch die Freigabe per SecureGo plus -App abgesichert.

- Die TAN (bzw. Freigabe) übernimmt die Funktion einer 'elektronischen Unterschrift'.
- Jede TAN (bzw. Freigabe) kann dabei nur für einen Vorgang verwendet werden. Nach Abschluss des Vorgangs wird die verwendete TAN ungültig.

Durch die Verwendung von PIN und TAN (bzw. Freigabe) ist sichergestellt, dass nur Sie mit Ihrer Zugangskennung (Online-Zugang) oder Ihrem Alias Bankgeschäfte mit der Online-Anwendung durchführen und vertrauenswürdige Informationen abfragen können.

Geheimhaltung

Bitte achten Sie unbedingt darauf, dass Sie Ihre Zugangskennung (Online-Zugang), Ihren Alias, Ihre PIN und Ihre TANs (bzw. die Zugangsmedien Smartphone oder Sm@rt-TAN plus-Karte) immer unter Verschluss halten und kein unberechtigter Dritter Zugriff auf diese Daten bekommt. Behandeln Sie diese sensiblen Daten wie Bargeld.

Zugangswege

Bitte geben Sie die PIN und TAN nur auf den Ihnen von uns mitgeteilten und autorisierten Zugangswegen ein. Vergewissern Sie sich immer, dass Sie auch auf einer echten Seite Ihrer Bank sind. Dies überprüfen Sie im durch einen Abgleich der Internet-Adresse im Browser, der sogenannten URL. Bereits minimale Abweichungen weisen auf eine gefälschte Internetseite hin. Bitte prüfen Sie, ob die Internet-Adresse (URL) zur Bankhaus Anton Hafner KG gehört. Die URL finden Sie in der Vereinbarung über die Nutzung des Online-Bankings'. Alternativ können Sie diese auch bei uns erfragen.

Falls Sie eine andere Adresszeile vorfinden, beenden Sie die Verbindung sofort.

Für Fragen stehen wir jederzeit zur Verfügung.