HAUCK & AUFHÄUSER

PRIVATBANKIERS SEIT 1796

Sicherheitshinweise für das Hauck & Aufhäuser Online Banking

Die Sicherheit Ihres Kontos und Ihrer Daten haben für uns höchste Priorität. Darum entwickeln wir unsere Sicherheitsarchitektur ständig weiter und kooperieren dabei auch mit externen Spezialisten und Beratern.

Darüber hinaus können Sie selbst einiges für die Sicherheit Ihres Hauck & Aufhäuser Online Bankings tun:

- Loggen Sie sich möglichst nicht über einen Ihnen unbekannten Computer (z. B. im Internetcafé) in das Online Banking ein.
- Ändern Sie Ihre PIN regelmäßig und benutzen Sie dabei Kombinationen aus Buchstaben in Groß- und Kleinschreibung und Zahlen. Verwenden Sie dabei keine Kombinationen, die einen privaten Bezug haben, wie beispielsweise Name, Geburtsdatum, Telefonnummer, Postleitzahl o. Ä. Führen Sie keine Online-Transaktionen aus, wenn Sie vermuten, dass Ihr PC von einem trojanischen Pferd oder einem Virus befallen ist.
- Nutzen Sie immer den Log-Out-Button am rechten oberen Rand, um das Online Banking zu verlassen. Löschen Sie nach Verlassen des Online Bankings immer den Zwischenspeicher (Cache), sofern nicht nur Sie an Ihrem Computer arbeiten.
    - Bei dem **Microsoft Internet Explorer** erfolgt das in den folgenden Schritten: Extras → Internetoptionen → Allgemein → Temporäre Internetdateien → Dateien löschen.
    - **Bei Firefox:** Extras → Einstellungen → Datenschutz → Private Daten → Jetzt löschen.
- Schalten Sie bei dem Microsoft Internet Explorer die Möglichkeit ab, verschlüsselte Seiten auf der Festpatte zwischenzuspeichern. Aktivieren Sie die Option „Verschlüsselte Seiten nicht auf der Festplatte speichern“ unter Internetoptionen → Erweitert → Sicherheit.
- Setzen Sie ein Virenschutzprogramm ein und aktualisieren Sie dieses regelmäßig – möglichst täglich.
- Setzen Sie eine Personal Firewall ein, die Ihrem PC zusätzlichen Schutz bietet. Links zu Programmen bekannter Hersteller finden Sie in unserem Download Center. Vergewissern Sie sich, dass Ihre Speichermedien virenfrei sind.

Welche Bankgeschäfte können Sie über unser Online Banking abwickeln?

- Umsätze der letzten 18 Monate abfragen
- Abfrage Ihres Kontostandes
- Abfrage Ihres bewerteten Depotbestandes
- Überweisungen
- Terminüberweisungen
- EU-Standardüberweisungen
- Daueraufträge

(Die Daten werden täglich konform zu unserer Kontokorrent-/Depotverbuchung aktualisiert.)

Personalisierte Sicherheitsmerkmale und Authentifizierungsinstrumente

Als personalisierte Sicherheitsmerkmale und Authentifizierungsinstrumente nutzt Hauck & Aufhäuser eine Persönliche Identifikationsnummer (PIN) und das mobileTAN-/SMS-TAN-Verfahren. Aus diesem Grund ist es sehr wichtig, Ihre PIN und Ihr Mobilgerät mit der

hinterlegten Mobilfunknummer vor dem Zugriff durch Unberechtigte zu schützen. Beide Verfahren zusammen bilden zurzeit einen hohem technischen Schutz vor Manipulation und unberechtigtem Zugriff auf Ihre Daten.

Sicherheitshinweis

Technische Verbindung zum Online Banking

Der Teilnehmer ist verpflichtet, die technische Verbindung zum Online Banking nur über die von der Bank gesondert mitgeteilten Online Banking-Zugangskanäle (zum Beispiel Internetadresse) herzustellen.

Geheimhaltung der personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Authentifizierungsinstrumente

1. Der Teilnehmer hat:

- seine personalisierten Sicherheitsmerkmale geheim zu halten und nur über die von der Bank gesondert mitgeteilten Online Banking-Zugangskanäle an diese zu übermitteln sowie
- sein Authentifizierungsinstrument vor dem Zugriff anderer Personen sicher zu verwahren.

Denn jede andere Person, die im Besitz des Authentifizierungsinstruments ist, kann in Verbindung mit dem dazugehörigen Personalisierten Sicherheitsmerkmal das Online Banking-Verfahren missbräuchlich nutzen.

2. Insbesondere ist Folgendes zum Schutz des personalisierten Sicherheitsmerkmals sowie des Authentifizierungsinstruments zu beachten:

- Das personalisierte Sicherheitsmerkmal (PIN oder TAN) darf nicht elektronisch gespeichert werden (zum Beispiel auf Ihrem PC).
- Bei Eingabe des personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
- Das Personalisierte Sicherheitsmerkmal darf nicht außerhalb des Online Banking-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.
- Die PIN und der Nutzungscode für die elektronische Signatur dürfen nicht zusammen mit dem Authentifizierungsinstrument verwahrt werden.