HAUCK
AUFHÄUSER
LAMPE

# Sicherheitshinweise für das Hauck Aufhäuser Lampe 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 Lampe Online Bankings tun:

**Sorgen Sie für Schutz auf Ihrem PC:**

- Aktualisieren Sie Ihr Virenschutzprogramm am besten täglich und automatisieren Sie diesen Vorgang.
- Setzen Sie eine Personal Firewall ein, die Ihrem PC zusätzlichen Schutz bietet.
- Schalten Sie bei Ihrem Browser (z.B. Microsoft Edge oder Google Chrome) die Möglichkeit ab, verschlüsselte Seiten auf der Festplatte zwischen zu speichern und halten Sie Ihr Betriebssystem und die von Ihnen verwendeten Programme immer auf dem aktuellen Stand.
- Führen Sie keine Online-Transaktionen aus, wenn Sie vermuten, dass Ihr PC von einem Trojaner oder einem Virus befallen ist.
- Achten Sie immer auf Ungewöhnliches bei der Nutzung des persönlichen Bereiches, um mögliche Manipulationen durch einen Trojaner zu erkennen.
- Loggen Sie sich möglichst nicht über einen Ihnen unbekannten Computer (z. B. im Internetcafé) in das Online Banking ein.

**Schützen Sie Ihre Zugangsdaten:**

- Halten Sie Ihre personalisierten Sicherheitsmerkmale geheim und übermitteln Sie diese nur über die von der Bank gesondert mitgeteilten Online Banking-Zugangskanäle.
- Verwahren Sie Ihr Authentifizierungsinstrument (PIN und Mobilgerät) sicher vor dem Zugriff anderer Personen.
- Bei Eingabe des personalisierten Sicherheitsmerkmals ist sicherzustellen, dass andere Personen dieses nicht ausspähen können.
- Verwahren Sie den Anmeldenamen, die PIN und ggfs. das Authentifizierungsinstrument getrennt voneinander.
- Geben Sie das personalisierte Sicherheitsmerkmal nicht außerhalb des Online Banking-Verfahrens, beispielsweise per E-Mail, weiter.
- Ändern Sie Ihre PIN regelmäßig und benutzen Sie dabei Kombinationen aus Buchstaben in Groß- und Kleinschreibung, Sonderzeichen und Zahlen. Verwenden Sie dabei keine Kombinationen, die einen privaten Bezug haben.
- Geben Sie niemals mehr als eine TAN gleichzeitig ein.
- 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.

**Wichtig Hinweise:**

- Wir werden Sie niemals auffordern, eine „Testüberweisung“ oder eine „Rücküberweisung“ durchzuführen.
- Ebenso werden wir Sie auch niemals bitten, eine Sicherheitssoftware im Rahmen der mobileTAN/SMS-TAN für Ihr Smartphone zu installieren, auch nicht per SMS oder Telefonanruf.
- Sie werden niemals von uns angerufen und nach Ihrer Zugangsnummer und der vollständigen PIN gefragt.