HAUCK
AUFHÄUSER
LAMPE

Sicherheitshinweise für das Hauck Aufhäuser Lampe Online Banking

Die Sicherheit Ihres Kontos und Ihrer Daten haben für uns höchste Priorität. Deshalb verbessern wir kontinuierlich unsere Sicherheitsmaßnahmen und arbeiten auch mit externen Spezialisten zusammen.

Auch Sie können aktiv zur Sicherheit Ihres Hauck Aufhäuser Lampe Online Bankings beitragen:

Wichtige Hinweise:

- Wir werden Sie niemals per Telefon oder E-Mail nach Ihrer PIN oder Ihren TANs fragen, Ebenso werden wir Sie nie auffordern auf einer Website sensible Daten, wie Ihre IBAN, PIN oder TAN einzugeben.
- Es wird niemals von Ihnen verlangt, eine „Testüberweisung“ oder eine „Rücküberweisung“ durchzuführen.
- Wir fordern Sie auch niemals auf, eine Sicherheitssoftware im Zusammenhang mit der mobileTAN/SMS-TAN auf Ihrem Smartphone zu installieren, weder per SMS oder Anruf.

Schützen Sie Ihren Computer:

- Halten Sie Ihr Betriebssystem und alle Programme stets aktuell. Installieren Sie Sicherheitsupdates zeitnah.
- Aktualisieren Sie Ihr Virenschutzprogramm regelmäßig, idealerweise täglich und automatisieren Sie diesen Prozess.
- Verwenden Sie eine Personal Firewall ein für zusätzlichen Schutz.
- Deaktivieren Sie die Funktion, verschlüsselte Seiten Ihrem Browser (z.B. Microsoft Edge oder Google Chrome) auf der Festplatte zwischen zu speichern.
- Führen Sie keine Online-Transaktionen durch, wenn Sie den Verdacht haben, dass Ihr PC infiziert ist.
- Achten Sie auf ungewöhnliche Aktivitäten in Ihrem Online Banking um mögliche Manipulationen frühzeitig zu erkennen.
- Vermeiden Sie das Einloggen in das Online Banking über unbekannte Computer (z. B. in Internetcafés) oder öffentliche Netzwerke.
- Schützen Sie Ihren Computer mit einem Kennwort.

Sichern Sie Ihre Zugangsdaten:

- Bewahren Sie Ihre persönlichen Sicherheitsmerkmale sicher auf und verwenden Sie ausschließlich die von der Bank vorgegebenen Online Banking-Zugangskanäle.
- Halten Sie Ihr Authentifizierungsinstrument (PIN und Mobilgerät) sicher vor dem Zugriff Dritter.
- Achten Sie darauf, dass bei der Eingabe Ihrer Zugangsdaten niemand mitlesen kann.
- Verwahren Sie den Anmeldenamen, die PIN und ggfs. das Authentifizierungsinstrument getrennt voneinander.
- Geben Sie Ihre Zugangsdaten niemals außerhalb des Online Banking weiter, z.B. per E-Mail.
- Ändern Sie Ihre PIN regelmäßig und wählen Sie eine Kombinationen aus Groß- und Kleinbuchstaben, Sonderzeichen und Zahlen. Vermeiden Sie dabei persönliche Bezüge.
- Geben Sie niemals mehr als eine TAN gleichzeitig ein.
- Nutzen Sie immer den Log-Out-Button, um das Online Banking zu verlassen und löschen Sie den Zwischenspeicher (Cache), wenn Sie Ihren Computer mit anderen teilen.

Stand: 01.07.2024