

## Wichtige Sicherheitshinweise für Ihr Online-Banking

### Sicherheitsvorkehrungen für Ihren Computer

- Stellen Sie bei der Anmeldung im Internetbanking sicher, dass Sie mit der richtigen Webseite verbunden sind (<https://raiba.cz>) und überprüfen Sie das Sicherheitszertifikat der Verbindung – Durch einen Click auf das Symbol mit dem geschlossenen Schloss kann man Informationen über die gesicherte Verbindung und das Zertifikat anzeigen lassen.
- Verwenden Sie ein aktuelles Betriebssystem und einen aktuellen Internet-Browser und installieren Sie regelmäßig die automatischen Softwareupdates.
- Zur Sicherheit sollten Sie ein Virenschutzprogramm und eine Firewall installieren und diese immer auf dem neuesten Stand halten.
- Achten Sie darauf, dass möglichst wenige Personen mit dem PC arbeiten, an dem Sie Online-Banking nutzen.
- Zum Surfen im Internet und zum Online-Banking sollten Sie stets einen PC-Benutzer ohne Administratorenrechte verwenden.
- Benutzen Sie keinen öffentlichen Computer oder WLAN zum Online-Banking – Sie haben keine Informationen über die Sicherheitsvorkehrungen.
- Verschlüsseln Sie Ihre eigenen WLAN-Verbindungen.
- Downloaden Sie Programme und Apps nur von vertrauenswürdigen Quellen.

### Wichtige Hinweise zur Sicherheit Ihres Online-Bankings

- Gehen Sie sorgfältig mit Ihren Zugangsdaten um. Speichern Sie keine Kennwörter oder Benutzernamen im Browser oder auf der Festplatte.
- Öffnen Sie keine Dateianhänge und Links von zweifelhaften E-Mails. Überprüfen Sie zuerst die E-Mail-Adresse des Absenders, achten Sie auf Grammatikfehler oder schlechte tschechische/deutsche Sprache. Betrügerische oder zweifelhafte E-Mails sollten Sie umgehend löschen.
- **Die Volksbank Raiffeisenbank Nordoberpfalz eG wird niemals Ihre Zugangsdaten zum Internetbanking per Telefon, E-Mail oder SMS abfragen.**
- Prüfen Sie die Richtigkeit der Transaktionsdaten bevor Sie Zahlungen mit der TAN-Nummer freigeben.
- Vereinbaren Sie mit Ihrer Bank ein möglichst niedriges Überweisungslimit.
- Überprüfen Sie regelmäßig Ihre Kontobewegungen.
- Verwenden Sie immer starke Passwörter und ändern Sie diese regelmäßig – am besten ist eine Kombination von Groß- und Kleinbuchstaben, Ziffern und Zeichen und halten Sie die Länge des Passwortes ein. Verwenden Sie niemals leicht zu erratene Passwörter wie z.B. Geburtsdatum oder Namen von Personen oder Haustieren oder Zahlenreihen wie 1234 usw.
- Aus Sicherheitsgründen fordert das E-Banking-System einmal pro Jahr eine Passwortänderung an.
- Bei Auffälligkeiten oder Verdacht auf Missbrauch Ihrer Zugangsdaten (Passwort/PIN) melden Sie dies so bald wie möglich telefonisch +420 354 524 5-11 oder persönlich an die Bank. Sie können auch mit 3 fehlerhaften Anmeldeversuchen das Passwort/die PIN selbst sperren.