

## Checkliste **Umsichtiges Verhalten beim Online-Banking**

---

### **Sicherer Computer**

- Nutzen Sie zum Online-Banking nur einen vertrauten, sicher eingerichteten Computer (siehe auch Checkliste **Sicherer Computer**).

### **Eingabe sensibler Daten (zum Beispiel PIN, TAN)**

- Geben Sie Ihre Daten nur auf verschlüsselten Webseiten ein. Diese erkennen Sie am Kürzel „https://“ in der Adressleiste Ihres Browsers sowie am geschlossenen Vorhängeschloss in der Status- oder Informationszeile.
- Wenn Ihr Browser Sie beim Betreten der Webseite auf ein ungültiges Zertifikat hinweist und Ihnen anbietet eine Ausnahmeregelung (Sicherheitsausnahme) zu bestätigen, sollten Sie diese auf keinen Fall akzeptieren und statt dessen die Online-Banking-Sitzung abbrechen.

### **Links und Dateianhänge in E-Mails**

- Öffnen Sie keine Links oder Dateianhänge in E-Mails, wenn Sie nicht absolut sicher sind, von wem diese E-Mail stammt.
- Treffen Sie besondere Vorsicht, um Phishing auszuschließen (siehe auch Checklisten **Erkennen von Phishing-E-Mails** bzw. **Erkennen von Phishing-Webseiten**).

### **Überweisungen überprüfen**

- Überprüfen Sie regelmäßig Ihre Kontoauszüge auf Unregelmäßigkeiten.
- Stellen Sie Unregelmäßigkeiten bei Ihren Überweisungen fest, melden Sie diese sofort Ihrer Bank.
- Sollten Sie das Gefühl haben, dass Ihre Zugangsdaten abhanden gekommen oder in falsche Hände geraten sind, kontaktieren Sie sofort Ihre Bank.