

# Checkliste: Beim Online-Banking auf Nummer sicher gehen

1

## Zugangsdaten sicher aufbewahren

- Bewahren Sie TAN-Listen und Zugangsdaten sicher auf und geben Sie diese niemals an Dritte weiter. Daten sollten keinesfalls auf dem Handy gespeichert oder auf einem Notizzettel im Geldbeutel herumgetragen werden.
- Bankdaten sollten ausschließlich zum Online-Banking oder in vertrauenswürdigen Online-Shops genutzt werden.
- Erstellen Sie sichere Passwörter (keine Namen, Geburtsdaten, etc.) und wechseln Sie diese in regelmäßigen Abständen.
- Ihre Bank oder andere Dienstleister werden Sie keinesfalls auffordern, sensible Daten per E-Mail oder Telefon preiszugeben. Löschen bzw. ignorieren Sie deshalb derartige Anfragen.

2

## Auf eine sichere Datenübertragung achten

- Nutzen Sie eine verschlüsselte WLAN-Verbindung.
- Achten Sie bei der Übertragung der Daten zu Ihrem Online-Banking-Anbieter auf eine verschlüsselte Kommunikation („https“ in der Adresszeile sowie ein Schlosssymbol in der Statusleiste des Browsers)
- Nutzen Sie für das Online-Banking lediglich den heimischen PC und keine offenen WLAN-Netzwerke oder Internet-Cafés.
- Halten Sie Ihre Betriebssoftware stets auf dem neuesten Stand und nutzen Sie ein Anti-Viren-Programm.

3

## Sicherheitsmaßnahmen beim Online-Banking

- Vereinbaren Sie mit Ihrer Bank ein tägliches Überweisungslimit.
- Überprüfen Sie Ihre Kontoauszüge regelmäßig auf verdächtige Kontobewegungen und melden Sie diese gegebenenfalls Ihrer Bank.
- Tippen Sie die Adresse von Hand in das Adressfeld des Browsers ein, wenn Sie die Online-Banking-Seite Ihres Anbieters aufrufen möchten.
- Achten Sie beim Betreten der Seite auf Veränderungen. Werden Sie beispielsweise beim Login nach einer TAN gefragt, handelt es sich um eine Phishing-Seite.
- Zur Verifizierung ihrer Webseite bieten Online-Banking-Anbieter ein Zertifikat an. Dieses sollten Sie überprüfen.

Weitere Informationen zur Sicherheit im Online-Banking, finden Sie in [unserem Servicebereich](#).