EDEKABANK

So schützen Sie sich vor Betrug im OnlineBanking

➔ **Starke Passwörter verwenden**
Das kann zum Beispiel ein kurzes und komplexes Passwort sein, das mindestens 8-12 Zeichen bestehend aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthält.

➔ **Bankverbindung geheim halten**
Veröffentlichen Sie diese nicht zum Beispiel auf einer eigenen Webseite. Vorsicht gilt auch beim Onlineshopping, etwa wenn Sie sich nicht sicher über die Seriosität des Onlineshops sind.

➔ **Zwei-Faktor-Authentisierung nutzen**
Dabei bestätigen Sie zum Beispiel beim Login über zwei Faktoren, dass dies wirklich Ihr Benutzerkonto ist. Diese Faktoren können etwa ein Passwort und die Freigabe über eine Smartphone-App sein.

➔ **Transaktionen überprüfen**
Lesen Sie zum Beispiel die Details einer Überweisung, etwa an wen Sie Geld überweisen, genau durch, bevor Sie diese bestätigen.

➔ **Öffentliches WLAN und fremde Geräte meiden**
Nutzen Sie für das OnlineBanking möglichst nur eigene Geräte. Betreiben Sie OnlineBanking zudem nicht über öffentliches WLAN

➔ **Kommunikation hinterfragen**
Mit gefälschten E-Mails oder vorgetäuschten Anrufen versuchen Kriminelle, an Ihre Bankdaten oder an andere sensible Informationen zu gelangen. Klicken Sie daher nicht unüberlegt auf Links in einer E-Mail, egal wie seriös diese wirkt. Kriminelle verschicken oft Links zu gefälschten Internetseiten in täuschend echt aussehenden E-Mails. Ihre Bank fragt jedoch niemals nach Ihren Zugangsdaten zum Onlinebanking, Ihrer PIN oder Ihren TANs

➔ **Richtige App wählen**
Installieren Sie die entsprechende Banking-App nur von vertrauenswürdigen Quellen. Gehen Sie sicher, dass Sie keine gefälschte App herunterladen. Rufen Sie am besten die Webseite Ihrer Bank auf und suchen Sie dort nach der entsprechenden App

➔ **Geräte und Anwendungen auf dem neuesten Stand halten**
Führen Sie Updates für Betriebssystem und Software durch, sobald diese verfügbar sind. Installieren und aktivieren Sie auch Antiviren-programme