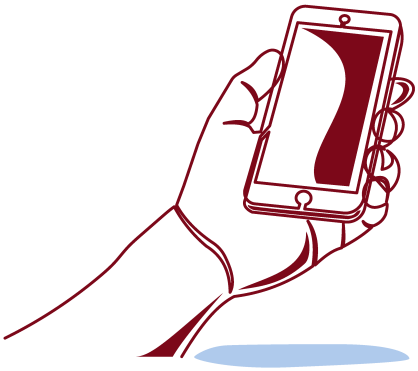
# Telefon-Masche: Vorsicht vor Kriminellen, die sich als Bankangestellte ausgeben!

19.03.2021
von

Altmann, Kathleen

## Schlagworte

Verbraucher
PIN
Onlinebanking
TAN
Verbraucherschutz
Dossier Sicherheitstipps
Onlinebanking



Sie geben sich dreist als Bankangestellte aus: Trickreich versuchen Kriminelle per Telefon, an Ihre Onlinebanking-Zugangsdaten zu gelangen oder Sie zu einer Zahlung zu veranlassen. So funktioniert die Betrugsmasche im Detail und so schützen Sie sich:

**Betrugsszenario 1:** Die Kriminellen rufen unter dem Vorwand an, aus Sicherheitsgründen Ihre Kontodaten oder auch andere persönliche Daten, wie Ihre Adresse, abgleichen zu wollen. Alternativ wird auch Hilfe bei der Umstellung auf ein anderes TAN-Verfahren angeboten. Auf dem Display Ihres Telefons erscheint vermeintlich der Name Ihrer Bank oder die Nummer des Kundenservices. Tatsächlich ist diese Rufnummernanzeige manipuliert, um Sie zu täuschen.

In einigen Fällen wird versucht, über eine Fernwartungs-software Zugang zum Computer zu erhalten. Ziel der Krimi-nellen ist es dabei, Sie so zu manipulieren, dass Sie unbeabsichtigt eine Zahlung per TAN freigeben.

**Betrugsszenario 2:** Der Anruf wird schriftlich angekündigt: Sie erhalten ein scheinbar offizielles Schreiben Ihrer Bank per Brief oder E-Mail. Darin wird der Anruf eines Bankange-stellten angekündigt, der Ihren Onlinebanking-Zugang

überprüfen will. Die Kriminellen verfahren in diesem Fall wie in Szenario 1, um unrechtmäßig an Ihre Daten zu gelangen.

## Worauf es die Kriminellen abgesehen haben

Konkret geht es dem angeblichen Bankangestellten nur darum, Ihre geheimen Zugangsdaten zu erfahren. Darunter fallen die Geheimzahlen (PINs) für Ihre Bankkarten, für Ihr Telefon- und Onlinebanking oder Transaktionsnummern (TANs), mit denen in Ihrem Namen Überweisungen durchgeführt oder weitere TAN-Verfahren aktiviert werden können.

Dabei „gleicht" der Anrufende auch andere persönliche Daten, wie beispielsweise die Adresse, mit Ihnen ab. In einigen Fällen werden Sie auch aufgefordert, Vorgänge über Ihre Banking-App zu autorisieren, entweder um Ihr Konto zu bestätigen oder um vermeintliche Zahlungen ins Ausland zu stoppen. Leisten Sie der Aufforderung nicht sofort Folge, wird meist mit einer angeblichen Kontosperrung gedroht oder damit, dass die vermeintlichen Zahlungen ins Ausland gebucht würden.

Wichtig: Eine Mitarbeiterin oder ein Mitarbeiter einer Bank wird Sie niemals nach Ihrer kompletten Telefon-Banking-PIN, Ihrer Onlinebanking-PIN oder einer Transaktionsnummer (TAN) fragen.

## Tipps für Ihren Schutz

1. Geben Sie keine vertraulichen Zugangsdaten, wie Ihre PINs oder TANs, an Dritte weiter.

2. Verschicken Sie keine Fotos oder Scans Ihres TAN-Aktivierungsbriefs über das Internet, wenn Sie dazu aufgefordert werden. Versenden Sie den Aktivierungsbrief auch nicht mit der Post. Der Aktivierungsbrief ist nur für Ihre eigenen Unterlagen bestimmt.

3. Gewähren Sie keinen Zugriff auf Ihren Computer oder Mobiltelefon, laden Sie in diesem Zusammenhang

keine Fernwartungsoftware herunter.

4. Falls Sie einen verdächtigen Anruf erhalten: Nehmen Sie sich Zeit, überlegen Sie und lassen Sie sich nicht unter Druck setzen. Sollten Sie Zweifel an der Seriosität des Anrufenden haben, legen Sie sofort auf und rufen Sie selbst bei Ihrer Bank oder beim Kundenservice an. Überprüfen Sie die Telefonnummer, z.B. auf der Internetseite des Unternehmens.

5. Vermuten Sie, dass Unbefugte Ihre Onlinebanking- oder Telefon-Banking-PIN kennen könnte, ändern Sie diese umgehend. Sollte dies nicht möglich sein, sperren Sie Ihren Onlinebanking-Zugang. Sie erhalten dann neue Zugangsdaten von Ihrer Bank. Erstatten Sie im Betrugsfall Strafanzeige bei der Polizei. Informieren Sie auf jeden Fall Ihre Bank.

6. Lesen Sie den Inhalt erhaltener TAN-Mitteilungen vollständig und prüfen Sie, ob Sie wirklich eine Zahlung autorisieren möchten.

7. Seien Sie misstrauisch. Ein gesundes Misstrauen hilft auch anderen: Sprechen Sie daher auch mit Ihrer Familie und Freunden über diese Betrugsmethode.