Verbraucherzentrale
Hamburg

Doppelt hält besser: TAN-Verfahren beim Online-Banking

Mit der verpflichtenden Zwei-Faktor-Authentifizierung soll der Missbrauch im digitalen Zahlungsverkehr eingedämmt werden. Ob ChipTAN, PhotoTAN oder PushTAN - Verbraucherinnen und Verbraucher können zwischen mehreren TAN-Verfahren wählen.

DAS WICHTIGSTE IN KÜRZE

1. Seit 14. September 2019 gelten in der Europäischen Union neue Sicherheitsvorgaben fürs Online-Banking. TAN-Listen auf Papier dürfen seitdem nicht mehr genutzt werden.
2. Die Banken und Sparkassen haben ihre Authentifizierungsverfahren entsprechend umgestellt.

3. Viele Kreditinstitute setzen auf eigene Smartphone-Apps für die TAN-Verfahren. Verbraucherinnen und Verbraucher, die kein Smartphone besitzen, können nur auf TAN-Generatoren oder SMS ausweichen.

Stand: 03.12.2025

Bankkundinnen und Bankkunden können Online-Überweisungen nur noch mit einer starken Kundenauthentifizierung freigeben. Was das bedeutet? Bei jedem Zahlungsauftrag und jedem Login ins Online-Banking-Portal müssen mindestens zwei voneinander unabhängige Sicherheitsmerkmale, sogenannte Faktoren zum Einsatz kommen müssen. Es reicht also nicht mehr, die alte TAN-Liste hervorzukramen. Das Ganze nennt sich Zwei-Faktor-Authentifizierung. Mögliche Faktoren sind:

- **Sein** – körperliche, „biometrische“ Merkmale, wie Fingerabdruck oder Augeniris
- **Wissen** – zum Beispiel die ausschließlich dem Kunden bekannte PIN (persönliche Identifikationsnummer) oder ein Passwort
- **Besitz** – etwas, das nur der Kunde besitzt und das nicht kopiert werden kann, wie zum Beispiel ein Smartphone oder ein Tan-Generator (Transaktionsnummer)

Derzeitige TAN-Verfahren statt TAN-Listen auf Papier

Laut Zweiter Zahlungsdienste-Richtlinie (kurz: PSD II) ist die Verwendung der alten iTAN-Listen auf Papier seit Mitte September 2019 nicht mehr ausreichend sicher und deshalb nicht mehr zulässig. Erlaubt sind nur noch TAN-Verfahren, bei denen für jede Transaktion jeweils eine TAN neu generiert wird.

TAN-Verfahren	Sicherheit
ChipTan (oder Smart-Tan) mit Tan-Generator (Lesegerät)	Sehr hoch

BestSign (mit Zusatzgerät)	Sehr hoch (mit Zusatzgerät von Postbank) Hoch (mit Postbank-App auf Smartphone)
PhotoTan (mit Lesegerät)	Sehr hoch (mit Lesegerät) Hoch (mit PhotoTan-App auf Smartphone)
QR-Tan (oder QR-Tan+)	Sehr hoch (mit QR-Tan-App auf Smartphone)
App-Tan (oder VR-SecureGo, EasyTan, Tan2go, PushTan, SpardaSecureApp)	Hoch (mit PushTan-App auf Smartphone)
SMS-Tan (oder MobileTan, mTan)	(per SMS über das Handy) entspricht nicht mehr dem technischen Standard

Wichtig: Damit diese Verfahren auch wirklich sicherer sind, benötigen Sie immer zwei Geräte, zum Beispiel PC und Smartphone, Smartphone und TAN-Generator … Wickeln Sie Ihr Online-Banking übers Smartphone ab und generieren damit per App auch PhotoTan oder QR-Tan, macht dies die Vorteile der Zwei-Faktor-Authentifizierung zunichte.

Bei der Stiftung Warentest können Sie sich über die von den Banken jeweils genutzten Verfahren informieren **?** Weiterlesen auf test.de

GUT ZU WISSEN

Beim Authentifizierungsverfahren setzt jede Bank auf ein anderes Modell. So können sich Verbraucherinnen und Verbraucher kaum einen Überblick verschaffen.

Mögliche Zusatzgeräte bzw. TAN-Generatoren erhalten Sie bei Ihrer Bank oder bei Elektronikhändlern. Achtung! Durch die Nutzung der angebotenen Sicherheitsverfahren können Ihnen Mehrkosten entstehen – zum Beispiel für jede SMS-TAN oder für einen TAN-Generator.

Online-Shopping mit Kreditkarte

Die Vorgaben zur starken Kundenauthentifizierung sollen auch für Kreditkartenzahlungen beim Online-Shopping gelten. Die bislang übliche Authentifizierung über die Eingabe von Kreditkartennummer und Prüfziffer ist nicht mehr ausreichend. Kunden müssen zusätzlich beispielsweise eine Transaktionsnummer (TAN), die zuvor an ihr Mobiltelefon gesendet wurde, und außerdem ein Passwort nennen.

Hiervon gibt es einige wenige Ausnahmen, zB bei geringen Beträgen.

https://www.vzhh.de/themen/finanzen/konto-karte/doppelt-haelt-besser-tan-verfahren-beim-online-banking