Presseinformation

26. März 2019

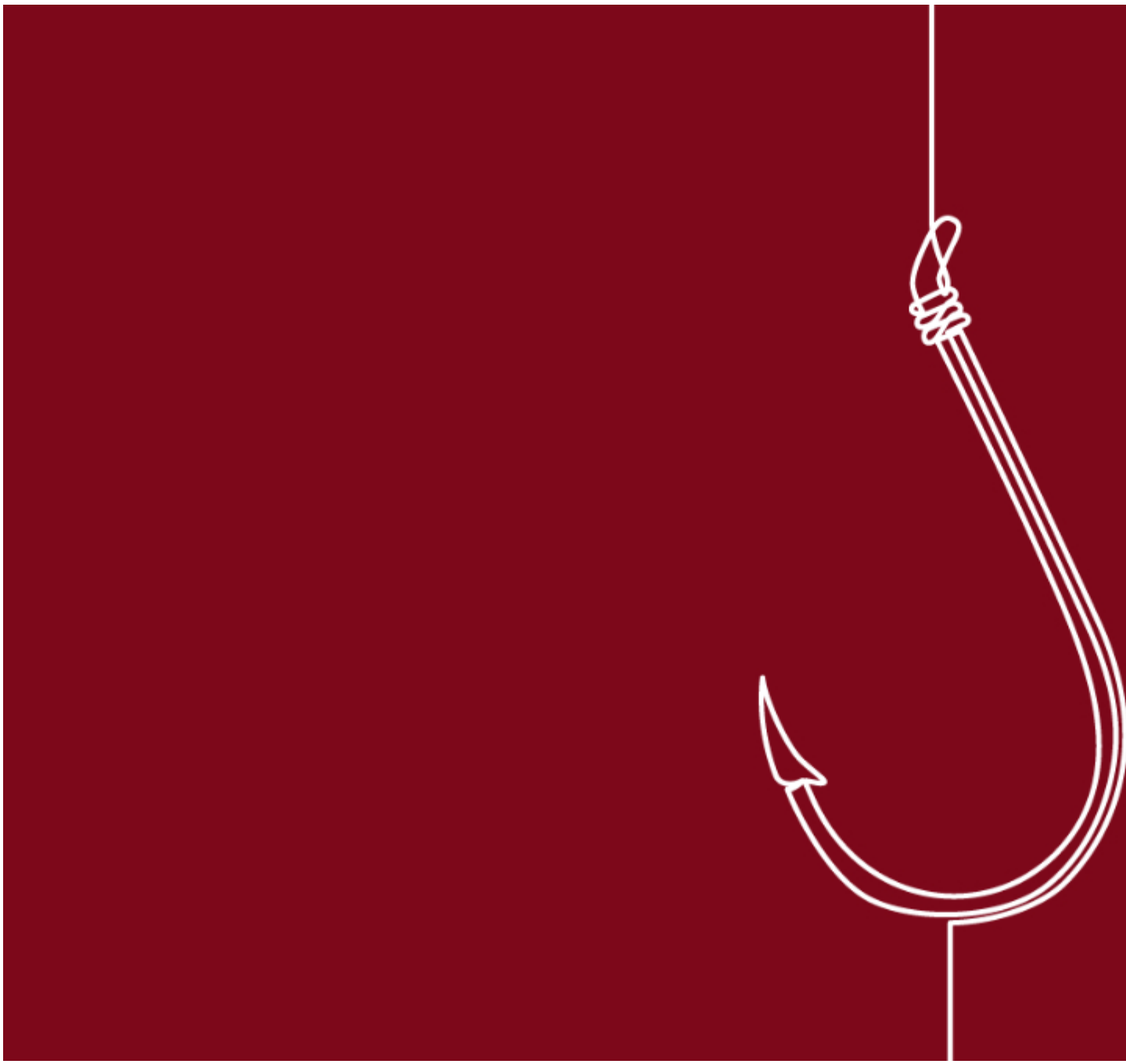
Kontakt

Sylvie Ernoult (in Elternzeit)
Bundesverband deutscher Banken e.V.
Pressesprecherin
Tel. +49 30 1663-1210
sylvie.ernoul-t@bdb.de

Schlagworte

Phishing
Cyberkriminalität
Verbraucher
Onlinebanking
PIN
TAN

Bankenverband warnt vor iTAN-Phishing



- Betrüger versuchen per E-Mail Daten abzugreifen
- Drei Tipps wie Kunden sich vor Betrug schützen können

Wer derzeit sein iTAN-Verfahren fürs Online-Banking auf ein neueres TAN-Verfahren umstellen will, sollte aufmerksam sein: Betrüger versuchen die Abschaffung der papierhaften TAN-Liste für ihre Zwecke zu nutzen. Bis zum 14. September 2019 müssen Bankkunden auf ein moderneres TAN-Verfahren mit einer Zwei-Faktoren-Authentifizierung umsteigen.

Betrüger nutzen dies aus und nehmen – wie die eigene Bank auch - per Mail Kontakt mit den Kunden auf. Die E-Mail enthält dann einen Link zu einer gefälschten Webseite, die dem Online-Banking-Auftritt der eigenen Bank täuschend ähnlich sein kann. Folgt der Kunde dem Link und loggt sich ein, fischt der Betrüger zunächst seine Zugangsdaten ab. In einer weiteren E-Mail oder im Online-Banking über die gefälschte Webseite wird der Kunde nunmehr zur Eingabe der iTAN aufgefordert, mit der er die vermeintlich neue TAN-App freischalten soll. Auch diese fischt der Betrüger ab und nutzt sie dann, um sich Zugang zur echten TAN-App zu verschaffen, die er auf einem eigenen Gerät installiert hat. Jetzt kann er unbemerkt Überweisungen im Namen des Kunden tätigen.

Der gesamte Vorgang des Abfischens von Zugangsdaten und iTAN dauert unter Umständen nicht länger als ein paar Minuten. Auch die gefälschten E-Mails weisen mittlerweile einen hohen Grad an Perfektion auf. In der Vergangenheit konnten solche Nachrichten oft schon an der mangelhaften Rechtschreibung erkannt werden. Dies ist inzwischen häufig nicht mehr der Fall. Zudem personalisieren die Kriminellen die E-Mails immer öfter, Bankkunden werden also mit ihrem richtigen Namen angesprochen. Das macht es schwieriger, den Betrugsversuch bereits auf den ersten Blick zu entlarven.

Mit diesen drei Tipps können Kunden jedoch das Risiko minimieren, Opfer dieser kriminellen Machenschaften zu werden:

Tipp 1: Wer nimmt Kontakt auf? Handelt es sich dabei tatsächlich um die eigene Bank? Hinweise, ob es sich um eine gefälschte E-Mail handelt, finden sich zum Beispiel im Absender der E-Mail.

Tipp 2: Geben Sie die Online-Banking-Adresse der eigenen Bank selbst in die Leiste des Browsers ein. Auf keinen Fall sollte der in der E-Mail verwendete Link angeklickt werden! Ob es sich beim Einloggen wirklich um die verschlüsselte Seite Ihrer Bank handelt, erkennen Sie auch daran, dass in der Browserleiste ein Schloss-Symbol erscheint und die Adresse mit „https…“ beginnt.

Tipp 3: Prüfen Sie die E-Mail auf sonstige Auffälligkeiten, wie beispielsweise Rechtschreibfehler! Im Zweifel sollten Kunden ihre Bank anrufen, um nachzufragen.

Verdächtige E-Mails sollten immer der eigenen Bank gemeldet werden, damit diese dagegen vorgehen und auch andere Bankkunden davor schützen kann, Opfer von Kriminellen zu werden.