6 Vorsicht bei Anfragen per E-Mail oder SMS

Antworten Sie niemals auf vermeintliche E-Mails oder SMS Ihrer Bank, die Sie zu einer Bestätigung Ihrer sensiblen Daten, etwa über die Abfrage von PINs oder TANs, auffordern. Klicken Sie auch auf keine Links, um solche Daten einzugeben. Ihre Bank fragt Ihre Daten niemals per E-Mail oder SMS ab.

7 Achtung bei Anrufen vermeintlicher Bankmitarbeiter

Wenn Sie ein vermeintlicher Mitarbeiter Ihrer Bank anruft und Sie dazu drängt, gemeinsam mit ihm eine Transaktion von Ihrem Konto durchzuführen, beenden Sie das Gespräch umgehend. Ihre Bank wird Sie niemals zu einer solchen Aktion drängen.

8 Was tun, wenn es passiert ist?

Sollten Sie tatsächlich Opfer eines Phishing-Falls geworden sein, wenden Sie sich umgehend an Ihre Bank und erstatten Sie Anzeige bei der Polizei. Die Phishing-Nachricht kann in diesem Fall als Beweis dienen.

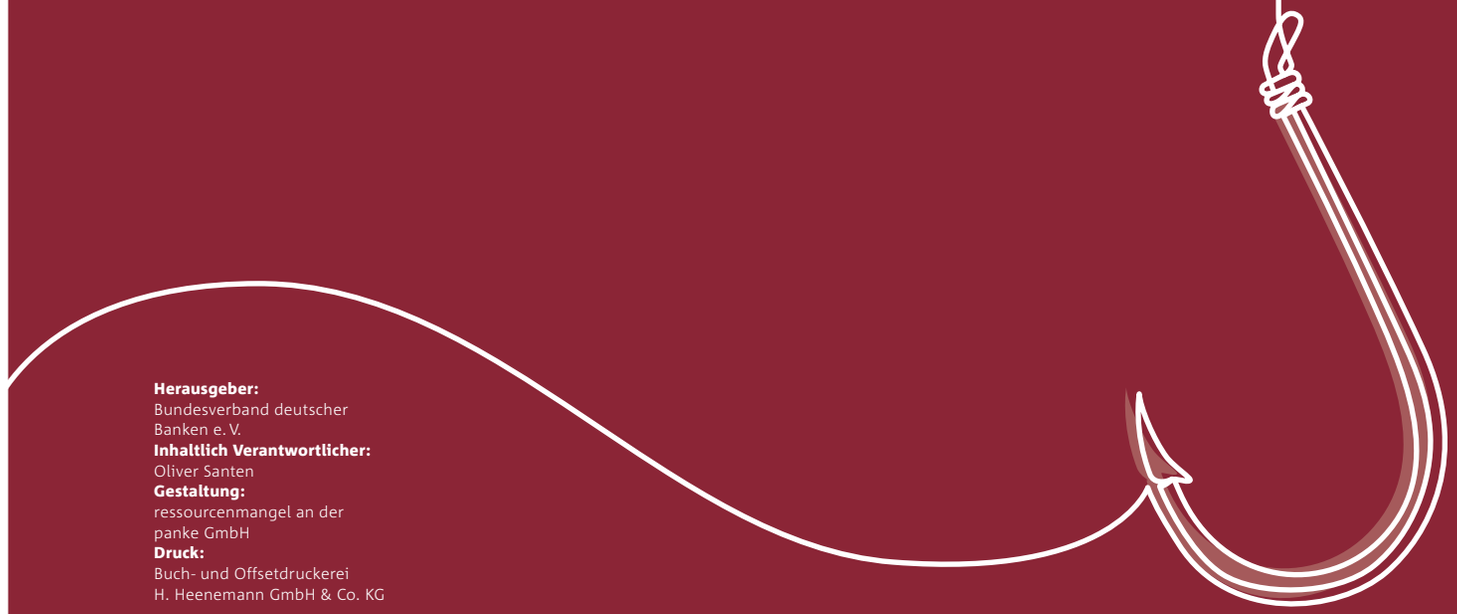
So erreichen Sie den Bankenverband

Bundesverband deutscher Banken
Burgstr. 28
10178 Berlin
+49 30 1663-0

bankenverband@bdb.de
bankenverband.de

bankenverband

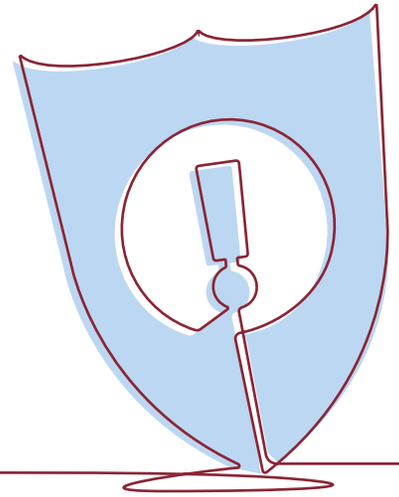
Wie schütze ich mich vor **Phishing?**



Herausgeber:
Bundesverband deutscher Banken e. V.
Inhaltlich Verantwortlicher:
Oliver Santen
Gestaltung:
ressourcenmangel an der panke GmbH
Druck:
Buch- und Offsetdruckerei H. Heenemann GmbH & Co. KG

Berlin, Oktober 2019

Mehr als die Hälfte der Bankkunden nutzen Onlinebanking oder erledigen ihre Bankgeschäfte unterwegs, über das Smartphone. Kriminelle versuchen immer wieder Daten auszuspähen und missbrauchen digitale Identitäten, um sich zu bereichern. Dieses Ausspionieren, das Abfischen von Daten, wird „Phishing“ genannt. Damit Sie als Kunde Ihre Bankgeschäfte auf Ihrem Computer oder Smartphone sicher betreiben können, ist es wichtig, einige grundsätzliche Regeln zu beachten.



1 **Computer und Smartphone** sichern

Der heimische Computer kann ein Einfallstor für Kriminelle sein. Wenn er nicht ausreichend geschützt ist, steht die „Haustür“ offen. Als Onlinebanking-Nutzer müssen Sie gewisse Sorgfaltspflichten beachten: Nutzen Sie unbedingt einen Virenscanner und eine Firewall auf allen Geräten und veranlassen Sie regelmäßige Updates – auch für die übrige Software einschließlich Ihres Betriebssystems. Installieren Sie verfügbare Updates umgehend. Damit gewährleisten Sie einen ausreichenden Schutz Ihres Computers gegen Viren und Trojaner. Onlinebanking sollten Sie daher niemals auf unbekannten Rechnern betreiben, weil Sie nicht sicher sein können, ob der Computer ausreichend geschützt ist.

Auch für Ihr Smartphone gilt: Wenn Sie Bankgeschäfte unterwegs erledigen und Banking Apps nutzen, müssen Betriebssystem und Apps auf dem aktuellen Stand gehalten werden.

2 **Autorisierte Banking Apps** nutzen

Nutzen Sie außerdem eine geeignete App für den Zugang zu Ihrer Bank. Installieren Sie Banking Apps einzig aus dem autorisierten App Store (Google Play Store / Apple App Store) Ihres Smartphones oder Tablets. Hierfür sollten Sie keinen „Hinweisen“ aus E-Mails oder von Webseiten nachgehen. Lassen Sie bei Gratis-Versionen von ansonsten käuflich zu erwerbenden Apps Skepsis walten, denn es könnte sich um Schadsoftware handeln.

3 **PINs und TANs** niemals speichern

Speichern Sie niemals Kennwörter, persönliche Geheimzahlen (PINs) und TANs unverschlüsselt in Apps, in einer Cloud oder auf Ihrer Festplatte. Auch als Telefonnummern abgespeicherte Informationen im Adressbuch bieten keinen ausreichenden Schutz.

4 **Zugangsdaten** ändern

Ändern Sie regelmäßig Ihre Zugangsdaten, zum Beispiel Passwörter oder PINs. Dies gilt für Ihre gesamten Nutzerkonten, nicht nur fürs Onlinebanking.

5 **Banking-Webseite** prüfen

Bei Phishing-Angriffen versuchen Betrüger unter anderem, Sie per E-Mail oder SMS auf die vermeintliche Onlinebanking-Webseite Ihrer Bank zu locken. Es handelt sich dabei um Fälschungen, die mit dem Ziel versandt werden, Ihre Daten abzufangen. Bevor Sie sich einloggen, überprüfen Sie stets, ob es sich wirklich um die verschlüsselte Seite Ihrer Bank handelt. Das erkennen Sie unter anderem daran, dass im Internet-Browser ein Schloss-Symbol erscheint und die Webadresse mit „https://...“ beginnt.