bankenverband

Vorsicht,
Betrug per Telefon

Sie geben sich als Enkel, Polizist, Rechtsanwalt oder Techniker aus: Betrüger am Telefon versuchen mit verschiedensten Maschen, Ihr Vertrauen zu gewinnen oder Druck auf Sie auszuüben. Ziel ist es, an Ihre sensiblen Daten wie PINs und TANs (Transaktionsnummern) zu gelangen oder Sie direkt zu einer Zahlung zu veranlassen. Dieses Faltblatt informiert Sie über gängige Betrugsmaschen und gibt Ihnen Tipps, wie Sie sich bestmöglich schützen können.

Die Gewinnspiel-Masche

„Wir wollen Ihnen Ihren Gewinn auszahlen, benötigen aber dazu Zugang zu Ihrem Konto per Onlinebanking." So oder so ähnlich versuchen kriminelle Anrufer, Sie zur Beantragung und Freischaltung eines Onlinebanking-Zugangs bei Ihrer Bank zu überreden. Anschließend werden Sie vom Telefonbetrüger aufgefordert, ihm die für den neuen Online-Zugang erhaltenen Zugangsdaten, die persönliche Identifikationsnummer (PIN) und Transaktionsnummern (TANs), auszuhändigen.

Der gleiche Trick wird auch in Bezug auf das Telefon-Banking angewendet: Sie sollen dem Kriminellen Ihre Telefon-Banking-PIN mitteilen oder eine neue bestellen, die dann von Ihnen (telefonisch) erfragt oder aus Ihrem Briefkasten gestohlen wird. Mit dieser Information könnte der Kriminelle über Ihr Konto verfügen.

Der angekündigte Anruf

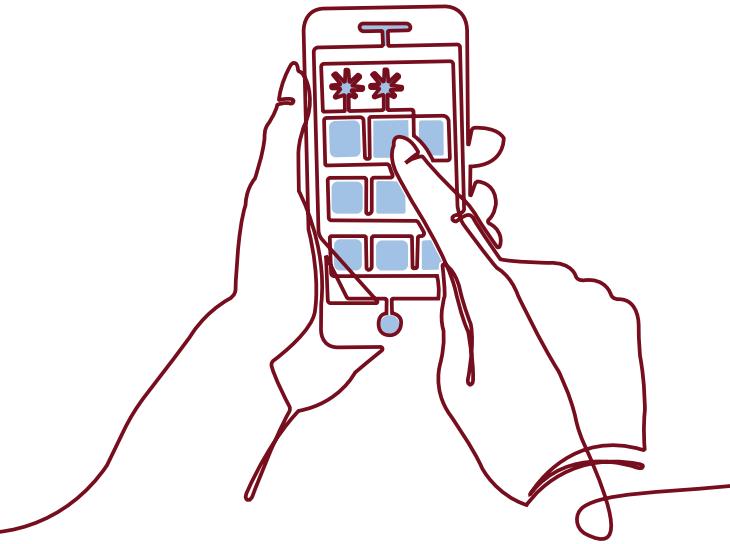
Sie erhalten ein offiziell anmutendes Schreiben per Brief oder E-Mail, das dem Erscheinungsbild Ihrer Bank oder eines bekannten Unternehmens gleicht. Darin wird ein Anruf

angekündigt. Der vermeintliche Mitarbeiter der Bank oder des Unternehmens hat es auf Ihre geheimen Zugangsdaten abgesehen, wie Girocard- oder Kreditkarten-PINs, Telefon-Banking-PINs, Onlinebanking-PINs oder TANs. Mit diesen Daten könnte der Täter Ihren Kontostand abfragen, Überweisungen durchführen oder sogar Änderungen Ihrer Kundendaten, wie zum Beispiel Ihrer Adresse oder Ihrer Handynummer vornehmen.

Der „Techniker“-Anruf

Sie erhalten den Anruf eines vermeintlichen Technikers eines bekannten Unternehmens. Dieser ruft Sie unter dem Vorwand an, die Leistung Ihres Computers zu verbessern oder Sicherheitslücken zu schließen. Dazu sei es jedoch erforderlich, dass Sie eine Fernwartungssoftware herunterladen und anschließend starten. Damit hätte nun der kriminelle Anrufer ohne Ihr Zutun beispielsweise die Möglichkeit, eine Spionagesoftware zu installieren, um Ihre persönlichen Daten auszuspähen.

Nach erbrachter Beratung werden Sie vom Anrufer aufgefordert, umgehend eine Servicepauschale per Onlinebanking zu überweisen. Während der Transaktion ändert der Anrufer den Betrag, ohne, dass Sie es merken. Alternativ werden Sie



dazu aufgefordert, eine fremde Website aufzurufen und dort Ihre Kreditkartendaten oder weitere sensible Zahlungsdaten einzugeben.

Wie Sie sich verhalten können

Zögern Sie, wird der kriminelle Anrufer versuchen, Druck auf Sie auszuüben, indem er Ihnen mit finanziellen Einbußen oder Schäden droht, falls Sie zum Beispiel einen bestimmten Link nicht unverzüglich aufrufen oder Ihre persönlichen Daten nicht in eine bestimmte Anwendung eingeben. Auch andere Druckmittel werden gern gebraucht, wie das Androhen einer Kontosperre, die Einschaltung eines Inkassobüros oder eines Rechtsanwalts etc. Lassen Sie sich nicht einschüchtern, sondern legen Sie im Zweifel einfach auf.

Wichtig: Wenden Sie sich bei jeglichem Missbrauch Ihrer Bankdaten – auch beim Verdacht – umgehend an Ihre Bank. Kontaktieren Sie zudem die Polizei und erstatten Sie Strafanzeige.

Tipps zum Schutz

- Seien Sie auch am Telefon misstrauisch und nutzen Sie Ihren gesunden Menschenverstand.

- Gehen Sie verantwortungsbewusst mit all Ihren persönlichen Daten um. Dazu gehören neben Ihren sensiblen Daten, wie zum Beispiel Kartendaten, PINs und TANs, auch Ihre Adresse, Ihre Telefonnummern oder Ihr Geburtsdatum. Überlegen Sie immer, ob diese Informationen für den gewollten Vorgang überhaupt benötigt werden.

- Geben Sie keine PINs oder TANs an Dritte weiter – auch nicht an Familienangehörige.

- Vertrauen Sie nicht allein auf die übermittelte, das heißt im Telefondisplay anzeigte Nummer des Anrufers. Diese könnte manipuliert sein.

- Sollten Sie Zweifel an der Seriosität des Gesprächspartners haben, lassen Sie sich Namen und Telefonnummer geben, um zurückzurufen, und legen Sie vorsichtshalber auf. Überprüfen Sie vor dem Rückruf die Telefonnummer, zum Beispiel auf der Unternehmenswebsite, über die Auskunft oder im Telefonbuch.

- Vermuten Sie, dass ein Unbefugter Ihre Onlinebanking- oder Telefon-Banking-PIN kennen könnte, ändern Sie diese umgehend bzw. beantragen Sie einen neuen Zugang bei Ihrer Bank. Informieren Sie auch Ihre Bank über Ihren Verdacht.

- Beachten Sie: Ein Bankmitarbeiter wird Sie niemals nach Ihrer kompletten Telefon-Banking-PIN, Ihrer Onlinebanking-PIN oder einer TAN fragen.

So erreichen Sie den Bankenverband

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

bankenverband@bdb.de
bankenverband.de

Herausgeber:
Bundesverband deutscher Banken e. V.
Inhaltlich Verantwortlicher:
Oliver Santen
Gestaltung:
ressourcenmangel an der panke GmbH
Druck:
PIEREG Druckcenter Berlin GmbH

Berlin, Oktober 2020