Falsche Bankmitarbeiter

Achtung - Abzocke am Telefon und an der Haustür!

Wenn sich am Telefon oder an der Haustür fremde Personen als Mitarbeiter Ihrer Hausbank ausgeben, ist höchste Wachsamkeit gefragt und Misstrauen angezeigt. Sehr wahrscheinlich drohen hier ein Betrug und finanzieller Schaden, wenn Sie den Anleitungen, die Sie von diesen Personen erhalten, folgen. Wird der Betrug bemerkt, ist es oft schon zu spät.
Die Maschen der Täter sind hierbei ganz unterschiedlich und laufen ggf. in mehreren Schritten ab.
Und: Die Täter haben ggf. tatsächlich detaillierte Kenntnisse von vertraulichen Informationen zu den finanziellen Verhältnissen der Angerufenen, kennen vielleicht sogar einzelne Umsatzbuchungen.

Wie haben die Betrüger im konkreten Einzelfall diese Kenntnisse erlangt?

Letztlich können dem viele Gegebenheiten zugrunde liegen. Möglicherweise erfolgen zunächst „unauffällige, angeblich anonyme Meinungsumfragen“ oder vorangegangene vermeintlich echte Anrufe Ihrer Bank, bei denen Sie sich mit Ihren Bankdaten legitimieren sollten. Unter Umständen haben Sie ein nicht benötigtes Zusatzblatt Ihres Kontoauszugs in den Abfalleimer bei Ihrer Bank / zu Hause geworfen oder es werden verschiedenen Daten aus verschiedenen Quellen zusammengeführt. Denkbar sind auch Phishing-Mails, über die zuvor Daten ausgespäht wurden.

Hinweis auf verdächtige Abbuchungen

Ein Beispiel von vielen in den letzten Wochen: Ein 79-jähriger Mann aus dem Raum Bonn-Endenich erhielt einen Telefonanruf. Der Anrufer nannte seinen angeblichen Namen, sagen wir Herr Brockmann, und stellte sich als Mitarbeiter der örtlichen Sparkasse (Sicherheitspersonal, Mitarbeiter der Betrugsprävention, …) vor. Er teilte mit, dass es auf dem Konto des Angerufenen zu verdächtigen Abbuchungen gekommen sein. Das Konto sei nun gesperrt worden. Die Bank wolle mit dem Bankkunden die verdächtigen Abbuchungen abgleichen und prüfen, ob die Umsätze tatsächlich vorgesehen seien.

Einzelne Maschen der Täter

Erforderlich sei angeblich z.B.

- die Nennung mehrere TANs, damit die bereits getätigten Überweisungen rückgängig gemacht und rücküberwiesen werden können.
- aufgrund der vorsorglichen Kontosperrung, müsse die PIN am Telefon genannt werden und die Debitkarte an einen weiteren Bankmitarbeiter ausgehändigt werden, der diese zeitnah abhole; ggf. wird geäußert, der Bankkunde erhalte eine neue Karte und Zugangsdaten.
- das Einrichten bzw. Eröffnen eines Sicherheitskontos. Man habe die verdächtigen Abbuchungen stoppen können, damit nichts Weiteres geschehe, solle der Betroffene möglichst sofort sein komplettes Guthaben von ihrem aktuellen Girokonto auf das Sicherheitskonto übertragen.
  Hier werden Sie mitunter nicht um eine TAN-Freigabe oder ähnliches gebeten, sondern angehalten, die Zahlung und die Freigabe selbst zu initiieren.

Beachten Sie:

Wie bei anderen Telefonbetrugsmaschen kommt es auch bei diesem Phänomen u.U. vor, dass die Täter die Rufnummernanzeige am Telefon manipulieren, sodass aufmerksame Bankkunden tatsächlich die Telefonnummer ihrer

Hausbank sehen (Call-ID-Spoofing). Hierdurch soll Vertrauen beim Angerufen geschaffen werden. Informieren Sie sich bitte zu dieser technisch möglichen Manipulation unter: https://bonn.polizei.nrw/seniorenpraevention-0.

Tipps der Polizei – So schützen Sie sich vor den Maschen

Die Polizei gibt Ihnen die folgenden Tipps:

- Lassen Sie sich nicht unter Druck setzen.
- Legen Sie den Hörer auf, wenn Ihnen etwas merkwürdig erscheint.
- Sprechen Sie am Telefon niemals über Ihre persönlichen und finanziellen Verhältnisse.
- Übergeben/Überweisen Sie niemals Geld oder Wertgegenstände an unbekannte Personen.
- Händigen Sie niemals einem Abholer Ihre Debitkarte aus! Geben Sie am Telefon niemals eine PIN oder TAN preis! Kein Bankmitarbeiter wird das je von Ihnen verlangen.
- Geben Sie eine TAN preis, kann in diesem Moment eine Überweisung autorisiert werden.
- Sprechen Sie mit Ihrer Familie oder anderen Vertrauten über den Anruf.
- Falls Sie einen dubiosen Anruf Ihrer Hausbank erhalten haben, zögern Sie nicht, legen Sie auf. Und rufen Sie dann Ihre Bank selbst an unter der Ihnen aus den Bankunterlagen bekannten Nummer. Nutzen Sie nicht die Rückruffunktion. (s. Call-Id-Spoofing)
- Wenn Sie unsicher sind: Rufen Sie die Polizei unter der 110 (ohne Vorwahl) oder Ihre örtliche Polizeidienststelle an.

Wenn Sie bereits Opfer geworden sind:

- Erstatten Sie immer eine Strafanzeige. Nur so erhält die Polizei Kenntnis von der Straftat und kann die Täterinnen oder Täter verfolgen.
- Außerdem erhält Sie dadurch Informationen zum Ausmaß dieses Deliktsfelds, kann Zusammenhänge herstellen und ggf. Tatserien erkennen. Eine Strafanzeige können Sie persönlich auf der nächstgelegenen Polizeidienststelle oder online unter Internetwache Polizei NRW erstatten.
- Leisten Sie auf keinen Fall weitere Geldzahlungen.
- Informieren Sie umgehend Ihr kontoführendes Geldinstitut, um eventuell ggf. getätigte Geldflüsse noch anzuhalten oder rückgängig zu machen.

Weiterführende Informationen:

https://polizei-beratung.de/startseite-und-aktionen/aktuelles/

https://bonn.polizei.nrw/

https://bonn.polizei.nrw/seniorenpraevention-0

Bei weiteren Fragen wenden Sie sich an:

Polizeipräsidium Bonn - Direktion K – KK KP/O
Seniorenberatung
Königswinterer Straße 500, 53227 Bonn
Telefon 0228-15-7666 (Seniorentelefon) oder -7676
(Geschäftszimmer)
seniorenberatung.bonn@polizei.nrw.de