Kriminelle geben sich am Telefon als Bank-Mitarbeiter aus

05.03.2021 17:11 von Martina Jansen (Kommentare: 0)

Kriminelle geben sich am Telefon als Bank-Mitarbeiter aus

Volksbank Schermbeck eG

Warnung vor Phishing-Telefonanrufen

Schermbeck. Aktuell häufen sich Betrugsversuche, bei denen sich psychologisch geschulte Täter Zugriff auf das Konto der Bankkunden erschleichen wollen. Indem sie sich als Bankmitarbeiter ausgeben, versuchen sie an die Zugangsdaten und Passwörter des Bankkunden zu gelangen. In der Folge kommt es zu Kontoplünderungen oder Identitätsdiebstahl. Grundsätzlich gilt: Legen Sie bei Zweifeln direkt auf, geben Sie niemals Kennwörter oder TAN-Nummern preis und rufen Sie Ihre Bank selbst zurück.

Beispiel eines solchen Telefonanrufs

Es ist früher Abend, das Telefon klingelt. Der Bankkunde meldet sich. Am anderen Ende vermeintlich die Bank. Die Nummer auf dem Bildschirm dürfte passen. Der Anrufer teilt mit, es sei eine verdächtige Transaktion aufgefallen. Mehrere tausend Euro seien überwiesen worden, was sehr auffällig sei. Nun bittet man den Bankkunden, sich im Online-Banking anzumelden und die Überweisung zu prüfen. Komme der Bankkunde dieser Aufforderung nicht nach, sehe man sich leider gezwungen, den Zugang zu sperren. Zur Sicherheit müsse der Bankkunde einmal eine TAN (Transaktionsnummer, mit der z.B. Überweisungen bestätigt werden müssen) erzeugen und diese dem Anrufer mitteilen.

Dabei gehen die psychologisch geschulten Täter äußerst geschickt vor, nutzen vorher ausgespähte Kundendaten, um Vertrauen aufzubauen und setzten die Bankkunden durch angebliche Dringlichkeit unter Druck. Eine typische Masche dabei: „Geben Sie mir doch schnell Ihre TAN-Nummern, damit ich diese sperren kann." Haben die Täter erstmal eine solche TAN-Nummer des Kunden, können sie fast beliebig auf das Kundenkonto zugreifen.

In einem solchen Fall wurde die betroffene Bankkundin skeptisch und legte auf. Einen kurzen Moment später klingelte das Telefon erneut. Diesmal wurde statt der Nummer der Bank der Bankname angezeigt, den die Kundin im Telefon eingespeichert hatte. Am anderen Ende der Leitung meldete sich die gleiche Frau wie beim ersten Telefonat. Die Bankkundin legte auf und meldete den Fall ihrer Bank.

Geben Sie keine Daten weiter – Ihre Hausbank wird nie eine TAN-Nummer von Ihnen erfragen

Empfänger solcher Telefonanrufe sollten nicht auf die Forderungen eingehen, sondern einfach auflegen. Geben Sie keinesfalls Daten weiter und informieren Sie Ihren Bankberater über den Betrugsversuch. Falls Sie Ihre Daten bereits preisgegeben haben, empfehlen wir Ihnen, Ihr Online-Banking direkt selbst zu sperren. Hinweise dazu finden Sie auf den Internetseiten Ihrer Hausbank.

Dabei ist die beschriebene Phishing-Masche nicht neu und seit Jahren bekannt: Manchmal gaben sich Betrüger am Telefon als Bankmitarbeiter aus, ein anderes Mal als Mitarbeiter des Rechenzentrums der Bank oder der Firma Microsoft. Ziel ist es immer, an die Zugangsdaten, Passwörter und TAN-Nummern des Kunden zu kommen, um damit auf das Online-Banking und so auf die Gelder der Bankkunden zugreifen zu können.

Was kann ich tun, um mich zu schützen

Grundsätzlich sollten alle Computer oder mobilen Geräte mit einem aktuellen Virenscanner geschützt sein. Wechseln Sie Ihre Kennwörter regelmäßig. Geben Sie niemals TAN-Nummern oder Kennwörter an Telefon preis. Legen Sie im Zweifel direkt auf und rufen Sie Ihre Bank selbst zurück. Stellen Sie auf die aktuellen Verfahren und Apps ihrer Bank um, z.B. auf die VR-BankingApp und die VR-Secure-Go-App der Volksbank. So ist garantiert, dass Zugang zum Online-Banking und TAN-Nummern getrennt bleiben, auch wenn Sie nur ein Mobilgerät nutzen.

Alle Informationen finden Sie auch auf der Homepage der Volksbank Schermbeck unter www.vb-schermbeck.de im Menüpunkt Banking&Service.

Text: Volksbank Schermbeck