AKTUELLE WARNUNG

Aktuell kommt es vermehrt zu Betrugsfällen, bei denen sich Kriminelle telefonisch als Bankmitarbeiter ausgeben und versuchen, Zugriff auf Smartphones und Online-Banking zu erhalten. Diese Betrugsmasche ist besonders gefährlich, da sie technisch raffiniert und psychologisch gut vorbereitet ist.

So funktioniert die Betrugsmasche: Die Täter kontaktieren ihre Opfer telefonisch und nutzen dabei **manipulierte Rufnummern** („Call-ID-Spoofing"), sodass im Display scheinbar die echte Nummer der Bank erscheint. Unter einem plausiblen Vorwand – etwa einer angeblichen Sicherheitslücke oder einer verdächtigen Transaktion – bauen sie Vertrauen auf. Im nächsten Schritt fordern die Betrüger dazu auf, eine **Fernwartungs-App (z. B. AnyDesk, TeamViewer, RustDesk oder ähnliche Anwendungen wie „Super Proxy") aus dem offiziellen App-Store zu installieren.** Diese Programme sind grundsätzlich legal, werden hier jedoch missbräuchlich eingesetzt. Sobald das Opfer den Zugriffscode weitergibt, können die Täter das Smartphone aus der Ferne steuern und den Bildschirm live mitverfolgen. Dadurch umgehen sie Sicherheitsverfahren wie die Zwei-Faktor-Authentifizierung, da sie TANs und Eingaben direkt sehen und nutzen können. In der Folge führen sie unbemerkt Überweisungen aus oder versuchen weitere Zugriffe (z. B. Bestellung digitaler Karten).

Besonders perfide:
- Es werden echte oder täuschend ähnliche Telefonnummern verwendet.
- Die Täter sprechen überzeugend und liefern glaubwürdige Erklärungen.
- Die Angriffe betreffen nicht nur ältere Menschen – auch jüngere, beruflich eingespannte Personen - oft unter Zeitdruck - sind gefährdet.

Wichtiger Hinweis: Keine Bank fordert ihre Kunden telefonisch dazu auf, Fernwartungssoftware zu installieren oder Zugangsdaten weiterzugeben.

So schützen Sie sich:
- Installieren Sie niemals Fernwartungs-Apps auf Aufforderung eines Anrufers.
- Legen Sie im Zweifel sofort auf und rufen Sie Ihre Bank über die Ihnen bekannte Nummer selbst zurück, nicht über die Rückruffunktion.
- Geben Sie keine PINs, TANs oder Zugangsdaten am Telefon weiter.
- Seien Sie misstrauisch bei Aufforderungen zu angeblichen „Sicherheitsmaßnahmen" oder Überweisungen auf „Sicherheitskonten".

Sofortmaßnahmen im Verdachtsfall:
- Trennen Sie Ihr Gerät vom Internet.
- Deinstallieren Sie die installierte App.
- Kontaktieren Sie umgehend Ihre Bank zur Sperrung.
- Erstatten Sie Anzeige bei der Polizei.

Fazit: Die Täter nutzen gezielt Vertrauen und Stresssituationen aus. Der wichtigste Schutz ist Aufmerksamkeit und ein gesundes Misstrauen. **Bitte informieren Sie auch Ihr Umfeld über diese Betrugsmasche.**

VR Bank
Mittelhaardt eG