VR-Bank Mittelfranken Mitte eG warnt vor zunehmenden Betrugsmaschen

Ansbach, November 2026. In den vergangenen Monaten registriert die VR-Bank Mittelfranken Mitte eG eine deutliche Zunahme an Betrugsversuchen, bei denen Kriminelle versuchen, das Vertrauen von Bankkundinnen und -kunden auszunutzen. Besonders häufig geben sich die Täter am Telefon oder online als vermeintliche Bank- oder IT-Mitarbeiter aus, um an sensible Daten zu gelangen oder ungewollte Überweisungen auszulösen. Die Bank ruft daher zu erhöhter Aufmerksamkeit auf und informiert über die aktuell verbreitetsten Methoden.

Eine der gängigsten Varianten ist der sogenannte **Call-ID-Spoofing-Betrug.** Dabei erscheint auf dem Display der Anrufenden die echte Telefonnummer der VR-Bank, obwohl der Anruf tatsächlich von Betrügern stammt. In vielen Fällen wird ein angeblicher Fehler bei einer Kontobelastung geschildert. Um eine vermeintliche Rückbuchung anzustoßen, sollen Kunden am Telefon Kontodaten oder sogar TAN-Codes weitergeben. Oft haben die Täter bereits im Vorfeld über gefälschte Links Zugangsdaten abgegriffen und benötigen nun lediglich die Zwei-Faktor-Freigabe, um eine Überweisung endgültig abzuschließen.

Aktivierungscodes im Visier der Kriminellen

Besonders perfide ist eine weitere Masche, bei der Kriminelle die Aktivierung von Freigabe-Apps ausnutzen. Dabei erbeuten sie zunächst über einen manipulierten Link die Zugangsdaten zum Online-Banking. Kurz darauf erhalten die Opfer einen echten Brief zur App-Aktivierung – und nahezu zeitgleich einen Anruf eines „Bankmitarbeiters", der den Aktivierungscode erfragt. Wer diesen preisgibt, verschafft den Tätern vollumfänglichen Zugriff auf das Konto.

Zudem häufen sich **Anrufe angeblicher IT-Mitarbeiter,** etwa von „Microsoft". Unter dem Vorwand eines Sicherheitsproblems fordern die Täter dazu auf, eine spezielle App zu installieren, die Remote-Zugriff auf den Computer ermöglicht. Ihnen gelingt es so, heimlich Schadsoftware einzuschleusen oder Bankdaten zu stehlen. Die VR-Bank betont, dass Microsoft oder andere große Softwareanbieter niemals unangekündigt anrufen und schon gar keinen Zugriff auf private Geräte verlangen.

Betrugsfallen auf Online-Marktplätzen

Auch über Online-Marktplätze wie eBay Kleinanzeigen oder Vinted kommt es vermehrt zu Vorfällen. Kunden erhalten gefälschte Zahlungsbestätigungen oder Links zu nachgebauten Banking-Seiten. Geben sie dort ihre Zugangsdaten ein, wird im Hintergrund bereits Geld auf Konten der Betrüger überwiesen. Viele Betroffene bemerken dies erst, wenn es zu spät ist.

Zusätzlich warnt die VR-Bank vor **vermeintlich attraktiven Geldanlagen,** die über soziale Netzwerke oder dubiose Finanzplattformen beworben werden. Hinter den verlockend dargestellten Angeboten verbergen sich oft professionell gestaltete Betrugsseiten, die lediglich darauf ausgerichtet sind, Kontodaten abzugreifen oder hohe Vorauszahlungen zu kassieren.

Wenn Betrüger gezielt Vertrauen aufbauen

Ebenfalls zunehmend verbreitet ist das sogenannte **Love-Scamming (Liebesbetrug).** Hier bauen Kriminelle über soziale Netzwerke, Messenger-Dienste oder Online-Partnerbörsen gezielt eine scheinbar vertrauensvolle Beziehung zu ihren Opfern auf. Über Wochen oder sogar Monate hinweg werden intensive Kontakte gepflegt und emotionale Bindungen geschaffen. Sobald ausreichend Vertrauen aufgebaut wurde, schildern die Täter angebliche Notlagen, beispielsweise medizinische Notfälle, Reiseprobleme oder finanzielle Engpässe, und bitten um Geldüberweisungen. Besonders tragisch ist, dass Betroffene häufig nicht nur finanzielle Verluste erleiden, sondern auch emotional stark belastet werden. Die VR-Bank rät deshalb, bei Online-Bekanntschaften besonders vorsichtig zu sein und niemals Geld an Personen zu überweisen, die man ausschließlich über das Internet kennt.

Eine seit vielen Jahren bekannte, aber weiterhin erfolgreiche Betrugsmasche ist der sogenannte **Enkeltrick.** Dabei geben sich Betrüger am Telefon oder per Messenger-Nachricht als nahe Angehörige aus, häufig als Enkel, Kinder oder andere Familienmitglieder. Unter einem Vorwand, beispielsweise einem Unfall, einer dringenden Rechnung oder einer finanziellen Notlage, wird versucht, die Opfer zu einer schnellen Überweisung oder Bargeldübergabe zu bewegen. In einigen Fällen treten die Täter auch als vermeintliche Polizeibeamte oder andere Vertrauenspersonen auf, um zusätzlichen Druck auszuüben. Die VR-Bank empfiehlt, bei solchen Forderungen grundsätzlich misstrauisch zu sein und die betreffende Person immer über die bekannte Telefonnummer selbst zurückzurufen, bevor Geld überwiesen oder persönliche Informationen weitergegeben werden.



Foto: adobe_stock/fizkes

Vorsicht vor Betrugsmaschen im Internet: Kriminelle versuchen zunehmend, über gefälschte Anrufe, Nachrichten oder Webseiten an sensible Bankdaten zu gelangen. Die VR-Bank Mittelfranken Mitte eG informiert über aktuelle Risiken und gibt Hinweise zum Schutz der eigenen Konten.

Sichere Technik braucht wachsame Nutzer

Die VR-Bank Mittelfranken Mitte eG weist darauf hin, dass moderne Sicherheitsverfahren wie IP-Adressabgleich, Zwei-Faktor-Authentifizierung und starke Verschlüsselung das Online-Banking grundsätzlich sehr sicher machen. Doch der Schutz kann nur wirken, wenn Kunden keine vertraulichen Informationen preisgeben und Links sowie unerwartete Anrufe kritisch prüfen. Bei Auffälligkeiten sollten Betroffene sofort den offiziellen Kundenservice kontaktieren – und zwar über die bekannten und offiziellen Kontaktwege, nicht über Nummern, die in E-Mails, Chats oder unerwarteten Anrufen genannt werden.

Die Bank appelliert deshalb an alle Kunden: „Geben Sie niemals TAN-Codes, Passwörter oder Aktivierungscodes am Telefon weiter und klicken Sie nicht auf unbekannte Links." Wachsamkeit sei der effektivste Schutz gegen moderne Betrugsversuche. Die VR-Bank Mittelfranken Mitte eG stehe ihren Kunden jederzeit als verlässlicher Ansprechpartner zur Seite.

Kontakt bei Verdacht:
Telefon: 09 81 1 81 0
E-Mail: info@vr-mfr.de

VR-Bank Mittelfranken Mitte eG