

Raiffeisen, Volksbank und Sparkasse warnen vor Betrugsmaschinen

Raiffeisen, Volksbank und Sparkasse warnen vor einer Welle an Betrugsfällen. Neu ist der massive Einsatz von Künstlicher Intelligenz – Stichwort Stimmenfälschung, Betrugsfälle im Zusammenhang mit Kryptowährungen und weiterhin Telefonbetrug: durch verschiedene Täuschungsmaschinen stehen manchmal Existenzen auf dem Spiel.

"Wir kennen Fälle, in denen Menschen durch vermeintliches Online-Trading über 100.000 Euro verloren haben. Doch oft ist damit noch nicht Schluss: Ein angeblicher Anwalt oder eine falsche Aufsichtsbehörde verspricht anschließend, das Geld zurückzuholen – verlangt dafür jedoch vorab 10 Prozent der fiktiven Gesamtsumme als „Gebühr“. Am Ende ist auch dieses Geld verschwunden. Leider sind uns sogar Fälle bekannt, in denen so die Ersparnisse eines ganzen Lebens verloren gegangen sind.", erzählt **Gunde Bauhofer, Geschäftsführerin der Südtiroler Verbraucherzentrale.**

Die Beispiele von Betrugsmaschinen sind vielfältig. Den Betroffenen wird suggeriert, sie würden in Technologien wie **Künstliche Intelligenz (KI)** und **Kryptogeld bzw. Blockchain** investieren, was für viele verlockend klingt – dabei werden in Wahrheit überhaupt keine Investitionen getätigt.

Besonders perfide ist der Einsatz der sogenannten **Deepfake-Technologie**, mit der Stimmen oder Videos von Familienangehörigen oder vertrauten Personen täuschend echt nachgeahmt werden. Unter dem Vorwand, in einer Notlage helfen zu wollen, werden die Opfer gedrängt, kurzfristig Geld zu überweisen. Dafür sammeln die Betrüger zuvor gezielt Stimmproben über Telefonate, die sie anschließend in betrügerischen Anrufen verwenden.

Parallel dazu werden vermeintlich lukrative Investitionsangebote in Kryptowährungen verbreitet. Kriminelle geben sich dabei als Finanzexperten, Behördenvertreter oder Bankmitarbeitende aus und versuchen, Betroffene zur Überweisung von Geld oder zur Preisgabe sensibler Daten zu bewegen.

Ein besonderes Risiko besteht bei Krypto-Zahlungen: Einmal überwiesene Beträge können nicht zurückgeholt werden.

Kriminelle kontaktieren potenzielle Opfer telefonisch, per SMS oder E-Mail, imitieren offizielle Banknummern und erstellen gefälschte Webseiten, die denen des Online-Bankings oder Zahlungsdienstleistern wie Nexi täuschend ähnlich sind. Ziel dieser Angriffe ist es, **vertrauliche Daten** wie PIN, Passwörter oder Autorisierungscode zu erlangen, um

betrügerische Transaktionen durchzuführen. Seriöse Banken verlangen niemals von ihren Kunden die Herausgabe solcher vertraulichen Daten.

Charakteristisch für viele dieser Betrugsversuche ist der Aufbau massiven psychologischen Drucks. Unter Hinweis auf angeblich dringenden Handlungsbedarf oder einmalige Gewinnchancen werden Betroffene zu schnellen Entscheidungen gedrängt.

Empfehlungen zum Schutz vor Betrug:

- Ungewöhnliche Kontaktaufnahmen kritisch hinterfragen, insbesondere bei Geldforderungen über neue Telefonnummern oder per Videoanruf. Im Zweifel das Gespräch beenden und die bekannte offizielle Nummer selbst kontaktieren.
- Niemals Passwörter, PINs oder TANs für Online-Banking oder Krypto-Wallets weitergeben.
- Keine Links in unaufgeforderten E-Mails oder SMS anklicken.
- Offizielle Webseiten und Apps direkt über die bekannte Adresse aufrufen.
- Bei größeren Überweisungen oder Unsicherheiten den persönlichen Kontakt mit der eigenen Bank suchen.
- Autorisieren sie niemals Überweisungen, deren Herkunft oder Zweck Ihnen unklar ist
- Lassen Sie sich nicht unter Druck setzen: Kriminelle nutzen häufig Dringlichkeit und Angst, um ihre Opfer zu manipulieren.

Bei alledem wichtig: Nicht aus einem Gefühl der Bedrängnis heraus handeln. Ein kurzes Innehalten und eine sorgfältige Überprüfung der Situation können helfen, finanzielle Schäden zu vermeiden. Bei Fragen oder Unklarheiten stehen die Raiffeisenkassen, die Volksbank, die Sparkasse oder die Südtiroler Verbraucherzentrale gerne zur Verfügung.

Kontakt:

Südtiroler Volksbank AG
Media Relations

Maria Santini
maria.santini@volksbank.it