NACHRICHTEN
Österreich

17. Juni 2025

Phishing-Betrug schlägt zu: 69-Jähriger verliert tausende Euro!

Unbekannter Betrüger ergaunert telefonisch mehrere tausend Euro von älterem Mann. Tipps zur Vermeidung von Online-Banking-Betrug.

Darmstadt, Deutschland - Ein 69-jähriger Mann ist Opfer eines Phishing-Betrugs geworden, bei dem ein unbekannter Täter ihm telefonisch erklärte, sein Girokonto sei gehackt worden. Mit einer sogenannten Fernzugriffssoftware gelang es dem Betrüger, Zugriff auf das Onlinebanking des Opfers zu erlangen. Über den Computer des Mannes wurden angebliche Rücküberweisungen angezeigt, die den Eindruck erweckten, dass diese notwendig wären, um einen Hacker zu identifizieren. Am Ende kam es zu tatsächlichen Überweisungen, die dem älteren Herren einen Schaden von mehreren tausend Euro verursachten. Dies berichtet das **Gailtal Journal**.

Diese Art des Betrugs zeigt, wie leicht Kontoinhaber in die Falle

von Cyberkriminellen geraten können. So rufen oft Betrüger an, die sich als Mitarbeiter einer Bank ausgeben und verlangen einen Datenabgleich über spezifische Apps, wie die VR-SecureGoPlus-App. In einem ähnlichen Fall führte dies zu 28 Überweisungen in Höhe von über 6.700 Euro, wobei die Bank im Nachhinein für den Schaden aufkam, da der Kunde keine grobe Fahrlässigkeit nachweisen konnte. Dies wurde durch ein Urteil des Landgerichts Darmstadt entschieden, veröffentlicht auf **test.de**.

Rechtslage bei Online-Banking-Betrug

Im Kontext von Online-Banking-Betrug ist die rechtliche Situation für Betroffene wichtig. Laut den gesetzlichen Grundlagen sind Banken verpflichtet, unberechtigte Zahlungen zu erstatten, es sei denn, sie können grobe Fahrlässigkeit des Kunden nachweisen. Ein Beispiel zeigt, dass eine Bank für einen Verlust von über 100.000 Euro zur Hälfte haftete, weil ihre Mitarbeiterin nicht auf deutliche Betrugsanzeichen reagierte. Dies sagt auch viel über die Verantwortung von Banken aus, ihre Kunden zu schützen. Informationen über diese rechtlichen Rahmenbedingungen sind auf **anwalt.de** zu finden.

Das Bundeskriminalamt berichtete, dass die Zahl der Cybercrime-Fälle 2024 um 15 % gestiegen ist. Verbraucher verlieren durch solche Betrugsfälle häufig erhebliche Summen, während Banken oftmals die Haftung abweisen. Dabei ist eine sofortige Meldung des Betrugs an die Bank unerlässlich, um Ansprüche nicht zu gefährden und eine Erstattung unberechtigter Transaktionen zu sichern.

Schutzmaßnahmen und Prävention

Um sich vor Phishing und anderen Betrugsformen zu schützen, sollten Verbraucher einige wichtige Sicherheitsvorkehrungen treffen. Dazu zählt die Nutzung von Zwei-Faktor-Authentifizierung sowie das Aufstellen sicherer Passwörter. Das Erkennen von Phishing-Angriffen ist ebenfalls entscheidend:

Achten Sie auf ungewöhnliche Absender, Dringlichkeit von Forderungen und Rechtschreibfehler in der Kommunikation.

Nach einem Betrugsfall ist es ratsam, schnell zu handeln: Konten sollten gesperrt, Strafanzeigen erstattet und alle relevanten Beweise dokumentiert werden. Im Fall von Phishing und anderen Online-Banking-Betrügereien ist es nicht nur wichtig, vorsichtig zu sein, sondern auch seine Rechte ernst zu nehmen und notfalls rechtliche Schritte zu erwägen.

Details	
Vorfall	Betrug
Ursache	Phishing
Ort	Darmstadt, Deutschland
Schaden in €	100000
Quellen	• **gailtal-journal.at** • **www.test.de** • **www.anwalt.de**