AMTSGERICHT MÜNCHEN
- Pressesprecher -

Pressemitteilung 09 vom 24.03.2025

Phishing bei Kleinanzeigen

Kein Anspruch gegen die Bank auf Ersatz nicht autorisierter Abbuchungen bei grober Fahrlässigkeit

Der Kläger bot Anfang August 2023 über das Portal Kleinanzeigen.de einen Gegenstand zum Verkauf an, woraufhin der Kläger von einem vermeintlichen Kaufinteressenten kontaktiert wurde. Dieser veranlasste den Kläger dazu, seine Kreditkartendaten auf einer Phishing-Seite einzugeben.

Am 02.08.2023 um 15:08 Uhr erhielt der Kläger auf seinem Handy schließlich eine mobileTAN per SMS für die Aktivierung eines neuen Geräts. Dieses Gerät wurde von dem Betrüger bei der beklagten Bank per Banking-App kurz darauf auch registriert.

Am 02.08.2023 um 15:11 Uhr und 21:16 Uhr erfolgten zwei Abbuchungen in Höhe von 2.200 € und 207,25 €. Der Kläger veranlasste sofort eine Kartensperrung und verlangte von der Bank die Rückbuchung der beiden Abbuchungen. Da die Bank dies verweigerte, verklagte der Kläger sie vor dem Amtsgericht München auf Zahlung von 2.407,25 € nebst Zinsen.

Der Kläger behauptete, die mit der SMS erhaltene mobileTAN nicht weitergegeben zu haben und auch sonst nirgendwo eingegeben zu haben.

Das Amtsgericht wies die Klage mit Urteil vom 21.01.2025 ab. Insoweit führte es aus:

„*Es liegt zur Überzeugung des Gerichts eine grob fahrlässige Sorgfaltspflichtverletzung [des Klägers] vor. Der Kläger hat in grober Weise die im (Zahlungs-)Verkehr zu fordernde Sorgfalt nicht an den Tag gelegt, indem er seine Kreditkartendaten sowie seine persönlichen Sicherheitsmerkmale an Dritte herausgegeben hat. Jeder auch nur durchschnittlich aufmerksame Marktteilnehmer weiß, dass Kreditkartendaten und persönliche Sicherheitsmerkmale wie SMS-TANs keinen Dritten, insbesondere keinen Kaufinteressenten auf Kleinanzeigen, mitgeteilt werden dürfen. […]*

Das Gericht geht davon aus, dass der Kläger auf der Phishing-Seite „sicher bezahlen“ die erhaltene SMS-TAN zur Freigabe eines neuen Endgeräts eingegeben hat. Mit Hilfe dieser TAN konnte der Täter dann ein neues Endgerät registrieren und die streitgegenständlichen Verfügungen ausführen.

Der Kläger war unstreitig auf der Phishing-Seite „sicher bezahlen“ und wurde dort aufgefordert zur Eingabe seiner Kreditkartendetails. Der Kläger hat auch unstreitig am 02.08.2023 um 15:08 Uhr per SMS eine TAN erhalten zur Registrierung eines neuen Endgeräts. Daher sieht das Gericht in dieser Konstellation eine sekundäre Darlegungslast auf der Klägerseite dazu, wie die TAN zeitnah an den Täter gelangt ist, wenn nicht dadurch, dass der Kläger sie auf der Phishing-Seite angegeben hat. […]

Der Kläger ist als Verkäufer auf der Plattform [Kleinanzeigen.de] aufgetreten. Warum man als Verkäufer und damit als Person, die Geld erhalten soll, eine (vorgetäuschte) Zwei-Faktor-Freigabe erteilt, erschließt sich dem Gericht nicht. Der Kläger mag ggfs. nicht bewusst die per SMS erhaltene TAN auf der Phishing-Seite eingegeben haben und es mag ihm auch nicht erinnerlich sein. Indessen lässt sich der Vorgang plausibel nicht anders erklären. […] Es darf von jedem verständigen Nutzer der Bezahlstruktur im Internet erwartet werden, dass er die grundlegende Bedeutung derartiger Freigabecodes versteht.“

Urteil des Amtsgerichts München vom 21.01.2025
Aktenzeichen: 222 C 15098/24
Das Urteil ist rechtskräftig.

München, 24.03.2025
Pressestelle Amtsgericht München