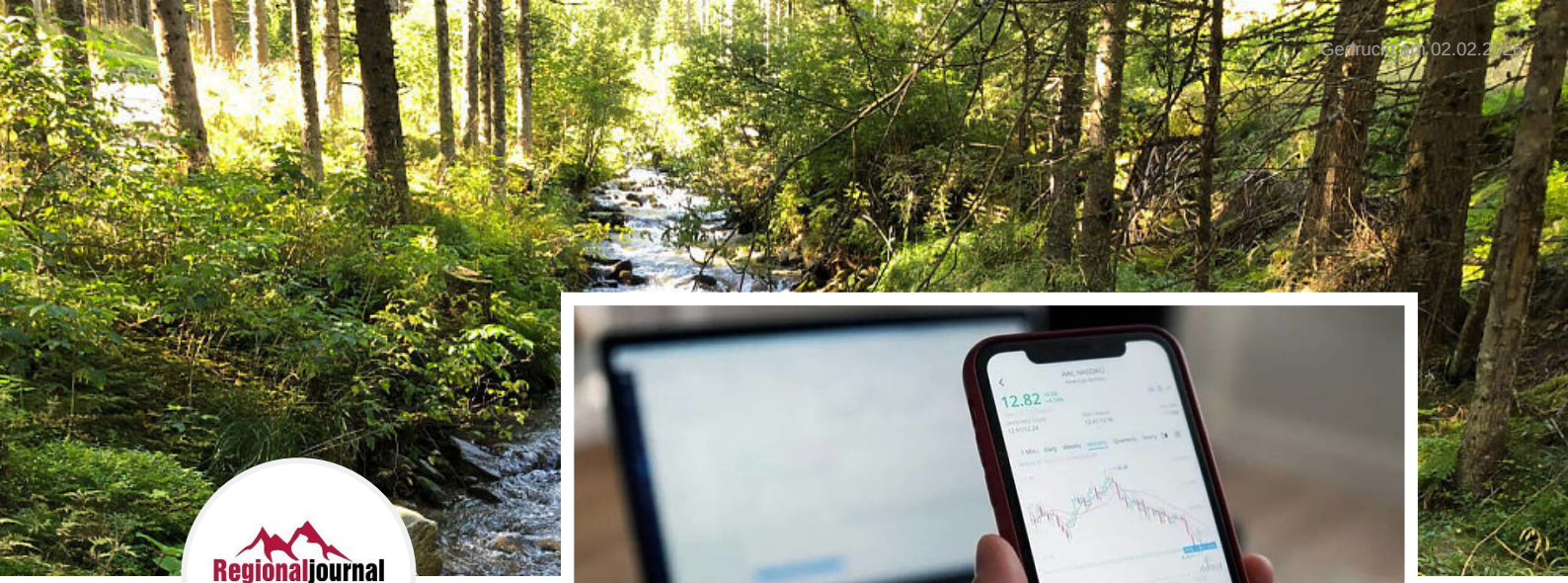

Regionaljournal Steiermark

Neue Betrugsvariante | Präventionstipps sollen Straftaten verhindern

Kriminalisten warnen vor einer aktuellen, und vor allem neuen Betrugsvariante. Die Opfer werden getäuscht und deren bestehenden Kryptowährungskonten raffiniert „leergeräumt“. Die Polizei befürchtet, dass es mit dieser Variante bald viele Opfer mit großen Schadenssummen geben könnte.

Ob mittels Phishing, Bestellbetrug, Falscher Polizist oder vielen andere Methoden, Betrüger sind raffiniert und einfallsreich. Das Ziel ist dabei immer dasselbe, Opfer zu finden, zu täuschen und schließlich deren Geld widerrechtlich zu erhalten. Das zeigt auch eine aktuelle neue Betrugsform, welche derzeit den Ermittlern des Grazer Kriminalreferates auffällt. Erste Opfer sind bereits zu beklagen.

Vorgehensweise

Die Täter wenden sich per SMS an die Opfer. Durch sogenanntes „Spoofing“ verwenden sie dabei die identen Telefonnummern von ihren echten Kryptowährungsanbietern. Aufgrund dessen scheinen die Nachrichten der Täter auch im selben Nachrichten-/Chatverlauf wie vom tatsächlichen Kryptodienstanbieters auf. Die Opfer, welche ihre Kryptowährungen auf sogenannten Wallets gespeichert haben, werden mit dem täuschenden Hinweis, dass es zu einem versuchten Fremdzugriff auf diesem Wallet gekommen wäre aufgefordert, eine vermeintliche Servicenummer zu kontaktieren.

Fremdzugriff auf Wallet als Täuschungshandlung

Opfer, welche dann diese vermeintliche Servicenummer kontaktieren, treten somit erstmals ungeahnt selbst mit ihren Betrügern in Kontakt. Die Täter stellen dann im Zuge der Konversation, sichere „Wallets“ zur Verfügung. Die Opfer installieren diese und vertrauen hier den „falschen“ Anbietern blind. Sobald das „Geld“ von den „echten“ Wallets auf die „betrügerischen“ Wallets überwiesen wurde, findet auch

bereits der finale Betrug statt. Die Täter leeren sofort das Konto.

Präventionsmaßnahmen

- Vertrauen Sie niemals „blind“ einer Nachricht bzw. Aufforderung
- Überzeugen Sie sich immer, ob diese Nachricht tatsächlich seriös ist
- Treten Sie im Zweifel über die Plattform Ihres Kryptowährungsanbieters in Kontakt
- Kontaktieren Sie im Zweifel immer die Polizei (133)
- Erstatten Sie Anzeige, wenn Sie bereits Opfer einer Straftat wurden