AKTUELLE NACHRICHTEN
Deutschland
NACHRICHTEN AG

Vorsicht! Telefonbetrug im Landkreis: 3.000 Euro verloren!

Ein 67-jähriger Mann aus Hersfeld-Rotenburg fiel auf Phishing herein. Polizei warnt vor Telefonbetrug und gibt Schutzmaßnahmen.

Am 26. Februar 2025 erhielt ein 67-jähriger Mann aus dem Landkreis Hersfeld-Rotenburg einen betrügerischen Anruf von einer Frau, die sich als Mitarbeiterin der Sparkasse ausgab. Während des Telefongesprächs wurde er dazu gebracht, einen Link in einer parallel versendeten SMS zu bestätigen, um sein Bankkonto zu sperren. Die vermeintliche Mitarbeiterin nutzte diese Situation, um unbefugten Zugriff auf sein Konto zu erlangen. Am darauf folgenden Tag informierte ihn seine echte Bankberaterin über die unberechtigten Abbuchungen von seinem Konto.

Die Polizei hat inzwischen ermittelt, dass der Mann durch diese betrügerischen Machenschaften einen finanziellen Schaden von

schätzungsweise 3.000 Euro erlitten hat, welcher teilweise durch Rückbuchungen gemildert werden konnte. Solche Phishing-Angriffe, bei denen Kriminelle sich als vertrauenswürdige Personen oder Institutionen ausgeben, um an persönliche Daten und finanzielle Informationen zu gelangen, nehmen in der heutigen Zeit zu. Wie die Sparkasse informiert, kontaktieren Banken ihre Kunden niemals per E-Mail oder Telefon, um nach sensiblen Daten zu fragen. Die Methode, Betrüger zu entlarven, erfordert Aufmerksamkeit und Wachsamkeit von den Kunden.

Sichere Methoden zur Erkennung von Betrug

Um sich vor Phishing und anderen Betrugsversuchen zu schützen, rät die Polizei zu einer Reihe von Sicherheitsmaßnahmen. Es ist fundamental, misstrauisch zu sein, wenn der Anrufer keine klare Identität preisgibt oder ungewöhnliche Fragen zur Kontrolle von Kontoinformationen stellt. Insbesondere sollten Gespräche sofort beendet werden, wenn nach Geld, TANs, persönlichen Daten oder Überweisungen gefragt wird. Authorisierte Bankmitarbeiter und die Polizei sollten stets über bekannte Telefonnummern kontaktiert werden, anstatt die Rückruffunktion des Telefons zu verwenden.

Phishing-Methoden und Schutzmaßnahmen

Phishing wird auf vielfältige Weisen betrieben, einschließlich E-Mail-Phishing, bei dem gefälschte Nachrichten von Banken oder Online-Händlern versendet werden. Auch Smishing (Phishing über SMS) und Vishing (Phishing via Telefon) sind gängige Praktiken, die Kriminelle verwenden. Eine entsprechende Aufklärung ist notwendig, und die Sparkasse empfiehlt, keine Links in verdächtigen Nachrichten anzuklicken und E-Mail-Absenderadressen genau zu prüfen. Achten Sie auf unpersönliche Anrede und Rechtschreibfehler, die oft Anzeichen für betrügerische Kommunikation sind.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) weist darauf hin, dass Phishing-Angriffe häufig und schwer zu erkennen sind. Die Einhaltung präventiver Maßnahmen kann ernsthafte finanzielle Schäden verhindern. Bei einem Verdacht auf einen Phishing-Angriff sollten Sie sofort Ihre Zugangsdaten ändern, Ihr Bankinstitut informieren und den Vorfall bei der Polizei melden.

Zusammengefasst ist es von entscheidender Bedeutung, sich über die gängigen Phishing-Methoden zu informieren und sich der Gefahren bewusst zu sein. Die Bedrohung von digitalen Betrugsversuchen bleibt ein zentrales Thema in der Sicherheitsdebatte und erfordert sowohl von den Banken als auch von den Nutzern erhöhte Wachsamkeit.

Details	
Quellen	• **rhoenkanal.de** • **www.sparkasse.de**