NACHRICHTEN
Österreich
03. Januar 2025

Achtung Betrug! So erkennen Sie gefährliche Scam-SMS auf einen Blick!

Die ÖGK warnt vor Betrugsversuchen via SMS und E-Mail, die persönliche Daten abgreifen wollen, und gibt wichtige Tipps zur Vorsicht.

Deutschland - In einem besorgniserregenden Trend haben Cyberkriminelle ihre Taktiken verfeinert und zielen nun verstärkt auf ahnungslose Opfer über gefälschte SMS-Nachrichten ab, berichtet die **ÖGK**. Diese als „Smishing“ bekannte Betrugsform, eine Kombination aus SMS und Phishing, versucht, persönliche Daten wie Bankkontoinformationen und Passwörter zu stehlen. Die Nachrichten kommen oft in einem drängenden Ton, um den Empfänger dazu zu bringen, auf einen Link zu klicken oder persönliche Informationen preiszugeben. Die ÖGK rät eindringlich, solche Nachrichten zu ignorieren und niemals auf enthaltene Links zu klicken oder sensiblen Informationen preiszugeben.

Vor allem vor Fake-Nachrichten von angeblichen Paketzustellern, Banken oder Gewinnspielen sollte große Vorsicht geboten sein. Wie **Heise** berichtet, geben sich Betrüger gerne als seriöse Institutionen aus, was die Gefahr erhöht, dass ihre Nachrichten als echt wahrgenommen werden. Bekannte Beispiele hierfür sind SMS von vermeintlichen Zustellunternehmen, in denen erklärt wird, dass Zollgebühren zu bezahlen seien, um ein Paket zu erhalten. Dabei wird häufig ein Link angegeben, der direkt auf eine betrügerische Website führt.

Woran man Betrug erkennt

Um sich zu schützen, sollten Empfänger im Voraus überprüfende Maßnahmen ergreifen: Ein sorgfältiger Blick auf die Absendernummer kann verraten, ob es sich um einen Betrugsversuch handelt – oft haben Scam-Nachrichten ausländische Vorwahlen oder sind von unbekannten E-Mail-Adressen. Ebenso ist eine unpersönliche Ansprache ein Zeichen für potenziellen Betrug. Banksachbearbeiter nutzen in der Regel den Namen des Kunden. Zudem sind Rechtschreibfehler häufig ein Indikator für unseriöse Nachrichten. Absender, die mit drohenden Botschaften um schnelle Reaktion bitten, sollten sofort skeptisch gemacht werden, da dies eine gängige Methode der Betrüger ist, um Druck auszuüben.

Um sich zu schützen, gilt: Bei Verdacht auf einen Betrugsversuch sollten die offiziellen Kontaktstellen der betreffenden Unternehmen konsultiert werden. Es wird dringend empfohlen, nicht auf Links in solchen Nachrichten zu klicken und keine persönlichen Daten preiszugeben.

Details	
Vorfall	Betrug
Ort	Deutschland
Quellen	• **salzburg.orf.at** • **www.heise.de**