Achtung! DPD warnt vor gefährlichem Smishing: So schützen Sie sich!

DPD warnt vor „Smishing“ – betrügerische SMS zu Paketzustellungen. Verbraucher sollten vorsichtig sein und Sicherheitsmaßnahmen beachten.

Deutschland - Aktuell warnt der Paketdienst DPD vor einer betrügerischen SMS-Welle, die sich als Paketbenachrichtigungen ausgibt. In diesen Nachrichten wird behauptet, dass eine Paketzustellung gescheitert sei, und die Empfänger werden aufgefordert, einen Termin zur Neuansprache zu vereinbaren. Diese Betrugsmasche, die als „Smishing“ bekannt ist, zielt darauf ab, persönliche Daten zu stehlen oder Schadsoftware auf den Smartphones der Betroffenen zu installieren. DPD hebt hervor, dass derartige Nachrichten oft verdächtige Links enthalten, die zu Phishing-Seiten führen, wo die Nutzer ihre Daten preisgeben könnten. Wer auf die Links klickt, läuft Gefahr, finanziellen Schaden zu erleiden, beispielsweise durch ungewollte Abonnements oder entleerte Bankkonten. Darüber

hinaus kann Schadsoftware im Hintergrund arbeiten und hohe Kosten für Premium-SMS verursachen. DPD empfiehlt daher, Links in solchen Nachrichten zu ignorieren und stattdessen die offizielle App oder Webseite zu verwenden, da sie ausschließlich über die Domains dpd.de, dpdhl.de oder depot-info.de kommunizieren.

In diesem Kontext lenkt die Verbraucherzentrale NRW den Fokus auf die Gefahren, die von solchen Nachrichten ausgehen. Absender dieser SMS könnten Handynummern aus gehackten Datenbanken oder unseriösen Adressverkäufen beziehen. Zudem deuten persönliche Anreden in den SMS häufig darauf hin, dass Nummern automatisiert aus Telefonbucheinträgen stammen. Verbraucher wird geraten, in ihren Nachrichten-Apps zu überprüfen, dass nur Nachrichten von gespeicherten Kontakten empfangen werden. Einige Sicherheits-Apps und Smartphones bieten zudem Spam-Filter, um unerwünschte SMS zu reduzieren. Generell sollten Links von unbekannten Absendern nicht geöffnet werden, und Nutzer sollten auf keinen Fall neue Apps installieren, die von solchen Nachrichten empfohlen werden.

Verhaltensregeln zum Schutz

Wenn eine unerwünschte SMS empfangen wird, empfiehlt es sich, darauf nicht zu reagieren. Jede Antwort könnte die Absender wissen lassen, dass die Nummer aktiv genutzt wird. Stattdessen sollten solche Nachrichten umgehend gelöscht werden. Im Hinblick auf die Sicherheit von Smartphones rät die Verbraucherzentrale, bei verdächtigen Links, die angeklickt wurden, sofort das Gerät in den Flugmodus zu versetzen und unbekannte Apps zu deinstallieren. Darüber hinaus ist es ratsam, persönliche oder Bankdaten immer mit Vorsicht zu behandeln. Im Verdachtsfall sollten Banken umgehend informiert und Karten gesperrt werden.

Smishing ist eine spezielle Form des Phishings, die insbesondere über SMS oder Messenger-Nachrichten abläuft. Die

Cyberkriminalität ist ein sich ständig ausbreitendes Problem, und die Methoden zur Durchführung von Phishing-Angriffen entwickeln sich weiter. Laut Kaspersky sind Phishing-Angriffe die häufigste Methode für Cyberangriffe, und sie nutzen häufig die Schwachstelle „Mensch“, indem sie soziale Manipulation (Social Engineering) einsetzen, um Vertrauen zu erwecken und sensible Daten zu stehlen. Zu den gängigsten Methoden zählen neben Smishing auch Techniken wie Deceptive Phishing und Vishing.

Um sich vor solchen Gefahren zu schützen, sollten Nutzer regelmäßig ihre Betriebssysteme und Apps aktualisieren und Sicherheitsmechanismen wie Drittanbietersperren beim Mobilfunkanbieter aktivieren. Bei Zahlungsforderungen unbedingt kontaktieren Sie Ihre Bank und, falls notwendig, die Polizei. Es könnte auch ratsam sein, nach einer Phishing-Attacke eine Hausrat- oder spezielle Cyberversicherung in Betracht zu ziehen, um potenziellen Schäden vorzubeugen.

Details	
Vorfall	Betrug
Ursache	Phishing
Ort	Deutschland
Quellen	• **www.ruhr24.de** • **www.verbraucherzentrale.nrw** • **www.kaspersky.de**