Vorsicht „Smishing“: Betrüger stehlen Kreditkarteninformationen mit Nachrichten von angeblichen Paketdienstleistern oder Zoll

- Kriminelle geben sich über Whatsapp, per Mail oder SMS als Zoll oder Paketdienstleister aus und fordern Opfer zur Herausgabe ihrer Kreditkarteninformationen auf
- Betroffene aller Altersgruppen werden mit angeblich unbezahlten Paketgebühren in geringer Höhe geködert
- Experten der ING Deutschland warnen: „Geben Sie niemals Ihre persönlichen Daten an Dritte weiter.“

Frankfurt am Main, 24. Mai 2023: Immer mehr Menschen erhalten derzeit über Nachrichtenkanäle wie Whatsapp, E-Mail oder SMS Zahlungsaufforderungen zu angeblich unbezahlten Paketgebühren. Hinter der Betrugsmasche – auch als „Smishing“ (Kombination aus SMS und Phishing) bekannt – stecken Kriminelle, die täuschend echte Nachrichten versenden und sich als Zoll oder Paketdienstleister ausgeben. Um die oftmals geringe Summe zu begleichen, sollen Empfänger über einen Link in der Nachricht persönliche Daten und Kreditkarteninformationen preisgeben.

Mit den Kontakt- und Kreditkartendaten aktivieren die kriminellen Absender mobile Bezahldienste wie Apple Pay oder Google Pay auf einem fremden Gerät. Aufgrund der Zwei-Faktor-Authentifizierung wird dafür meist noch ein Einmalpasswort benötigt, das die Betroffenen vom eigentlichen Zahlungsdienstleister per E-Mail oder SMS erhalten. Wird dieses Passwort weitergegeben, kann die Aktivierung auf dem Fremdgerät vollzogen werden. Jetzt haben Betrüger freie Hand und können auf Kosten der Betroffenen Gelder überwiesen oder Online-Einkäufe tätigen.

Besonders perfide: Viele Betroffene geben die Informationen arglos weiter, da der erforderliche Betrag meist nur etwa 1,99 Euro beträgt und sie in Zeiten boomenden Online-Handels tatsächlich oft ein Paket erwarten. Hinzu kommt, dass die kriminellen Fake-Nachrichten täuschend echte Symbole oder das Design bekannter Marken beinhalten.

Nico Rudolf, Teamleiter operative Betrugsprävention bei der ING Deutschland, warnt davor, sensible Daten auf Nachfrage Dritter herauszugeben: „Wer aktuell auffällige Nachrichten erhält

und sich unsicher ist, sollte sich umgehend auf einschlägigen Portalen wie der Verbraucherzentrale oder bei seiner Hausbank informieren. Geben Sie niemals persönliche Login-Daten, Codes oder sonstige sensible Informationen an Dritte weiter und seien Sie lieber einmal mehr misstrauisch. Leider ist in den meisten Fällen der Mensch selbst der Unsicherheitsfaktor."

Das können Sie tun, wenn Daten weitergegeben wurden:

- Sperren Sie umgehend Ihre Kreditkarte – oft funktioniert das direkt in der Banking-App. Die Hotline steht (häufig) auf der Karte selbst, auf Kontoauszügen oder der offiziellen Webseite des Finanzhauses.
- Schalten Sie Ihr Telefon bzw. Smartphone in den Flugmodus. So verhindern Sie, dass Kriminelle, die verdeckt eine App oder einen Virus auf Ihr Smartphone geladen haben, weitere Daten erbeuten.
- Sichern Sie die Beweise und fertigen Sie Screenshots oder Fotos der Nachrichten an, die Sie von den Kriminellen erhalten haben. Erstatten Sie anschließend bei der Polizei Anzeige und geben Sie alle relevanten Informationen weiter oder übergeben Sie direkt Ihr Smartphone zur Beweissicherung vor Ort.
- Behalten Sie Ihr Konto im Auge und kontaktieren Sie bei zweifelhaften Abbuchungen oder Kontobewegungen Ihren Kreditkartenanbieter oder Ihre Hausbank. Dasselbe gilt für Ihren Mobilfunkanbieter.

So verhindern Sie Betrug:

- Öffnen Sie niemals Links oder Dateien aus SMS, Mails oder Whatsapp-Nachrichten, deren Herkunft Sie nicht kennen. Falls Sie es doch gemacht haben, geben Sie keine Persönliche Daten wie Bankinformationen an Dritte heraus und installieren Sie auch niemals Apps oder sonstige Anwendungen.
- Seien Sie bei Nachrichten von unbekannten Absendern skeptisch. Lieber einmal mehr bei der offiziellen Kundenhotline des Paketdienstleisters nachfragen.
- Löschen Sie die Nachrichten und antworten Sie der unbekannten Nummer nicht.
- Erwarten Sie tatsächlich ein Paket, vergewissern Sie sich über die offizielle Internetseite des Paketdienstleisters über den Status Ihrer Sendung, etwa über die Tracking- oder Sendungsnummer.

Weiterführende Informationen zum Thema Betrugsmaschen finden sich auf dem Blog der ING Deutschland.

Sollten Sie künftig keine Verbraucherinformationen mehr von uns wünschen, genügt ein kurzer Hinweis an: presse@ing.de

Medienkontakt

ING Deutschland

Sebastian Göb

Tel.: +49 (0) 152 38927131

E-Mail: Sebastian.goeb@ing.de

Die ING in Deutschland

Mit über 9 Millionen Kundinnen und Kunden sind wir die drittgrößte Bank in Deutschland. Unsere Kernprodukte sind Girokonten, Baufinanzierungen, Spargelder, Verbraucherkredite und Wertpapiere. Bei der Kreditvergabe an kleine und mittlere Firmen arbeiten wir im Geschäftskundensegment Business Banking mit der Online-Plattform Lendico zusammen. Im Bereich Wholesale Banking bieten wir Bankdienstleistungen für große, internationale Unternehmen an. Mit über 6.000 Kolleginnen und Kollegen sind wir in Frankfurt am Main (Hauptquartier), Berlin, Hannover, Nürnberg und Wien vertreten.