Media Title : The Star
Headline : Small 'delivery fee' leads to big loss
Date : 18 August 2025
Section : Nation
Page : 7

Small 'delivery fee' leads to big loss

Fraudsters posing as couriers use phishing tactics to steal banking details

By DIVYA THERESA RAVI
newsdesk@thestar.com.my

PETALING JAYA: It is almost becoming part and parcel of stories about the risks of online shopping.

Delivery and courier companies are cautioning online shoppers of scam tactics. Some of these scams even involve victims being tricked into divulging their personal details.

The phishing tactic would see scammers randomly send out messages to recipients, claiming a delivery is pending and buyers need only click on a given link for more details of their parcel.

Often, the scammers would request for a minimal "delivery fee" of a few ringgit from their victims just so they could secretly record the smartphone activities including their online banking details such as the login name and password.

In a recent case, a woman lost about RM2,350 after she was tricked into making a RM1.75 "delivery fee" payment for a parcel she never received.

> **"When victims provide the information the scammers seek, their accounts are hacked into and lead to unauthorised cash withdrawals."**
>
> Zaini Yahman

Ninja Van Malaysia chief sales officer Fariz Maswan said the company recorded over 17,000 scam-related cases last year with 40% of it occurring in the Klang Valley alone.

"We already have more than 3,500 reports in the first three months this year," said Fariz in a statement to *The Star*.

He said scammers had sent out messages under his company's name to hoodwink victims into paying for parcels they never ordered.

"Some victims received parcels they never ordered and were pressured to pay under Cash on Delivery (COD) terms.

"Others get fake delivery messages of what we call 'ghost scams'," he said.

"We are actively educating the public through our social media channels, sharing scam alerts and tips on how to spot red flags in such deceptions.

"We are also working with the government and we hope to stay ahead of the scammers.

"This will help Malaysians shop online with more confidence," Fariz said.

Pos Malaysia's chief operations officer Zaini Yahman said similar complaints of such fake calls and messages were also received by the company's clients.

"These fraudulent messages ask the recipients to update personal details such as addresses and banking information by clicking on malicious links or downloading APK files," said Zaini.

He cited a case last year where a customer's mobile number was compromised when she received a short message service (SMS) claiming her parcel could not be delivered.

"The message included a link to change the delivery date but it did not mention any specific shipment details.

"The customer was redirected to a page where a fee of RM1.37 was requested for a re-delivery.

"Unfortunately, when she proceeded to pay the fee, a charge of RM2,334.58 was imposed and the funds were siphoned from her account. It turned out to be a phishing link.

"When victims provide the information the scammers seek, their accounts are hacked into and lead to unauthorised cash withdrawals," he said.

Malaysian eHailing Association chief activist Jose Rizal said another scamming trend that has been identified is when scammers attempt to access personal accounts, posing as delivery riders and request for the one-time passwords (OTPs) under the guise of verifying deliveries.

"Victims are told they have a pending delivery and in order to receive their parcel, they would need to click on a given link and pay a fee for 'Customs Department taxes' or 'delivery charges'," said Jose.

"We have urged delivery companies to further enhance the identification of their delivery riders and provide proper digital proof to prevent customers from falling victim to such scams involving the delivery of parcels," said Jose.