

PB SCAM RANGER



BULLETIN

Series 5: Parcel Scam

WHAT IS A PARCEL SCAM?

Parcel scams are tactics used by fraudsters to trick victims into revealing personal information or transferring money. Scammers often disguise themselves as delivery service representatives, sending phishing emails, text messages, or calling you on “unclaimed” or “undelivered” package. These scams create fear and urgency, leading victims to act quickly without verifying the situation.



CASE STUDY

A RETIREE LOSSES RM2 MILLION TO PARCEL SCAM

1. A retiree received a call from an unknown number claiming she have an unclaimed parcel containing fake ICs and documents in Melaka.
2. The call was then transferred to a fake police officer from IPK Melaka for investigation.
3. The retiree was instructed to update her personal information through WhatsApp and was pressured to make multiple payments for a so-called “investigation”.
4. The next day, the retiree received another phone call from scammer asking for a payment for audit purposes by another party.
5. To clear the name that linked to the suspicious parcel, she performed multiple transactions over the counter.
6. After seeking advice from her relatives, she then realised that she has been scammed and lost RM2 million.



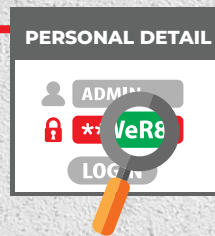
RED FLAGS TO LOOK OUT FOR!



Notifications on parcels you never ordered or have no idea of.



Fear tactics urging immediate action or payments.



Requests to share personal information through WhatsApp, SMS, or unsecured links.



Received call or messages from unknown number impersonating as delivery staff, police, or government officials.



HOW TO AVOID BEING A VICTIM?



Verify Before You Act – Always confirm with the official courier company using their official website or customer service hotline.



Never Share Personal Details – Courier companies and authorities will not ask for banking details, IC numbers, or passwords over the phone.



Be Wary of Urgency – Take your time to verify; scammers use fear tactics to make you act quickly.



Seek a Second Opinion – If in doubt, consult family members or call the courier's official hotline before making any payment.

Verify the legitimacy of the recipient's account number by checking it on **Semak Mule PDRM**.

<https://semakmule.rmp.gov.my/>



The screenshot shows the homepage of the Semak Mule PDRM website. It features the Google logo at the top, followed by the URL <https://semakmule.rmp.gov.my/>. Below the URL is a navigation bar with the text "JABATAN BIASATAN JENAYAH KOMERSIL" and "POLIS DIRAJA MALAYSIA". The main content area includes a language selection dropdown (labeled 1: Choose your Language), a search bar (labeled 2: Key in the Account Number), and a "Semak" button (labeled 3: Click Semak). The search bar contains the text "No Akaun Bank".

The screenshot shows the search results page. It displays the text "Rekod" and "Carian untuk No Akaun Bank: 16452600065760". Below this is a table with two columns: "No. Akaun" and "Repot". The "No. Akaun" column contains the value "16452600065760", and the "Repot" column contains the value "2". A large red warning triangle with an exclamation mark is overlaid on the table. Below the table, a red box contains the text "Sebanyak 122 Kali Carian Telah Dibuat".

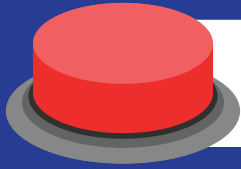
Do NOT make any transactions to the recipient if this disclaimer pops up

DO NOT PROCEED with any transactions if the recipient's account number is flagged with the disclaimer above

HOW TO REPORT IF YOU FALL VICTIM TO A SCAM

 03-2177 3555

 pbesecure@publicbank.com.my



ACTIVATE THE KILL SWITCH

The Kill Switch is a central switch that temporarily disables Online Banking, ATM Cards, and Credit/Debit Cards to prevent further unauthorised transactions.



WAYS TO ACTIVATE THE KILL SWITCH :

- PBe Website
- PBe Login
- MyPB App
- PB enterprise Login

Report Fraud/Scam Incident

If you suspect your account has been compromised, report it via the "Report Fraud/Scam Incident" link.

Report Phishing Links

If you encounter a suspicious website impersonating Public Bank, report it through the "Report Phishing" link.



"We continue to improve best practices in protecting our customers' accounts. This includes working closely with the authorities to address the evolving nature of scams and frauds." said Public Bank's Managing Director & Chief Executive Officer, Tan Sri Tay Ah Lek.

BANK FOR THE PEOPLE

 **PUBLIC BANK**

 **PUBLIC ISLAMIC BANK**
WHOLLY-OWNED SUBSIDIARY OF PUBLIC BANK