

PB SCAM RANGER

BULLETIN



Series 6: Festive Season Online Purchase Scam



FESTIVE JOY

STARTS WITH

SAFE SHOPPING

The festive season is here, so let's keep it merry and secure! With increased shopping activity during this time, scammers may take the opportunity to exploit unsuspecting shoppers and drain their bank accounts. This is why it is important to stay alert, take the right precautions, and keep yourself safe this holiday season.

WHAT IS AN ONLINE PURCHASING SCAM?



An Online Purchasing Scam is a type of fraud where **scammers pretend to be legitimate sellers** on online platforms. They trick people into buying products that will never be delivered or are not as advertised. Scammers often lure victims in with irresistible, too-good-to-be-true deals.



Red Flags to Look For!



Products are sold at prices that seem too good to be true compared to reputable retailers.



Reviews are all five-star, sound generic, or were posted on the same day.



The “seller” uses high-pressure tactics and urges you to make payment quickly, claiming the product is a “limited time offer” or “low in stock.”



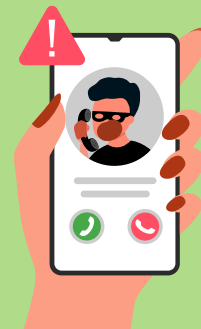
The seller requests additional payments such as shipping insurance, customs fees, or security deposits.



How it work?



Scammers advertise products on social media platforms at unbelievably low prices.



Tempted by the incredible deal, victims contact the scammer to make a purchase.



Victims are then instructed to make multiple payments to a third-party account.



In the end, the victims do not receive the item and are eventually blocked by the scammer.





How to Avoid Falling Victim



Only purchase from trusted and verified online shopping platforms or websites.



Decline any extra fees or additional payments requested to “secure” the product.



Never click on unknown links received from unfamiliar sources.



Avoid sellers who use pressure tactics to push you into making an immediate purchase.



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 bar, there are three numbered instructions with red lines pointing to specific elements on the page:

- ① Choose your Language: Points to the language selection menu (English, 中文, Tamil).
- ② Key in the Account Number: Points to the input field for the account number.
- ③ Click Semak: Points to the SEMAK button.

The page also displays the logo of the JABATAN Siasatan Jenayah Komersil (Commercial Crime Investigation Department) and the text "Semak Akaun yang ada Report".

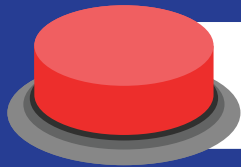
The screenshot shows the search results page of the Semak Mule PDRM website. It displays the search results for the account number 16452600065760. The results show a "No. Akaun" of 16452600065760 and a "Repot" of 2. A red warning triangle icon is displayed in the center, and a red box at the bottom contains the text "Sebanyak 122 Kali Carian Telah Dibuat". Below the search results, there is a red banner with a white text box that reads "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**

 **pbsecure@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