

PB SCAM RANGER

BULLETIN



Series 3 : Job Application Scam

WHAT IS A JOB APPLICATION SCAM?

Scammers post fake job advertisements on social media platforms and untrusted job portals, offering high commissions to mislead individuals seeking legitimate employment. They often urge victims to pay upfront fees to complete assigned tasks in order to receive the promised commission.

CASE STUDY



STUDENT LOSES RM34,000 TO PART-TIME JOB SCAM



Here's How It Happened :

- 1 A fresh graduate, eager to earn income, came across a part-time job advertisement on Facebook offering high commissions and attractive benefits.
- 2 Interested, he contacted the admin via WhatsApp and was given tasks to complete in exchange for commission.
- 3 First, he was asked to like and share 25 social media posts and received RM250. Next, he wrote a product review on the company page and earned another RM400.
- 4 After completing both tasks, the admin instructed him to purchase items via a given link to earn RM5,000.
- 5 He spent RM2,800 but was met with excuses when asking for his promised commission.
- 6 The scammer continued demanding more payments, and in hope of recovering his money, the student borrowed from parents and friends — eventually transferring RM34,000.
- 7 He only realised it was a scam when the admin became unreachable.

RED FLAGS TO LOOK OUT FOR!



JOB OFFERED WITHOUT AN INTERVIEW

You're hired immediately without any verification of your work experience or a proper interview process.



ATTRACTIVE WORK BENEFITS

Terms like 'Remote work,' 'Flexible hours,' and 'Sign-on bonuses' may be used to lure you in.



UNREALISTICALLY HIGH SALARIES

Scammers offer simple tasks with exceptionally high commissions to tempt job seekers.



UPFRONT PAYMENTS REQUIRED

You're asked to make payments upfront to complete tasks or to receive your commission.



HOW TO AVOID BEING A VICTIM?



Do not make any payments in exchange for work. Legitimate employers will never ask for money to offer a job.



Always research and verify that you are dealing with a genuine company or employer.



Be cautious if the job is offered without an interview or proper documentation.



Avoid engaging with potential employers who pressure you to respond or act quick



Remember, offers that promise easy money with little effort is always a red flag.

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

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



**KEY IN THE
ACCOUNT
NUMBER**

**CLICK
"SEMAK MAKLUMAT"**

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