Media Title : The Sun
Headline : Civil servants hit by pay block after accounts flagged
Date : 14 December 2023
Section : National
Page : 6


**No pay for 169 civil servants with mule accounts**

**Serious consequences for those whose accounts are used to collect or transfer funds stolen or laundered from illegal activities: BNM**

Report on page 6

# Civil servants hit by pay block after accounts flagged

## Move based on suspicion of involvement of others in collection, transfer of stolen or laundered funds: BNM

BY **QALIF ZUHAIR**
*newsdesk@thesundaily.com*

**PETALING JAYA:** A total of 169 civil servants are unable to receive their monthly salaries as their accounts have been classified as being involved in "mule" activities.

Mule accounts are those suspected to be used by others to collect or transfer funds stolen or laundered from illegal activities, said Bank Negara Malaysia's (BNM) Link Department deputy director Hasjun Hashim.

She pointed out that the ripple effect of having one's account classified as a mule is severe.

"If a single account has been identified as a mule, all linked accounts will be closed. When this happens, there is a potential loss of jobs and diminished opportunities for the account holder's children," she said.

Meanwhile, Bukit Aman Commercial Crime Investigation Department's (CCID) statistics revealed a 37% rise in online crimes between January and November.

The figures rose from 23,608 cases to 32,366, with a corresponding increase in the value of losses reaching RM1.13 billion or a 46% rise compared with 2022.

Meanwhile, the Cyber999 Cyber Incident Response Centre managed by CyberSecurity Malaysia recorded a total of 5,480 cybersecurity incidents from January to November.

A total of 3,447 online fraud cases were reported to Cyber999 during this period, while 4,741 incidents were recorded by the centre for the whole of last year.

Speaking during the 2023 National Anti-Scam Tour in Putrajaya recently, Hasjun said so far, 43,000 mule accounts have been closed in the country.

"This is an intricate process where we have to trace the digital or paper trail of stolen money that has transited through multiple accounts in what is called 'layering'."

Hasjun warned that once money leaves the account, it is difficult to recover since it would have traversed multiple accounts within a short time.

"Recovering stolen funds involves a complex process. Even if traceable, the layering of transactions makes matching the amounts challenging.

"While some funds can be identified, the recovery process is time-consuming and success rates hover around just 30%."

Hasjun said many civil servants are targets of mule account scams as they can easily apply for loans, which makes them highly vulnerable.

She said while each banking app has a kill switch to halt further transactions in case of a scam, time is of the essence, which underlines the importance of immediately reporting such frauds.

To aid in the recovery of lost money, Hasjun said victims must quickly file a report with the police for them to initiate an investigation to trace the stolen money.

Hasjun said as a direct response to scammers exploiting victims' trust, BNM has mandated robust security measures for all banks to verify their customers.

"When performing substantial transactions, it is important to establish strong parameters for verification as stipulated by BNM," she said.

She added that individuals should remember the 3S – *soal* (question), *sekat* (block), and *sebar* (spread) to combat scams effectively.

CCID Senior Assistant Commissioner Zaldino Zaludin, who also spoke at the event, said scammers constantly change their *modus operandi* to employ a mix of old and new techniques.

"Our vulnerability lies in our willingness to engage with unknown callers or reply to messages from unfamiliar people."

Zaldino said the proliferation of fake links and deceptive advertisements is a significant threat and advised social media users to be extremely cautious.

He said victims fall for scams because they often overlook subtle discrepancies.

"We cannot run away from using our gadgets. Scammers exploit the fact that people rarely notice spelling differences.

"So always check the URL addresses because the alteration or addition of a single letter, variation in alphabets or subtle changes like a dot turning into a comma or a small 'i' becoming a capital 'I' could be a fraudulent link used by scammers," he said.

He urged the public to report scam incidents promptly so the authorities can freeze fraudulent transactions, as a first step to recover lost funds.