

Media Title : The Star
Headline : Expert: Youths should treat job offers with caution
Date : 18 April 2026
Section : Nation
Page : 7



Expert: Youths should treat job offers with caution

PETALING JAYA: Youths can be highly knowledgeable in the digital world, but lack corporate street smarts, which can make them vulnerable to scammers, says cybersecurity expert Prof Dr Selvakumar Manickam.

He said there is a need for students to conduct proper due diligence before they decide to enter the job market.

The Cybersecurity Research Centre director of Universiti Sains Malaysia said the current threat landscape is highly sophisticated and the digital habits of younger people can be easily exploited.

“Scammers use online platforms in distinct stages. Syndicates exploit the algorithm by pushing aspirational content such as luxu-

ry lifestyles, sports cars and the promise of ‘easy money’.

“The goal here isn’t for scammers to post job descriptions, but to bypass critical thinking and sell a lifestyle.

“Once a target clicks the ‘link in bio’ button, they are usually funnelled to other scam platforms.

“Scammers use bots to flood these channels with fake payment receipts and fabricated testimonials, creating a false consensus,” he added.

Selvakumar said school leavers should treat online job offers with caution, while a few practical checks can make a big difference.

“A starting point is verifying the entity independently. Provided links should not be

trusted; rather, the company must be looked up against official government business registries like the Companies Commission of Malaysia.

“If the company does not exist, or if it is registered as a food vendor but is offering an IT job, it is definitely a red flag.

“Legitimate corporate recruiters do not use free webmail email addresses, and the entire hiring process is not conducted via text messages.

“Caution is advised for offers promising high pay for simple work,” he added.

Selvakumar urged job seekers to search for the recruiter’s name, phone number, or job description online alongside words like

“scam” to see if others have reported issues.

“The company should always be called directly using the official number listed on its corporate website to confirm the job offer,” he said.

If the recruiter does not provide this information, this is a major warning sign.

“A legitimate employer pays the employee.

“If there is any request for an upfront payment, whether it is called a processing fee, a visa fast-track, or an equipment deposit, it is a scam,” he added.

He said current safeguards are helpful but not sufficient.

“Social media platforms have reporting tools, and governments

are introducing anti-scam regulations, but enforcement remains highly inconsistent.

“The landscape is currently too reactive and scammers exploit digital loopholes by creating new fake accounts quickly and moving victims to private channels long before automated systems catch on.”

He suggested mandatory identity verification for anyone operating as a recruiter online.

There should also be better cross-border cybersecurity cooperation to track these transnational trafficking-linked scams, and more advanced AI detection capable of flagging fraudulent job ads before they reach the user, he added.