

Media Title : The Star
Headline : DIGITAL NATIVES more prone to scams
Date : 20 August 2023
Section : Cover Story
Page : 4



DIGITAL NATIVES more prone to scams

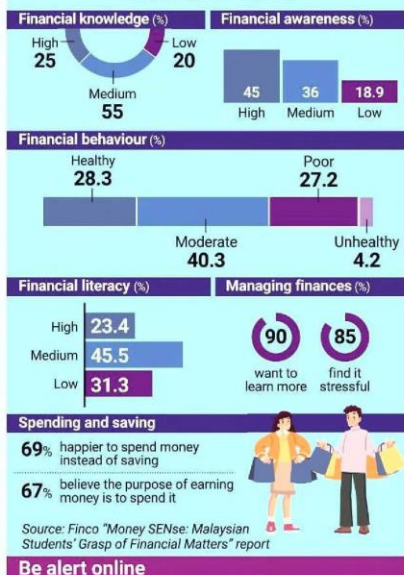
In the news...

Since January this year, at least seven students have reportedly been scammed.

Source: Media reports

Survey: Low financial literacy may be why students are falling prey to criminals

How financially literate are our students?



Be alert online



By JAAAYNE JEEVITA
jaayne@thestar.com.my

JUST about everyone has received some form of scam call, text message or email. With scammers targeting digital natives, who are mainly Gen Z, good financial literacy is key to preventing youths from being conned.

According to the soon-to-be-published Financial Industry Collective Outreach (Finco) "Money SENSE: Malaysian Students' Grasp of Financial Matters" report, 75% of secondary school students surveyed had low or medium financial knowledge with 91 survey responses admitting to have either shared their bank account information with close friends or considered doing so with strangers in exchange for money (see infographic).

Among the sensitive details shared, said Finco chief executive officer Clare Walker, were their bank account passwords and personal identification numbers (PIN). "It is possible that these students do not have their own bank accounts, so perhaps they end up sharing bank accounts with one another to accept deposits or make online purchases.

"As those under the age of 18 can only create a bank account with consent from a parent or legal guardian, they are likely to turn to their peers for help as they see no harm in sharing such sensitive information," she said, adding that students' lack of financial literacy aligns with how vulnerable they can be to online fraud and mule accounts.

The nationwide survey also found that more than 65% of the respondents prioritised short-term gratification over long-term financial planning, Walker told *StarEdu*.

Conducted between Sept 20 to Nov 24 last year, the survey, which saw the participation of 1,121 youths aged between 16 and 19, provided a glimpse into financial literacy levels among upper secondary students, and insights into their knowledge, awareness, behaviour and attitude towards money and financial products and services, as well as the

need for better teaching and learning support in the national curriculum, Walker said.

Finco, a collaborative initiative pioneered by the country's financial institutions with the support of Bank Negara Malaysia, aims to provide underprivileged children and youths with the guidance and educational tools they need to achieve their life goals, she added.



Walker

Vulnerable targets

CyberSecurity Malaysia (CSM) chief executive officer Datuk Dr Amirudin Abdul Wahab said low cybersecurity awareness among Malaysians has resulted in a high number of cybercrime victims, particularly among youngsters.

In-game microtransactions, he said, where players can purchase virtual goods with micropayments within a game, is popular among scammers.

"Youths spend most of their time playing online video games but their familiarity with navigating online platforms can give them a false sense of security, making them vulnerable targets to scammers.

"Some of the most common types of microtransactions range from in-game currencies and loot boxes to battle passes and season passes.

"These microtransactions can be addictive, especially for young gamers," he said.

Youths become easy targets when they do not understand the consequences of disclosing their personal data,

Walker warned.

Scammers can now impersonate legitimate personas or companies as they have very sophisticated means that allow them to create convincing facades, she said.

This, she added, makes it increasingly challenging for users, especially young people, to differentiate between genuine offers and deceptive traps.

"The anonymity of digital scammers further compounds the challenges faced by students, lulling them into a false sense of security and leading them to place trust in individuals they've never met.

"Because the younger generation have

We were scammed

Last year, I was approached by a job recruiter via WhatsApp and was interviewed via Google Meet the next day. He said he found my profile on LinkedIn. I realised something was off when I noticed that the account profile he was using was not his and all the questions asked were pre-recorded. He was not doing the talking. So, I asked him some questions to verify whether he was who he claimed

JANUARY

A Form Six student lost RM22,300, including inheritance from her late mother, after falling victim to a non-existent investment scheme on Telegram.

MARCH

A 23-year-old biomedical science student was asked to pay RM2,099 as "insurance" after buying a RM25 screen protector. She managed to get back RM1,575 she eventually paid to the shop with assistance from the police.

JULY

Several students fell victim to scammers on social media, in an attempt to exchange their eBeliRahmah RM200 ewallet credit for cash. One of them, an undergraduate student aged 20, said she needed cash to pay her tuition fees.

FEBRUARY

A university student in Sabah lost almost RM50,000 after being deceived by a love scam syndicate. The 19-year-old victim experienced the misfortune after meeting a man through Telegram and later connecting on WhatsApp.

APRIL

A student in her 20s was baited with free mobile calls and cash vouchers totalling RM1,000. She lost RM120,000, which included her father's money, instead. The hoax started when she answered a call purporting to be from a telecommunications provider. The caller offered to credit her account with vouchers worth RM1,000 after she completed an online form with information of her bank account, bank card, and father's bank account as a guarantor. Within hours, large sums of money were withdrawn from both accounts.

The Stargraphics

grown up using online services, they are often less vigilant and more trusting, making them more susceptible to falling for elaborate scams if they are not aware of these tactics.

"Scam websites and messages are so genuine-looking that it takes trained eyes and minds to differentiate genuine offers from scams," she said.

Some common tactics which students might fall for include scammers offering small, more believable rewards or money for "low-risk" activities, or a paying job which eventually leads to them being scammed out of a larger amount of money, Walker shared.

She said it is unusual for students, especially those from the B40 communities, to have realistic financial objectives as they lack exposure and guidance.

Despite students having a basic understanding of starting salaries, most of them underestimate things like the cost of living, causing them to plan their budgets inaccurately and thus setting unrealistic financial objectives, she added.

"When students are not equipped with the necessary financial knowledge to make realistic financial objectives and plans, they often end up trying to scrimp and save by reducing spending on necessities in order to achieve their goals.

"When they eventually realise this practice is not feasible, they may give up on their plans altogether, or resort to taking loans or high-interest credit to fund these goals, which might also explain the high debt and bankruptcy rate among young people," she said.

Students who set unrealistic financial goals, said Universiti Sains Malaysia (USM) criminologist Assoc Prof Dr Geshina Ayu Mat Saat, may be willing to do anything to cope with essential needs, or improve their incomes for a better lifestyle.

The pressure to achieve these unrealistic financial goals drives them to easily fall prey to scams in an effort to receive fast and easy money, she said.

Awareness not enough

The Finco survey findings, which are in line with a 2019 study sponsored by the FINRA Investor Education

Foundation, the BBB Institute for Marketplace Trust and the Stanford Center on Longevity that cited low financial literacy and low household income as among the reasons why youngsters are more likely to be victimised by scammers, show that good financial education from an early age is important, especially for students with low levels of academic achievement.

"Raising awareness alone is not enough. We must teach key concepts and introduce financial planning tools which relate to real-life situations that students will encounter as they transition into adulthood.

"This can help them understand how to set financial goals and work towards achievable milestones," Walker said, adding that practical experience, which includes managing money through part-time work and managing a savings account, can help make complex financial concepts more relevant and easy to understand, and raise awareness of good spending habits and attitudes towards money.

"This opens up real-time opportunities for parents, guardians and educators to guide young people needing to make consequential financial decisions that can lead to expensive borrowing, poor financial planning and high levels of debt which have long-term effects on their financial well-being.

"Children from low-income households who see their parents spending a larger share of their incomes on necessities, and setting a small percentage aside as savings, may eventually adopt this habit," she said.

According to Geshina, different kinds of scams attract different types of people. During the Sijil Pelajaran Malaysia (SPM) examination season, education scams aimed at parents and students are popular, she said.

These include dubious institutions offering cheap tuition or registration fees, gifts like laptops, and low entry requirements.

If a service or product is too good to be true, it often is; pay attention to your gut, she advised, adding that victims are classified by specific behaviours, emotions and cognitions.

Citing an example, she said those who are impulsive, gullible, irre-

sponsible, overly trusting, lonely and not able to recognise deception cues, tend to fall prey despite being aware of scams.

The lure of easy money captivates students since they do not have a fixed income, she said, adding that specific emotions like greed may be a contributing factor.

"Scammers typically fish for potential victims like students through online advertisements, invitations, product reviews and testimonials on more than one platform.

"Criminals behind love scams use at least three platforms – usually Twitter, Instagram and a dating app like Tinder, Omi or Bumble – to con their victims.

"Once the student opens the door for communication by accepting a request or confirming interest, the scammer already has a good chance of succeeding," Geshina said, adding that ways or mechanisms to detect signs of scams before and during the process of the crime being committed focus on the use of language, security of data systems, and fraudulent survey websites.

Don't fall for the guise

Universities and educational institutions, Amirudin said, must help educate students to identify, and protect themselves against, common scams.

"Students dealing with financial issues, and those who feel pressured to keep up with their peers, are more likely to be scammed because they are lured by the promise of quick and easy money.

"They can easily fall for fake advertisements and false information on social media. Their vulnerability becomes more alarming when they are not able to recognise the latest modus operandi used by online scammers," he said, adding that students often have little experience when it comes to performing online transactions safely and may not fully grasp the risks involved.

"Plus, they tend to trust their peers or people they meet online easily," said Amirudin.

Petaling Jaya District Police Headquarters Commercial Crime Investigation Division investigating officer Insp Ajass Muhammad Ibrahim said there has been an increase in scam victims aged between 13 and 25 since

the movement control order was imposed in 2020, as many were using their handphones regularly during this period for virtual lessons, gaming and online purchases.

"Students are easy targets as they are attracted to 'good deals'.

"Despite constantly being on social media, many of them are still unaware of scams – just look at how some students use

their parents' payment information to buy gaming credits.

"Parents must teach their children to utilise social media responsibly and keep an eye out for criminals trying to swindle unsuspecting youths," he said during a safety talk at Menara Star on Aug 9.

The police, he said, has approached schools to educate students through talks on potential dangers of online scams.

The Royal Malaysia Police (PDRM) is also collaborating with Universiti Tunku Abdul Rahman (UTAR) and the Malaysia Crime Prevention Foundation in conducting surveys on the effectiveness of anti-scam campaigns in the prevention of commercial crime.

UTAR Assistant Prof Dr Sharon Wilson Ramendran said three surveys on Malaysian youths' susceptibility and risk factors in investment scams, factors that influence financial cybercrime, and factors that cause job and youth scams, are ongoing. The findings, she said, would be revealed next year.

CyberSAFE, an initiative to highlight the various issues users are likely to face online, has already been introduced in schools, Amirudin said, adding that CSM has also developed the National Cyber Security Awareness Module to curb cyberthreats among the population, including schoolchildren.

There are also awareness programmes, such as the Klik Dengan Bijak initiative by the Malaysian Communications and Multimedia Commission that trains users with the knowledge and skills of safe, vigilant and responsible Internet use so that they become positive and ethical netizens, said Amirudin.

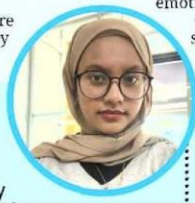
The materials on the Klik Dengan Bijak website, he added, offer advice on maintaining computer security, and spotting fake profiles on ecommerce websites and listings, among others.



Geshina



Insp Ajass



to be. Everything went silent and suddenly, I was blocked on WhatsApp. Luckily, I didn't lose anything or give away my personal details. Be careful with personal details shared online even if it's just done for fun. Scammers will pry into your social media profiles. Always think of the consequences of your actions and your safety.

– Nur Fatimah Irdina Adlan, 22

A person claiming to be my boss messaged me on WhatsApp a few months back, saying he had changed his phone number. I did not suspect anything because the profile photo was of my boss. The scammer asked me to buy a Google Play gift card worth RM1,000 for 'office business', assuring that I would be reimbursed. I did what I was told and was asked to buy two more cards amounting

to RM1,500. At this point, my bank account had already been wiped clean. When I told the scammer I had no money left, I was asked to borrow funds from my friends. I called my boss' original phone number only to discover that I had been scammed. My boss and I have since lodged a police report but I don't think I will ever get my money back.

– A student who only wants to be known as Izyan, 23