UPM
UNIVERSITI PUTRA MALAYSIA
BERILMU BERBAKTI
PUTRA®
PERTANIAN UNTUK RAKYAT
INSTITUT PENYELIDIKAN PENUAAN MALAYSIA (MyAgeing®)
MALAYSIAN RESEARCH INSTITUTE ON AGEING

DIGITAL LITERACY FOR OLDER PERSONS

MODULE 6
Online Scams and Fraud Prevention

By
Siti Anom Ahmad
Fakhrul Zaman Rokhani
Siti Farra Zillah Abdullah
Mohamad Fazdillah Bagat
Foong Hui Foh

Malaysian Research Institute on Ageing (MyAgeing®), Universiti Putra Malaysia

DIGITAL LITERACY FOR OLDER PERSONS

MODULE 6
Online Scams and Fraud Prevention

Siti Anom Ahmad
Fakhrul Zaman Rokhani
Siti Farra Zillah Abdullah
Mohamad Fazdillah Bagat
Foong Hui Foh

UPM
UNIVERSITI PUTRA MALAYSIA
BERILMU BERBAKTI

PUTRA
PERTANIAN UNTUK RAKYAT

INSTITUT PENYELIDIKAN PENUAAN MALAYSIA (MyAgeing®)
MALAYSIAN RESEARCH INSTITUTE ON AGEING

Published by:
Malaysian Research Institute on Ageing
Universiti Putra Malaysia
43400 UPM Serdang
Selangor Darul Ehsan

☎ 03-9769 2750
✉ myageing@upm.edu.my
🌐 http://www.myageing.upm.edu.my

Cover design : **Pointlink Ventures**
Typesetting : **Pointlink Ventures**

PREFACE

MODULE 6:
ONLINE SCAMS AND FRAUD PREVENTION

Malaysian Research Institute on Ageing (MyAgeing®)
Universiti Putra Malaysia

As digital adoption among older persons continues to grow, so too does their exposure to online threats. Scammers are becoming increasingly sophisticated, targeting vulnerable groups, especially older persons, with fraudulent schemes through e-commerce platforms, social media, messaging apps, and even voice and video technology. These threats can lead not only to financial loss but also to emotional distress, eroded trust, and long-term insecurity.In line with our mission to empower older persons with safe and confident digital engagement, the Malaysian Research Institute on Ageing (MyAgeing®), Universiti Putra Malaysia, introduces Module 6: Online Scams and Fraud Prevention as part of our *Digital Literacy for Older Persons program*. Module 6 complements the existing five modules, which cover mobile devices, navigation, communication, online shopping, and identifying trusted online content. It expands the learning journey by introducing key topics such as online shopping scams, charity scams, communication scams, and impersonations. The module also includes tips on how to stay safe online, steps to take when faced with suspicious activity, and how to report scams effectively.

This self-learning resource has been thoughtfully designed to be clear, concise, and accessible for older learners. Our goal is not only to bridge the digital divide, but also to ensure that older persons are informed, confident, and safeguarded in their online interactions.

We encourage all older adults, family members, and community trainers to engage with this module and share its contents widely. With collective awareness and action, we can foster a safer and more inclusive digital space for all.

We sincerely hope you find this module helpful. Thank you.

"With Knowledge We Serve"

MODULE 6

Online Scams and Fraud Prevention

Synopsis

This module aims to equip older learners with essential knowledge and practical skills to recognize, prevent, and respond to various types of online scams and fraudulent activities. With the increasing use of digital platforms, individuals are more vulnerable to cyber threats, especially scams that exploit trust and digital inexperience.

The module introduces the concept of online fraud, explores common scams such as online shopping scams, charity scams, communication scams, and impersonations, and provides practical tips to protect personal information and maintain online safety. Learners will also gain insights into the importance of reporting scams and seeking appropriate help from trusted channels.

By the end of this module, participants will be more confident in navigating the online environment securely and will be empowered to educate others in their community about scam prevention.

Expected Outcome

At the end of the module, you should be able to:

- Describe what online scams and fraud are and understand their potential risks and impacts.
- Identify different types of scams including online shopping scams, charity scams, communication scams, and impersonations.
- Recognize warning signs or red flags of fraudulent activities online.
- Apply practical safety tips to protect themselves from online scams, such as secure browsing habits, creating strong passwords, and verifying information sources.
- Demonstrate the ability to act responsibly when encountering suspicious content or messages.
- Report scams using proper channels such as government websites, helplines, or digital platforms.
- Promote safe digital practices within their own communities, especially among peers and other older persons.

ChecBric Assessment Tool

Based on your prior knowledge and the knowledge acquired after completion of this module, kindly complete the survey below using the following scale:

Scale:

0 - No knowledge	**2** - Knowledgeable and able to clarify well
1 - Limited knowledge	**3** - Competent and can put to practice fully

No	Learning Achievement	Before	After
i.	I understand the nature and impact of online scams and fraud		
ii.	I am able to identify different types of scams related to online shopping		
iii.	I am aware of how charity scams operate and how to avoid them		
iv.	I am able to identify and protect against scams through communication channels such as SMS, email, and messaging apps		
v.	I am able to identify and respond to impersonation scams involving AI-generated videos, voice cloning, or manipulated images		
vi.	I demonstrate knowledge of strategies to protect personal data and avoid online scams		
vii.	I know how and where to report scams and seek help if targeted		

6.0 Introduction to Online Scams & Fraud Prevention

As digital technology continues to transform daily life, it brings convenience and increased risks, particularly from online scams and fraud. Scammers exploit human trust, sophisticated technologies, such as impersonation and deepfake multimedia (i.e. audio/pictures/videos), and a general lack of digital awareness to deceive their targets.

Online scams and fraud encompass various deceptive practices where fraudsters manipulate individuals into revealing sensitive personal details, making unauthorized payments, or falling victim to false promises. Common digital platforms scammers use include e-commerce websites, social media, messaging apps, emails, and even voice or video calls. Scammers often exploit trust, urgency, fear, or curiosity to deceive victims, causing not only financial harm but also significant emotional distress and lasting insecurity.

Older adults are frequently targeted because scammers perceive them as more trusting, less digitally aware, and thus more vulnerable. These deceptive schemes can lead to significant financial loss, emotional distress, and long-term feelings of insecurity.

Understanding and recognizing these risks is essential. By learning about these scams and understanding their signs, older adults can confidently engage online, protect themselves from potential threats, and contribute to creating safer online spaces for themselves and their communities.

6.1 Type of Online Scams

With the rapid growth of internet usage, online scams have become increasingly common, targeting individuals through various digital platforms. Scammers often exploit trust, urgency, or curiosity to deceive victims into sharing personal information, making payments, or clicking on harmful links. Understanding the different types of online scams is the first step toward prevention. This section highlights some of today's most common online scams, including online shopping, charity, communication, and impersonation. By recognizing these tactics, individuals can stay alert and protect themselves from falling victim to digital fraud.

6.1.1 Online Shopping Scams

The rapid growth of e-commerce platforms and online marketplaces has created new opportunities for consumers and scammers. Online shopping scams exploit the convenience of digital transactions by deceiving individuals into buying fake, misrepresented, or never-delivered products. Scammers often use promotional tactics, urgency cues, and appealing visuals to gain trust quickly and push for fast payment. As digital shopping becomes more common, it is crucial to build awareness among older persons on distinguishing genuine offers from fraudulent ones.

a) What are Online Shopping Scams?

Online shopping scams involve cybercriminals posing as legitimate sellers to steal money or personal information. The scammers try to trick you while you're buying something on the internet. They pretend to sell things online, but their real goal is to take your money without giving you the item, or they send you something fake or different from what you ordered. These scams can happen on websites, social media, or messaging apps.

b) Scam Medium

Online shopping scams are carried out through various digital platforms that shoppers commonly used to find products and make purchases. Scammers exploit the trust placed in familiar online environments, often blending seamlessly into legitimate spaces like websites, social media, messaging apps, and email. Understanding where and how these scams occur is the first step to staying safe while shopping online.

The most common media used for online shopping scams:

i. Fake E-commerce Websites

Scam shopping websites often appear legitimate but are, in fact, fraudulent. They typically lure victims by offering prices that seem too good to be true. To further deceive shoppers, these sites frequently copy branding elements such as logos, layouts, and product listings from well-known platforms like Shopee, Lazada, or Amazon, making distinguishing them from the real ones difficult.

ii. Social Media Platforms

Scammers often post fake advertisements on social media platforms like Facebook, Instagram, and TikTok. They trick people into buying items by sending them links or asking them to order through direct messages (DMs). After payment, the product is never delivered, or a cheap, low-quality fake is sent instead.

iii. Messaging Apps

Scammers use messaging apps like WhatsApp, Telegram, or SMS to send out scam links or fake promotions. These messages often claim to offer urgent deals, gifts, or special voucher codes to trick people into clicking the links.

iv. Scam Emails

Scammers send emails that look like they are from trusted sellers or delivery companies. These emails often include fake invoices, order details, or tracking links that try to steal your personal or payment information.

v. Online Marketplaces

Online marketplaces like Mudah.my, Carousell, and Facebook Marketplace have made it easy for Malaysians to buy and sell used goods, cars, gadgets, and more. Unfortunately, scammers have also taken advantage of these platforms by posing as genuine sellers. They lure buyers with attractive deals and then trick them into unsafe payments. Common tactics include "too good to be true" listings, requests for direct bank transfers, refusing secure payment methods, and disappearing after receiving money.

vi. Search Engine Ads

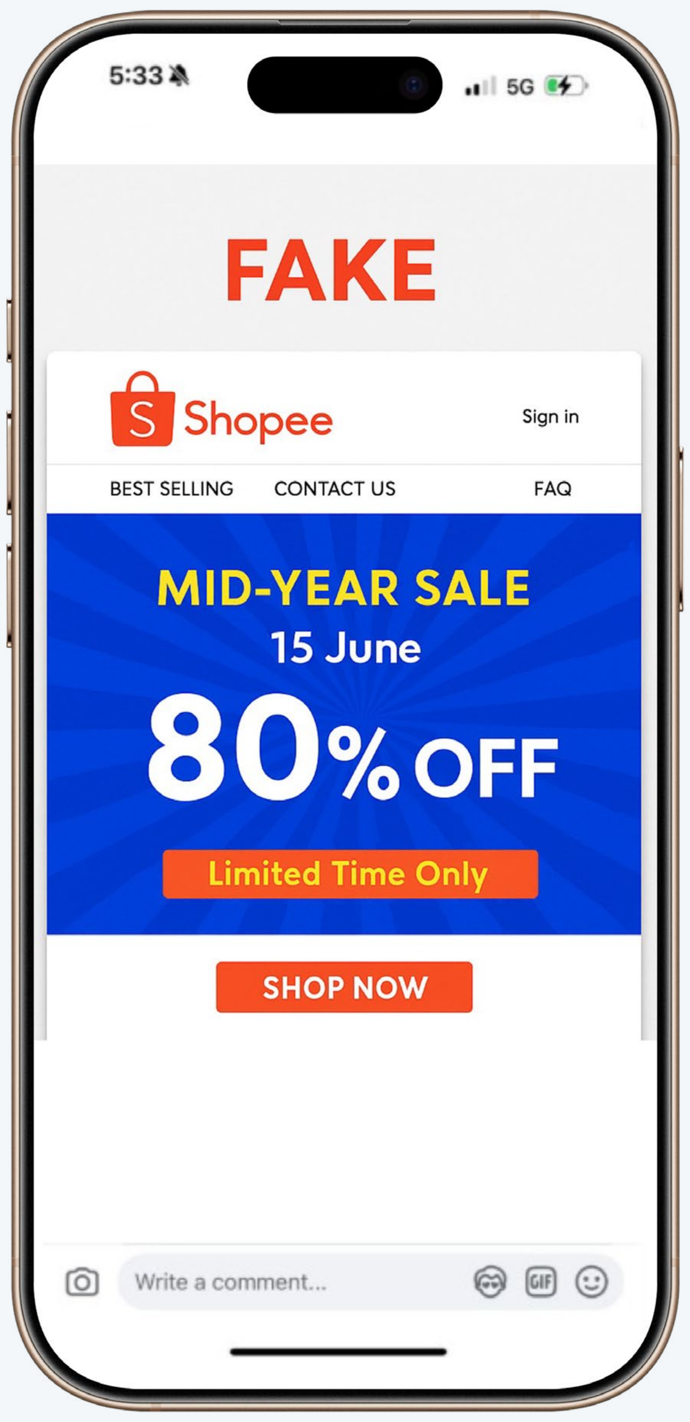
Online shopping scammers are increasingly using search engine ads (like those on Google, Bing, or Yahoo) to trick people into visiting fake websites.

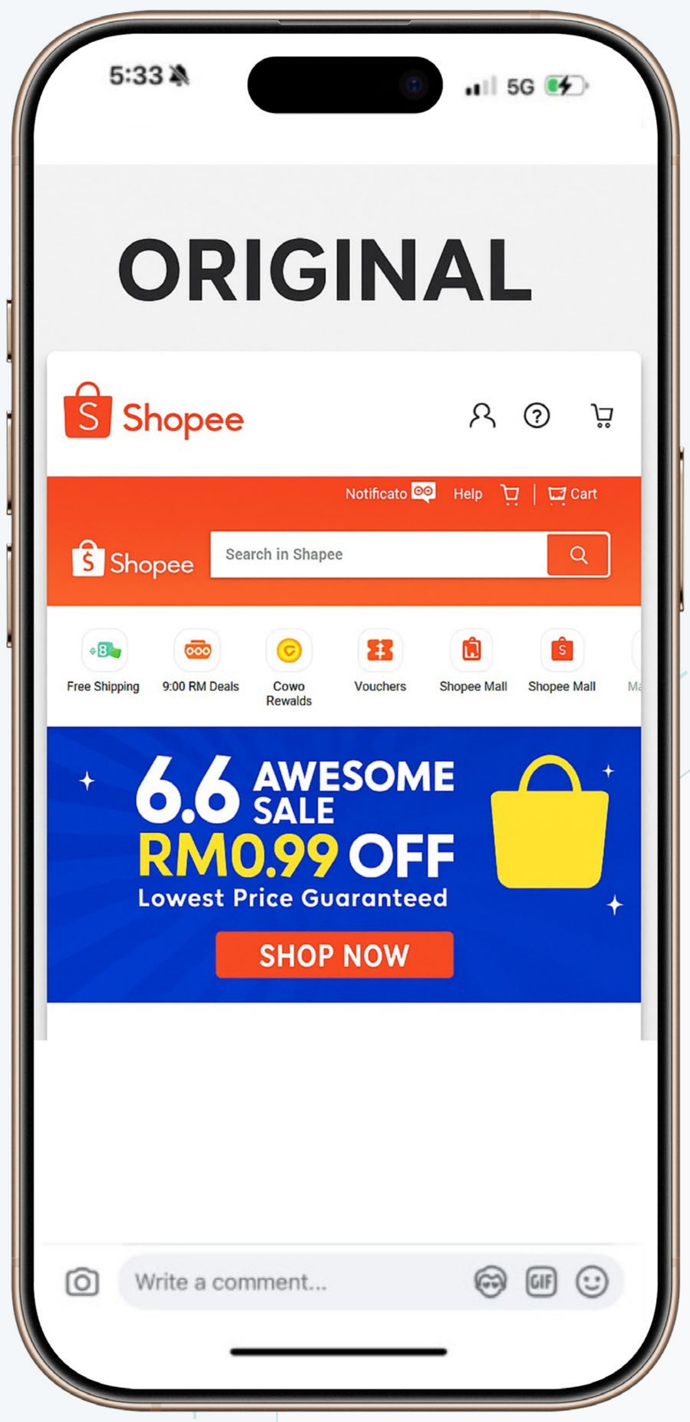
c) Common Methods of Online Shopping Scams

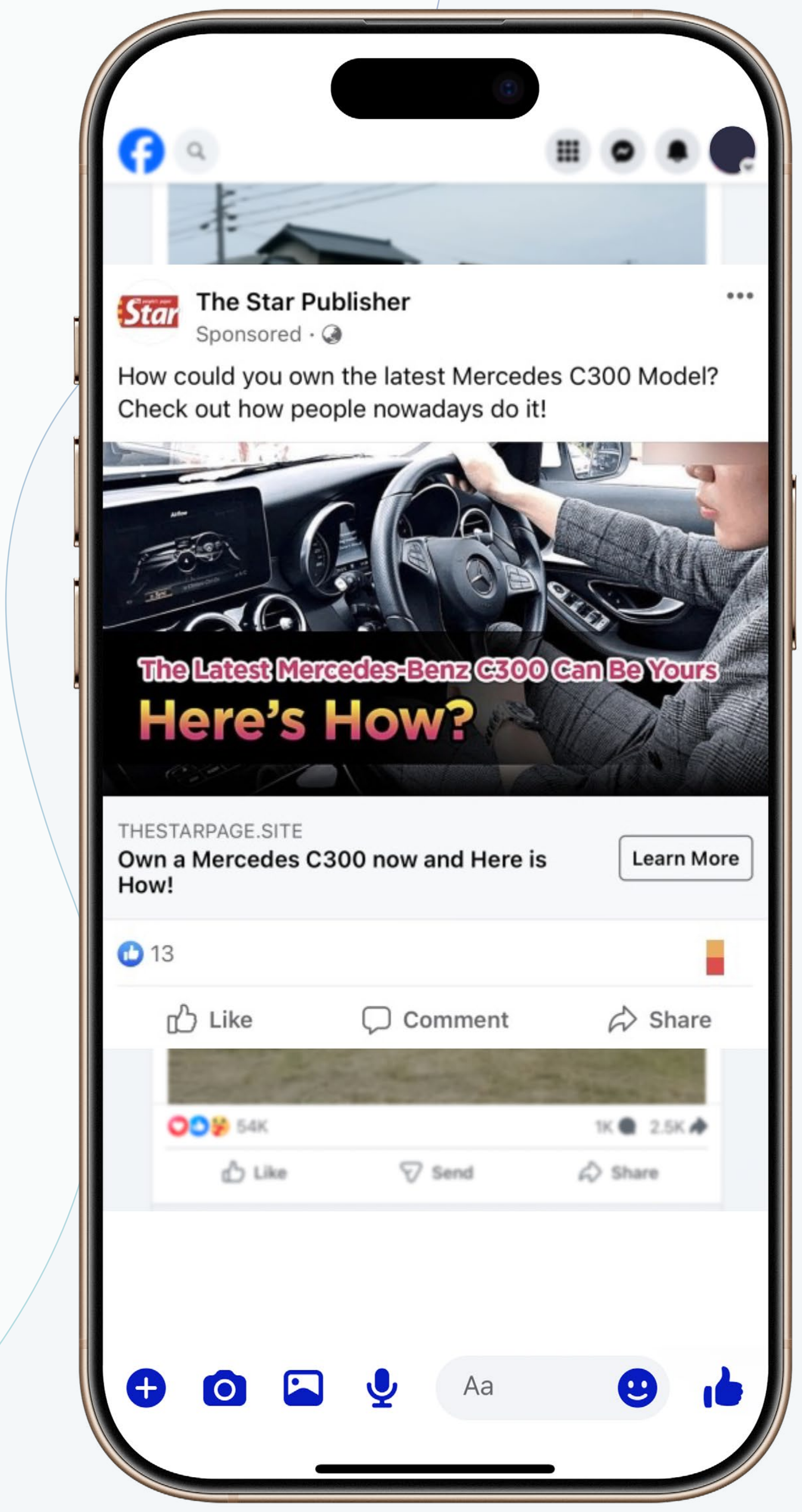
Some common ways scammers trick people:

i. Fake E-Commerce Websites

These websites look like real online shops, but scammers create them to fool you. They often offer popular products at very low prices. You place an order, make a payment, but the item never arrives, or you get something completely different or fake.







The Star Publisher
Sponsored ·

How could you own the latest Mercedes C300 Model? Check out how people nowadays do it!

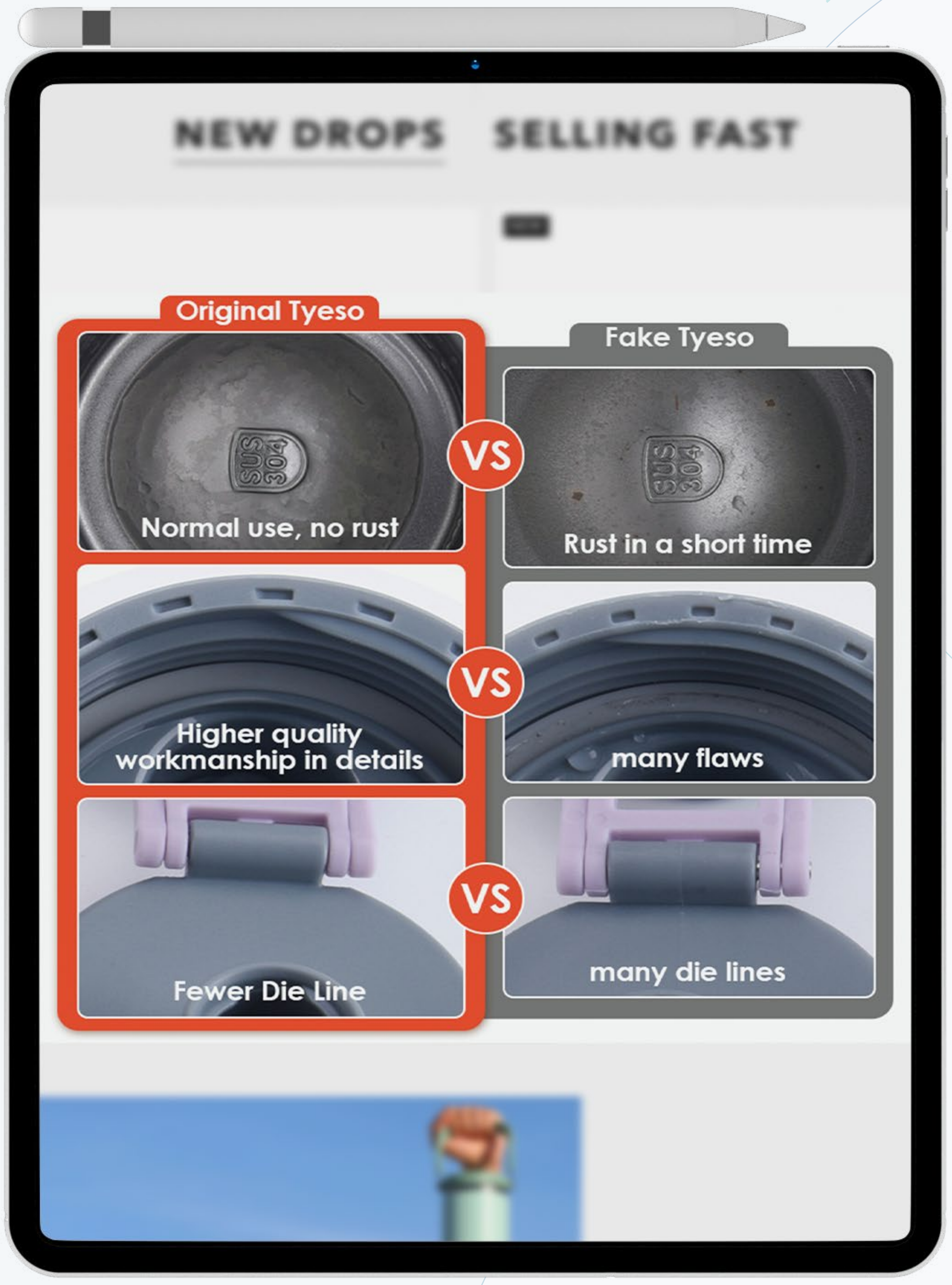
THESTARPAGE.SITE
Own a Mercedes C300 now and Here is How!

ii. Misleading Advertisements

Scammers post attractive ads on Facebook, Instagram, or websites, showing high-quality products. But the real product is cheap, different, or never delivered.

iii. Counterfeit Goods (Fake Items)

These are imitations of popular products (e.g., branded handbags, smartphones, shoes) that are sold as if they are real. You pay thinking you're getting the real item, but it's a fake product that looks similar but is of poor quality and not worth the price.

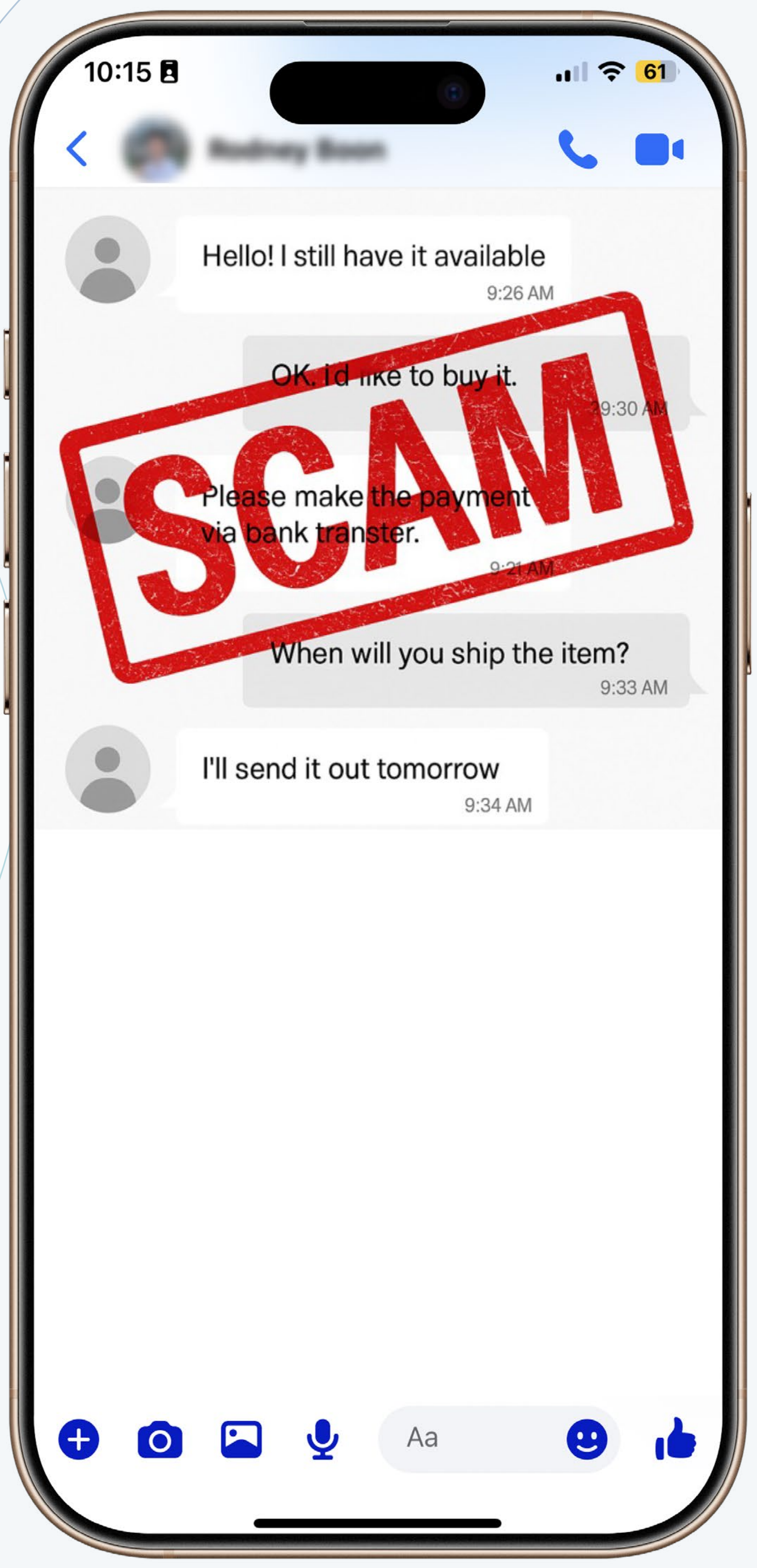


▲

The difference between real and fake product
Source: Authentic product details from Tyeso official store

iv. Payment and Non-Delivery Scams

Scammers ask you to make a direct bank transfer, then disappear after receiving your money. They may also use fake receipts or courier tracking numbers. The product is never delivered, and the seller stops responding.


10:15

[redacted]

Hello! I still have it available 9:26 AM

OK, I'd like to buy it. 9:30 AM

Please make the payment via bank transfer. 9:31 AM

When will you ship the item? 9:33 AM

I'll send it out tomorrow 9:34 AM

d) Warning Signs of Online Shopping Scams

- **Too-good-to-be-true prices**
  Unrealistically cheap items, like iPhones for RM100

- **No HTTPS**
  No padlock icon or HTTPS in the URL (http:// instead of https://)

- **Recently registered domain**
  The domain is new or unrelated
  to the product niche

- **Poor design and grammar**
  Lots of typos, blurry images, or broken links

- **No contact info or fake info**
  No physical address or fake-looking phone numbers

- **Limited payment options**
  Only accepts bank transfer or cryptocurrency

- **No return/refund policy**
  Or vague, poorly written policies

- **Fake reviews**
  Overly positive or copy-paste style reviews

- **Pressure tactics**
  "Only 1 left!" or countdown timers to rush buyers

e) How to Protect Yourself from Online Shopping Scams?

✓ Do This	✗ Avoid This
Shop only on trusted platforms like Shopee, Lazada, Amazon, or official brand websites.	Avoid shopping through random ads, pop-ups, or unknown websites offering unbelievable deals.
Check the website address carefully. Make sure it starts with "https://" and has a 🔒 lock icon.	Don't enter personal or payment information on websites that look suspicious or lack proper security features.
Read customer reviews and check seller ratings before purchasing.	Avoid buying from sellers with no reviews, low ratings, or many complaints.
Be cautious of prices that are too low or pressure tactics like "limited time only!".	Don't rush to buy because of low prices or messages that create urgency without verification.
Use safe payment methods like credit cards, e-wallets, or cash on delivery (COD).	Avoid paying via direct bank transfer or to personal accounts – they offer little or no protection.
Keep your personal information private and secure.	Never share your IC number, bank PIN, or OTP with anyone, even if they are from a trusted company.

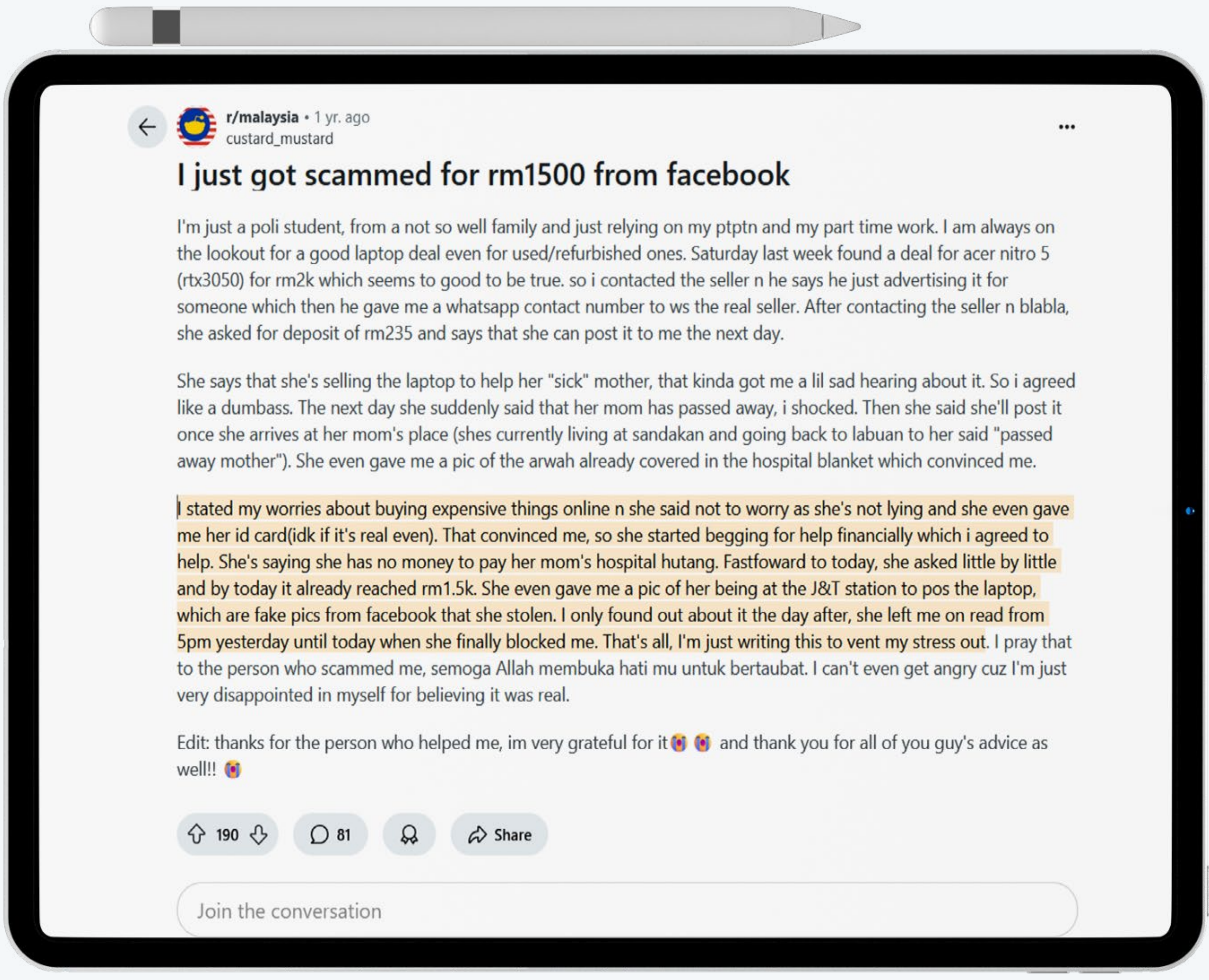
f) Real-Life Cases

In the first quarter of 2025, the Royal Malaysia Police reported 12,110 online fraud cases, resulting in losses of approximately RM573.7 million. This marks a rise from 10,715 cases and RM519.9 million in losses during the last quarter of 2024. From January to March 2025, there was a 36.9% increase in online shopping scams, compared to the same period in 2024, with 2,238 cases and losses exceeding RM19 million **(Malay Mail, Mar 2025).**

The losses due to e-commerce scams have also been rising exponentially, from RM28mil in 2019 to RM140mil in 2022, hitting RM144.8mil in August 2023. [1]. These figures highlight the growing concern of online shopping scams in Malaysia, emphasizing the importance of educating individuals, especially older adults, on how to protect themselves while shopping online.

Below are some real examples of how far scammers will go using cheap prices, sympathy ploys, and fake evidence to make victims send money.

Date	Scam Medium	Methods	Source
2024	Social media	Facebook Marketplace	reddit.com
2025	Online Website	Carousell	The Star
2025	Messaging Apps	Shopee Pay Later	Malay Mail



r/malaysia • 1 yr. ago
custard_mustard

I just got scammed for rm1500 from facebook

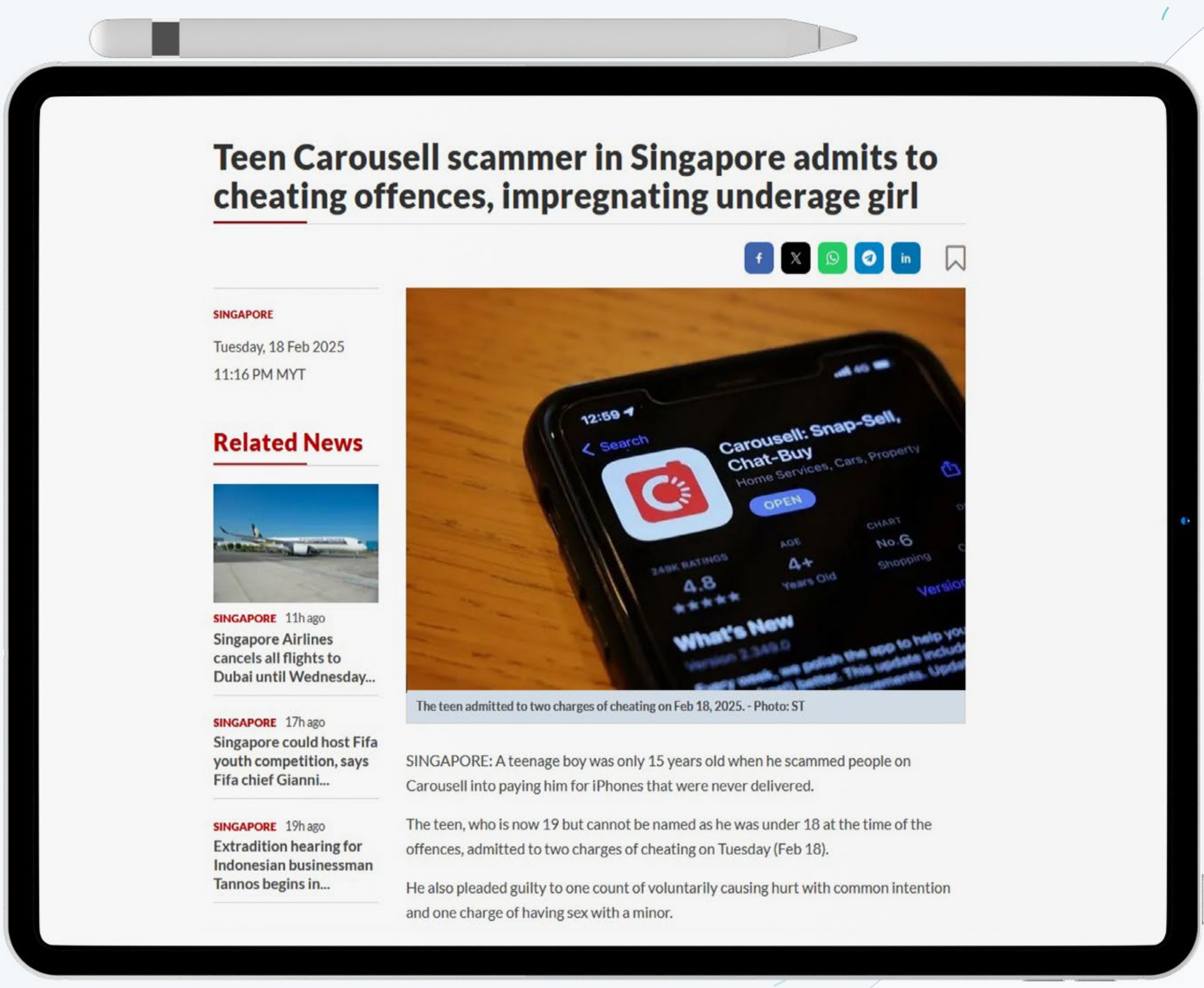
I'm just a poli student, from a not so well family and just relying on my ptptn and my part time work. I am always on the lookout for a good laptop deal even for used/refurbished ones. Saturday last week found a deal for acer nitro 5 (rtx3050) for rm2k which seems to good to be true. so i contacted the seller n he says he just advertising it for someone which then he gave me a whatsapp contact number to ws the real seller. After contacting the seller n blabla, she asked for deposit of rm235 and says that she can post it to me the next day.

She says that she's selling the laptop to help her "sick" mother, that kinda got me a lil sad hearing about it. So i agreed like a dumbass. The next day she suddenly said that her mom has passed away, i shocked. Then she said she'll post it once she arrives at her mom's place (shes currently living at sandakan and going back to labuan to her said "passed away mother"). She even gave me a pic of the arwah already covered in the hospital blanket which convinced me.

I stated my worries about buying expensive things online n she said not to worry as she's not lying and she even gave me her id card(idk if it's real even). That convinced me, so she started begging for help financially which i agreed to help. She's saying she has no money to pay her mom's hospital hutang. Fastfoward to today, she asked little by little and by today it already reached rm1.5k. She even gave me a pic of her being at the J&T station to pos the laptop, which are fake pics from facebook that she stolen. I only found out about it the day after, she left me on read from 5pm yesterday until today when she finally blocked me. That's all, I'm just writing this to vent my stress out. I pray that to the person who scammed me, semoga Allah membuka hati mu untuk bertaubat. I can't even get angry cuz I'm just very disappointed in myself for believing it was real.

Edit: thanks for the person who helped me, im very grateful for it😭 😭 and thank you for all of you guy's advice as well!! 😭

190
81
Share
Join the conversation



Teen Carousell scammer in Singapore admits to cheating offences, impregnating underage girl

SINGAPORE
Tuesday, 18 Feb 2025
11:16 PM MYT

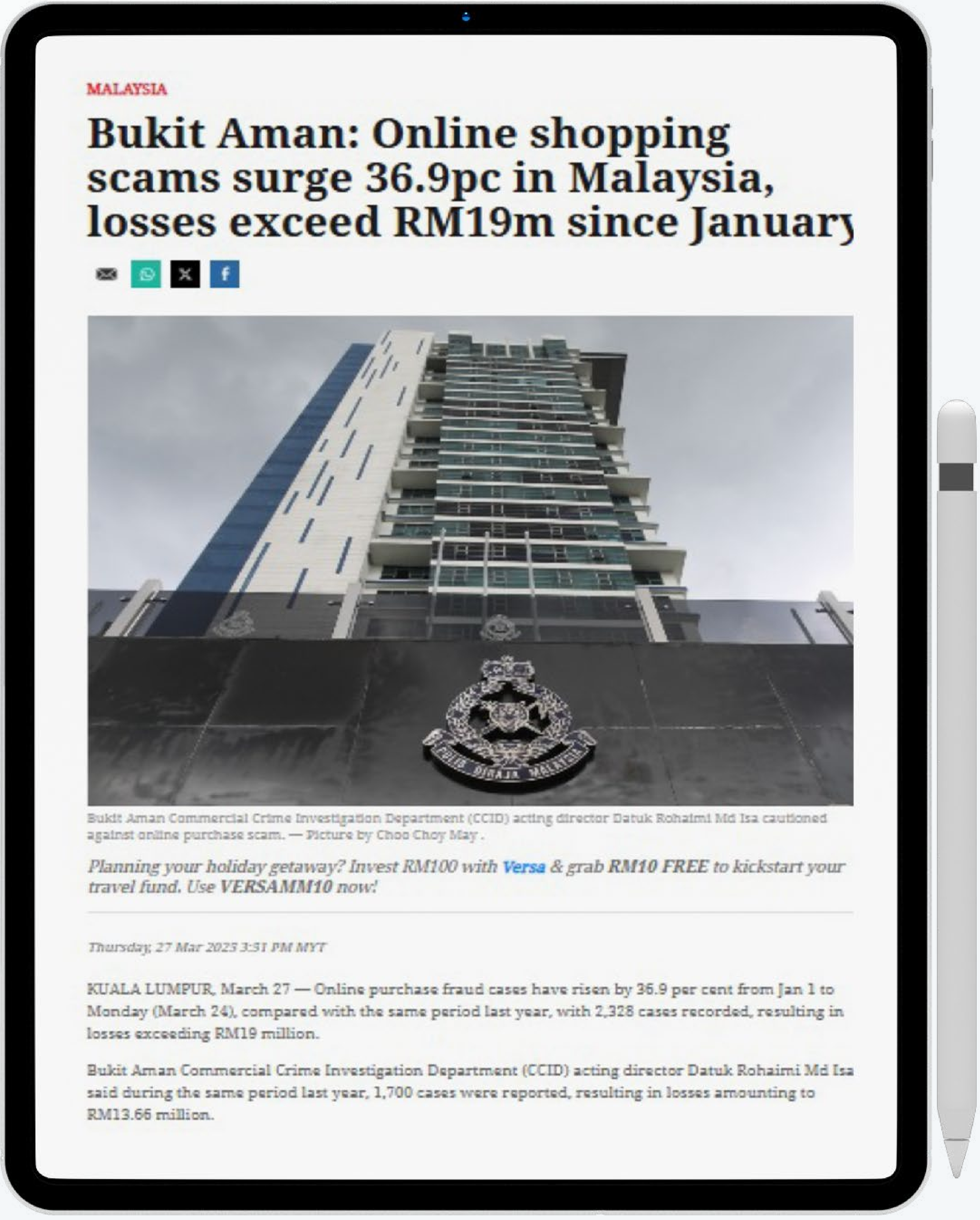
Related News
SINGAPORE 11h ago
Singapore Airlines cancels all flights to Dubai until Wednesday...
SINGAPORE 17h ago
Singapore could host Fifa youth competition, says Fifa chief Gianni...
SINGAPORE 19h ago
Extradition hearing for Indonesian businessman Tannos begins in...
12:59
Search
Carousell: Snap-Sell, Chat-Buy
Home Services, Cars, Property
OPEN
4.8
4+
Years Old
No.6
Shopping
What's New

The teen admitted to two charges of cheating on Feb 18, 2025. - Photo: ST

SINGAPORE: A teenage boy was only 15 years old when he scammed people on Carousell into paying him for iPhones that were never delivered.

The teen, who is now 19 but cannot be named as he was under 18 at the time of the offences, admitted to two charges of cheating on Tuesday (Feb 18).

He also pleaded guilty to one count of voluntarily causing hurt with common intention and one charge of having sex with a minor.



MALAYSIA

Bukit Aman: Online shopping scams surge 36.9pc in Malaysia, losses exceed RM19m since January

Bukit Aman Commercial Crime Investigation Department (CCID) acting director Datuk Rohaimi Md Isa cautioned against online purchase scam. — Picture by Choo Choy May .

*Planning your holiday getaway? Invest RM100 with Versa & grab **RM10 FREE** to kickstart your travel fund. Use **VERSAMM10** now!*

Thursday, 27 Mar 2025 3:51 PM MYT

KUALA LUMPUR, March 27 — Online purchase fraud cases have risen by 36.9 per cent from Jan 1 to Monday (March 24), compared with the same period last year, with 2,328 cases recorded, resulting in losses exceeding RM19 million.

Bukit Aman Commercial Crime Investigation Department (CCID) acting director Datuk Rohaimi Md Isa said during the same period last year, 1,700 cases were reported, resulting in losses amounting to RM13.66 million.

g) Key Takeaways

- Online shopping scams are increasing with the rise of e-commerce.
- Scammers trick buyers through fake websites, social media ads, messaging apps, emails, and online marketplaces.
- Common scam methods include fake listings, misleading ads, counterfeit goods, and non-delivery after payment.
- Watch for red flags like super low prices, no HTTPS, fake reviews, and urgent “limited-time” offers.
- Protect yourself by shopping on trusted sites, using secure payments, and never sharing personal details like PIN or OTP.
- Losses from online scams in Malaysia are rising—over RM573 million in Q1 2025—highlighting the need for awareness, especially among older adults.

6.1.2 Charity Scams

Many of us are kind and generous especially when it comes to helping others. Whether it is donating to a children's home, flood victims, or the poor, giving is a part of who we are. But sadly, not everyone is honest. Some people pretend to be from charities to steal your money or personal information. Older adults are often targeted because scammers think they are more trusting and unfamiliar with modern digital tools and technology. But with a little knowledge and some simple steps, we can protect ourselves and our loved ones. Remember it is good to give but even better to give safely.

a) What Are Charity Scams?

Charity scams involve imposters posing as legitimate charitable organizations or representatives to solicit donations. The scammers often fabricate stories or use emotional appeals to convince individuals to contribute money or personal information.

b) Scam Medium

Charity scams are often carried out through commonly used communication platforms, which can make them appear trustworthy and legitimate. By targeting familiar and informal communication methods, they make it harder to detect the scam. Knowing where these scams happen is the first step to protecting yourself.

These scams can occur through various channels including:

i. Phone Calls

Scammers may call pretending to be from a known charity and ask for immediate donations or personal details.

ii. Social Media Platforms

Fake charity pages or viral donation posts often appear on your feed, urging you to transfer money quickly.

iii. Emails

You may receive emails claiming to be from charities with emotional stories and links to fake donation sites.

iv. House-to-House

Individuals may show up at your door with donation boxes or fake documents asking for cash contributions.

v. In-Person Interactions

Scammers approach you in markets or public places, pretending to collect funds on behalf of an organization.

vi. Websites

Fraudulent websites that look like real charity pages may ask for donations through personal bank accounts or fake payment links.

c) Common Methods of Charity Scams

i. Fake or Impersonation of Legitimate Charities

Scammers use names and branding similar to well-known charities to appear credible. These impersonated names are designed to build trust quickly and confuse victims. A scammer uses the name "Red Crescent Emergency Relief" to mimic the Malaysian Red Crescent Society (MRCS) but has no official link.

ii. Emotional Appeals

Scammers share sad stories or dramatic images to trigger sympathy and push you to donate. These appeals often focus on children, the poor, or disaster victims. You receive a WhatsApp message with emotional photos of flood victims and an urgent request for donations.

iii. Urgent Requests / Pressure Tactics

Scammers try to create a sense of emergency, claiming that immediate donations are needed to save lives or respond to a disaster. Someone calls you saying a child will die without medical help unless you donate now.

iv. Unsolicited Contact

Scammers reach out without any prior communication, whether through phone calls, social media, emails, WhatsApp or even door-to-door visits. A man visits your house claiming he's from "Rumah Orang Tua ABCD" and asks for a cash donation but cannot show valid documents or proof.

v. False Promises

Scammers may offer incentives such as prizes, gifts, or tax exemptions in exchange for your donation. These are used to make the request more attractive. After donating, you're told you've won a free trip to Langkawi or are eligible for tax relief, but nothing arrives.

d) Warning Signs of Charity Scams

🚩 **Pressure to donate immediately**
You are told to act fast.

🚩 **Unsolicited contact**
You receive calls, WhatsApp messages, emails, or social media message out of nowhere asking for donations.

🚩 **Fake or unknown charity name**
The name sounds unfamiliar, suspicious, or very similar to a well-known charity.

🚩 **Emotional stories without proof**
Overly emotional photos or stories are used to make you feel guilty, but no official documents or details are given.

Asked to send money to a personal bank account
Real charities use official accounts, not names like "Abu Bin Ali" or "ABCDE Enterprise".

No receipts or acknowledgement given
You're not provided with a receipt or donation proof after giving money.

No website or official info
The group cannot be found online or lacks an official website, registration number, or contact details.

Claims of rewards or tax benefits
They promise prizes, gift cards, or tax exemptions if you donate.

Can't answer basic questions
When you ask about their registration, who they help, or how the money is used, they avoid the question.

Too good to be true
If something feels off or sounds unbelievable.

e) How to Protect Yourself from Charity Scams?

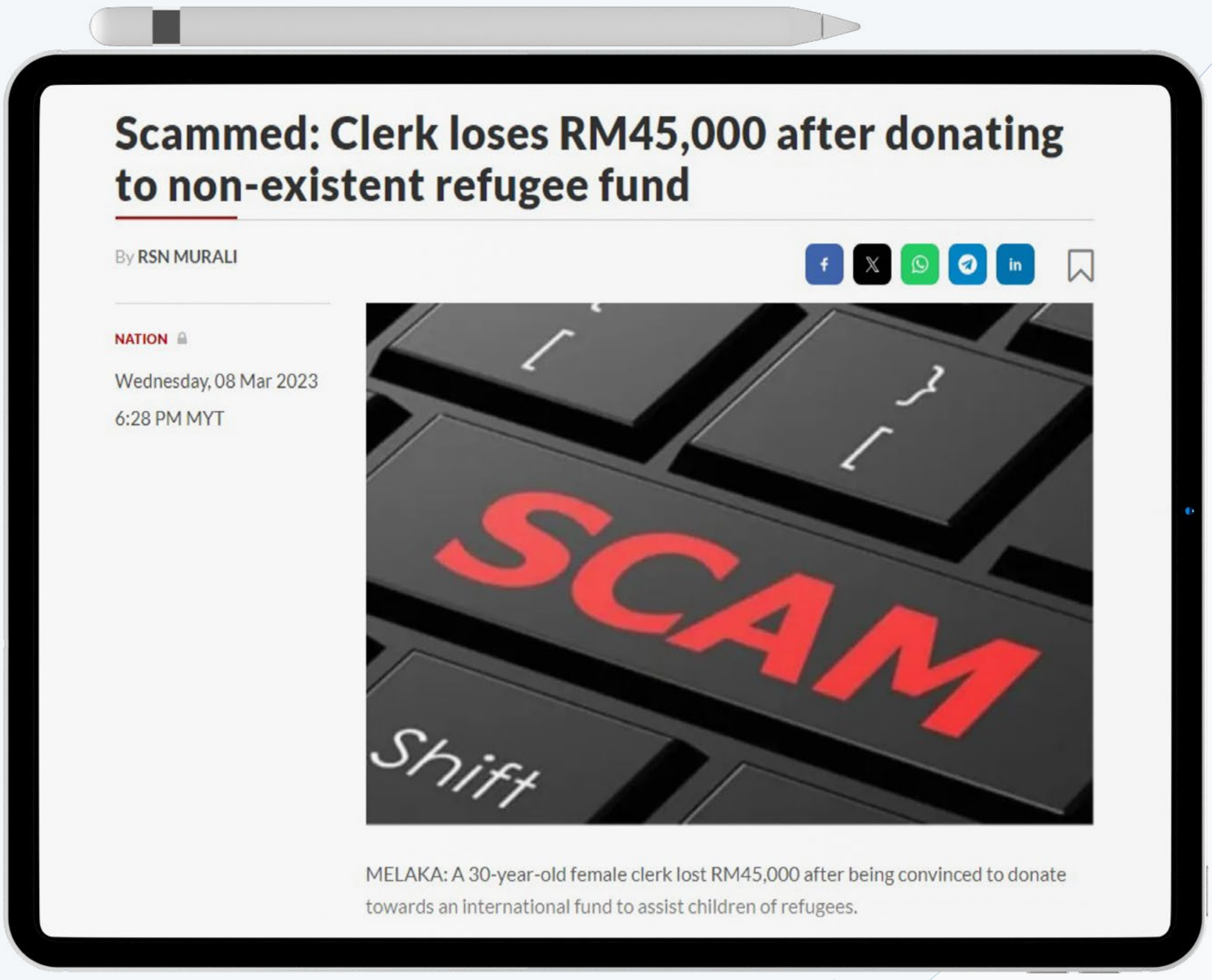
✓ Do This	✗ Avoid This
Verify. Check charity bank account details at: semakmule.rmp.gov.my	Don't give money to strangers.
Consult trusted individuals. Ask family/ friends first.	Don't feel rushed to donate.
Secure payment method. Use a bank or credit card (traceable payments)	Don't use cash or transfer to personal accounts
Install Caller ID and Spam Blocker	Don't share IC, bank details or passwords
Save emergency numbers	Don't trust people just because they look kind

f) Real-life Cases

Charity scams continue to exploit the generosity and compassion of individuals, especially during times of crisis or disaster. Scammers often pretend to represent legitimate charitable organizations, using emotional appeals and fake credentials to collect donations. These scams occur across various platforms, including social media, unsolicited visits, and face-to-face interactions, making them difficult to detect without proper vigilance.

Recent cases in Malaysia reveal how scammers approach victims through online channels as well as direct contact, often pressuring them to donate quickly or using fabricated stories to gain sympathy. These incidents highlight the importance of verifying the legitimacy of charitable requests and staying cautious when approached by unknown individuals or organizations.

Date	Scam Medium	Methods	Source
Apr 2023	Social Media	Unsolicited contact	The Star
May 2023	In-person interactions	Fake or impersonation of legitimate charities	Borneo Post
Oct 2023	In-person interactions	Fake or impersonation of legitimate charities	The Star



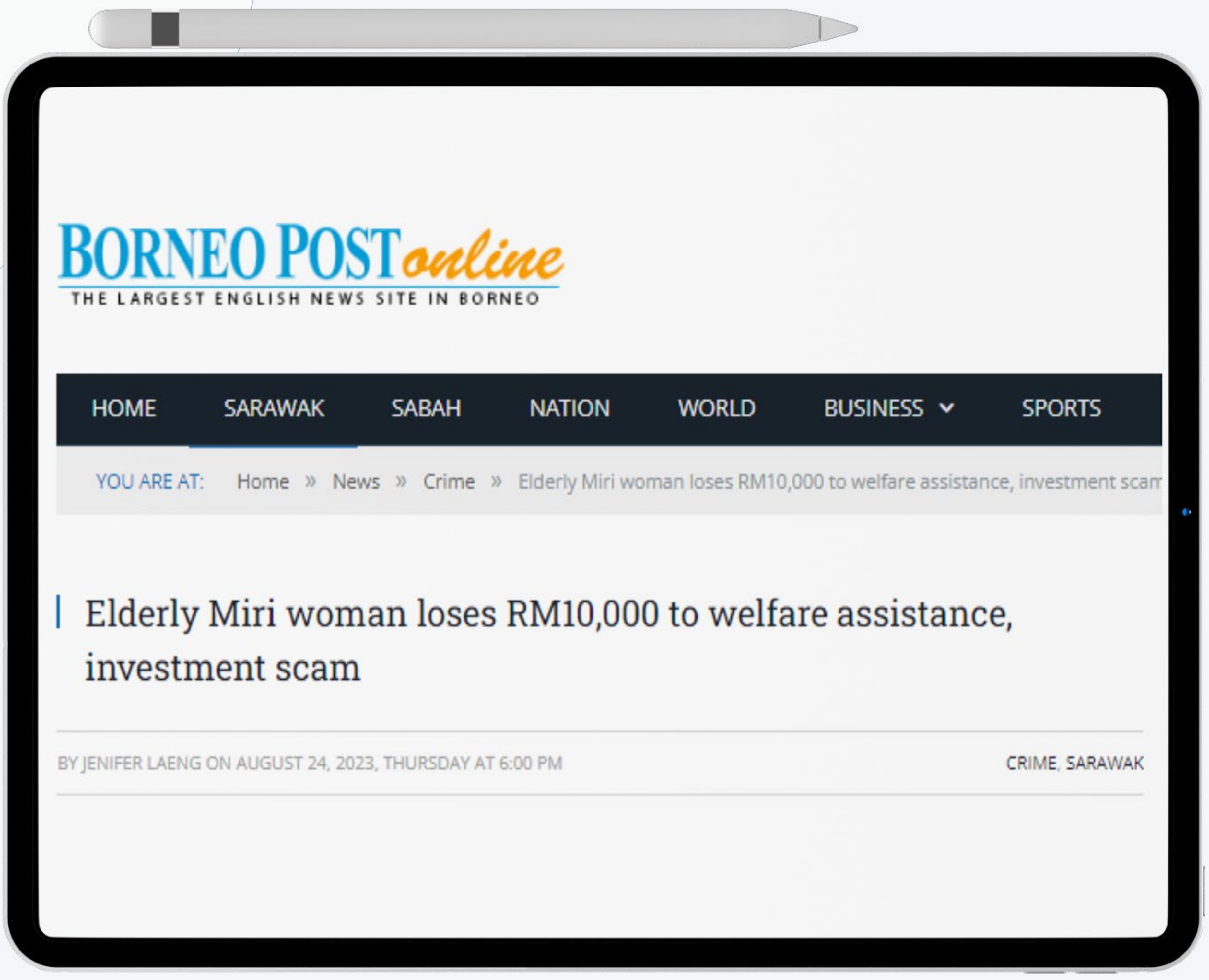
Scammed: Clerk loses RM45,000 after donating to non-existent refugee fund

By RSN MURALI

NATION

Wednesday, 08 Mar 2023
6:28 PM MYT

MELAKA: A 30-year-old female clerk lost RM45,000 after being convinced to donate towards an international fund to assist children of refugees.



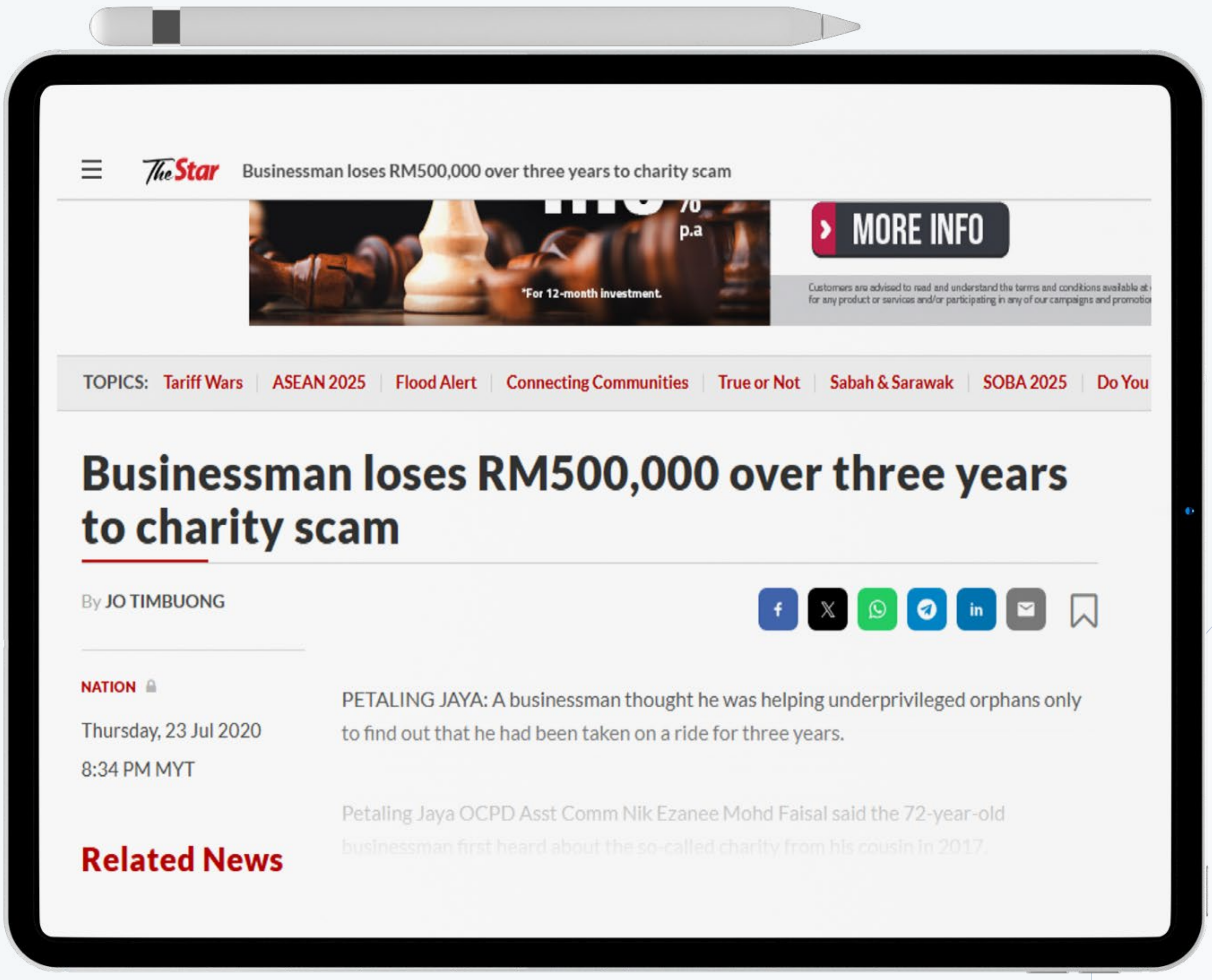
BORNEO POST online
THE LARGEST ENGLISH NEWS SITE IN BORNEO

YOU ARE AT: Home » News » Crime » Elderly Miri woman loses RM10,000 to welfare assistance, investment scam

Elderly Miri woman loses RM10,000 to welfare assistance, investment scam

BY JENIFER LAENG ON AUGUST 24, 2023, THURSDAY AT 6:00 PM

CRIME, SARAWAK



The Star Businessman loses RM500,000 over three years to charity scam

p.a
*For 12-month investment.
MORE INFO
Customers are advised to read and understand the terms and conditions available at
for any product or services and/or participating in any of our campaigns and promotio

TOPICS: Tariff Wars | ASEAN 2025 | Flood Alert | Connecting Communities | True or Not | Sabah & Sarawak | SOBA 2025 | Do You

Businessman loses RM500,000 over three years to charity scam

By JO TIMBUONG

NATION

Thursday, 23 Jul 2020

8:34 PM MYT

PETALING JAYA: A businessman thought he was helping underprivileged orphans only to find out that he had been taken on a ride for three years.

Petaling Jaya OCPD Asst Comm Nik Ezanee Mohd Faisal said the 72-year-old businessman first heard about the so-called charity from his cousin in 2017.

Related News

g) Key Takeaways

- Charity scams exploit compassion, especially during crises or disasters, by pretending to represent legitimate charitable causes or organizations.
- Scammers often use emotionally charged stories, fabricated appeals, and fake credentials to gain trust and rush victims into donating.
- These scams target older adults, assuming they are more trusting or less familiar with digital verification tools and scam tactics.
- Common scam methods include impersonating well-known charities, making unsolicited contact, pressuring for immediate donations, and offering false promises such as tax exemptions or rewards.
- Scams occur through various channels—phone calls, social media, emails, door-to-door visits, and fraudulent websites—making them hard to spot without vigilance.

- Warning signs include unfamiliar charity names, emotional pleas without evidence, lack of official documents, personal bank account requests, and no donation receipts or verification details.
- To protect yourself: verify the charity's registration and bank account (e.g., via semakmule.rmp.gov.my), use secure and traceable payment methods, consult trusted individuals before donating, and never give in to pressure or share personal financial information.
- Real cases in Malaysia show that charity scams remain active and evolving. Staying informed and cautious is the best defence against falling victim.

6.1.3 Communication Scams

Communication scams are one of the most common and rapidly evolving types of online scams. They rely on messages, calls, and digital interactions to trick individuals into revealing personal or financial information or into taking actions that benefit the scammer. Older persons are often targeted because they may be less familiar with digital warning signs and can be more trusting of official-looking messages or authoritative voices.

a) What Are Communication Scams?

A communication scam is a type of trick where someone contacts you through phone calls, SMS, WhatsApp, email, or Facebook to try to steal your personal information or money. Their goal is to gain your trust and trick you into sharing sensitive information or sending money.

Bank officers

Government officials

Delivery companies

Friends or family members

Strangers who appear friendly and kind

b) Scam Medium

Communication scams are fraudulent activities that occur through various digital and mobile communication channels. Scammers often use familiar and easily accessible platforms to reach their targets, making their tactics more convincing and harder to detect.

Emails	**Text messaging (SMS-Short Message Service)**	**Phone calls**	**Instant messaging apps/ Social media (e.g., WhatsApp, Facebook)**

Common mediums for communication scams include:

i. Email

Scammers send phishing emails that appear to be from legitimate sources—such as banks, service providers, or government agencies.

ii. Text Messaging (SMS)

Also known as "smishing," scam text messages are short and typically impersonate delivery services, banks, or government bodies

iii. Phone Calls

Voice scams (vishing) involve callers pretending to be officials, tech support, or family members in distress.

iv. Instant Messaging Apps (e.g., WhatsApp, Facebook Messenger)

These apps are increasingly used for scams due to their real-time, informal nature.

iv. Social Media Platforms

Scammers use platforms like Facebook or Instagram to create fake profiles, post counterfeit ads, or send private messages. They often:

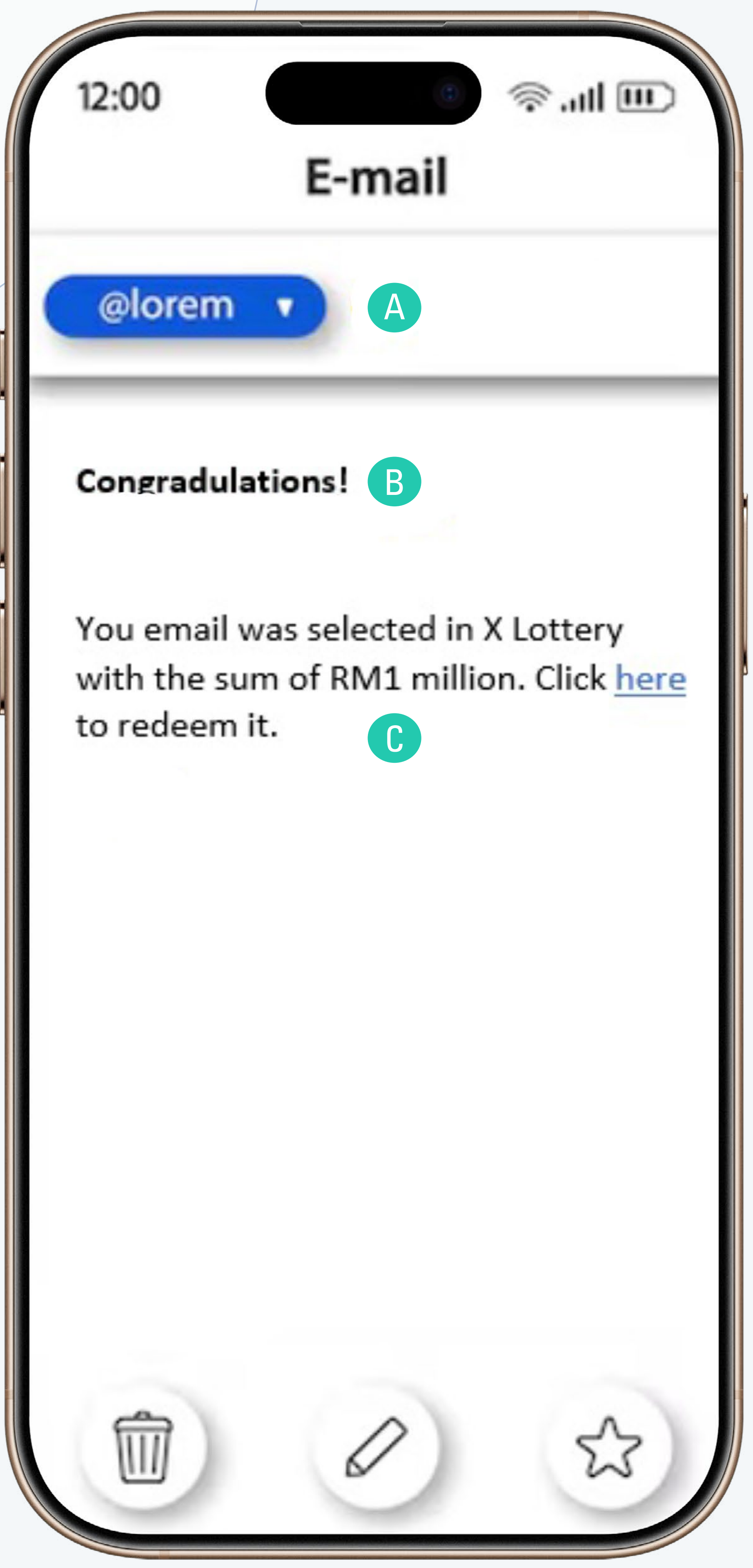
- Pretend to be sellers offering cheap or limited-time products,
- Share misleading investment opportunities,
- Impersonate friends or public figures to gain trust.

c) Common Methods of Communication Scams

i. Phishing Emails

Phishing emails are designed to look like official communications from well-known companies, such as banks, insurance firms, or government agencies. This phishing email attempts to scare you into clicking the link and then entering your email address, password and cell phone number into a phishing web form. Emails often include:

- A fake logo or name
- An urgent message ("Your account will be locked unless...")



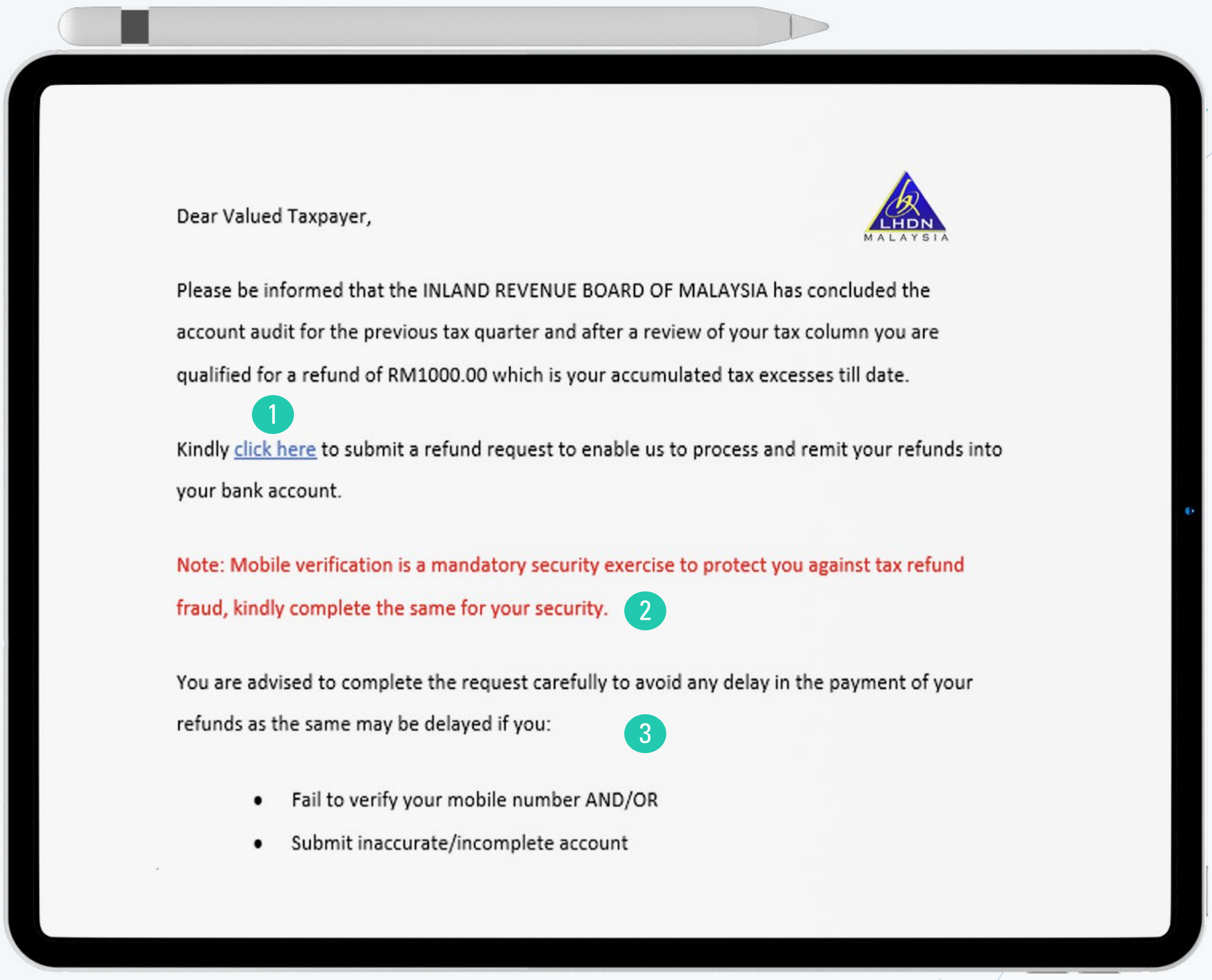
Congradulations!

You email was selected in X Lottery with the sum of RM1 million. Click here to redeem it.

A Fake logo or name

B Messages or posts with poor spelling and grammatical mistakes.

C Link takes the user to a phishing site



Dear Valued Taxpayer,

Please be informed that the INLAND REVENUE BOARD OF MALAYSIA has concluded the account audit for the previous tax quarter and after a review of your tax column you are qualified for a refund of RM1000.00 which is your accumulated tax excesses till date.

Kindly click here to submit a refund request to enable us to process and remit your refunds into your bank account.

Note: Mobile verification is a mandatory security exercise to protect you against tax refund fraud, kindly complete the same for your security.

You are advised to complete the request carefully to avoid any delay in the payment of your refunds as the same may be delayed if you:

- Fail to verify your mobile number AND/OR
- Submit inaccurate/incomplete account

1 Link takes the user to a phishing site

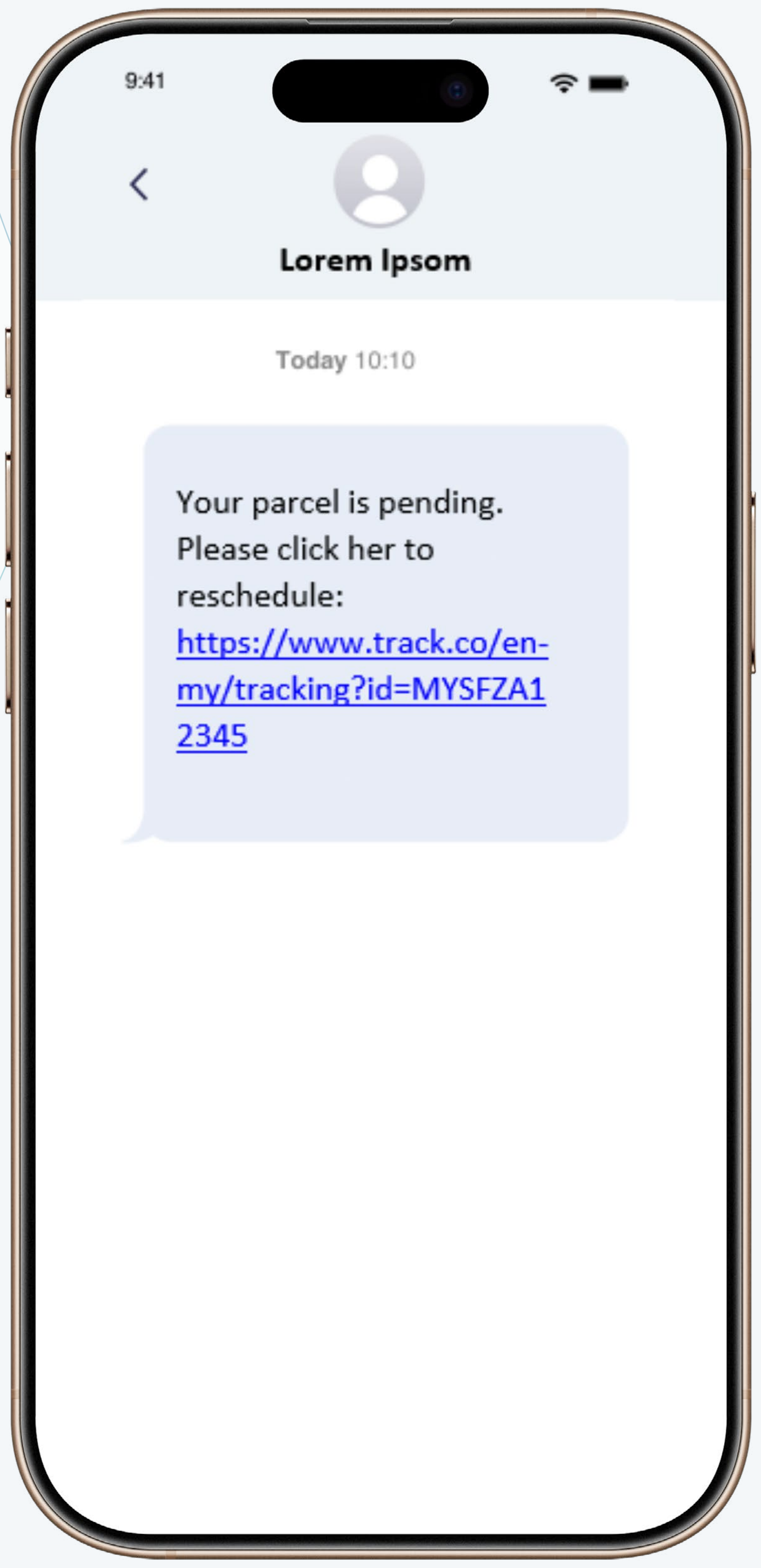
2 Account verification

3 Urgent and threatening

ii. Smishing (SMS Phishing)

SMS scams are text messages sent to your mobile phone that:

- Appear to come from service providers (e.g., courier, telecom, banks)
- May include a malicious link
- May ask you to call a number where a scammer impersonates a customer service agent



Your parcel is pending. Please click her to reschedule: https://www.track.co/en-my/tracking?id=MYSFZA12345

1. **Unexpected Message**
   - You weren't expecting a parcel but still received a delivery notice.
2. **Suspicious Link**
   - The URL looks odd or unfamiliar (e.g. track.co instead of an official courier site like poslaju.com.my or dhl.com).
3. **Sense of Urgency**
   - "Your parcel is pending. Please click here…" – this creates pressure to act quickly without thinking.
4. **Spelling/Grammar Errors**
   - "Click her" instead of "click here" — common in scam messages.
5. **No Details About the Courier**
   - Legit messages usually include the courier company's name and reference numbers that can be verified.

Tip:
Never click on unknown links. Always check with the courier company directly using their official website or app.

iii. Vishing (Voice Phishing)

Scammers call and pretend to be from:

- The police
- Your bank
- The tax department

They may threaten arrest, demand immediate payment, or request you "verify your identity."

Tip:
Never provide your personal or banking details over an unsolicited phone call.

iv. Instant Messaging Apps and Social Media Scams

Scammers use platforms like WhatsApp, Facebook Messenger, and even Facebook posts to deceive users. These scams often involve:

- Instant Messaging Apps (e.g., WhatsApp, Facebook Messenger)

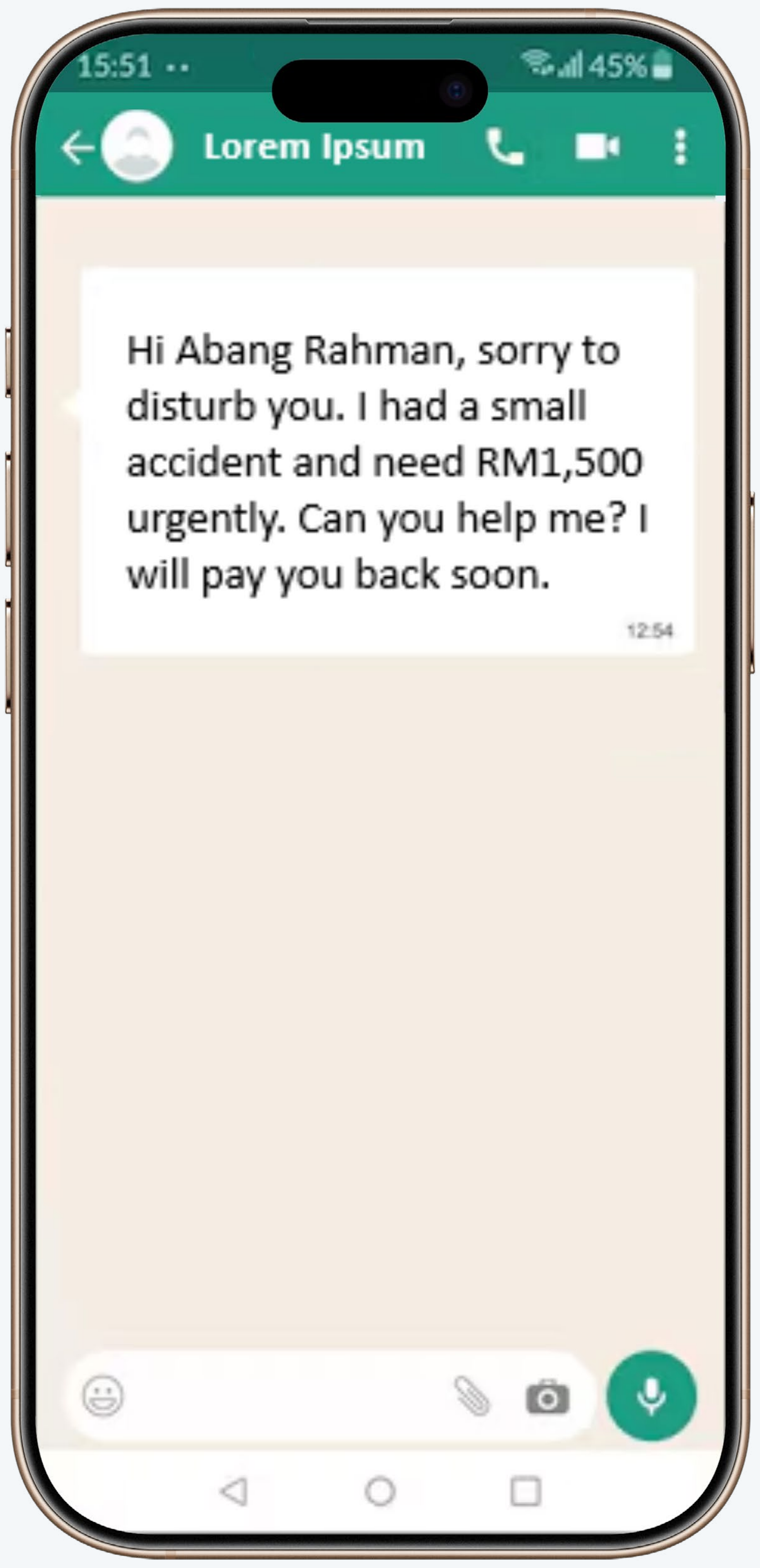
  Scammers may:

  ▶ Impersonate someone you know
  ▶ Use friendly or casual language to gain your trust
  ▶ Ask for money, mobile airtime top-up, or personal assistance

- Social Media (e.g., Facebook Posts)

  Scammers may:

  ▶ Share fake investment opportunities or donation requests
  ▶ Post links to malware or phishing websites
  ▶ Use fake profiles to gain likes, shares, or contact with victims

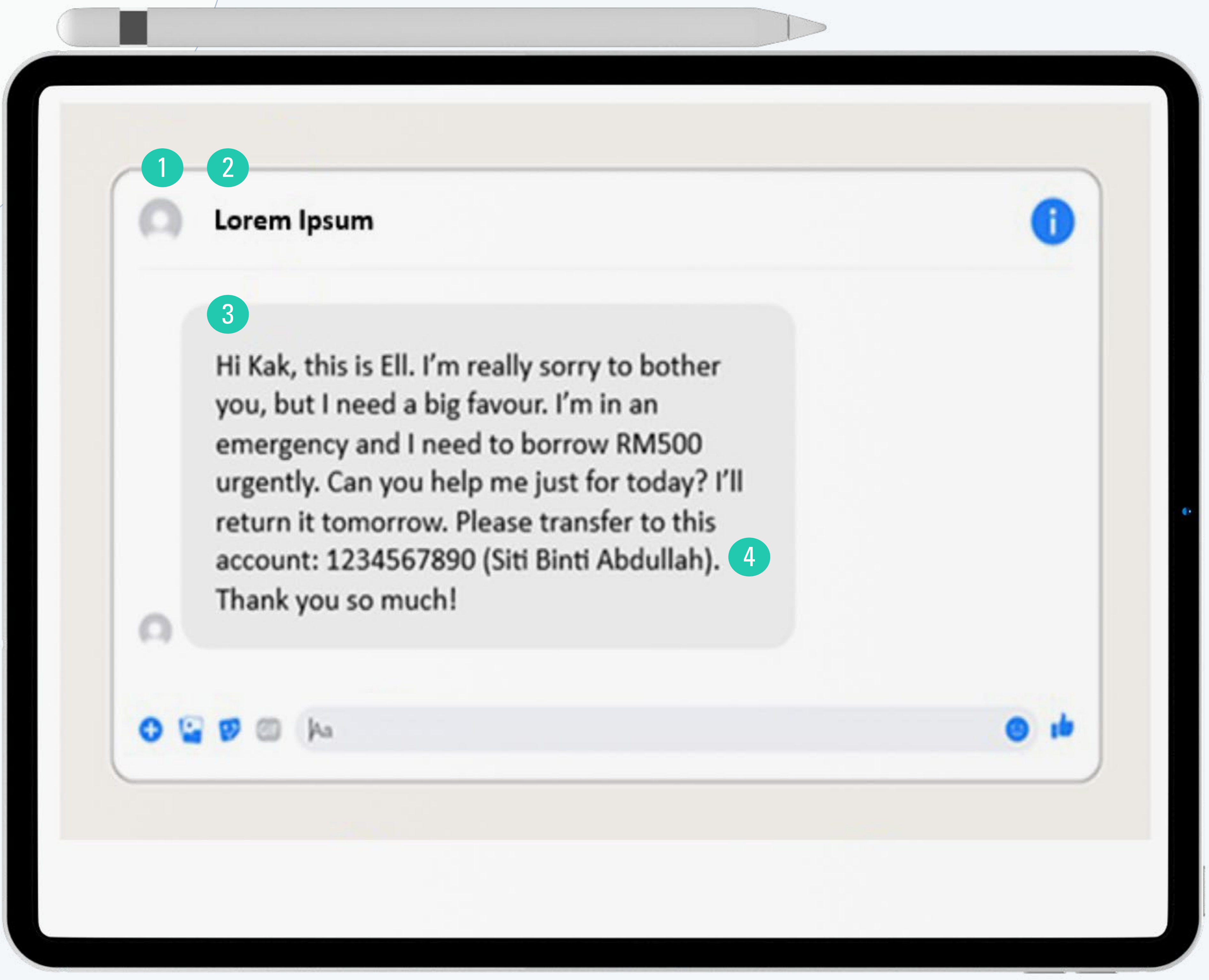


Hi Abang Rahman, sorry to disturb you. I had a small accident and need RM1,500 urgently. Can you help me? I will pay you back soon.

12:54

1. **Urgency and Pressure**
   - “Need RM1,500 urgently”
   - Scammers often create a sense of emergency to pressure you into acting quickly without thinking.
2. **Request for Money**
   - Asking for a specific amount (RM1,500) is a strong indicator of a scam, especially if it’s out of the blue.
3. **Unusual Situation**
   - An accident or emergency that hasn’t been confirmed through a phone call or other source.
4. **Vague Details**
   - The message lacks specific information (e.g. where the accident happened, who is involved, or what kind of treatment is needed).
5. **Only Text Communication**
   - No phone call or voice message to verify identity—scammers often avoid speaking directly.
6. **Profile Spoofing Possibility**
   - Even if the profile photo and name look familiar, scammers can fake these by using stolen images.

Tip:
Always verify before sending money — call the person directly to confirm the request.



Hi Kak, this is Ell. I'm really sorry to bother you, but I need a big favour. I'm in an emergency and I need to borrow RM500 urgently. Can you help me just for today? I'll return it tomorrow. Please transfer to this account: 1234567890 (Siti Binti Abdullah). Thank you so much!

1 Blurry images

2 Lack of profile information

3 Urging you to act fast

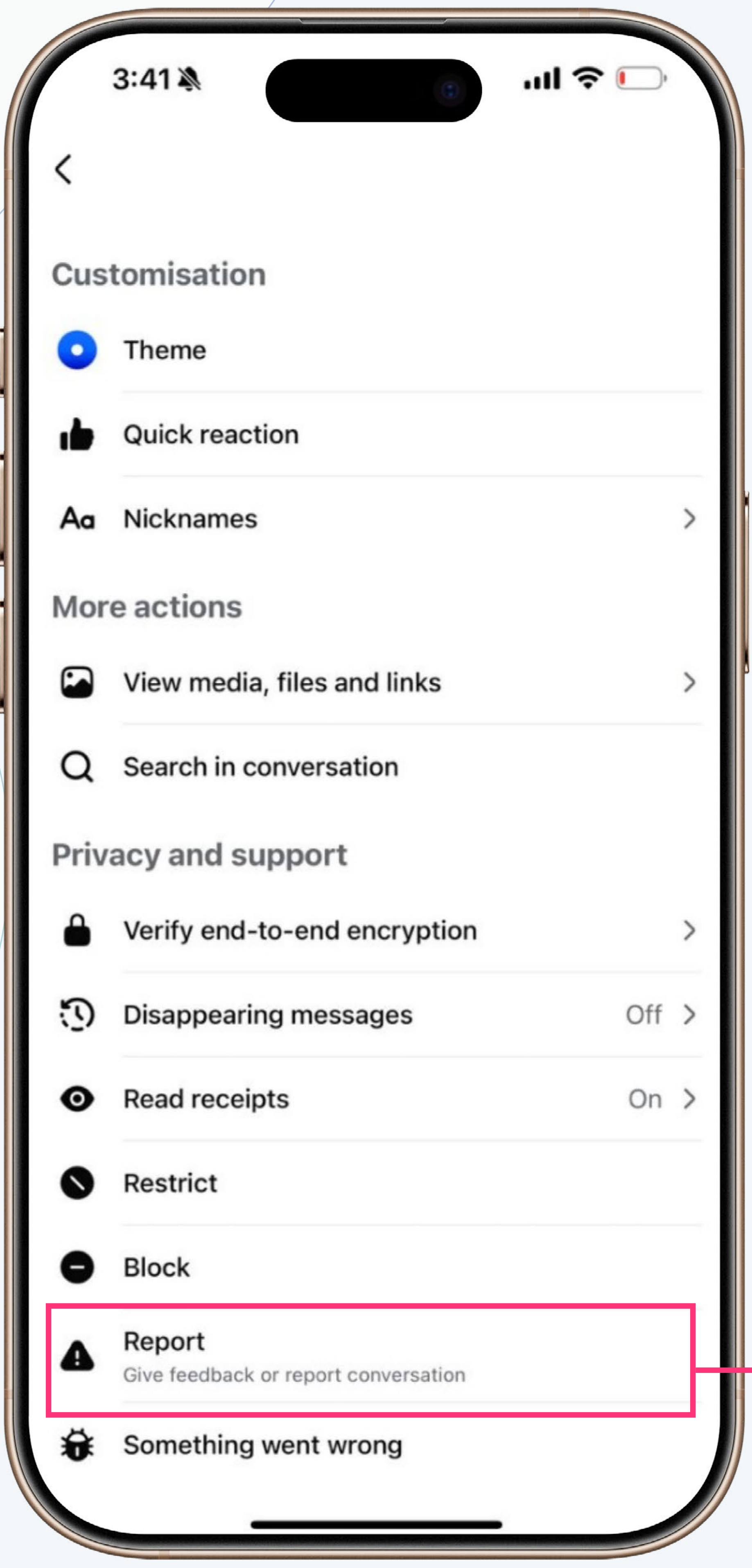
4 Using someone else's bank account

Tip:

- Do not transfer any money immediately.
- Call your friend directly using her phone number to confirm.
- Report the message as suspicious on the platform (WhatsApp/Facebook).
- Warn others in your contact list if you received the message from a shared group.

Even if a message seems to come from a trusted contact, **always verify first**, especially if it involves money or urgent help. Scammers often count on your emotional response to act quickly without thinking.

How to report through Facebook direct message



3:41

Customisation

Theme

Quick reaction

Nicknames

More actions

View media, files and links

Search in conversation

Privacy and support

Verify end-to-end encryption

Disappearing messages Off

Read receipts On

Restrict

Block

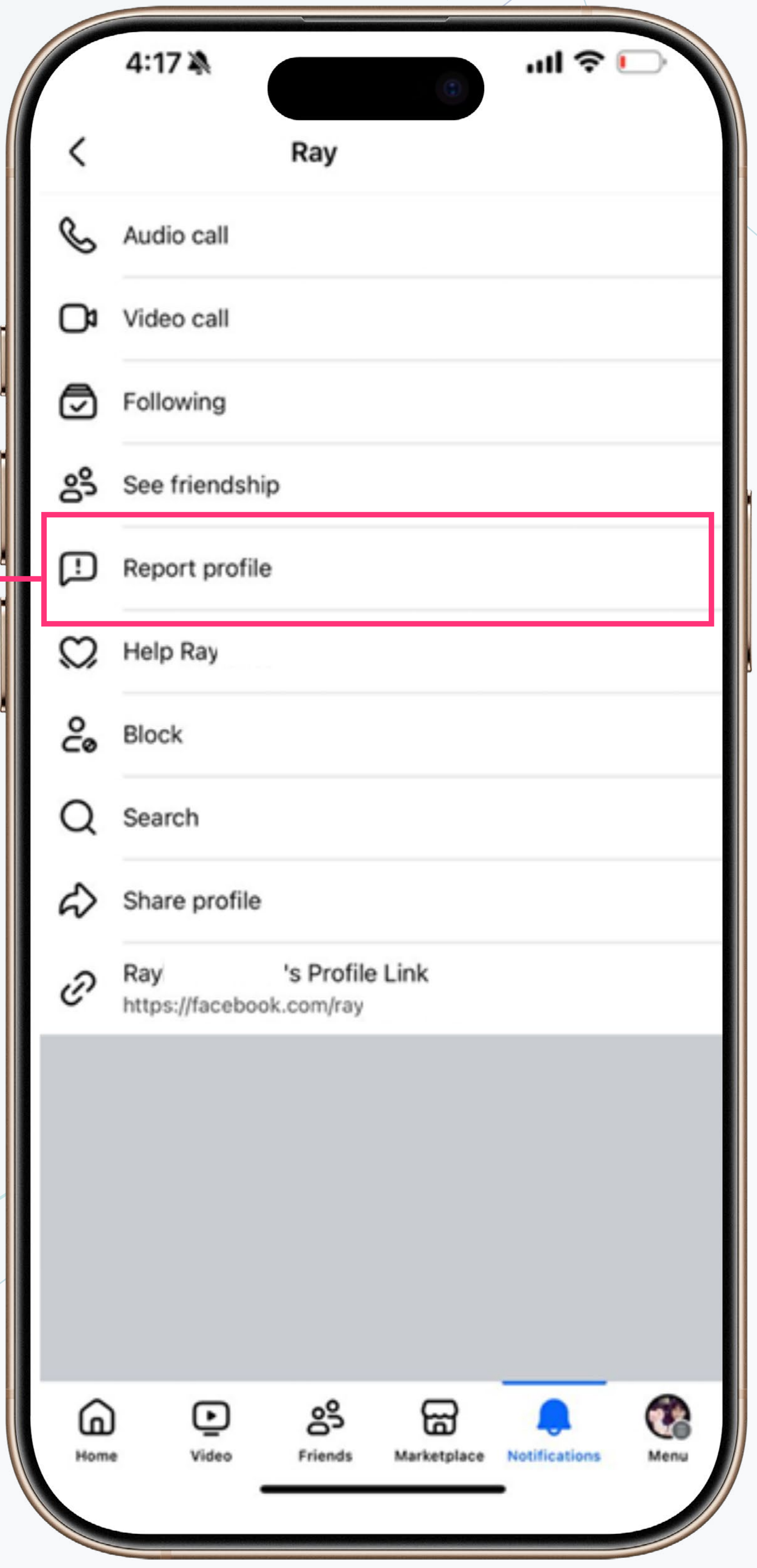
Report
Give feedback or report conversation

Something went wrong

1. Tap 🗨 or ➤ in the top right of their feed.
2. Tap the chat with the person you want to report.
3. Tap the person's name at the top of your chat.
4. Tap **Report**, then follow the on-screen instructions.

How to report through Facebook profile

1. Tap their username from their Feed or story post, or tap and search their username to go to their profile
2. Tap … (iPhone) or ⋮ (Android) above the post.
3. Tap **Report profile**, then follow the on-screen instructions,



4:17

Ray

Audio call

Video call

Following

See friendship

Report profile

Help Ray

Block

Search

Share profile

Ray 's Profile Link
https://facebook.com/ray

How to block and report someone on WhatsApp

1. **Open the Chat**
   - Tap on the chat with the person you want to block or report.
2. **Tap on Their Name or Number**
   - This opens their profile information.
3. **Scroll Down and Tap "Block"**
   - Confirm by selecting Block again.
   - This will stop them from calling or messaging you.
4. **Tap "Report Contact" (Optional but Recommended)**
   - You can choose to Report and Block at the same time.
   - This sends the last few messages to WhatsApp for review to help stop abuse.

> Blocking someone on **WhatsApp** does *not* delete your chat history — you can still **view old messages** unless you delete the chat manually.

d) Warning Signs of Communication Scams

Urgent or Threatening Language
Messages claiming your bank account will be locked or legal action will be taken unless you act immediately.

Unknown or Unverified Senders
Emails, text messages, or calls from unfamiliar numbers or addresses.

Requests for Personal or Financial Information
Scammers ask for sensitive details like your bank account, password, or identification number.

Spelling or Grammar Mistakes
Many scam messages contain awkward language, typos, or incorrect grammar.

Too-Good-to-Be-True Offers
Promises of lottery wins, free gifts, or high-return investments from unknown contacts.

Links to Unfamiliar Websites
Messages that include suspicious links or attachments—these may lead to fake login pages or install malware.

Impersonation of Friends or Family
Messages from known contacts asking for money urgently—always verify through a direct call before responding.

e) How to Protect Yourself from Communication Scams?

✓ Do This	✗ Avoid This
Verify sender directly using official contact details	Sending money based on text or chat messages alone
Be cautious with urgent or threatening messages	Rushing to respond under pressure or time limits
Check for grammar or spelling mistakes	Trusting messages with poor language or vague details
Use official apps or websites to confirm info	Clicking on unknown links or suspicious URLs
Report and block suspicious contacts	Ignoring your instincts when something feels “off”
Keep the apps updated with the latest security features	Sharing personal or banking info over messaging apps

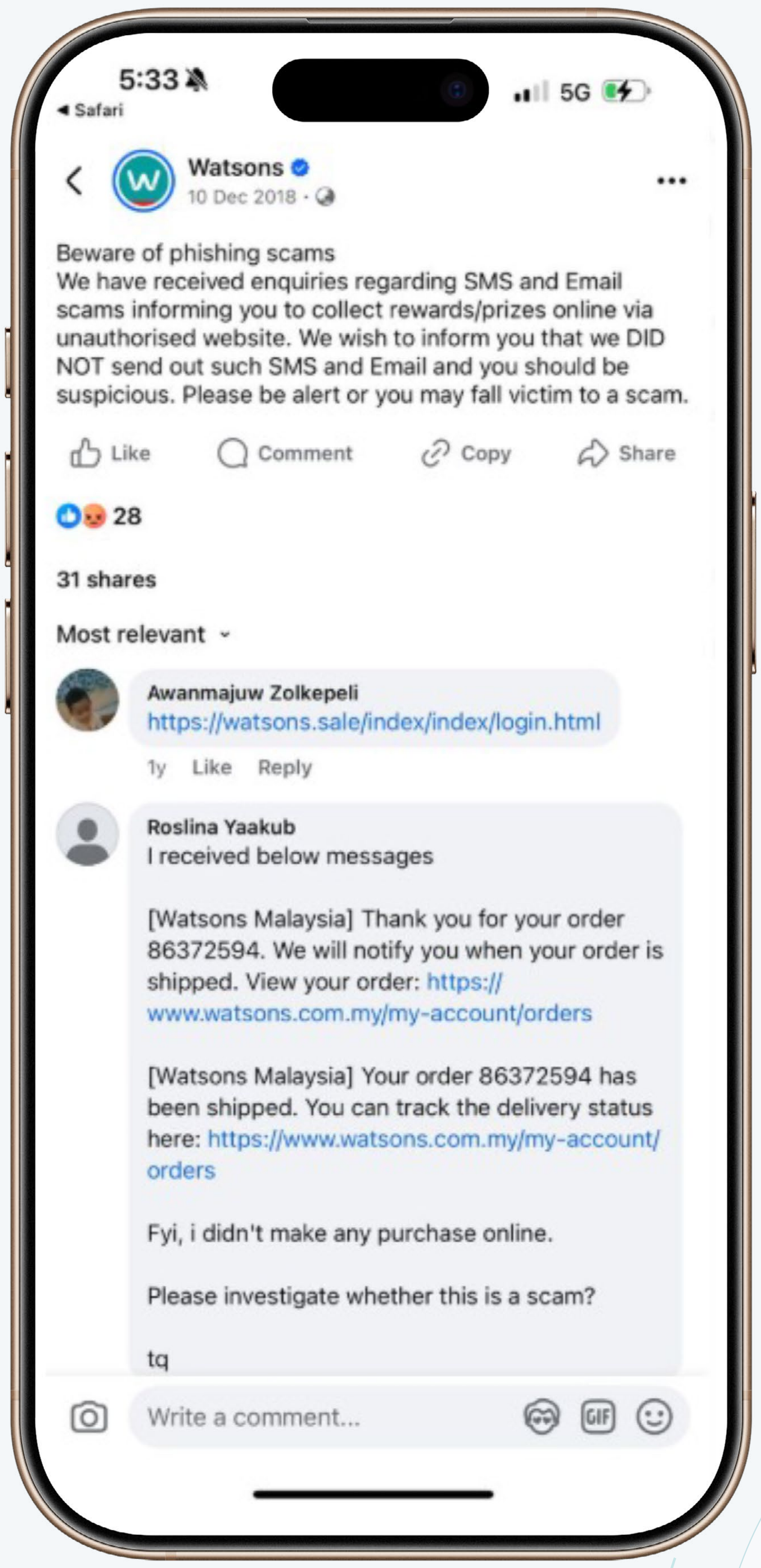
f) Real-life Cases

Communication scams in Malaysia have become one of the most frequently reported online threats, especially affecting individuals who may be less familiar with digital warning signs. These scams take advantage of common communication channels, such as SMS, email, WhatsApp, and social media—to reach victims quickly and directly. By impersonating trusted parties like government agencies, banks, delivery services, or even friends and family, scammers create a false sense of trust and urgency to manipulate victims into revealing personal information or transferring money.

Recent cases show that scammers use a variety of methods including phishing emails, smishing (SMS phishing), vishing (voice scams), and fraudulent messages on instant messaging platforms. In many instances, the messages appear official or emotionally persuasive, catching victims off guard. These scams not only result in financial losses but can also cause emotional distress and a lasting fear of using digital platforms.

Documented incidents in Malaysia clearly illustrate how widespread and convincing communication scams have become, and why it is essential for older persons and the wider public to stay informed, cautious, and proactive in verifying any suspicious messages or calls they receive.

Date	Scam Medium	Methods	Source
10 Dec 2018	SMS and email	Phishing email	Facebook
4 Mac 2025	Text messaging	Smishing (SMS Phishing)	Press statement – Jabatan Pengangkutan Jalan Malaysia
25 Jan 2024	Instant messaging apps	WhatsApp, Telegram	Utusan Malaysia
19 June 2023	Instant messaging apps	WhatsApp	Sinar Harian
13 April 2021	Instant messaging apps	WhatsApp	Sinar Harian
29 August 2019	Social media platform	Facebook posts	Facebook



Watsons
10 Dec 2018

Beware of phishing scams
We have received enquiries regarding SMS and Email scams informing you to collect rewards/prizes online via unauthorised website. We wish to inform you that we DID NOT send out such SMS and Email and you should be suspicious. Please be alert or you may fall victim to a scam.

Awanmajuw Zolkepeli
https://watsons.sale/index/index/login.html

Roslina Yaakub
I received below messages

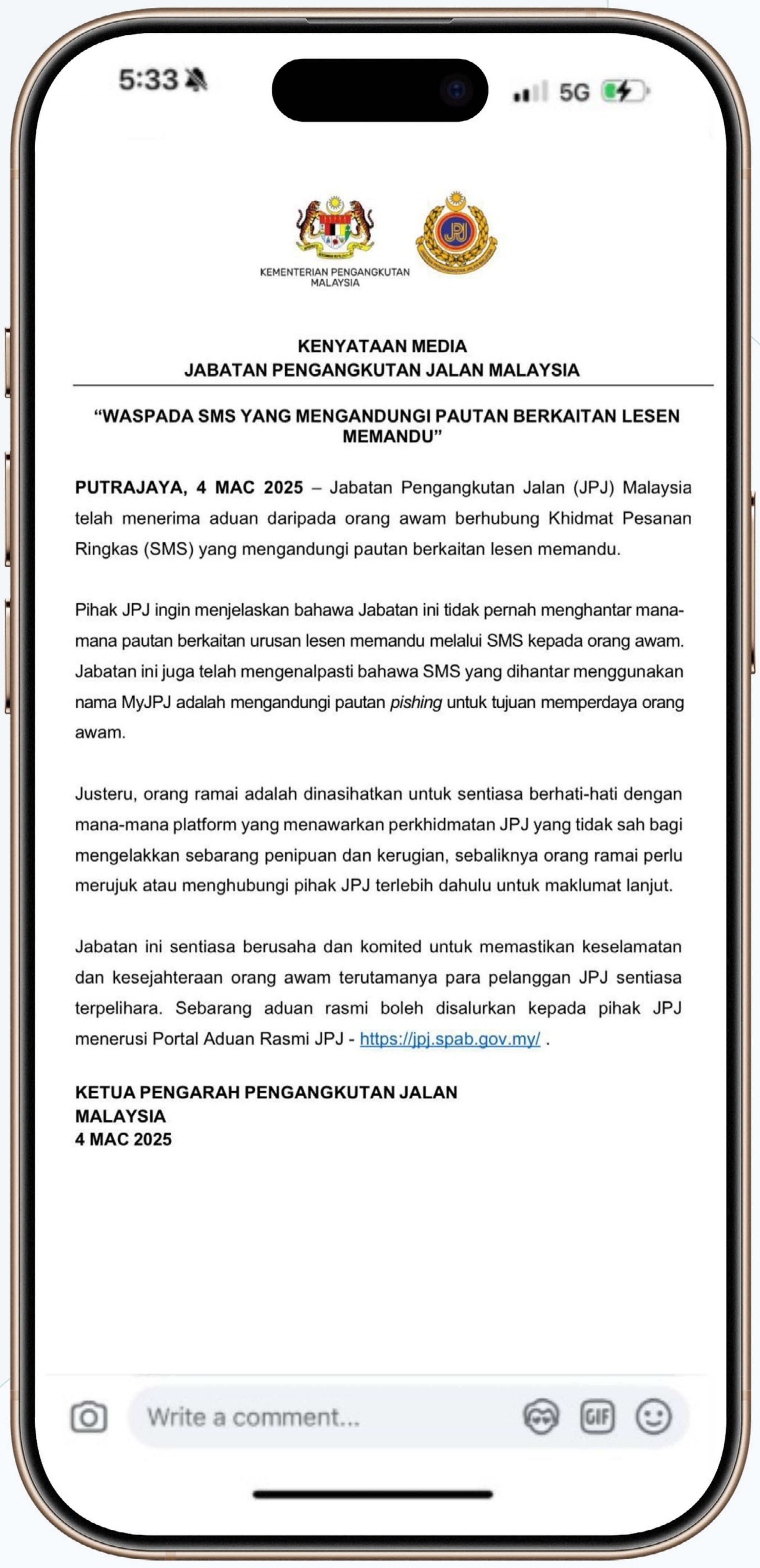
[Watsons Malaysia] Thank you for your order 86372594. We will notify you when your order is shipped. View your order: https://www.watsons.com.my/my-account/orders

[Watsons Malaysia] Your order 86372594 has been shipped. You can track the delivery status here: https://www.watsons.com.my/my-account/orders

Fyi, i didn't make any purchase online.

Please investigate whether this is a scam?

tq



KENYATAAN MEDIA
JABATAN PENGANGKUTAN JALAN MALAYSIA

“WASPADA SMS YANG MENGANDUNGI PAUTAN BERKAITAN LESEN MEMANDU”

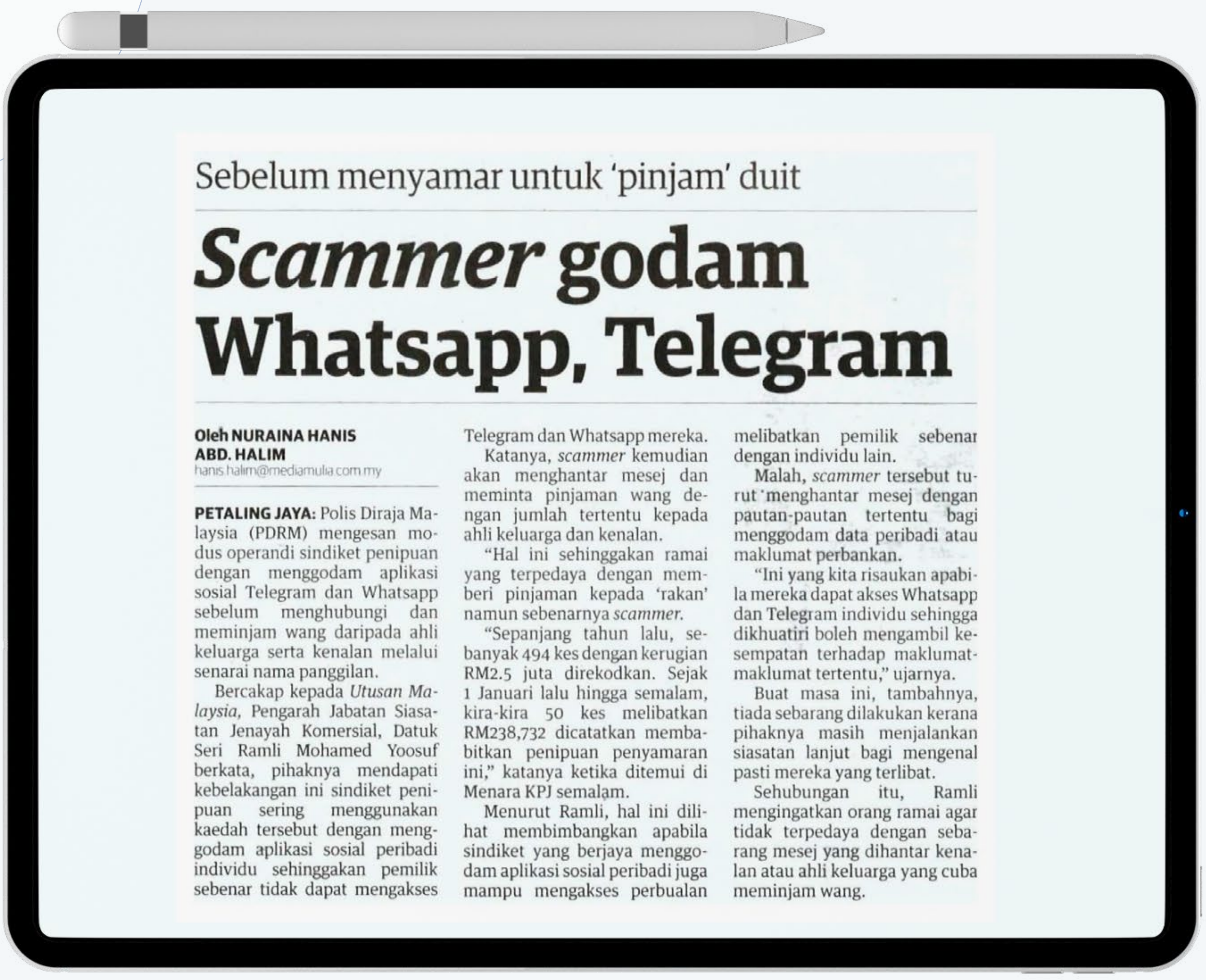
PUTRAJAYA, 4 MAC 2025 – Jabatan Pengangkutan Jalan (JPJ) Malaysia telah menerima aduan daripada orang awam berhubung Khidmat Pesanan Ringkas (SMS) yang mengandungi pautan berkaitan lesen memandu.

Pihak JPJ ingin menjelaskan bahawa Jabatan ini tidak pernah menghantar mana-mana pautan berkaitan urusan lesen memandu melalui SMS kepada orang awam. Jabatan ini juga telah mengenalpasti bahawa SMS yang dihantar menggunakan nama MyJPJ adalah mengandungi pautan *pishing* untuk tujuan memperdaya orang awam.

Justeru, orang ramai adalah dinasihatkan untuk sentiasa berhati-hati dengan mana-mana platform yang menawarkan perkhidmatan JPJ yang tidak sah bagi mengelakkan sebarang penipuan dan kerugian, sebaliknya orang ramai perlu merujuk atau menghubungi pihak JPJ terlebih dahulu untuk maklumat lanjut.

Jabatan ini sentiasa berusaha dan komited untuk memastikan keselamatan dan kesejahteraan orang awam terutamanya para pelanggan JPJ sentiasa terpelihara. Sebarang aduan rasmi boleh disalurkan kepada pihak JPJ menerusi Portal Aduan Rasmi JPJ - https://jpj.spab.gov.my/ .

KETUA PENGARAH PENGANGKUTAN JALAN
MALAYSIA
4 MAC 2025



Sebelum menyamar untuk 'pinjam' duit

Scammer godam Whatsapp, Telegram

Oleh NURAINA HANIS ABD. HALIM
hanis.halim@mediamulia.com.my

PETALING JAYA: Polis Diraja Malaysia (PDRM) mengesan modus operandi sindiket penipuan dengan menggodam aplikasi sosial Telegram dan Whatsapp sebelum menghubungi dan meminjam wang daripada ahli keluarga serta kenalan melalui senarai nama panggilan.

Bercakap kepada *Utusan Malaysia*, Pengarah Jabatan Siasatan Jenayah Komersial, Datuk Seri Ramli Mohamed Yoosuf berkata, pihaknya mendapati kebelakangan ini sindiket penipuan sering menggunakan kaedah tersebut dengan menggodam aplikasi sosial peribadi individu sehinggakan pemilik sebenar tidak dapat mengakses Telegram dan Whatsapp mereka.

Katanya, *scammer* kemudian akan menghantar mesej dan meminta pinjaman wang dengan jumlah tertentu kepada ahli keluarga dan kenalan.

"Hal ini sehinggakan ramai yang terpedaya dengan memberi pinjaman kepada 'rakan' namun sebenarnya *scammer*.

"Sepanjang tahun lalu, sebanyak 494 kes dengan kerugian RM2.5 juta direkodkan. Sejak 1 Januari lalu hingga semalam, kira-kira 50 kes melibatkan RM238,732 dicatatkan membabitkan penipuan penyamaran ini," katanya ketika ditemui di Menara KPJ semalam.

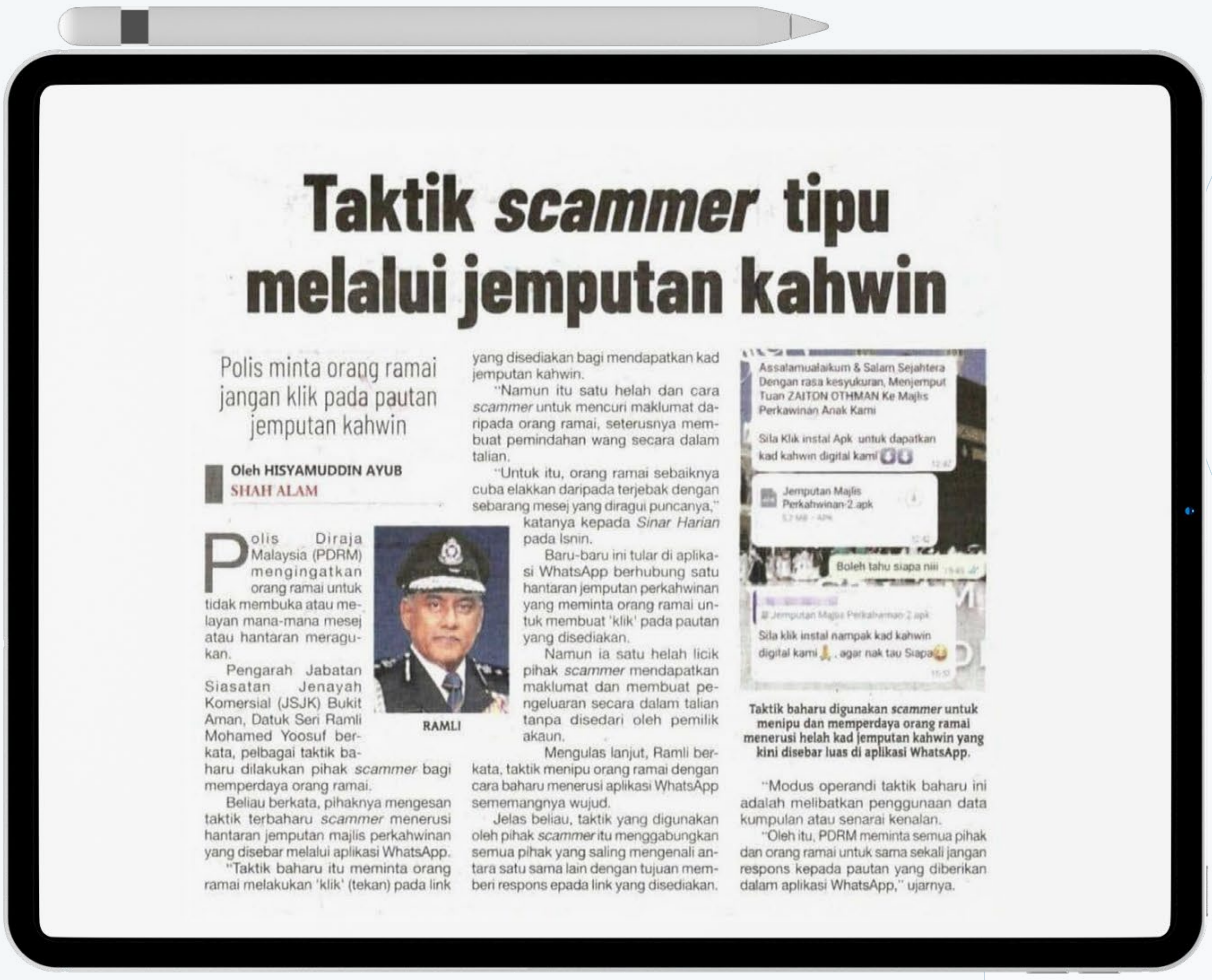
Menurut Ramli, hal ini dilihat membimbangkan apabila sindiket yang berjaya menggodam aplikasi sosial peribadi juga mampu mengakses perbualan melibatkan pemilik sebenar dengan individu lain.

Malah, *scammer* tersebut turut menghantar mesej dengan pautan-pautan tertentu bagi menggodam data peribadi atau maklumat perbankan.

"Ini yang kita risaukan apabila mereka dapat akses Whatsapp dan Telegram individu sehingga dikhuatiri boleh mengambil kesempatan terhadap maklumat-maklumat tertentu," ujarnya.

Buat masa ini, tambahnya, tiada sebarang dilakukan kerana pihaknya masih menjalankan siasatan lanjut bagi mengenal pasti mereka yang terlibat.

Sehubungan itu, Ramli mengingatkan orang ramai agar tidak terpedaya dengan sebarang mesej yang dihantar kenalan atau ahli keluarga yang cuba meminjam wang.



Taktik *scammer* tipu melalui jemputan kahwin

Polis minta orang ramai jangan klik pada pautan jemputan kahwin

Oleh HISYAMUDDIN AYUB
SHAH ALAM

Polis Diraja Malaysia (PDRM) mengingatkan orang ramai untuk tidak membuka atau melayan mana-mana mesej atau hantaran meragukan.

Pengarah Jabatan Siasatan Jenayah Komersial (JSJK) Bukit Aman, Datuk Seri Ramli Mohamed Yoosuf berkata, pelbagai taktik baharu dilakukan pihak *scammer* bagi memperdaya orang ramai.

RAMLI

Beliau berkata, pihaknya mengesan taktik terbaharu *scammer* menerusi hantaran jemputan majlis perkahwinan yang disebar melalui aplikasi WhatsApp.

"Taktik baharu itu meminta orang ramai melakukan 'klik' (tekan) pada link yang disediakan bagi mendapatkan kad jemputan kahwin.

"Namun itu satu helah dan cara *scammer* untuk mencuri maklumat daripada orang ramai, seterusnya membuat pemindahan wang secara dalam talian.

"Untuk itu, orang ramai sebaiknya cuba elakkan daripada terjebak dengan sebarang mesej yang diragui puncanya," katanya kepada *Sinar Harian* pada Isnin.

Baru-baru ini tular di aplikasi WhatsApp berhubung satu hantaran jemputan perkahwinan yang meminta orang ramai untuk membuat 'klik' pada pautan yang disediakan.

Namun ia satu helah licik pihak *scammer* mendapatkan maklumat dan membuat pengeluaran secara dalam talian tanpa disedari oleh pemilik akaun.

Mengulas lanjut, Ramli berkata, taktik menipu orang ramai dengan cara baharu menerusi aplikasi WhatsApp sememangnya wujud.

Jelas beliau, taktik yang digunakan oleh pihak *scammer* itu menggabungkan semua pihak yang saling mengenali antara satu sama lain dengan tujuan memberi respons epada link yang disediakan.

Assalamualaikum & Salam Sejahtera
Dengan rasa kesyukuran, Menjemput Tuan ZAITON OTHMAN Ke Majlis Perkawinan Anak Kami

Sila Klik instal Apk untuk dapatkan kad kahwin digital kami ⬇️⬇️

Jemputan Majlis Perkahwinan-2.apk

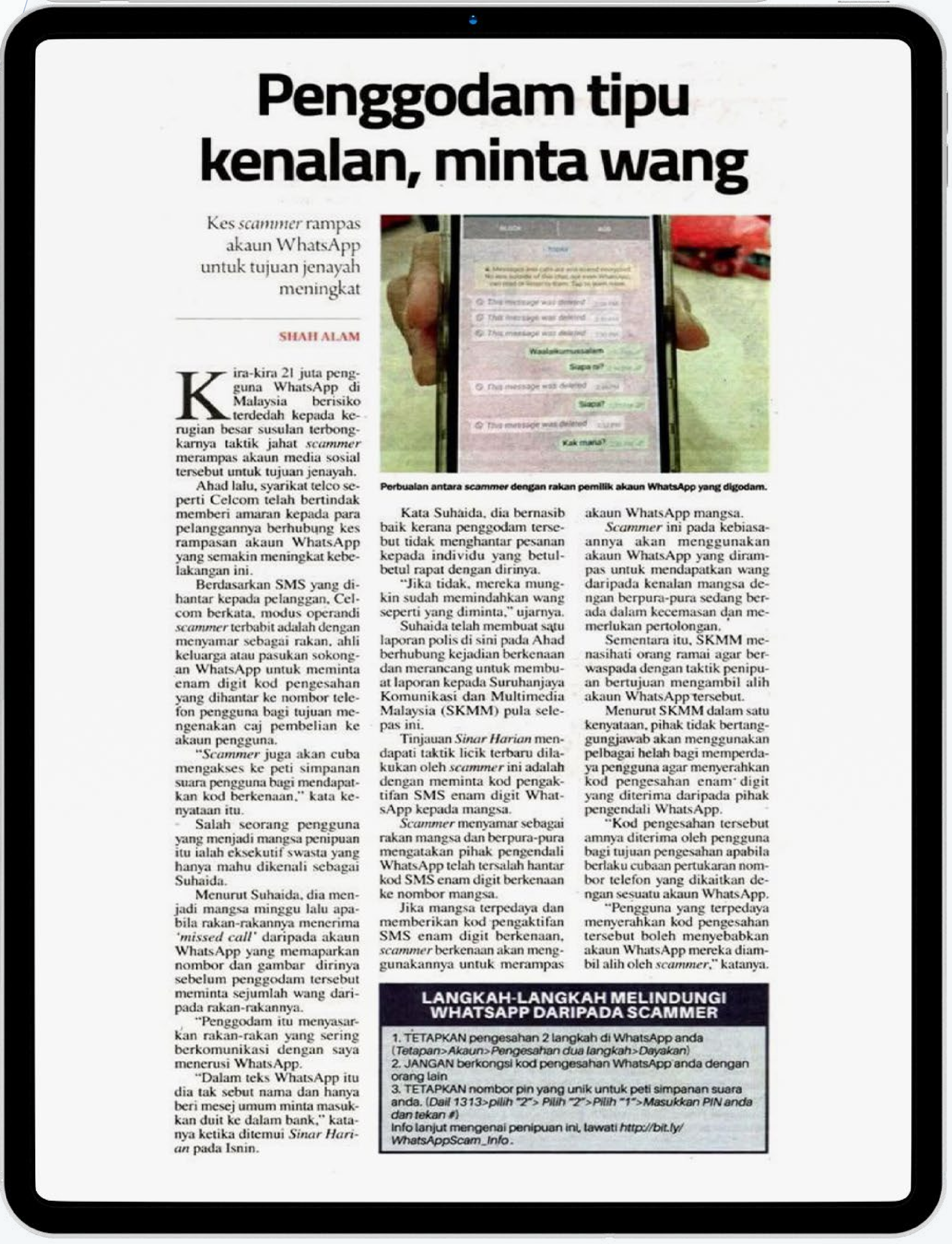
Boleh tahu siapa niii

Jemputan Majlis Perkahwinan-2.apk
Sila klik instal nampak kad kahwin digital kami 🙏 . agar nak tau Siapa😂

Taktik baharu digunakan *scammer* untuk menipu dan memperdaya orang ramai menerusi helah kad jemputan kahwin yang kini disebar luas di aplikasi WhatsApp.

"Modus operandi taktik baharu ini adalah melibatkan penggunaan data kumpulan atau senarai kenalan.

"Oleh itu, PDRM meminta semua pihak dan orang ramai untuk sama sekali jangan respons kepada pautan yang diberikan dalam aplikasi WhatsApp," ujarnya.



Penggodam tipu kenalan, minta wang

Kes *scammer* rampas akaun WhatsApp untuk tujuan jenayah meningkat

SHAH ALAM

Kira-kira 21 juta pengguna WhatsApp di Malaysia berisiko terdedah kepada kerugian besar susulan terbongkarnya taktik jahat *scammer* merampas akaun media sosial tersebut untuk tujuan jenayah.

Ahad lalu, syarikat telco seperti Celcom telah bertindak memberi amaran kepada para pelanggannya berhubung kes rampasan akaun WhatsApp yang semakin meningkat kebelakangan ini.

Berdasarkan SMS yang dihantar kepada pelanggan, Celcom berkata, modus operandi *scammer* terbabit adalah dengan menyamar sebagai rakan, ahli keluarga atau pasukan sokongan WhatsApp untuk meminta enam digit kod pengesahan yang dihantar ke nombor telefon pengguna bagi tujuan mengenakan caj pembelian ke akaun pengguna.

"*Scammer* juga akan cuba mengakses ke peti simpanan suara pengguna bagi mendapatkan kod berkenaan," kata kenyataan itu.

Salah seorang pengguna yang menjadi mangsa penipuan itu ialah eksekutif swasta yang hanya mahu dikenali sebagai Suhaida.

Menurut Suhaida, dia menjadi mangsa minggu lalu apabila rakan-rakannya menerima *'missed call'* daripada akaun WhatsApp yang memaparkan nombor dan gambar dirinya sebelum penggodam tersebut meminta sejumlah wang daripada rakan-rakannya.

"Penggodam itu menyasarkan rakan-rakan yang sering berkomunikasi dengan saya menerusi WhatsApp.

"Dalam teks WhatsApp itu dia tak sebut nama dan hanya beri mesej umum minta masukkan duit ke dalam bank," katanya ketika ditemui *Sinar Harian* pada Isnin.

This message was deleted
This message was deleted
This message was deleted
Waalaikumussalam
Siapa ni?
This message was deleted
Siapa?
This message was deleted
Kak mana?

Perbualan antara scammer dengan rakan pemilik akaun WhatsApp yang digodam.

Kata Suhaida, dia bernasib baik kerana penggodam tersebut tidak menghantar pesanan kepada individu yang betul-betul rapat dengan dirinya.

"Jika tidak, mereka mungkin sudah memindahkan wang seperti yang diminta," ujarnya.

Suhaida telah membuat satu laporan polis di sini pada Ahad berhubung kejadian berkenaan dan merancang untuk membuat laporan kepada Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) pula selepas ini.

Tinjauan *Sinar Harian* mendapati taktik licik terbaru dilakukan oleh *scammer* ini adalah dengan meminta kod pengaktifan SMS enam digit WhatsApp kepada mangsa.

Scammer menyamar sebagai rakan mangsa dan berpura-pura mengatakan pihak pengendali WhatsApp telah tersalah hantar kod SMS enam digit berkenaan ke nombor mangsa.

Jika mangsa terpedaya dan memberikan kod pengaktifan SMS enam digit berkenaan, *scammer* berkenaan akan menggunakannya untuk merampas akaun WhatsApp mangsa.

Scammer ini pada kebiasaannya akan menggunakan akaun WhatsApp yang dirampas untuk mendapatkan wang daripada kenalan mangsa dengan berpura-pura sedang berada dalam kecemasan dan memerlukan pertolongan.

Sementara itu, SKMM menasihati orang ramai agar berwaspada dengan taktik penipuan bertujuan mengambil alih akaun WhatsApp tersebut.

Menurut SKMM dalam satu kenyataan, pihak tidak bertanggungjawab akan menggunakan pelbagai helah bagi memperdaya pengguna agar menyerahkan kod pengesahan enam digit yang diterima daripada pihak pengendali WhatsApp.

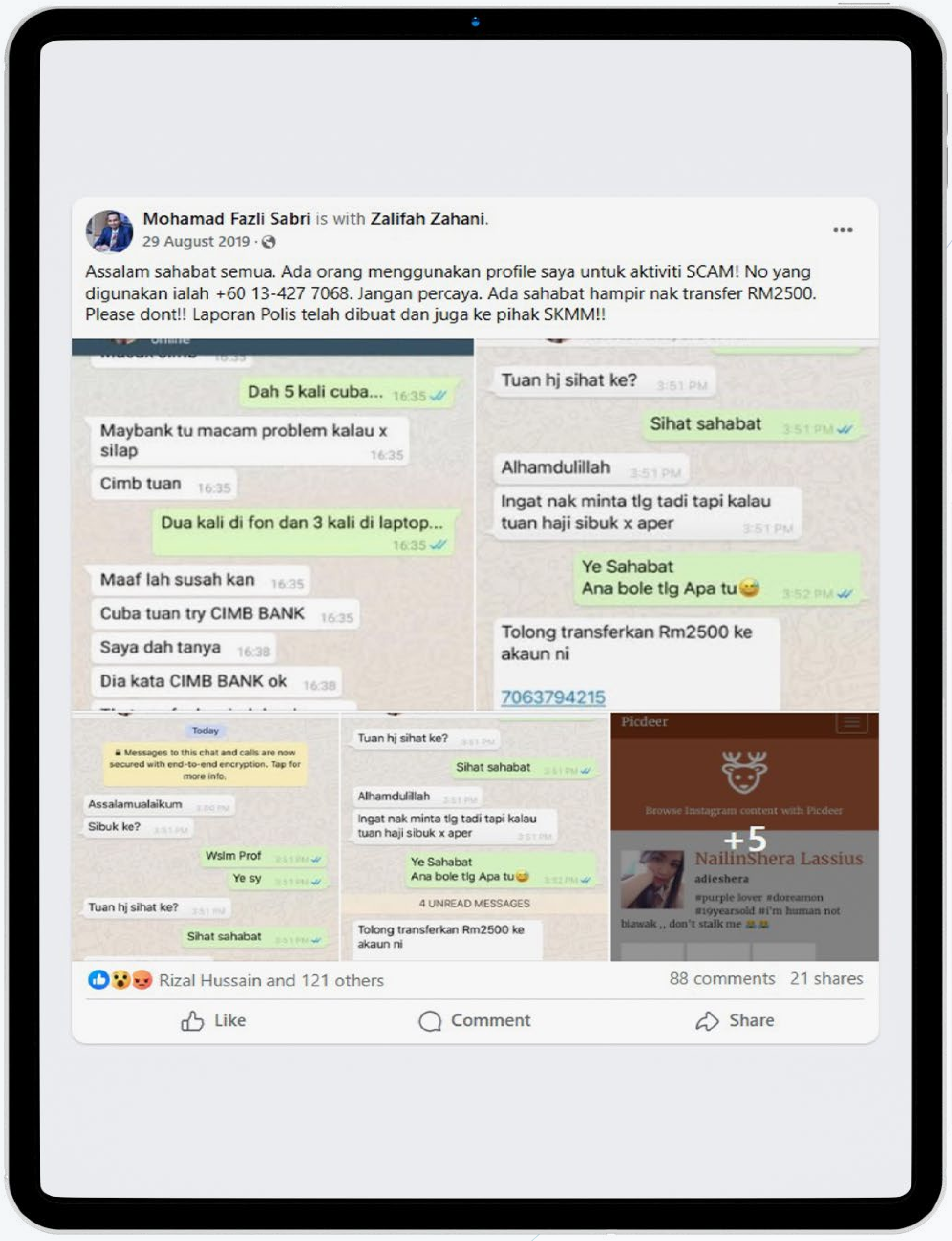
"Kod pengesahan tersebut amnya diterima oleh pengguna bagi tujuan pengesahan apabila berlaku cubaan pertukaran nombor telefon yang dikaitkan dengan sesuatu akaun WhatsApp.

"Pengguna yang terpedaya menyerahkan kod pengesahan tersebut boleh menyebabkan akaun WhatsApp mereka diambil alih oleh *scammer*," katanya.

LANGKAH-LANGKAH MELINDUNGI WHATSAPP DARIPADA SCAMMER

1. TETAPKAN pengesahan 2 langkah di WhatsApp anda (*Tetapan>Akaun>Pengesahan dua langkah>Dayakan*)
2. JANGAN berkongsi kod pengesahan WhatsApp anda dengan orang lain
3. TETAPKAN nombor pin yang unik untuk peti simpanan suara anda. (*Dail 1313>pilih "2"> Pilih "2">Pilih "1">Masukkan PIN anda dan tekan #*)

Info lanjut mengenai penipuan ini, lawati *http://bit.ly/WhatsAppScam_Info*.



Mohamad Fazli Sabri is with **Zalifah Zahani**.
29 August 2019 ·

Assalam sahabat semua. Ada orang menggunakan profile saya untuk aktiviti SCAM! No yang digunakan ialah +60 13-427 7068. Jangan percaya. Ada sahabat hampir nak transfer RM2500. Please dont!! Laporan Polis telah dibuat dan juga ke pihak SKMM!!

Dah 5 kali cuba... 16:35
Maybank tu macam problem kalau x silap 16:35
Cimb tuan 16:35
Dua kali di fon dan 3 kali di laptop... 16:35
Maaf lah susah kan 16:35
Cuba tuan try CIMB BANK 16:35
Saya dah tanya 16:38
Dia kata CIMB BANK ok 16:38

Tuan hj sihat ke? 3:51 PM
Sihat sahabat 3:51 PM
Alhamdulillah 3:51 PM
Ingat nak minta tlg tadi tapi kalau tuan haji sibuk x aper 3:51 PM
Ye Sahabat
Ana bole tlg Apa tu😅 3:52 PM
Tolong transferkan Rm2500 ke akaun ni

7063794215

Today
🔒 Messages to this chat and calls are now secured with end-to-end encryption. Tap for more info.
Assalamualaikum 3:50 PM
Sibuk ke? 3:51 PM
Wslm Prof 3:51 PM
Ye sy 3:51 PM
Tuan hj sihat ke? 3:51 PM
Sihat sahabat 3:51 PM

Tuan hj sihat ke? 3:51 PM
Sihat sahabat 3:51 PM
Alhamdulillah 3:51 PM
Ingat nak minta tlg tadi tapi kalau tuan haji sibuk x aper 3:51 PM
Ye Sahabat
Ana bole tlg Apa tu😅 3:52 PM
4 UNREAD MESSAGES
Tolong transferkan Rm2500 ke akaun ni

Picdeer
Browse Instagram content with Picdeer
+5
NailinShera Lassius
adieshera
#purple lover #doreamon #19yearsold #i'm human not biawak ,, don't stalk me

Lecturer loses over
RM500,000
to phone scam

Clerk Loses
RM250,000
In Phone Scam After Being Threatened With Arrest

Police: Two Kuching senior citizens suffer losses totalling
RM383,000
in phone scam

Police: Manjung records 52 phone scam cases involving
RM2.1m
in losses this year

Woman loses
RM3.9mil
to scammers

Johor police open 22 investigation papers on phone scams involving losses of
RM1.43m

Retiree loses
RM186,000
in phone scam

Perak police: 57-year-old woman loses
RM381,950
in phone

Civil Servant Lost
RM677,565
Over "Pos Laju" Phone Scam

Malaysian Man Loses
RM1 Million
in Life Savings in 14-Second Scam Call

Penang cops:
Woman loses
RM326,100
in phone scam

Two sisters lose
RM658,000
in phone scam

g) Key Takeaways

- Communication scams are among the most common scams targeting older persons, using phone calls, SMS, email, WhatsApp, and social media to deceive victims.
- Scammersimpersonatetrustedfigures—suchasbankofficers,government agents, delivery services, or even friends and family—to build trust and urgency.
- Common methods include phishing emails, smishing (SMS phishing), vishing (voice scams), and impersonation through messaging apps and social media.
- These scams often use emotional triggers, urgency, or threats to pressure victims into giving up personal information or making payments.
- Warning signs include suspicious links, urgent or threatening messages, poor grammar, unfamiliar senders, and unexpected requests for money.
- Always verify the identity of the sender or caller through a separate, trusted method before responding.

- Never share sensitive information like passwords, PINs, or OTPs over messaging apps or unverified contacts.
- Report and block suspicious contacts immediately to prevent further attempts and protect others.
- Real-life cases in Malaysia highlight the growing trend and sophistication of communication scams, emphasizing the importance of awareness and digital caution.

6.1.4 Impersonations

Impersonation scams are deceptive tactics to exploit that trust and create a sense of urgency, prompting the victim to share sensitive information or transfer money. Older adults are frequently targeted due to their trusting nature, emotional responsiveness, and unfamiliarity with digital manipulation techniques. As these scams become increasingly convincing, it is important to recognize the warning signs and verify identities through trusted channels before responding.

a) What are Impersonations?

Impersonation scams involve fraudsters pretending to be someone the victim knows, respects, or trusts—such as a family member, government authority, or representative from a reputable organization. The aim is to manipulate the victim into sharing personal information or transferring money. These scams rely on creating urgency, invoking fear, or exploiting emotional connections, and are especially dangerous because they appear highly convincing. With the rise of artificial intelligence, scammers are now using advanced techniques like deepfake videos and voice cloning to impersonate real people more convincingly than ever.

Below are common forms of impersonation used to deceive victims:

✅

i. **Family or Friend Impersonation**
Fraudsters claim to be your loved ones, needing urgent help or money due to fabricated emergencies.

✅

ii. **Authority Figure Impersonation**
Scammers pose as police officers or government officials, demanding fines or threatening arrest to intimidate victims into immediate action.

✅

iii. **Company or Service Provider Impersonation**
Scammers mimic representatives from banks or utility providers, claiming account issues or refunds to steal personal information.

✅

iv. **Tech Support Impersonation**
Scammers pretend to offer computer or mobile support to gain remote access and steal data.

✅

v. **AI-generated/Deepfake Impersonations (Emerging Trend)**
Using artificial intelligence (AI), scammers can create realistic videos, images, or voices of real people to trick you into believing the impersonation is genuine.

b) Scam Medium

Scammers use a variety of communication medium to carry out impersonation scams, ranging from traditional methods to advanced digital tools. While phone calls, emails, and social media remain common avenues for deception, emerging technologies such as artificial intelligence (AI) have introduced new, more convincing forms of impersonation. With AI, scammers can now replicate voices, create deepfake videos, and generate realistic images, making it increasingly difficult to detect fraud.

Common mediums for impersonations include:

a. Traditional Channels

Phone calls:
emails, messaging apps, social media.

Phone calls:
Scammers pretend to be family members, police, or government officers.

Emails:
Designed to look official, sometimes with fake logos, sender names, and urgent requests.

Messaging apps:
Fake accounts or stolen identities used to send deceptive messages.

Social media platforms (e.g., Facebook, Instagram):
Impersonators use cloned or hacked accounts to send friend requests or messages.

b. AI-generated impersonations

Deepfake Videos:
Realistic videos where someone's face and voice are faked using AI to convincingly mimic someone's appearance and actions.

Voice Cloning:
AI-generated voices that exactly replicate someone's voice.

AI-generated Images:
Realistic photos created and digital personas generated using AI to look realistic and trustworthy.

c) Common Methods of Impersonation

i. Creating a Sense of Urgency

Scammers often fabricate emergencies—such as a family member in trouble, a legal issue, or an overdue payment—to pressure the victim into acting quickly without verifying the situation.

ii. Emotional Manipulation

By pretending to be someone close or trustworthy, scammers play on emotions like fear, love, or concern to gain the victim's cooperation.

iii. Use of Personal Information

Fraudsters often use stolen or publicly available personal details (e.g., names of family members, job titles, photos) to appear legitimate and build trust.

iv. AI-generated Impersonation

- **Deepfake Videos**
  Scammers create fake videos that appear to show a trusted person—such as a family member, celebrity, or official—speaking directly to the viewer. These videos can be used to deliver emotional pleas, fake announcements, or instructions involving money or personal data.

- **Voice Cloning**
  Using samples of a person's voice, scammers generate AI-powered voice messages or phone calls that sound exactly like someone the victim knows. These voice clones may claim to need urgent help or ask for sensitive information such as banking details or one-time passwords (OTPs).

- **AI-generated Images**
  Fraudsters use AI to create realistic profile pictures and entire fake identities on social media and messaging platforms. These accounts may pose as new acquaintances, customer service agents, or even romantic interests—slowly building trust before making demands or asking for money.

d) Warning Signs of Impersonation Scams

Urgent or Unusual Requests

You are asked to send money or share personal information immediately, especially through unfamiliar channels.

Emotional Pressure

The message or call creates panic, fear, or concern—for example, a loved one is in trouble or a fine must be paid immediately.

Unfamiliar Contact Methods

The request comes from a new or suspicious phone number, email, or social media account, even if it claims to be someone you know.

Refusal to Allow Verification

The caller or sender avoids answering questions or discourages you from contacting others to verify the story.

Unusual Language or Tone

Messages may contain awkward wording, poor grammar, or a tone that feels out of character for the person they're claiming to be.

Requests for Untraceable Payments

You are asked to pay using gift cards, cryptocurrency, or direct transfers to unknown accounts.

e) How to Protect Yourself from Impersonation Scams?

✓ Do This	✗ Avoid This
Always verify the identity of the caller or sender through a trusted source (e.g., call your family member directly).	**Don't assume the request is real just because it sounds urgent or familiar.**
Take your time to think before acting, especially when you receive unexpected messages or calls.	**Avoid reacting immediately to emotional pressure or threats.**
Use privacy settings on social media and limit what personal information is shared publicly.	**Don't overshare personal details online, including family names or routines.**
Report suspicious calls, messages, or profiles to the platform or relevant authorities.	**Don't keep the incident to yourself—scammers often target multiple people.**

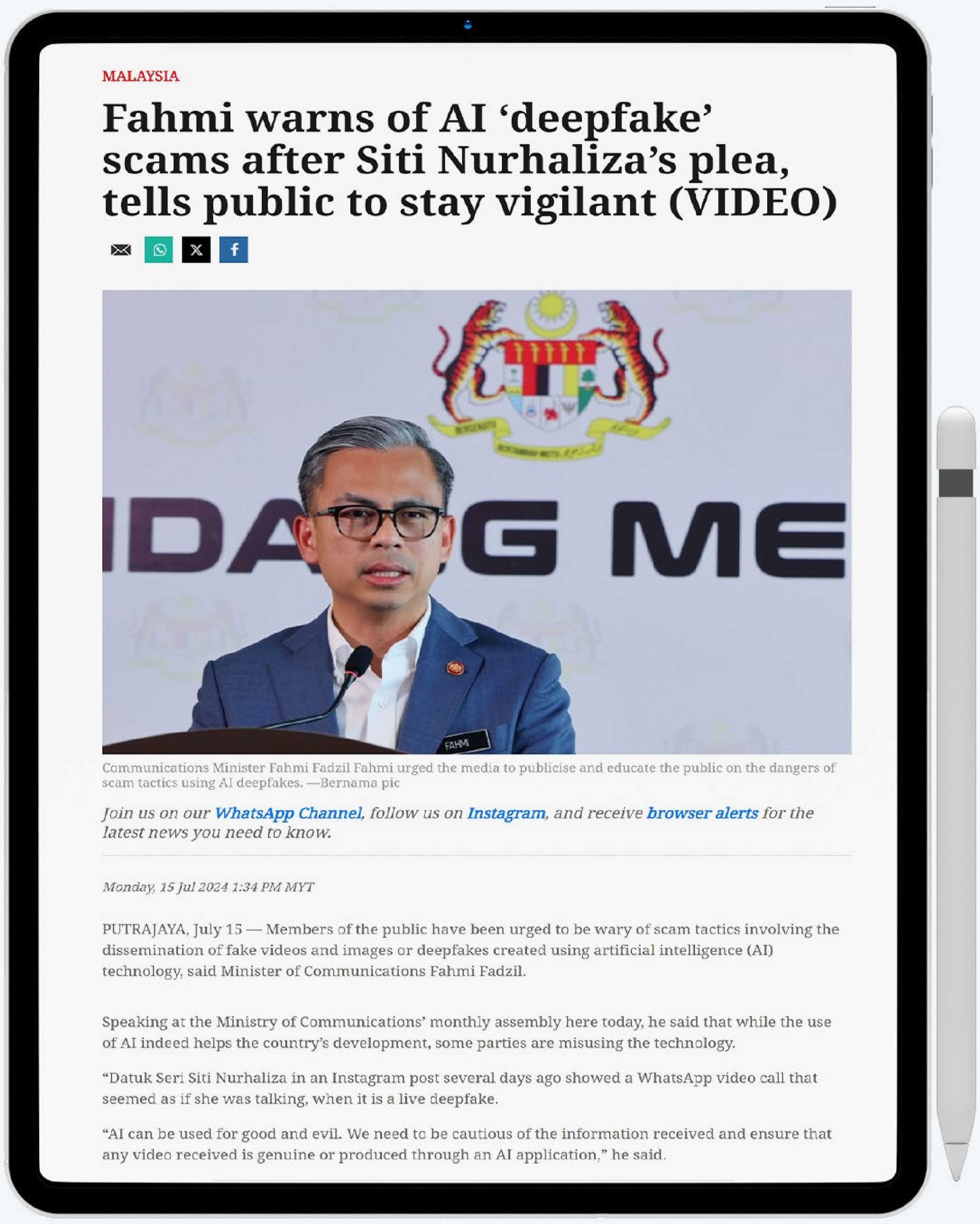
✓ Do This	✗ Avoid This
Educate family and friends, especially older relatives, about impersonation scams.	Don't assume everyone is aware of new scam tactics—share what you know.
Stay informed about emerging technologies like deepfakes and voice cloning. Know how they can be used in scams.	Don't dismiss new tech threats—awareness is your first line of defence.

f) Real-life Cases

In Malaysia, impersonation scams have become increasingly sophisticated, with recent cases revealing a sharp rise in the use of artificial intelligence (AI) to deceive victims. Scammers now impersonate public figures, authorities, and loved ones using advanced technologies such as deepfake videos, voice cloning, and AI-generated images. These scams exploit emotional triggers, trust in familiar identities, and personal data found online or leaked through breaches.

The following table presents several real-life cases reported between 2024 and 2025, showing the range of mediums and methods used to carry out these impersonation scams, and reinforcing the urgent need for public awareness and digital vigilance.

Date	Scam Medium	Methods	Source
15 July 2024	Deepfake videos and images	AI-generated methods	Malay Mail
15 October 2024	AI-generated impersonations	AI-generated methods	CNN
1 February 2025	Phone calls	Exploit personal details found online or stolen from data breaches	Malay Mail
8 June 2025	Deepfake video and voice cloning	AI-generated methods	Vanakkam Malaysia FMT



MALAYSIA

Fahmi warns of AI ‘deepfake’ scams after Siti Nurhaliza’s plea, tells public to stay vigilant (VIDEO)

Communications Minister Fahmi Fadzil Fahmi urged the media to publicise and educate the public on the dangers of scam tactics using AI deepfakes. —Bernama pic

*Join us on our **WhatsApp Channel**, follow us on **Instagram**, and receive **browser alerts** for the latest news you need to know.*

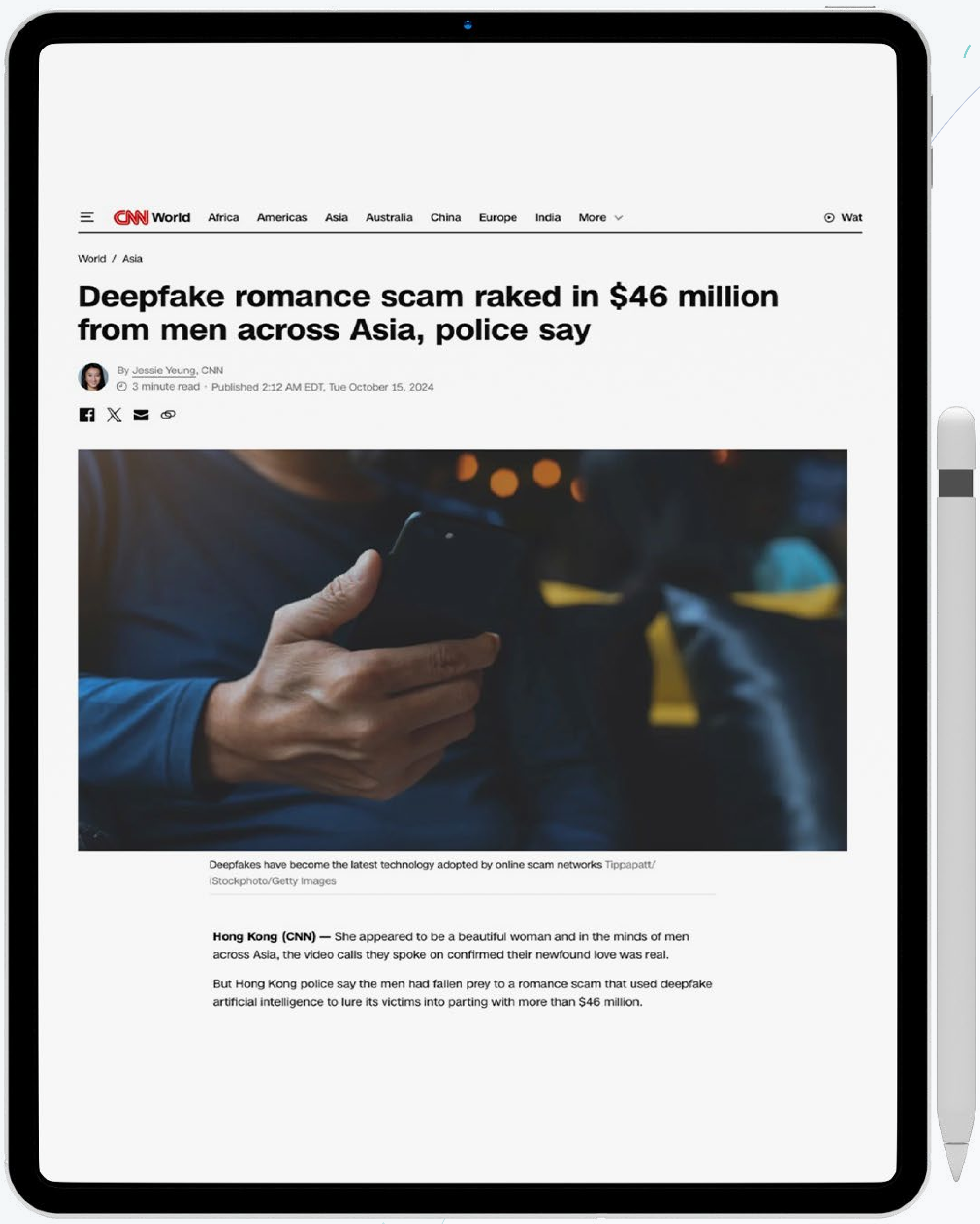
Monday, 15 Jul 2024 1:34 PM MYT

PUTRAJAYA, July 15 — Members of the public have been urged to be wary of scam tactics involving the dissemination of fake videos and images or deepfakes created using artificial intelligence (AI) technology, said Minister of Communications Fahmi Fadzil.

Speaking at the Ministry of Communications’ monthly assembly here today, he said that while the use of AI indeed helps the country’s development, some parties are misusing the technology.

“Datuk Seri Siti Nurhaliza in an Instagram post several days ago showed a WhatsApp video call that seemed as if she was talking, when it is a live deepfake.

“AI can be used for good and evil. We need to be cautious of the information received and ensure that any video received is genuine or produced through an AI application,” he said.



World / Asia

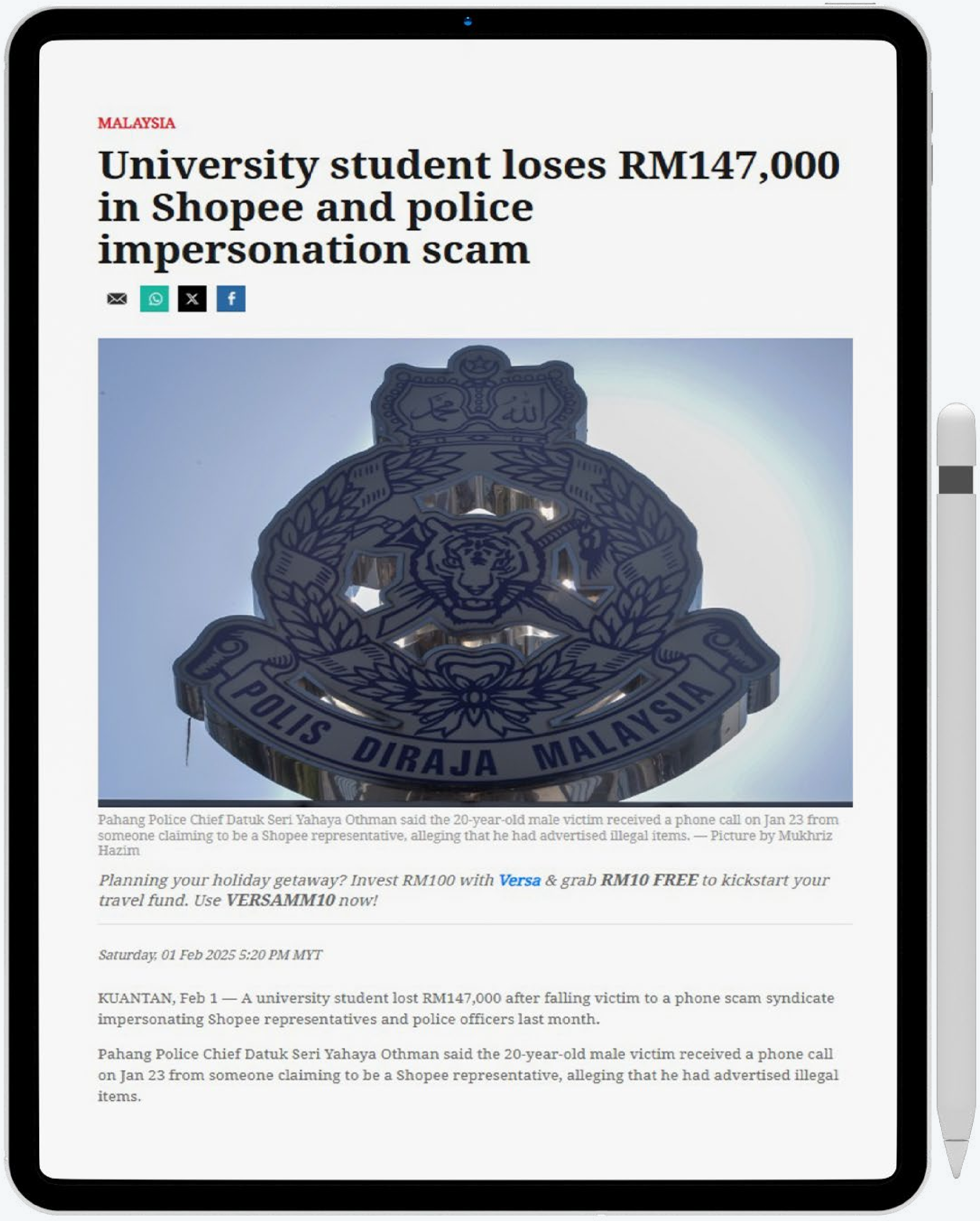
Deepfake romance scam raked in $46 million from men across Asia, police say

By Jessie Yeung, CNN
3 minute read · Published 2:12 AM EDT, Tue October 15, 2024

Deepfakes have become the latest technology adopted by online scam networks Tippapatt/iStockphoto/Getty Images

Hong Kong (CNN) — She appeared to be a beautiful woman and in the minds of men across Asia, the video calls they spoke on confirmed their newfound love was real.

But Hong Kong police say the men had fallen prey to a romance scam that used deepfake artificial intelligence to lure its victims into parting with more than $46 million.



MALAYSIA

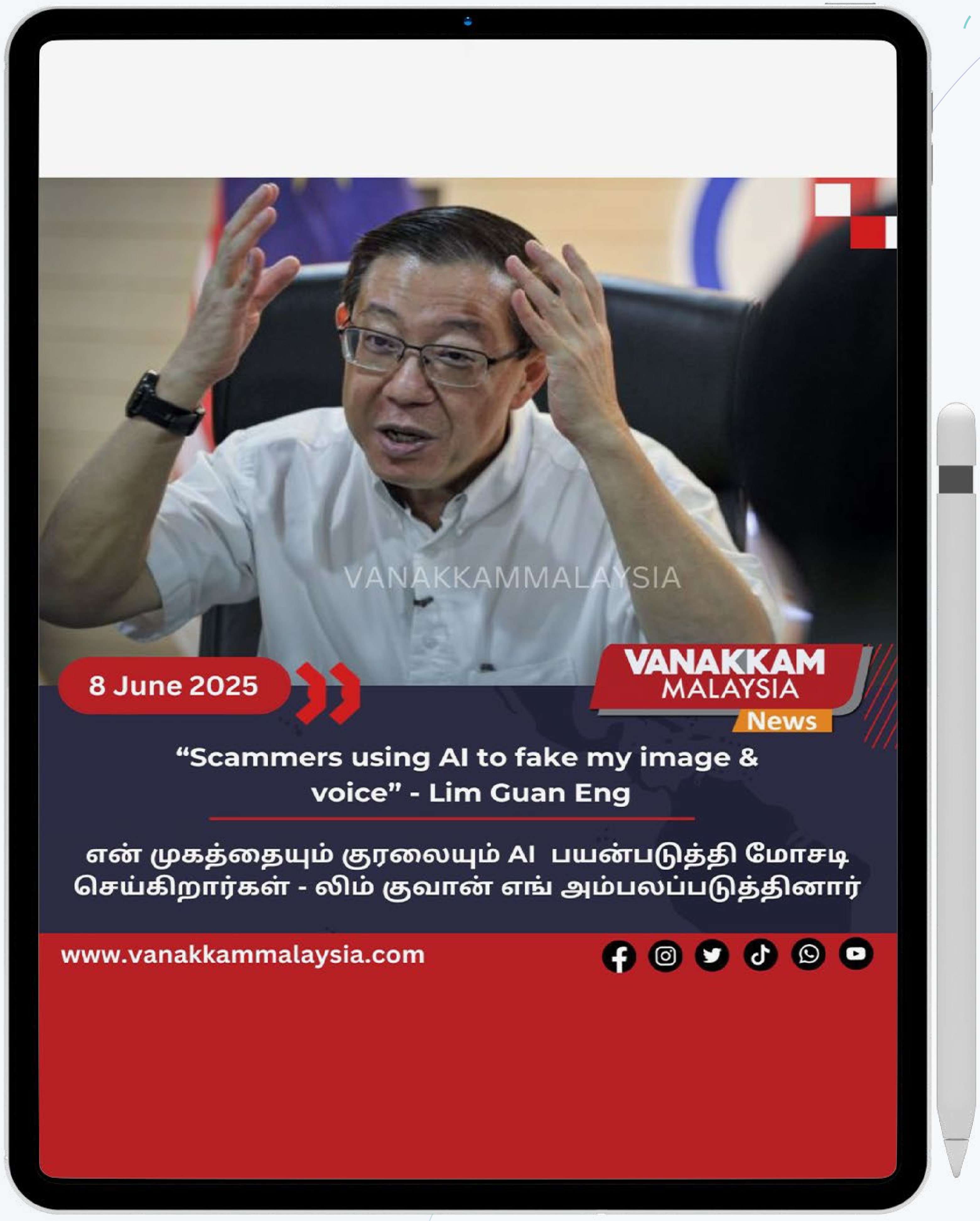
University student loses RM147,000 in Shopee and police impersonation scam

Pahang Police Chief Datuk Seri Yahaya Othman said the 20-year-old male victim received a phone call on Jan 23 from someone claiming to be a Shopee representative, alleging that he had advertised illegal items. — Picture by Mukhriz Hazim

Saturday, 01 Feb 2025 5:20 PM MYT

KUANTAN, Feb 1 — A university student lost RM147,000 after falling victim to a phone scam syndicate impersonating Shopee representatives and police officers last month.

Pahang Police Chief Datuk Seri Yahaya Othman said the 20-year-old male victim received a phone call on Jan 23 from someone claiming to be a Shopee representative, alleging that he had advertised illegal items.



8 June 2025

“Scammers using AI to fake my image & voice” - Lim Guan Eng

என் முகத்தையும் குரலையும் AI பயன்படுத்தி மோசடி செய்கிறார்கள் - லிம் குவான் எங் அம்பலப்படுத்தினார்

www.vanakkammalaysia.com

g) Key Takeaways

- Impersonation scams are increasingly deceptive and emotionally manipulative, exploiting trust, urgency, and fear to extract personal information or money—especially from older adults.
- Scammers impersonate trusted individuals or organizations, including family members, government officials, tech support, and service providers, using both traditional and digital communication channels.
- The rise of AI technologies—such as deepfake videos, voice cloning, and AI-generated images—has made these scams harder to detect and more convincing than ever.
- Common scam tactics include creating a false emergency, invoking emotional pressure, and using stolen personal data to build credibility.
- Warning signs to look out for: urgent requests, emotional distress narratives, refusal to allow identity verification, suspicious contact methods, and demands for untraceable payments.
- Protective actions include verifying identities through trusted channels, staying calm before responding, limiting personal information online, educating loved ones, and staying informed about emerging scam tactics.
- Real-life cases in Malaysia demonstrate how advanced impersonation scams are already affecting victims, underscoring the need for digital awareness, critical thinking, and prompt reporting of suspicious encounters.

6.1.5 Other Types of Online Scams

Online scams come in many forms and continue to evolve as technology advances. Some are designed to steal money, while others aim to gain personal information or manipulate emotions for profit. Among the most common are romance scams, financial scams, and job scams. These types of fraud can cause serious financial losses and emotional distress, making it important to stay alert and informed about how they work.

Romance Scams

i. What Are They?

Romance scams happen when someone pretends to be romantically interested in you to gain your trust, then asks for money or personal details. These scams usually begin on social media, dating sites, or messaging platforms. The scammer gradually builds trust and creates an emotional connection. Once the victim feels attached, the scammer begins to make requests, usually for financial assistance, or sensitive personal details that could later be misused.

Older persons are frequently targeted because scammers perceive them as:

- More financially stable, with retirement savings or pensions.
- More trusting or less familiar with online fraud tactics.
- Sometimes lonely or seeking companionship, which makes them more vulnerable to emotional manipulation.

Examples:

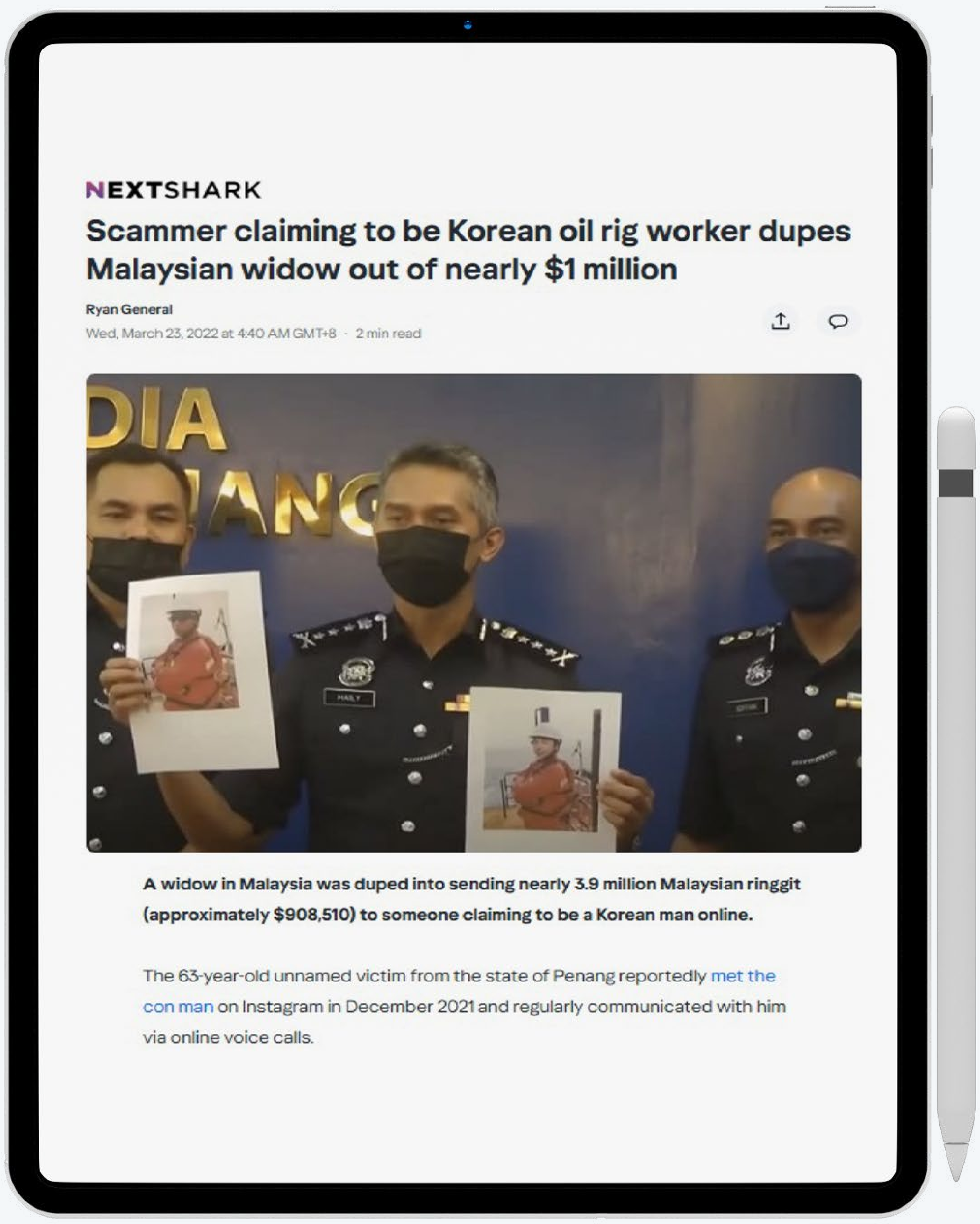
- Meeting someone online who quickly professes love.
- Requests for urgent money to cover medical expenses, travel costs, or family emergencies.
- Avoiding video calls or in-person meetings, always making excuses.
- Using stolen photos or fake identities, such as claiming to be a professional or military officer.
  emergencies.

The methods used in romance scams are similar to previous sections in this module:

- Online Shopping Scams: Victims are persuaded to transfer money, often under false promises of gifts, travel, or urgent needs.
- Charity Scams: Scammers appeal to empathy, claiming emergencies, illness, or financial hardship.
- Communication Scams: Contact usually begins with casual chats online and gradually becomes more frequent and emotional.
- Impersonation Scams: Fraudsters may use stolen photos or fake identities, claiming to be professionals, military officers, or widowed individuals.

ii. How to Protect Yourself:

✅ Be cautious with people who rush a relationship or ask for money.
✅ Never send money to someone you have not met in person.
✅ Be careful sharing personal photos or information, scammers may use them to blackmail you.
✅ Verify identities by checking photos, social media, and consistency of details.
✅ Talk to friends or family if you have doubts about an online relationship.



NEXTSHARK

Scammer claiming to be Korean oil rig worker dupes Malaysian widow out of nearly $1 million

Ryan General
Wed, March 23, 2022 at 4:40 AM GMT+8 · 2 min read

A widow in Malaysia was duped into sending nearly 3.9 million Malaysian ringgit (approximately $908,510) to someone claiming to be a Korean man online.

The 63-year-old unnamed victim from the state of Penang reportedly met the con man on Instagram in December 2021 and regularly communicated with him via online voice calls.

Financial Scams

i. What Are They?

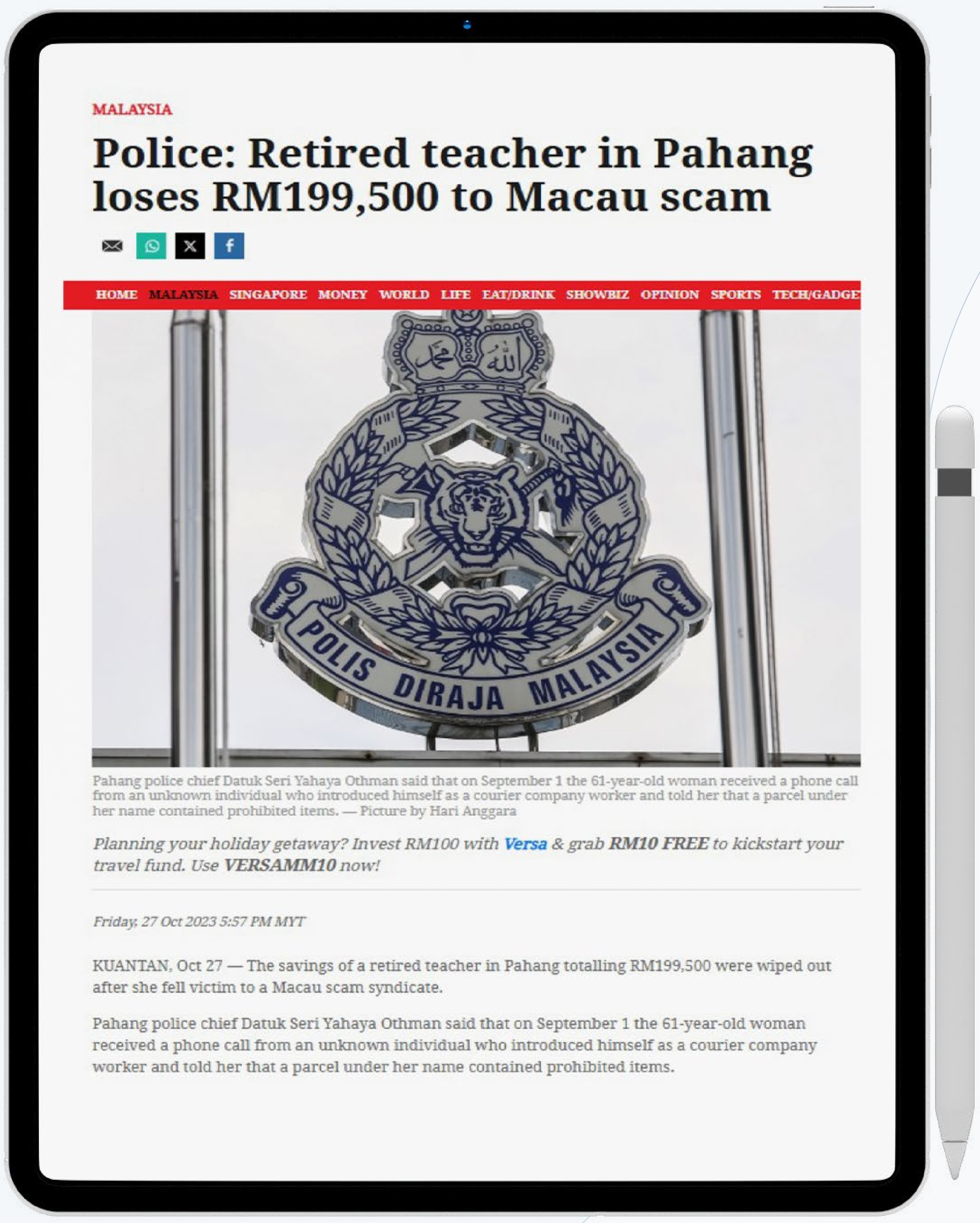
Financial scams trick victims into sending money or sharing banking information. Common forms include fake investment opportunities, loan offers, lottery winnings, or phishing emails that impersonate trusted institutions.

Examples:

- You receive an email claiming you've won a lottery but need to pay "processing fees."
- A scammer offers a quick-return investment scheme promising high profits with little risk.
- A fake bank email asks you to "verify your account" by clicking a link.

ii. How to Protect Yourself:

✅ Be suspicious of offers that sound too good to be true.
✅ Never send money or share banking info with unknown people or companies.
✅ Always verify bank or financial institution requests by contacting them directly.
✅ Use strong, unique passwords and enable two-factor authentication fo online banking.



MALAYSIA

Police: Retired teacher in Pahang loses RM199,500 to Macau scam

Pahang police chief Datuk Seri Yahaya Othman said that on September 1 the 61-year-old woman received a phone call from an unknown individual who introduced himself as a courier company worker and told her that a parcel under her name contained prohibited items. — Picture by Hari Anggara

*Planning your holiday getaway? Invest RM100 with Versa & grab **RM10 FREE** to kickstart your travel fund. Use **VERSAMM10** now!*

Friday, 27 Oct 2023 5:57 PM MYT

KUANTAN, Oct 27 — The savings of a retired teacher in Pahang totalling RM199,500 were wiped out after she fell victim to a Macau scam syndicate.

Pahang police chief Datuk Seri Yahaya Othman said that on September 1 the 61-year-old woman received a phone call from an unknown individual who introduced himself as a courier company worker and told her that a parcel under her name contained prohibited items.

Job Scams

i. What Are They?

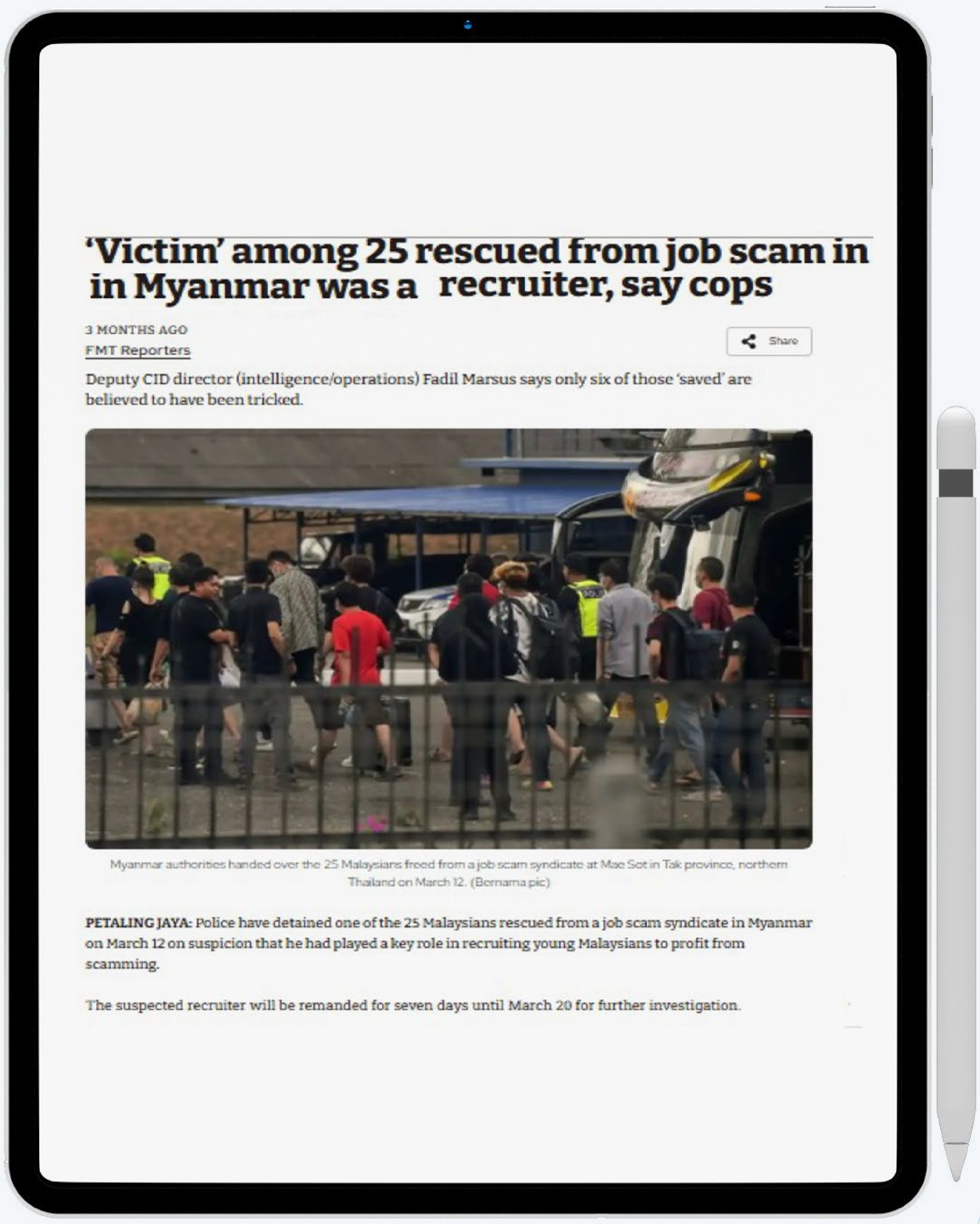
Job scams trick people into paying fees for fake jobs or stealing personal information by pretending to be a legitimate employer.

Examples:

- A fake recruiter asks you to pay for training, uniforms, or job placement.
- You're offered a job immediately without an interview.
- A job ad promises high pay for very easy work.

ii. How to Protect Yourself:

✅ Research the company. Check their official website and reviews.
✅ Never pay upfront for a job offer or training. Legitimate employers don't ask for money.
✅ Be wary of job offers that guarantee huge earnings with no experience.
✅ Watch for fake emails — check the sender's email address carefully.



'Victim' among 25 rescued from job scam in in Myanmar was a recruiter, say cops

3 MONTHS AGO
FMT Reporters

Deputy CID director (intelligence/operations) Fadil Marsus says only six of those 'saved' are believed to have been tricked.

Myanmar authorities handed over the 25 Malaysians freed from a job scam syndicate at Mae Sot in Tak province, northern Thailand on March 12. (Bernama pic)

PETALING JAYA: Police have detained one of the 25 Malaysians rescued from a job scam syndicate in Myanmar on March 12 on suspicion that he had played a key role in recruiting young Malaysians to profit from scamming.

The suspected recruiter will be remanded for seven days until March 20 for further investigation.

6.2 Protecting Yourself from Online Scams

The best way to prevent online scams is through awareness and action. Scams today are more complex and can happen through trusted platforms, for example shopping sites, social media, messaging apps, or even fake calls that sound like your loved ones. Whether the scam involves a fake product, a donation request, an impersonated message, or a cloned voice, knowing what to look for and how to respond can help you stay safe. This section provides guidance on recognizing warning signs, taking protective steps, knowing how to respond when in doubt, and continuing to stay informed as digital threats evolve.

6.2.1 Recognizing Warning Signs in Online Scams

Scams often look real and convincing but they usually share warning signs. Learning to spot these signs early can help prevent mistakes. Common red flags across all scam types:

- Messages creating a sense of urgency ("Act now!" or "Limited time only!")
- Poor spelling and grammar in official-looking messages
- Unexpected contact from government agencies or banks
- Pressure to keep the interaction secret from family and friends
- Too-good-to-be-true offers (free gifts, low prices, fast investment returns)
- Requests for private information (IC, bank details, OTPs, passwords)
- Suspicious senders (unknown numbers, odd email addresses, unfamiliar accounts)
- Untraceable payment methods (bank transfers to personal accounts, cryptocurrency)
- Refusal to allow time for verification or pressure to act immediately

6.2.2 Protective Measures

While specific tips are included under each scam in Section 6.1, this section offers general habits to reduce risk across all types of scams. Some protective measures include:

Use Official Apps: Download banking and shopping apps directly from official app stores

Enable Two-Factor Authentication: Add an extra layer of security to your accounts

Regular Updates: Keep your devices and apps updated with security patches

Trust Your Instincts: If something feels suspicious, it probably is

Establish a "Pause Rule": Wait 24 hours before responding to requests for money or information

Designated Family Contact: Choose a trusted family member to consult about suspicious messages

Keep a Scam Diary: Document suspicious contacts to recognize patterns

Regular Account Monitoring: Check bank and credit card statements weekly for unauthorized charges

Annual Security Review: Update passwords and security questions once a year

Limit what you share online: Be mindful of what you post on social media—details like birthdays, locations, and family names can help scammers impersonate you or your loved ones

6.2.3 Staying Informed

Scammers are always changing their methods. The best protection is to stay updated and make digital safety a regular part of life. Tips to stay informed:

- Follow Trusted Sources: Subscribe to consumer protection newsletters
- Join Community Groups: Many communities have scam alert networks for seniors
- Regular Learning: Attend local library or community centre sessions on digital safety
- Family Tech Time: Schedule regular sessions with family to review digital safety practices

Useful Resources

- #JanganKenaScam (https://www.jangankenascam.com/) is an anti-scam awareness portal, spearheaded by the banking industry in collaboration with Bank Negara Malaysia, Royal Malaysia Police (PDRM) and the Malaysian Communications and Multimedia Commission (MCMC)
- Verify details at Semak Mule website (https://semakmule.rmp.gov.my/)
- Sign up for scam alerts from Bank Negara Malaysia (https://www.bnm.gov.my/financial-fraud-alerts)
- Sign up for MyDigital ID (https://www.digital-id.my/) to reduce the risk of identity theft and counter AI-generated deepfakes
- Verify investment offers through the SC Investment Checker (www.sc.com.my/investment-checker)
- Join community awareness programs for seniors
- Share your experience to help others avoid similar scams

6.3 Reporting Scams and Seeking Help

Reporting online scams and seeking help is crucial if you have been scammed because it increases the chances of recovering lost funds, prevents further financial or personal harm, and helps authorities track down and stop scammers. By coming forward, you contribute valuable information that may assist investigators in identifying scam patterns and protecting others from falling victim to similar schemes. Additionally, seeking support from relevant organizations can provide emotional reassurance and guidance on protecting your personal information and minimizing potential long-term impacts. Timely reporting and reaching out for help empower both individuals and the wider community to combat online fraud more effectively.

If you have been scammed or suspect you are a victim of scammers, stay calm and here are some important points to take note of:

6.3.1 Recognizing You've Been Scammed

- Trust your instincts if something feels wrong
- Don't feel embarrassed – scammers are professional criminals. Tell someone you trust. Many victims feel embarrassed, but scams can happen to anyone. Speaking up can protect others in your circle.
- Act quickly – the faster you respond, the better chance of recovery
- Document everything – save messages, emails, and transaction details

6.3.2 Immediate Steps to Take

- Stop all communication with the scammer immediately
- Do not send any more money or personal information
- Change passwords for affected accounts
- Contact your bank to freeze accounts or stop payments
- Take screenshots of all communications as evidence

6.3.3 Where to Report Online Scams in Malaysia

Important Contact to Report Online Scams

National Scam Response Centre (NSRC)

- Call: 997

Commercial Crime Investigation Department (CCID) Royal Malaysia Police

- Call/ WhatsApp the CCID Hotline: 013-211 1222
- Website: https://semakmule.rmp.gov.my/

Malaysian Communications and Multimedia Commission (MCMC)

- Report to: aduan.skmm.gov.my
- Call: 1-800-188-030
- WhatsApp: 016 220 6262

CyberSecurity Malaysia

- Report via Cyber999 Help Centre: cyber999.my
- Call: 1-300-88-2999

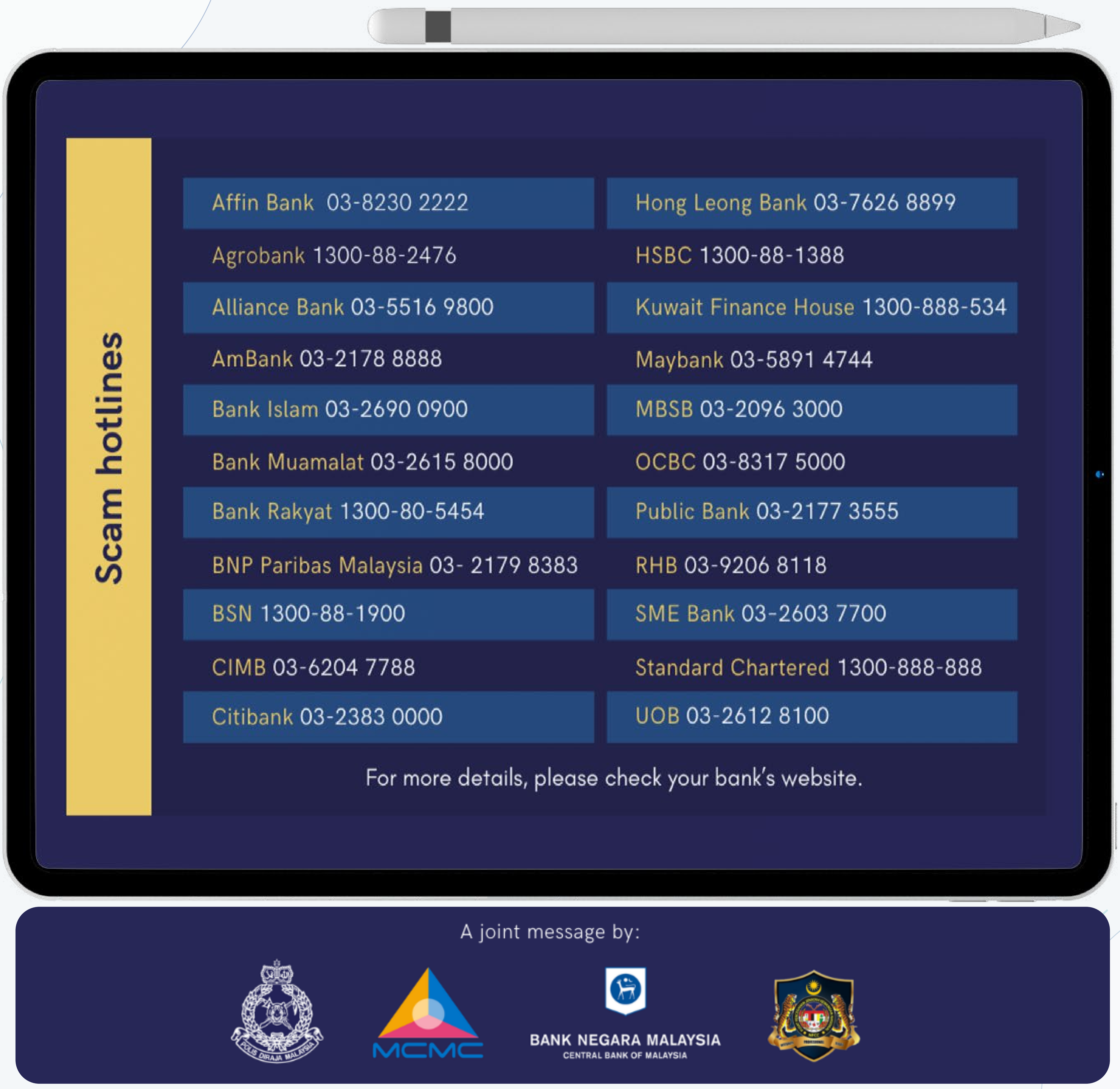
Tribunal for Consumer Claims

- Report
  - In person at Tribunal for Consumer Claims Malaysia (Tribunal Tuntutan Pengguna Malaysia – TTPM) counters nationwide
  - Online via the portal https://ttpm.kpdn.gov.my

Important Contact to Report Financial Scams

- Contact your bank's fraud department immediately (most have 24-hour hotlines) OR
- Contact the National Scam Response Centre at 997; and
- Lodge a police report at your nearest station
- Securities Commission Malaysia: Report investment scams at 03-6204 8999

If scammed, immediately call your bank's scam hotlines



Scam hotlines

Affin Bank 03-8230 2222	Hong Leong Bank 03-7626 8899
Agrobank 1300-88-2476	HSBC 1300-88-1388
Alliance Bank 03-5516 9800	Kuwait Finance House 1300-888-534
AmBank 03-2178 8888	Maybank 03-5891 4744
Bank Islam 03-2690 0900	MBSB 03-2096 3000
Bank Muamalat 03-2615 8000	OCBC 03-8317 5000
Bank Rakyat 1300-80-5454	Public Bank 03-2177 3555
BNP Paribas Malaysia 03- 2179 8383	RHB 03-9206 8118
BSN 1300-88-1900	SME Bank 03-2603 7700
CIMB 03-6204 7788	Standard Chartered 1300-888-888
Citibank 03-2383 0000	UOB 03-2612 8100

For more details, please check your bank's website.

A joint message by:

Bank's fraud department hotline
(Source: https://www.bnm.gov.my/financial-fraud-alerts)

6.3.4 Getting Support

i) Legal Assistance

- Bar Council Legal Aid Centre: Provides free or low-cost legal advice
- Over 20 centres nationwide offering free civil, family, labour, and public-interest law advice.
- Malaysian Bar website https://www.malaysianbar.org.my/article/about-us/contacts/legal-aid-centres/contact/find-legal-aid-centres

ii) Free Consultation

- University Legal Clinics
- UKM's Klinik Literasi & Bantuan Guaman provides free consultations and referrals for online-scam victims.
- Contact: klbg_guamanfuu@ukm.edu.my | +603-8911 8193
- https://www.ukm.my/fuu/kbgm/

iii) Emotional Support

- Befrienders KL: 03-7627 2929 (emotional support hotline)
- Consider joining support groups for scam victims
- Speak with trusted family members or friends

6.4 Conclusion

As digital technology becomes increasingly integrated into daily life, understanding and preventing online scams has become essential for safe digital engagement, particularly for older adults. This module has equipped learners with comprehensive knowledge and practical tools to navigate the digital landscape confidently and securely.

Key Learning Outcomes Achieved:

Enhanced Awareness:

Participants have gained a thorough understanding of various online scam types, including online shopping scams, charity scams, communication scams, and emerging AI-powered impersonation threats.

Recognition Skills:

Learners can now identify critical warning signs such as urgent pressure tactics, requests for personal information, too-good-to-be-true offers, and suspicious communication patterns across multiple digital platforms.

Protective Strategies:

The module has provided practical safety measures including verification techniques, secure payment methods, password management, and the importance of the "pause rule" before responding to suspicious requests.

Response Protocols:

Participants understand the proper channels for reporting scams in Malaysia and know immediate steps to take when encountering suspicious activities or falling victim to fraud.

Critical Takeaways:

Trust but Verify:

Always independently confirm the identity of unexpected contacts through official channels, especially when money or personal information is requested.

Technology Evolution:

Scammers increasingly use sophisticated AI tools like deepfakes and voice cloning, making verification more crucial than ever.

Community Protection:

Sharing knowledge about scams with family and peers creates a network of protection within communities.

Continuous Learning:

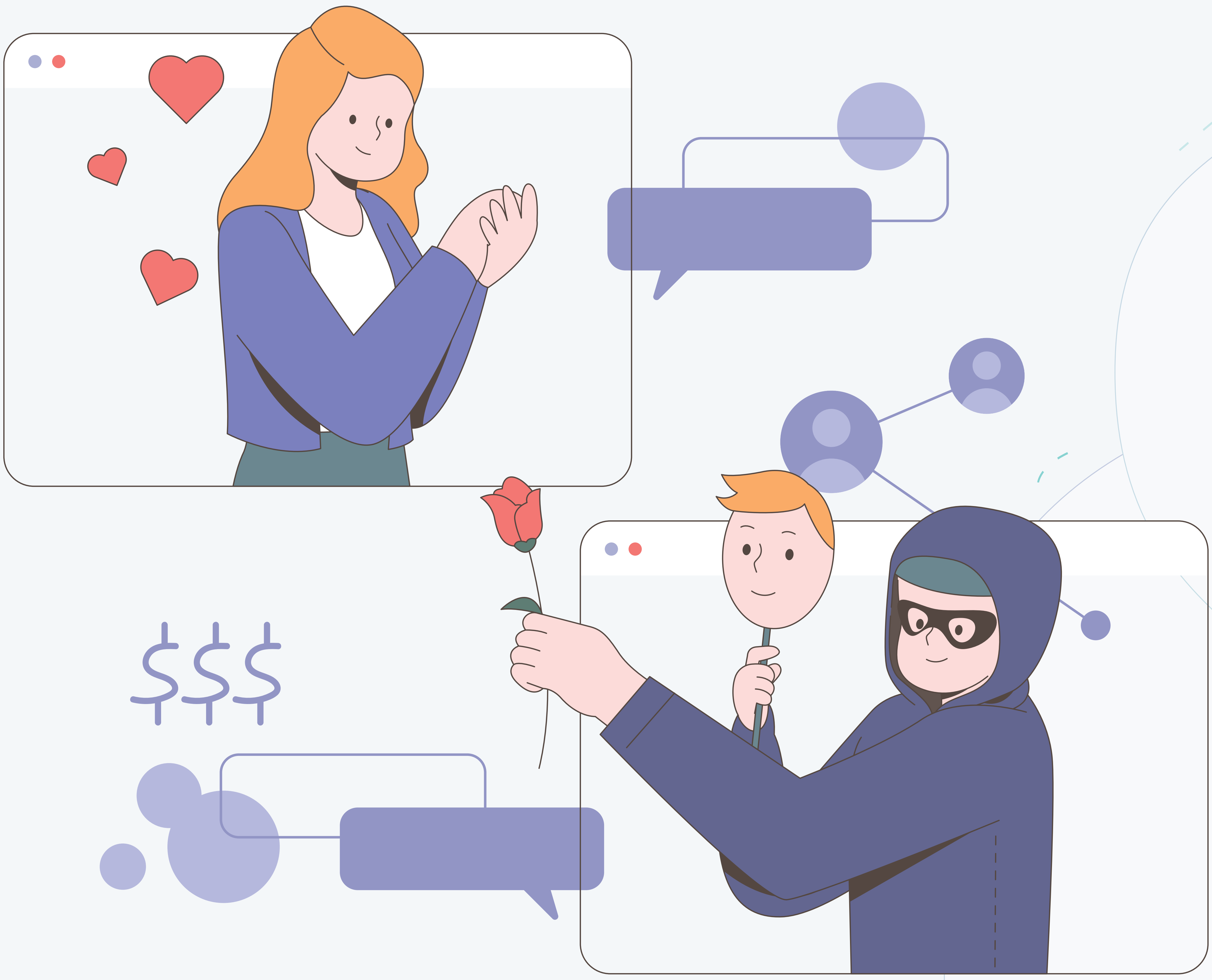
Staying informed about emerging scam tactics through trusted sources ensures ongoing protection as threats evolve.

Moving Forward:

The digital divide need not mean increased vulnerability. By applying the knowledge gained from this module, older adults can confidently engage with digital platforms while maintaining security. Remember that scammers exploit emotions, urgency, and trust—awareness of these tactics is the first line of defence.

The goal is not to avoid digital technology but to use it safely and wisely. With the practical skills and awareness developed through this module, participants are now empowered to enjoy the benefits of digital connectivity while protecting themselves and their communities from online threats.

Regular practice of these safety measures, combined with staying updated on new scam trends, will ensure continued protection in our increasingly digital world.



Glossary

Term	Definition	Page
AI (Artificial Intelligence)	Technology that allows computers to mimic human intelligence. Scammers utilise AI for creating deepfake videos and voice cloning to make scams appear more convincing.	30
Bank Transfer Scam	A fraud where victims are tricked into transferring money to a scammer's personal account.	7
Charity Scam	A fake donation request where scammers pretend to represent a charity or disaster fund.	11
Communication Scam	A scam is carried out through calls, SMS, email, or social media to steal money or information.	16
Counterfeit Goods	Fake products made to look like branded items and sold online.	6
Deepfake	A digitally manipulated video or image created using AI to imitate real people's faces or voices.	30
E-Commerce	Buying and selling goods or services online through platforms such as Shopee or Lazada.	4
Emotional Manipulation	A trick used by scammers to make you feel sympathy, fear, or urgency so you act without thinking.	31
Fake Website	A site that looks legitimate but is designed to steal your personal or financial details.	5, 7
Financial Scam	A trick involving fake investments, loans, or winnings that causes you to lose money.	39
Identity Theft	When someone uses your personal information (like your IC number or name) without permission to commit fraud or a crime.	29
Impersonation	When a scammer pretends to be someone you trust, such as a friend, family member, or government officer.	29
Link	A clickable word or image that leads to another webpage. Scammers may send fake links that direct users to malicious websites.	19
Messaging Apps	Applications like WhatsApp or Telegram are often used for chatting and are frequently targeted by scammers.	17
Online Shopping Scam	A scam where fake sellers trick buyers into paying for items that are never delivered.	4
OTP (One-Time Password)	A temporary code was sent for online transactions. Never share your OTP with anyone.	8
Personal Information	Private details, such as your full name, IC number, address, phone number, or bank account information, that can be used to identify you.	3
Phishing	A scam in which fraudsters send fake messages pretending to be from banks or companies to steal personal information.	17
Privacy Settings	Tools in apps or social media that let you control who can see your personal information.	32
Report	To notify an official authority (like your bank, MCMC, or police) about a scam or suspicious activity.	44–46
Romance Scam	A scam where someone pretends to fall in love online to gain your trust and money.	37

Term	Definition	Page
Scam	A dishonest plan or trick used to cheat people and take their money or personal data.	3
Secure Website	A site that begins with https:// and shows a lock icon (🔒), meaning it's safer for online use.	8
Semak Mule	An official Royal Malaysia Police website (semakmule.rmp.gov.my) to check if a bank account or phone number is linked to scams.	13
Smishing	A scam that uses SMS (text messages) to trick you into clicking fake links or sharing personal details.	19
Social Engineering	Scammers employ psychological tactics to persuade victims into disclosing confidential information.	3
Vishing	A phone call scam where the caller pretends to be from a bank, police department, or government agency to obtain your personal information.	19
Voice Cloning	An AI-generated imitation of someone's voice, used in impersonation scams.	31
Warning Signs	Clues that indicate possible scams include urgency, poor grammar, or requests for secrecy.	41
Verification	The process of confirming your identity before allowing access to an account or information.	42

Published by:
Malaysian Research Institute on Ageing
Universiti Putra Malaysia
43400 UPM Serdang
Selangor Darul Ehsan

☎ : 03-9769 2750
✉ : myageing@upm.edu.my
🌐 : http://www.myageing.upm.edu.my