KOMPILASI TEMUBUAL BERSAMA MEDIA MASSA

2016 – 2025

ZARINA SHUKUR

Pusat Kajian Keselamatan Siber
Fakulti Teknologi dan Sains Maklumat
Universiti Kebangsaan Malaysia

2025

KANDUNGAN

MUKA SURAT

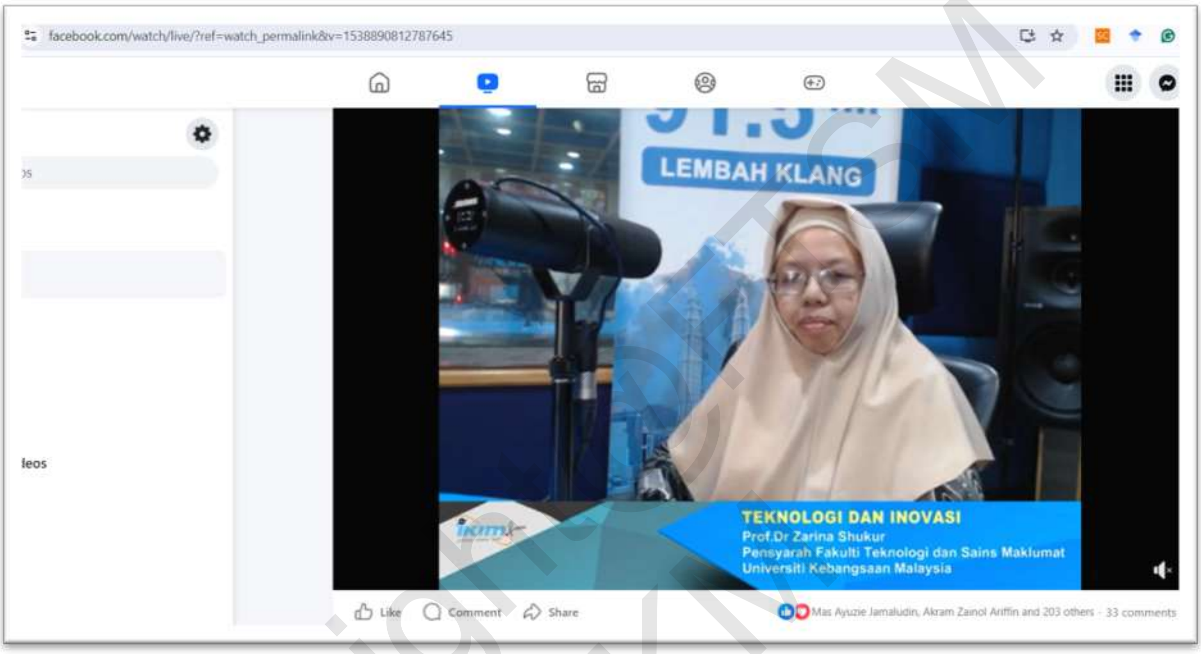
FORUM, TV, RADIO

KERATAN AKHBAR

DJ Syafiq Salleh. (2017, Mei 17). Teknologi dan Inovasi: CenterYou. *IKIM FM*

Pautan:
https://www.facebook.com/watch/live/?ref=watch_permalink&v=1538890812787645

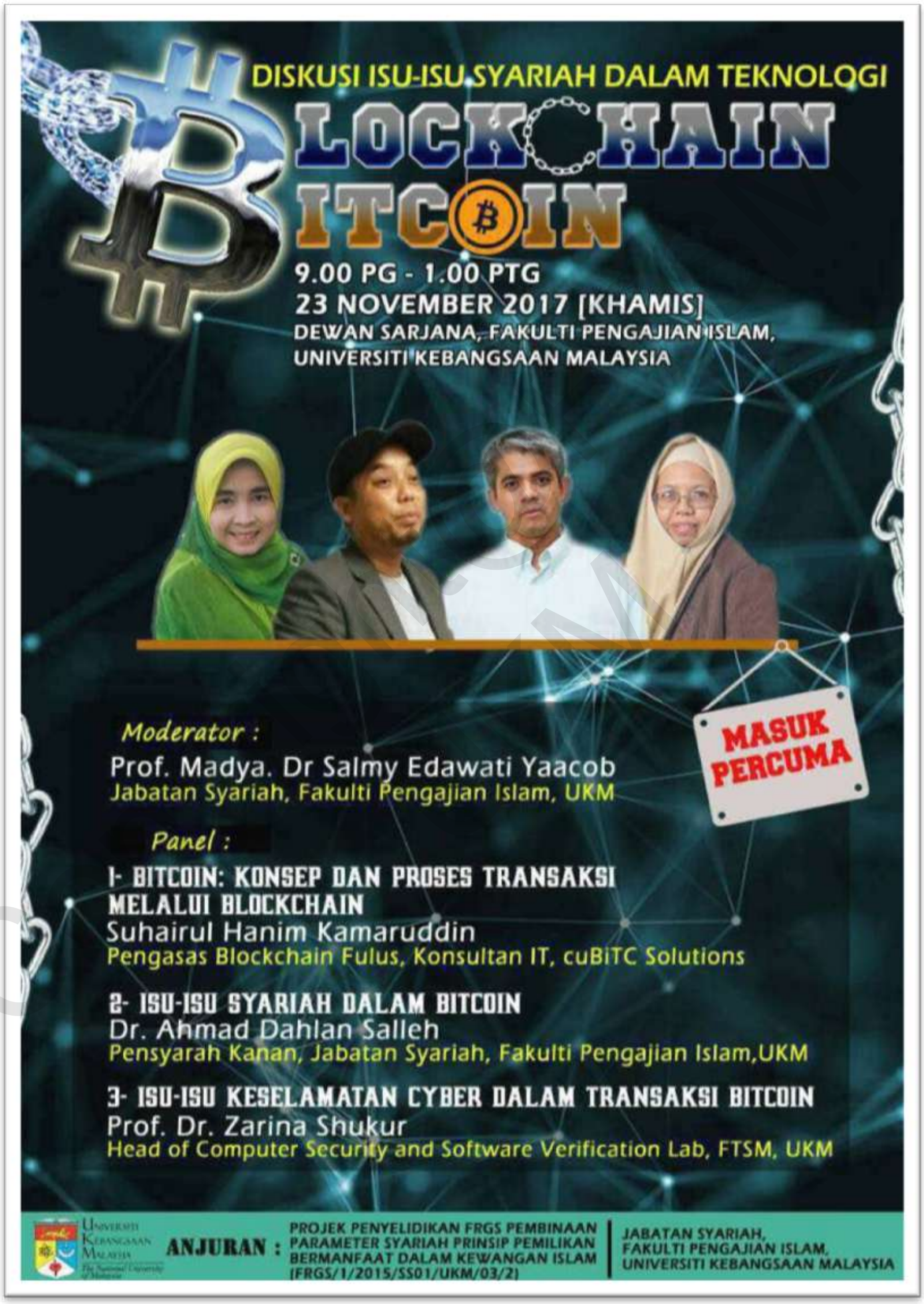
Tangkapan Layar:


facebook.com/watch/live/?ref=watch_permalink&v=1538890812787645
LEMBAH KLANG
TEKNOLOGI DAN INOVASI
Prof.Dr Zarina Shukur
Pensyarah Fakulti Teknologi dan Sains Maklumat
Universiti Kebangsaan Malaysia
ikim
leos
Like
Comment
Share

Mas Ayuzie Jamaludin, Akram Zainol Ariffin and 203 others · 33 comments

Moderator: Prof Madya Dr Salmy Edawati Yaacob. (2017, Nov 23). Isu-isu Syariah dalam Transaksi Bitcoin. Fakulti Pengajian Islam UKM.

Tangkapan Layar Poster:



DISKUSI ISU-ISU SYARIAH DALAM TEKNOLOGI

BLOCKCHAIN

BITCOIN

9.00 PG - 1.00 PTG
23 NOVEMBER 2017 [KHAMIS]
DEWAN SARJANA, FAKULTI PENGAJIAN ISLAM,
UNIVERSITI KEBANGSAAN MALAYSIA

MASUK PERCUMA

Moderator :
Prof. Madya. Dr Salmy Edawati Yaacob
Jabatan Syariah, Fakulti Pengajian Islam, UKM

Panel :

1- BITCOIN: KONSEP DAN PROSES TRANSAKSI MELALUI BLOCKCHAIN
Suhairul Hanim Kamaruddin
Pengasas Blockchain Fulus, Konsultan IT, cuBiTC Solutions

2- ISU-ISU SYARIAH DALAM BITCOIN
Dr. Ahmad Dahlan Salleh
Pensyarah Kanan, Jabatan Syariah, Fakulti Pengajian Islam,UKM

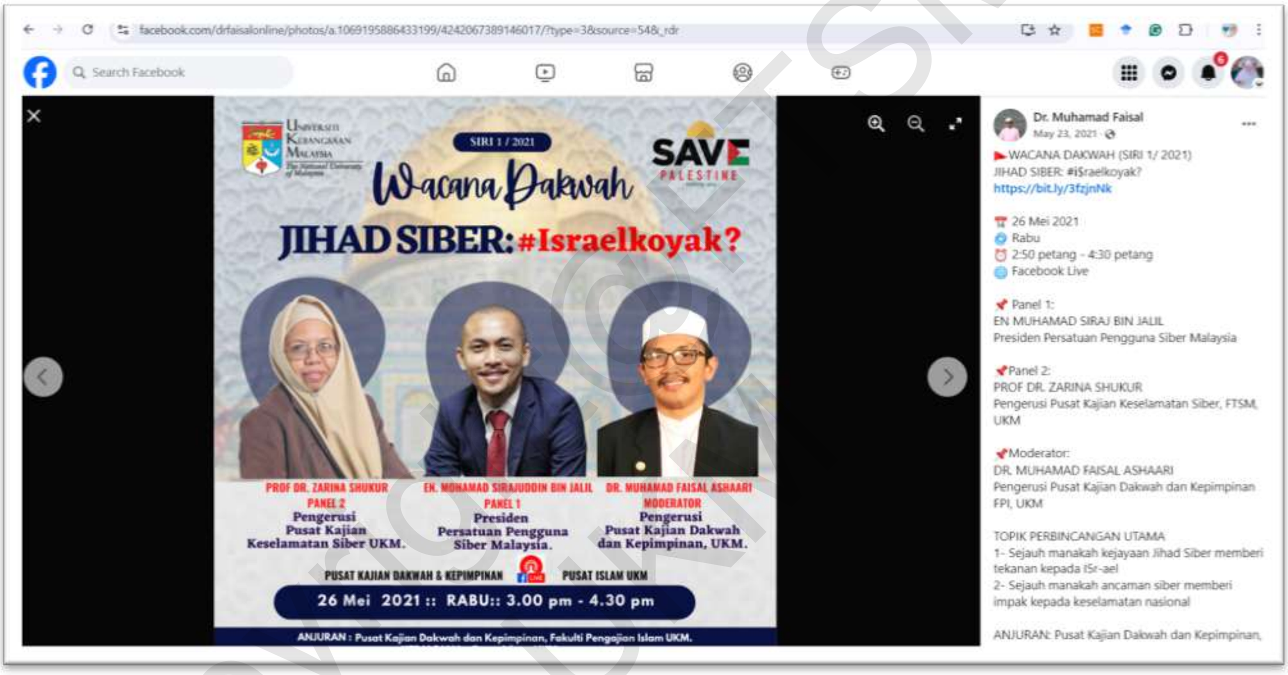
3- ISU-ISU KESELAMATAN CYBER DALAM TRANSAKSI BITCOIN
Prof. Dr. Zarina Shukur
Head of Computer Security and Software Verification Lab, FTSM, UKM

ANJURAN : PROJEK PENYELIDIKAN FRGS PEMBINAAN PARAMETER SYARIAH PRINSIP PEMILIKAN BERMANFAAT DALAM KEWANGAN ISLAM (FRGS/1/2015/SS01/UKM/03/2) | JABATAN SYARIAH, FAKULTI PENGAJIAN ISLAM, UNIVERSITI KEBANGSAAN MALAYSIA

Moderator: Dr Muhammad Faisal Ashaari. (2021, Mei 26). ***Wacana Dakwah Jihad Siber: #IsraelKoyak?*** **Pusat Islam UKM**

Pautan:
https://www.facebook.com/drfaisalonline/photos/a.1069195886433199/4242067389146017/?type=3&source=54&_rdr

Tangkapan Layar:


facebook.com/drfaisalonline/photos/a.1069195886433199/4242067389146017/?type=3&source=54&_rdr
Search Facebook
Universiti Kebangsaan Malaysia
SIRI 1 / 2021
Wacana Dakwah
SAVE PALESTINE
JIHAD SIBER: #Israelkoyak?
PROF DR. ZARINA SHUKUR
PANEL 2
Pengerusi Pusat Kajian Keselamatan Siber UKM.
EN. MOHAMAD SIRAJUDDIN BIN JALIL
PANEL 1
Presiden Persatuan Pengguna Siber Malaysia.
DR. MUHAMAD FAISAL ASHAARI
MODERATOR
Pengerusi Pusat Kajian Dakwah dan Kepimpinan, UKM.
PUSAT KAJIAN DAKWAH & KEPIMPINAN
PUSAT ISLAM UKM
26 Mei 2021 :: RABU:: 3.00 pm - 4.30 pm
ANJURAN : Pusat Kajian Dakwah dan Kepimpinan, Fakulti Pengajian Islam UKM.

Dr. Muhamad Faisal
May 23, 2021

WACANA DAKWAH (SIRI 1/ 2021)
JIHAD SIBER: #i$raelkoyak?
https://bit.ly/3fzjnNk

26 Mei 2021
Rabu
2:50 petang - 4:30 petang
Facebook Live

Panel 1:
EN MUHAMAD SIRAJ BIN JALIL
Presiden Persatuan Pengguna Siber Malaysia

Panel 2:
PROF DR. ZARINA SHUKUR
Pengerusi Pusat Kajian Keselamatan Siber, FTSM, UKM

Moderator:
DR. MUHAMAD FAISAL ASHAARI
Pengerusi Pusat Kajian Dakwah dan Kepimpinan FPI, UKM

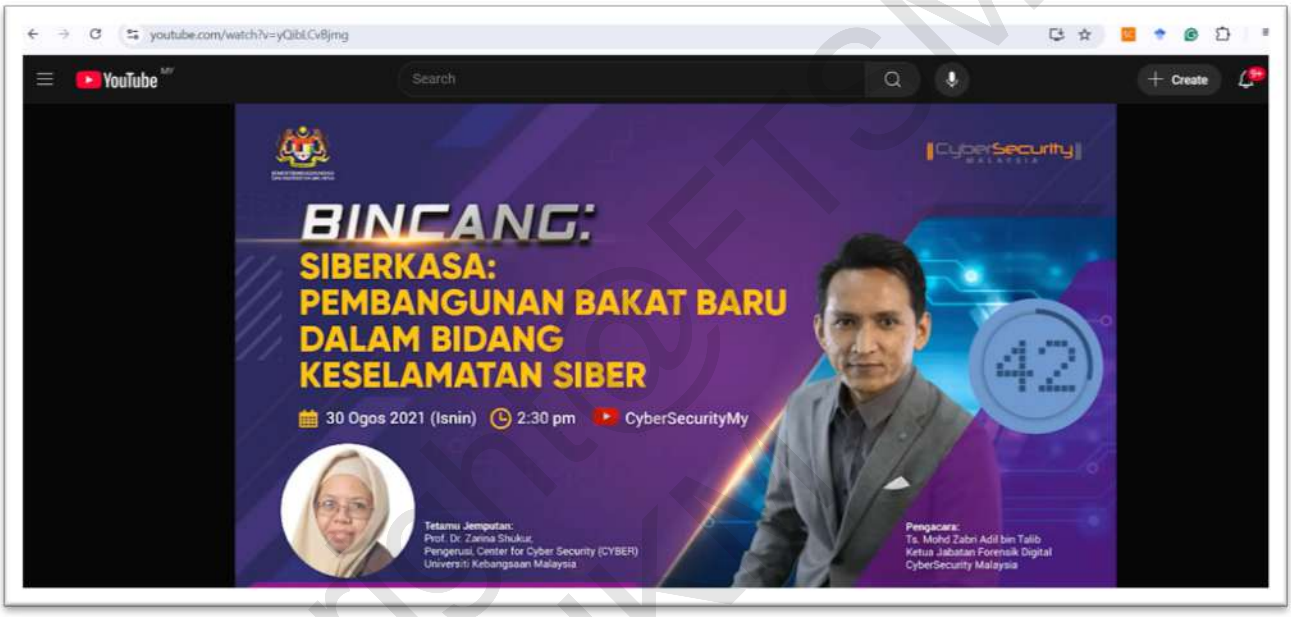
TOPIK PERBINCANGAN UTAMA
1- Sejauh manakah kejayaan Jihad Siber memberi tekanan kepada I5r-ael
2- Sejauh manakah ancaman siber memberi impak kepada keselamatan nasional

ANJURAN: Pusat Kajian Dakwah dan Kepimpinan,

Moderator: Ts. Mohd Zabri Adil bin Talib. (2021, Ogos 30). *SiberKasa: Pembangunan Bakat Baru dalam Bidang Keselamatan Siber*. CyberSecurity Malaysia.

Pautan:
https://www.youtube.com/watch?v=yQibLCvBjmg

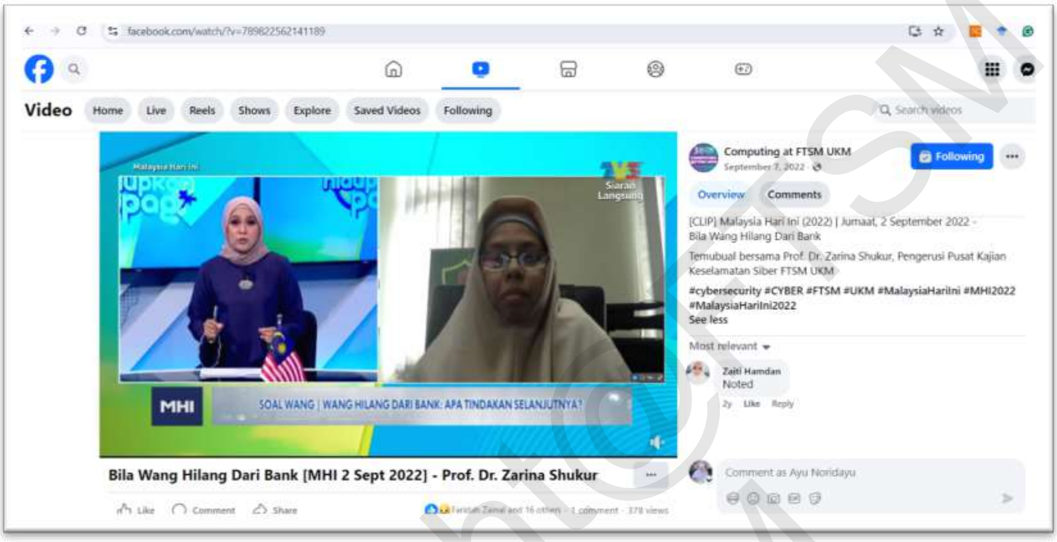
Tangkapan Layar:



Fazilah. (2022, Sep 02). Soal Wang: Wang Hilang Dari Bank: Apa Tindakan Selanjutnya? *MHI TV3* Penerbit Kim

Pautan:
https://www.facebook.com/watch/?v=789822562141189

Tangkapan layar:



Bila Wang Hilang Dari Bank [MHI 2 Sept 2022] - Prof. Dr. Zarina Shukur

Faridah Zainal and 16 others · 1 comment · 378 views

Computing at FTSM UKM
September 7, 2022

[CLIP] Malaysia Hari Ini (2022) | Jumaat, 2 September 2022 - Bila Wang Hilang Dari Bank

Temubual bersama Prof. Dr. Zarina Shukur, Pengerusi Pusat Kajian Keselamatan Siber FTSM UKM

#cybersecurity #CYBER #FTSM #UKM #MalaysiaHariIni #MHI2022 #MalaysiaHariIni2022
See less

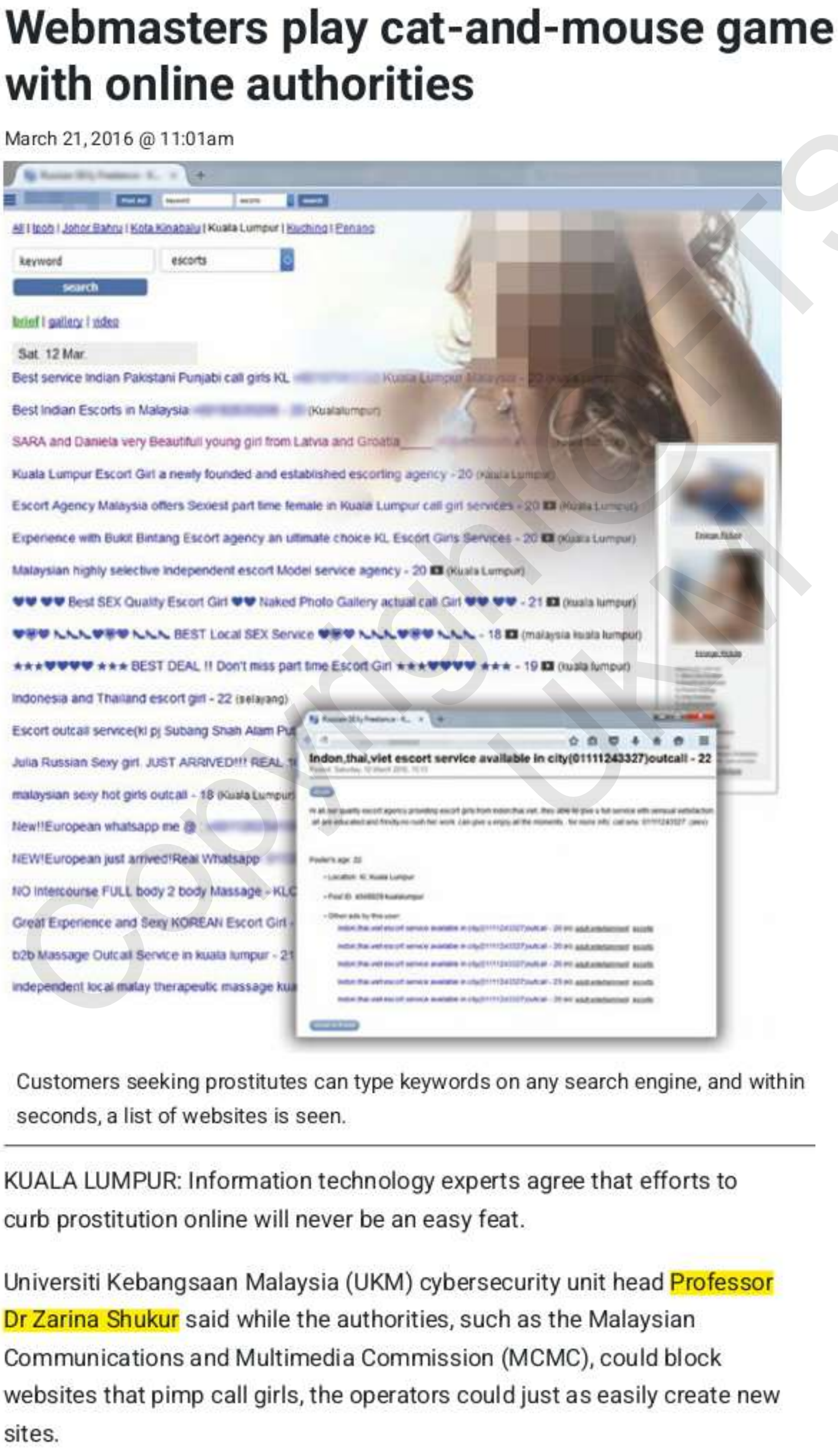
Zaiti Hamdan
Noted
2y Like Reply

Comment as Ayu Noridayu

Ano. (2016, March 21). Webmasters play cat-and-mouse game with online authorities. *New Straits Times*

Pautan:
https://www.nst.com.my/news/2016/03/134024/webmasters-play-cat-and-mouse-game-online-authorities?m=1#google_vignette

Tangkapan layar:



Webmasters play cat-and-mouse game with online authorities

March 21, 2016 @ 11:01am

All | Ipoh | Johor Bahru | Kota Kinabalu | Kuala Lumpur | Kuching | Penang

keyword | escorts

search

brief | gallery | video

Sat 12 Mar

Best service Indian Pakistani Punjabi call girls KL Kuala Lumpur Malaysia - 20

Best Indian Escorts in Malaysia (Kualalumpur)

SARA and Daniela very Beautifull young girl from Latvia and Groatia____

Kuala Lumpur Escort Girl a newly founded and established escorting agency - 20 (Kuala Lumpur)

Escort Agency Malaysia offers Sexiest part time female in Kuala Lumpur call girl services - 20 (Kuala Lumpur)

Experience with Bukit Bintang Escort agency an ultimate choice KL Escort Girls Services - 20 (Kuala Lumpur)

Malaysian highly selective independent escort Model service agency - 20 (Kuala Lumpur)

♥♥ ♥♥ Best SEX Quality Escort Girl ♥♥ Naked Photo Gallery actual call Girl ♥♥ ♥♥ - 21 (kuala lumpur)

♥♥♥ ↖↖↖♥♥♥ ↖↖↖ BEST Local SEX Service ♥♥♥ ↖↖↖♥♥♥ ↖↖↖ - 18 (malaysia kuala lumpur)

★★★♥♥♥♥ ★★★ BEST DEAL !! Don't miss part time Escort Girl ★★★♥♥♥♥ ★★★ - 19 (kuala lumpur)

Indonesia and Thailand escort girl - 22 (selayang)

Escort outcall service(kl pj Subang Shah Alam Pu

Julia Russian Sexy girl. JUST ARRIVED!!! REAL

malaysian sexy hot girls outcall - 18 (Kuala Lumpur)

New!!European whatsapp me @

NEW!European just arrived!Real Whatsapp

NO Intercourse FULL body 2 body Massage - KLC

Great Experience and Sexy KOREAN Escort Girl -

b2b Massage Outcall Service in kuala lumpur - 21

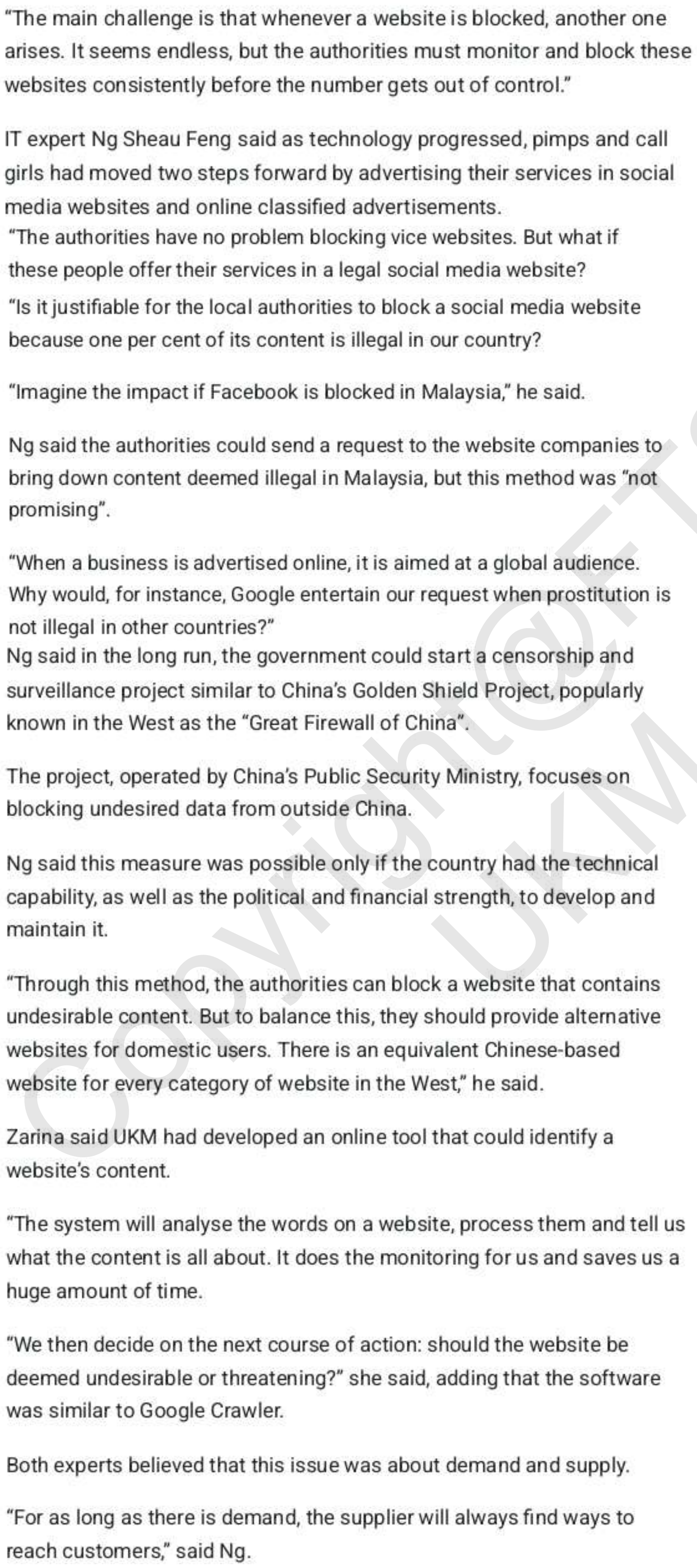
independent local malay therapeutic massage ku

Indon,thai,viet escort service available in city(01111243327)outcall - 22

Customers seeking prostitutes can type keywords on any search engine, and within seconds, a list of websites is seen.

KUALA LUMPUR: Information technology experts agree that efforts to curb prostitution online will never be an easy feat.

Universiti Kebangsaan Malaysia (UKM) cybersecurity unit head Professor Dr Zarina Shukur said while the authorities, such as the Malaysian Communications and Multimedia Commission (MCMC), could block websites that pimp call girls, the operators could just as easily create new sites.



"The main challenge is that whenever a website is blocked, another one arises. It seems endless, but the authorities must monitor and block these websites consistently before the number gets out of control."

IT expert Ng Sheau Feng said as technology progressed, pimps and call girls had moved two steps forward by advertising their services in social media websites and online classified advertisements.

"The authorities have no problem blocking vice websites. But what if these people offer their services in a legal social media website?

"Is it justifiable for the local authorities to block a social media website because one per cent of its content is illegal in our country?

"Imagine the impact if Facebook is blocked in Malaysia," he said.

Ng said the authorities could send a request to the website companies to bring down content deemed illegal in Malaysia, but this method was "not promising".

"When a business is advertised online, it is aimed at a global audience. Why would, for instance, Google entertain our request when prostitution is not illegal in other countries?"

Ng said in the long run, the government could start a censorship and surveillance project similar to China's Golden Shield Project, popularly known in the West as the "Great Firewall of China".

The project, operated by China's Public Security Ministry, focuses on blocking undesired data from outside China.

Ng said this measure was possible only if the country had the technical capability, as well as the political and financial strength, to develop and maintain it.

"Through this method, the authorities can block a website that contains undesirable content. But to balance this, they should provide alternative websites for domestic users. There is an equivalent Chinese-based website for every category of website in the West," he said.

Zarina said UKM had developed an online tool that could identify a website's content.

"The system will analyse the words on a website, process them and tell us what the content is all about. It does the monitoring for us and saves us a huge amount of time.

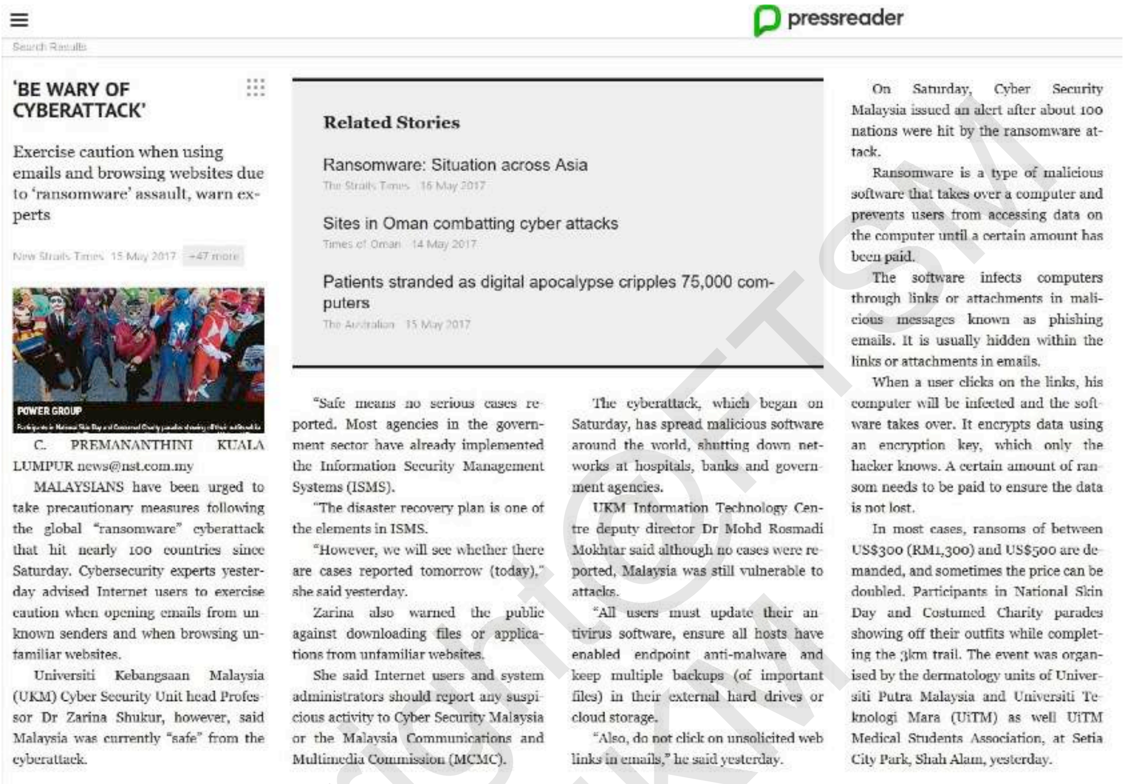
"We then decide on the next course of action: should the website be deemed undesirable or threatening?" she said, adding that the software was similar to Google Crawler.

Both experts believed that this issue was about demand and supply.

"For as long as there is demand, the supplier will always find ways to reach customers," said Ng.

Ano. (2017, May 15). Be Wary of Cyber Attack. New Straits Times

Tangkapan layar:



'BE WARY OF CYBERATTACK'

Exercise caution when using emails and browsing websites due to 'ransomware' assault, warn experts

New Straits Times 15 May 2017

POWER GROUP

[illegible]

Related Stories

Ransomware: Situation across Asia
The Straits Times 16 May 2017

Sites in Oman combatting cyber attacks
Times of Oman 14 May 2017

Patients stranded as digital apocalypse cripples 75,000 computers
The Australian 15 May 2017

C. PREMANANTHINI KUALA LUMPUR news@nst.com.my

MALAYSIANS have been urged to take precautionary measures following the global "ransomware" cyberattack that hit nearly 100 countries since Saturday. Cybersecurity experts yesterday advised Internet users to exercise caution when opening emails from unknown senders and when browsing unfamiliar websites.

Universiti Kebangsaan Malaysia (UKM) Cyber Security Unit head Professor Dr Zarina Shukur, however, said Malaysia was currently "safe" from the cyberattack.

"Safe means no serious cases reported. Most agencies in the government sector have already implemented the Information Security Management Systems (ISMS).

"The disaster recovery plan is one of the elements in ISMS.

"However, we will see whether there are cases reported tomorrow (today)," she said yesterday.

Zarina also warned the public against downloading files or applications from unfamiliar websites.

She said Internet users and system administrators should report any suspicious activity to Cyber Security Malaysia or the Malaysia Communications and Multimedia Commission (MCMC).

The cyberattack, which began on Saturday, has spread malicious software around the world, shutting down networks at hospitals, banks and government agencies.

UKM Information Technology Centre deputy director Dr Mohd Rosmadi Mokhtar said although no cases were reported, Malaysia was still vulnerable to attacks.

"All users must update their antivirus software, ensure all hosts have enabled endpoint anti-malware and keep multiple backups (of important files) in their external hard drives or cloud storage.

"Also, do not click on unsolicited web links in emails," he said yesterday.

On Saturday, Cyber Security Malaysia issued an alert after about 100 nations were hit by the ransomware attack.

Ransomware is a type of malicious software that takes over a computer and prevents users from accessing data on the computer until a certain amount has been paid.

The software infects computers through links or attachments in malicious messages known as phishing emails. It is usually hidden within the links or attachments in emails.

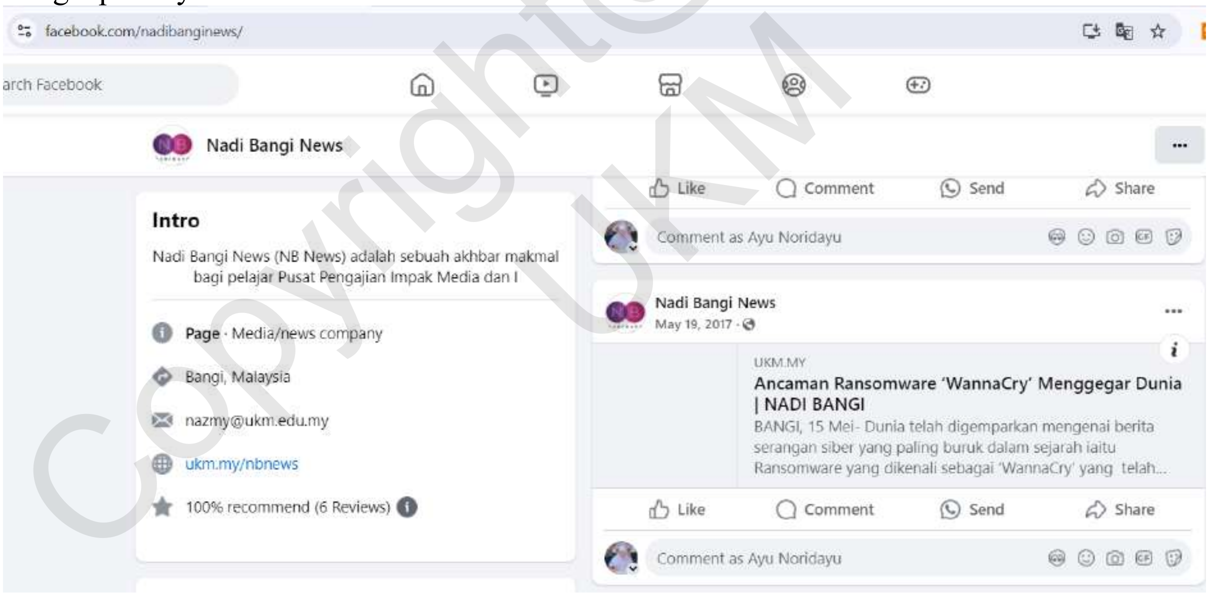
When a user clicks on the links, his computer will be infected and the software takes over. It encrypts data using an encryption key, which only the hacker knows. A certain amount of ransom needs to be paid to ensure the data is not lost.

In most cases, ransoms of between US$300 (RM1,300) and US$500 are demanded, and sometimes the price can be doubled. Participants in National Skin Day and Costumed Charity parades showing off their outfits while completing the 3km trail. The event was organised by the dermatology units of Universiti Putra Malaysia and Universiti Teknologi Mara (UiTM) as well UiTM Medical Students Association, at Setia City Park, Shah Alam, yesterday.

Annissa Adibah Kamaruzaman. (2017, May 19). Ancaman WannaCry Menggegar Dunia. ***Nadi Bangi***

Pautan:
https://l.facebook.com/l.php?u=http%3A%2F%2Fwww.ukm.my%2Fnbnews%2Fancaman-ransomware-wannacry-menggegar-dunia%2F%3Ffbclid%3DIwZXh0bgNhZW0CMTEAAR0_xXNUQ-S8RP6zdZepXMRRdJUM5ThLsNFDeWxfDHXNmkmY6K2eYVhXF_A_aem_SwkoSCMyyV83R4KmTuxBuQ%23.WR6D3aJJaUE.facebook&h=AT0rg2jMzeQy0syI3kUsqcBfwRy4Aa4OwHSawLmU4VckVuOh2EDU2oLtuUNfoYzOFsVek87F8p2rgZ-JvAn9DTzTSkJHknQkB2Ta6OjAbWPx1jUSjkXxojWtDiND6hTAp1KoNAAeuR3z42VkWr61&__tn__=H-R&c[0]=AT0q5dmDhiErhPJrUYNU0RyQGvux1z8z4qGViEb029BPi_y0QsYBQd0b-LoZtdDjgX8JH1NyDOj8WIyEK1smdbwZmqqTvql104rv4WiiPteJusoVT2fVeFp2kcex_H98d5pjzWps8hZsEYntY4RuKsxfRJupA020mm1xDviCXVDpbGbS6BOZ_EE3SQR0WzaRXN4osoePF7vm7lJ5g6cuQBc3BYc (pautan - page not found)

Tangkapan layar:



facebook.com/nadibanginews/

Comment as Ayu Noridayu

Intro

Nadi Bangi News (NB News) adalah sebuah akhbar makmal bagi pelajar Pusat Pengajian Impak Media dan I

Page · Media/news company

Bangi, Malaysia

nazmy@ukm.edu.my

ukm.my/nbnews

100% recommend (6 Reviews)

Nadi Bangi News
May 19, 2017 ·

UKM.MY
Ancaman Ransomware 'WannaCry' Menggegar Dunia | NADI BANGI
BANGI, 15 Mei- Dunia telah digemparkan mengenai berita serangan siber yang paling buruk dalam sejarah iaitu Ransomware yang dikenali sebagai 'WannaCry' yang telah...

Comment as Ayu Noridayu

Ahmad Fairuz Othman & Rizalman Hammim. (2017, Jun 10). New Cyber Law On The Card. New Straits Times

Pautan:
https://www.nst.com.my/news/nation/2017/06/247475/new-cyberlaw-cards

Tangkapan layar:

New cyberlaw on the cards

By **Ahmad Fairuz Othman, Rizalman Hammim**

Jun 10, 2017 @ 1:23pm

e Minister Datuk Seri Dr Ahmad Zahid Hamidi ple at the Sultan Iskandar Customs, Immigration ne Complex in Johor Baru yesterday. PIC BY N AHMAD TAJUDDIN

Get breaking news fast — follow us on WhatsApp and Telegram.

A NEW cyberlaw to ensure more efficient enforcement and punishment against online crimes will become a reality soon.

It will cover offences such as online recruitment and funding of terrorist activities, online gambling as well as cyber-related crimes.

FEATURED VIDEO

LATEST

3 min **Nation** Wan Saiful to lodge complaint against Azmin over claim on 'plot' against Muhyiddin

6 min **Corporate** Swift, top global banks working on blockchain-based overhaul

8 min **Corporate** Lufthansa announces 4,000 job cuts and higher profitability targets

Deputy Prime Minister Datuk Seri Dr Ahmad Zahid Hamidi said the draft of the Cyber Security Bill had been submitted to Attorney-General Tan Sri Mohamed Apandi Ali on Thursday. It is expected to be tabled at the next parliamentary sitting.

"Because the power in this matter falls under the National Security Council (NSC), the tabling will be done by the Prime Minister's Department."

He said the law was among the initiatives being implemented to boost the country's cybersecurity and to centralise its enforcement under a specific entity.

Zahid said the government was serious about tackling cyber offences with an average of 10,000 cyber-related complaints, some of them crime-related, lodged in Malaysia annually.

"The complaints received that were related to the Malaysian Communications and Multimedia Commission Act (1998), Sedition Act (1948) and Defamation Act (1957) have averaged around 10,000 per year.

"The government is serious when it comes to the question of cybercrime because it is part of the jurisdiction of enforcement agencies, which monitor any recruitment related to terrorism; or funding from domestic or foreign sources that are used for terrorism.

"They (enforcement agencies) also monitor those under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA) or other offences, such as online gambling.

"This is done to protect the interest of the people," he said at the Sultan Iskandar Customs, Immigration and Quarantine (CIQ) Complex here yesterday.

The Cyber Security Bill is expected to be tabled soon following a high-level meeting on the proposed National Cyber Security Agency, chaired by Zahid, in Putrajaya on Thursday.

Zahid said the power to enforce regulations on cybersecurity offences would be centralised under the NSC, including streamlining other agencies into one entity.

"The centralisation of cybersecurity under the NSC will involve the powers of CyberSecurity Malaysia (an agency under the Science, Technology and Innovation Ministry) falling under the NSC."

10 min

Nation

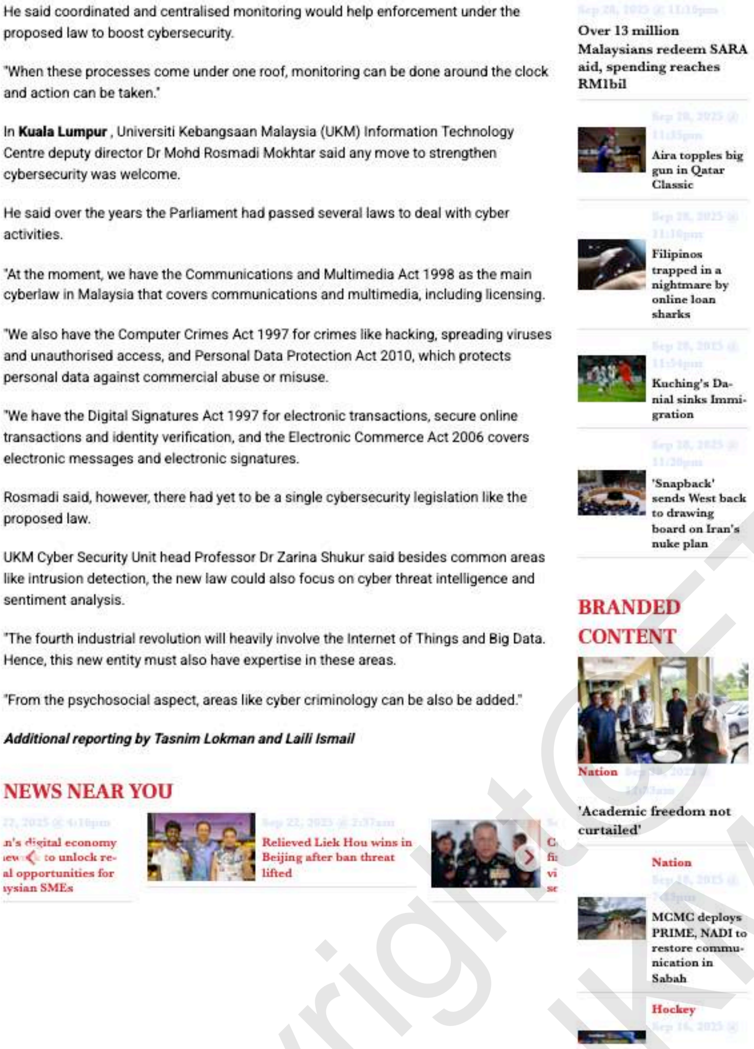
Engine leak forces GSF vessel to withdraw, flotilla still on track to Gaza

10 min

Nation

Wan Saiful: I collected SDs from Bersatu leaders, but not to topple Muhyiddin

WHAT TO READ NEXT



He said coordinated and centralised monitoring would help enforcement under the proposed law to boost cybersecurity.

"When these processes come under one roof, monitoring can be done around the clock and action can be taken."

In **Kuala Lumpur** , Universiti Kebangsaan Malaysia (UKM) Information Technology Centre deputy director Dr Mohd Rosmadi Mokhtar said any move to strengthen cybersecurity was welcome.

He said over the years the Parliament had passed several laws to deal with cyber activities.

"At the moment, we have the Communications and Multimedia Act 1998 as the main cyberlaw in Malaysia that covers communications and multimedia, including licensing.

"We also have the Computer Crimes Act 1997 for crimes like hacking, spreading viruses and unauthorised access, and Personal Data Protection Act 2010, which protects personal data against commercial abuse or misuse.

"We have the Digital Signatures Act 1997 for electronic transactions, secure online transactions and identity verification, and the Electronic Commerce Act 2006 covers electronic messages and electronic signatures.

Rosmadi said, however, there had yet to be a single cybersecurity legislation like the proposed law.

UKM Cyber Security Unit head Professor Dr Zarina Shukur said besides common areas like intrusion detection, the new law could also focus on cyber threat intelligence and sentiment analysis.

"The fourth industrial revolution will heavily involve the Internet of Things and Big Data. Hence, this new entity must also have expertise in these areas.

"From the psychosocial aspect, areas like cyber criminology can be also be added."

Additional reporting by Tasnim Lokman and Laili Ismail

NEWS NEAR YOU

22, 2025 @ 4:16pm
n's digital economy
iew to unlock re-
al opportunities for
ysian SMEs

Sep 22, 2025 @ 2:37am
Relieved Liek Hou wins in Beijing after ban threat lifted

C
fi
vi
se

Sep 28, 2025 @ 11:16pm
Over 13 million Malaysians redeem SARA aid, spending reaches RM1bil

Sep 28, 2025 @ 11:35pm
Aira topples big gun in Qatar Classic

Sep 28, 2025 @ 11:10pm
Filipinos trapped in a nightmare by online loan sharks

Sep 28, 2025 @ 11:54pm
Kuching's Danial sinks Immigration

Sep 28, 2025 @ 11:20pm
'Snapback' sends West back to drawing board on Iran's nuke plan

BRANDED CONTENT

Nation Sep 29, 2025 @ 10:03am
'Academic freedom not curtailed'

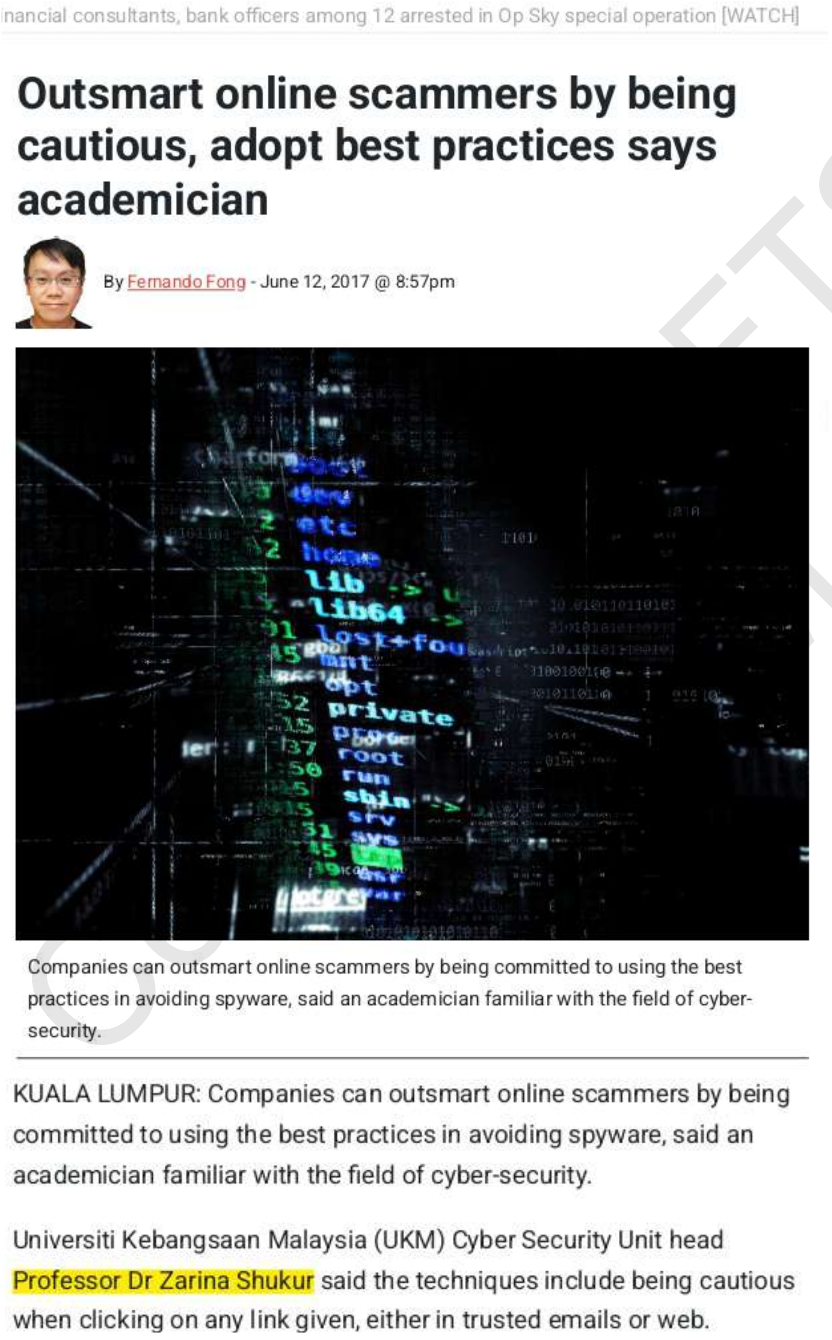
Nation
Sep 18, 2025 @ 7:43pm
MCMC deploys PRIME, NADI to restore communication in Sabah

Hockey
Sep 16, 2025 @

Fernando Fong. (2017, Jun 12). Outsmart online scammers by being cautious, adopt best practices says academician. ***New Straits Times***

Pautan:
https://www.nst.com.my/news/nation/2017/06/248258/outsmart-online-scammers-being-cautious-adopt-best-practices-says

Tangkapan layar:



inancial consultants, bank officers among 12 arrested in Op Sky special operation [WATCH]

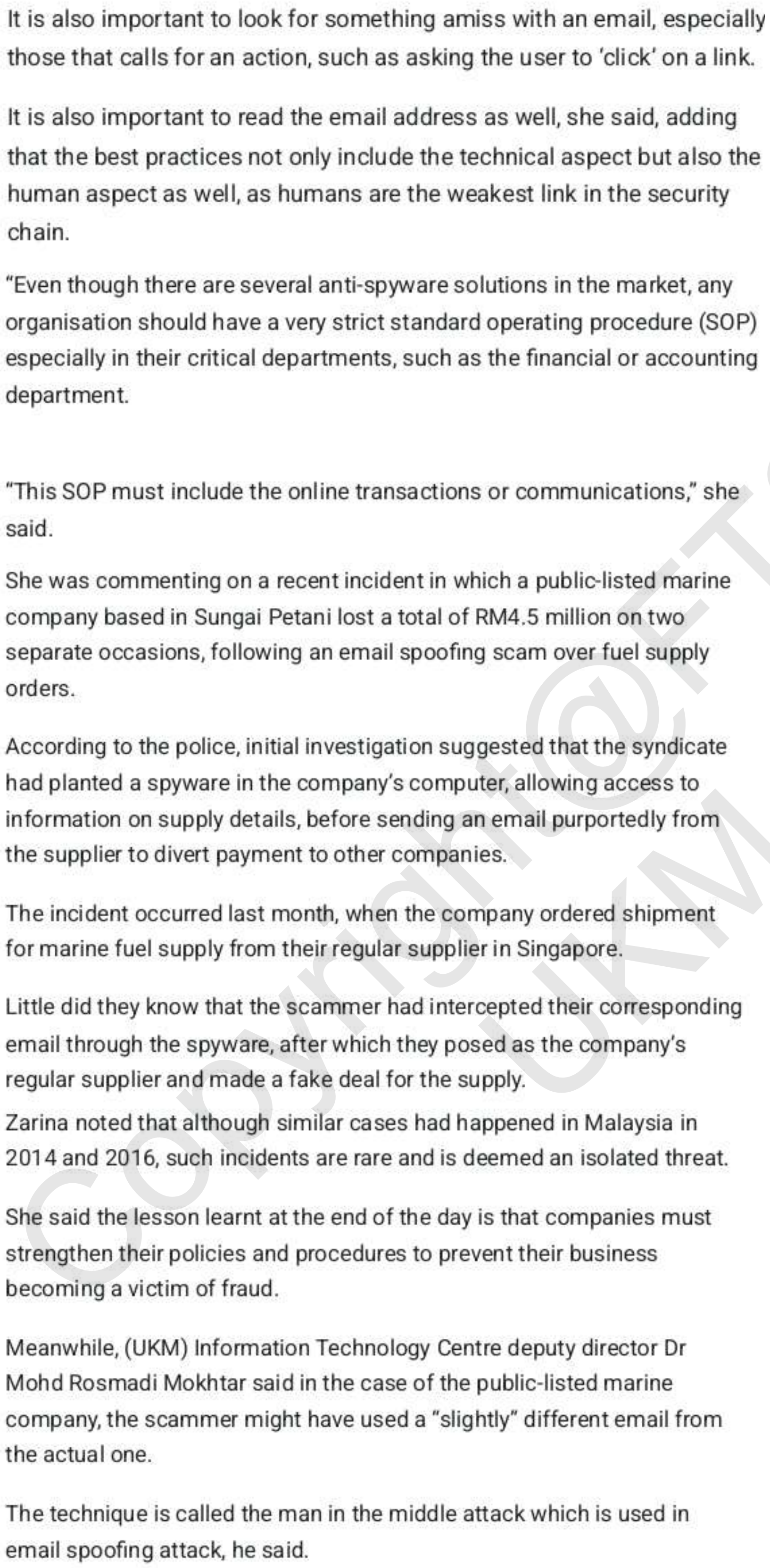
Outsmart online scammers by being cautious, adopt best practices says academician

By Fernando Fong - June 12, 2017 @ 8:57pm

Companies can outsmart online scammers by being committed to using the best practices in avoiding spyware, said an academician familiar with the field of cyber-security.

KUALA LUMPUR: Companies can outsmart online scammers by being committed to using the best practices in avoiding spyware, said an academician familiar with the field of cyber-security.

Universiti Kebangsaan Malaysia (UKM) Cyber Security Unit head Professor Dr Zarina Shukur said the techniques include being cautious when clicking on any link given, either in trusted emails or web.



It is also important to look for something amiss with an email, especially those that calls for an action, such as asking the user to 'click' on a link.

It is also important to read the email address as well, she said, adding that the best practices not only include the technical aspect but also the human aspect as well, as humans are the weakest link in the security chain.

"Even though there are several anti-spyware solutions in the market, any organisation should have a very strict standard operating procedure (SOP) especially in their critical departments, such as the financial or accounting department.

"This SOP must include the online transactions or communications," she said.

She was commenting on a recent incident in which a public-listed marine company based in Sungai Petani lost a total of RM4.5 million on two separate occasions, following an email spoofing scam over fuel supply orders.

According to the police, initial investigation suggested that the syndicate had planted a spyware in the company's computer, allowing access to information on supply details, before sending an email purportedly from the supplier to divert payment to other companies.

The incident occurred last month, when the company ordered shipment for marine fuel supply from their regular supplier in Singapore.

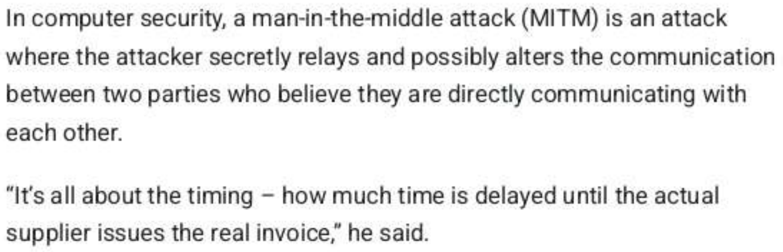
Little did they know that the scammer had intercepted their corresponding email through the spyware, after which they posed as the company's regular supplier and made a fake deal for the supply.

Zarina noted that although similar cases had happened in Malaysia in 2014 and 2016, such incidents are rare and is deemed an isolated threat.

She said the lesson learnt at the end of the day is that companies must strengthen their policies and procedures to prevent their business becoming a victim of fraud.

Meanwhile, (UKM) Information Technology Centre deputy director Dr Mohd Rosmadi Mokhtar said in the case of the public-listed marine company, the scammer might have used a "slightly" different email from the actual one.

The technique is called the man in the middle attack which is used in email spoofing attack, he said.



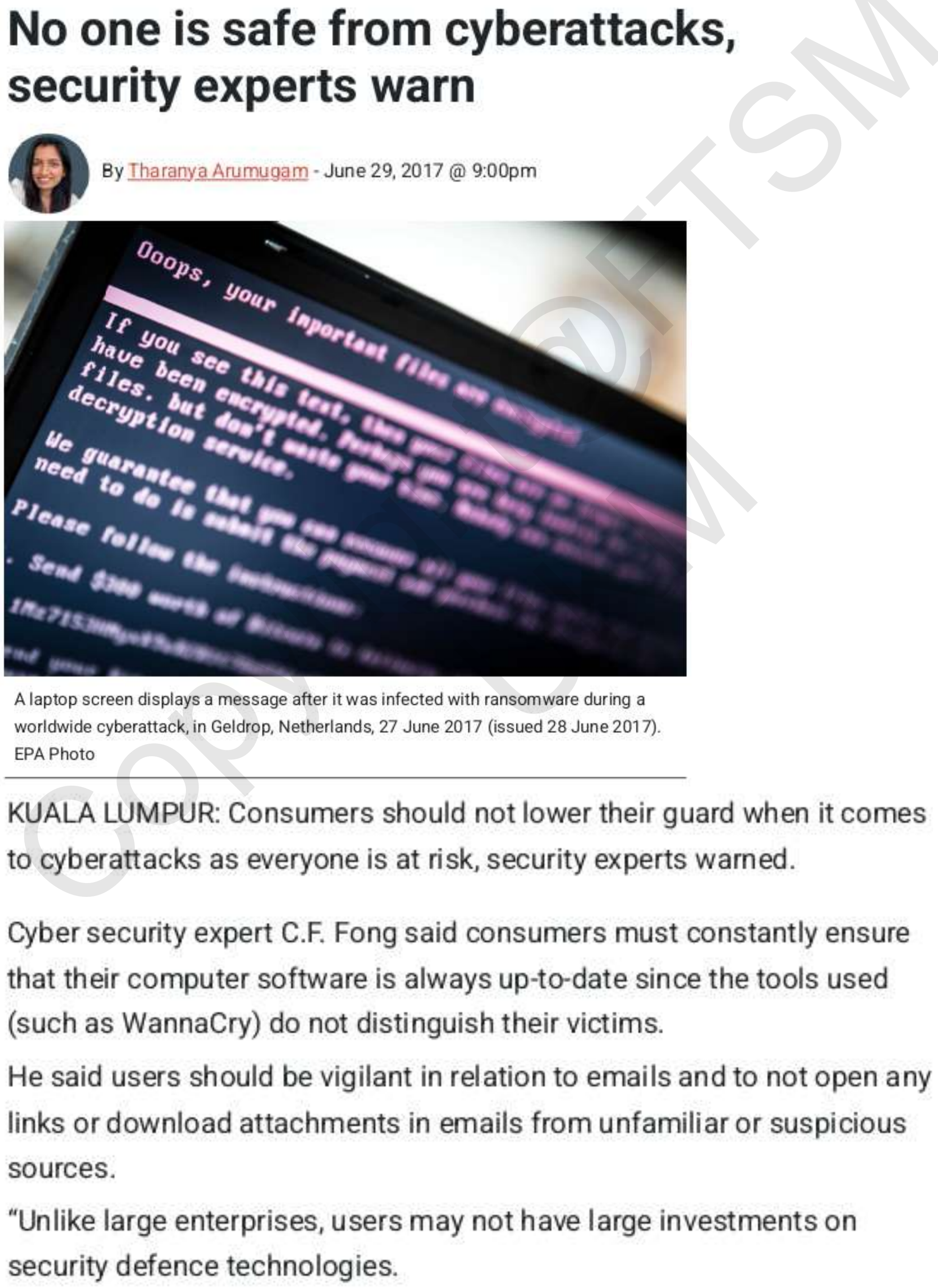
In computer security, a man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

"It's all about the timing – how much time is delayed until the actual supplier issues the real invoice," he said.

Tharanya Arumugam. (2017, Jun 29). No one is safe from cyber attacks, security experts warn. *New Straits Times*

Pautan:
https://www.nst.com.my/news/nation/2017/06/253054/no-one-safe-cyberattacks-security-experts-warn

Tangkapan layar:



Ooops, your important files are encrypted.
If you see this text, then your files are no longer
have been encrypted. Perhaps you are busy looking
files, but don't waste your time. Nobody can
decryption service.
We guarantee that you can recover all your files
need to do is submit the payment and purchase
Please follow the instructions:
Send $300 worth of Bitcoin to following

No one is safe from cyberattacks, security experts warn

By Tharanya Arumugam - June 29, 2017 @ 9:00pm

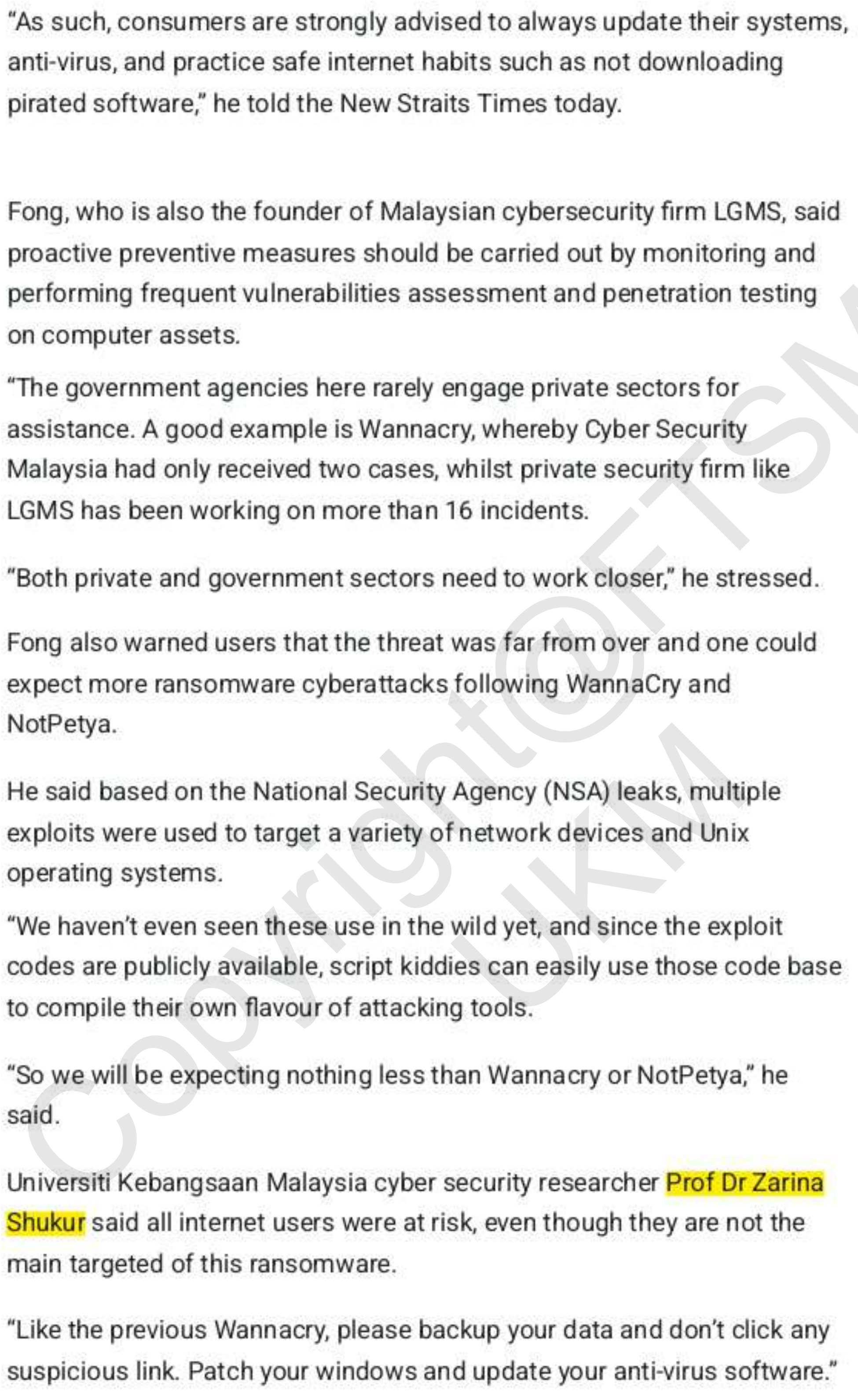
A laptop screen displays a message after it was infected with ransomware during a worldwide cyberattack, in Geldrop, Netherlands, 27 June 2017 (issued 28 June 2017). EPA Photo

KUALA LUMPUR: Consumers should not lower their guard when it comes to cyberattacks as everyone is at risk, security experts warned.

Cyber security expert C.F. Fong said consumers must constantly ensure that their computer software is always up-to-date since the tools used (such as WannaCry) do not distinguish their victims.

He said users should be vigilant in relation to emails and to not open any links or download attachments in emails from unfamiliar or suspicious sources.

"Unlike large enterprises, users may not have large investments on security defence technologies.



"As such, consumers are strongly advised to always update their systems, anti-virus, and practice safe internet habits such as not downloading pirated software," he told the New Straits Times today.

Fong, who is also the founder of Malaysian cybersecurity firm LGMS, said proactive preventive measures should be carried out by monitoring and performing frequent vulnerabilities assessment and penetration testing on computer assets.

"The government agencies here rarely engage private sectors for assistance. A good example is Wannacry, whereby Cyber Security Malaysia had only received two cases, whilst private security firm like LGMS has been working on more than 16 incidents.

"Both private and government sectors need to work closer," he stressed.

Fong also warned users that the threat was far from over and one could expect more ransomware cyberattacks following WannaCry and NotPetya.

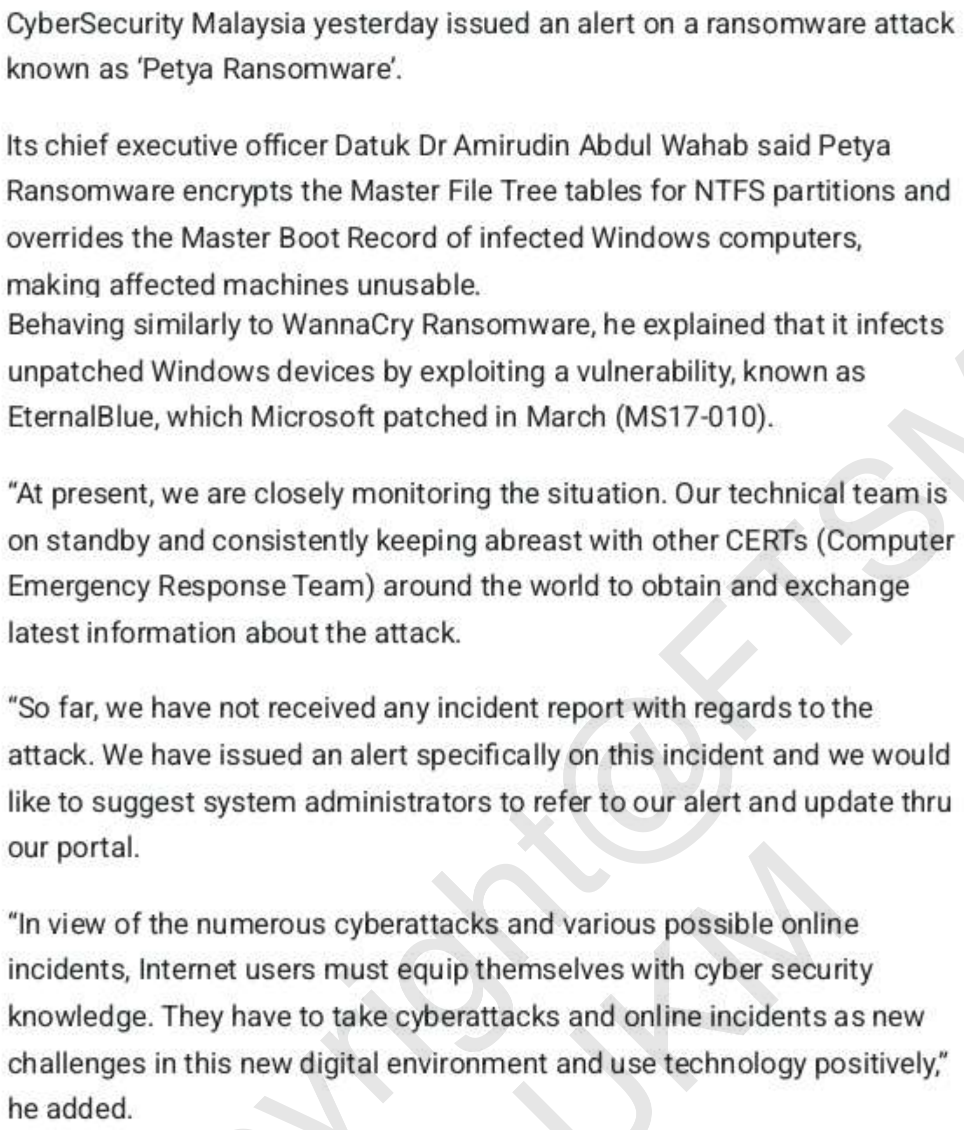
He said based on the National Security Agency (NSA) leaks, multiple exploits were used to target a variety of network devices and Unix operating systems.

"We haven't even seen these use in the wild yet, and since the exploit codes are publicly available, script kiddies can easily use those code base to compile their own flavour of attacking tools.

"So we will be expecting nothing less than Wannacry or NotPetya," he said.

Universiti Kebangsaan Malaysia cyber security researcher Prof Dr Zarina Shukur said all internet users were at risk, even though they are not the main targeted of this ransomware.

"Like the previous Wannacry, please backup your data and don't click any suspicious link. Patch your windows and update your anti-virus software."



CyberSecurity Malaysia yesterday issued an alert on a ransomware attack known as 'Petya Ransomware'.

Its chief executive officer Datuk Dr Amirudin Abdul Wahab said Petya Ransomware encrypts the Master File Tree tables for NTFS partitions and overrides the Master Boot Record of infected Windows computers, making affected machines unusable.

Behaving similarly to WannaCry Ransomware, he explained that it infects unpatched Windows devices by exploiting a vulnerability, known as EternalBlue, which Microsoft patched in March (MS17-010).

"At present, we are closely monitoring the situation. Our technical team is on standby and consistently keeping abreast with other CERTs (Computer Emergency Response Team) around the world to obtain and exchange latest information about the attack.

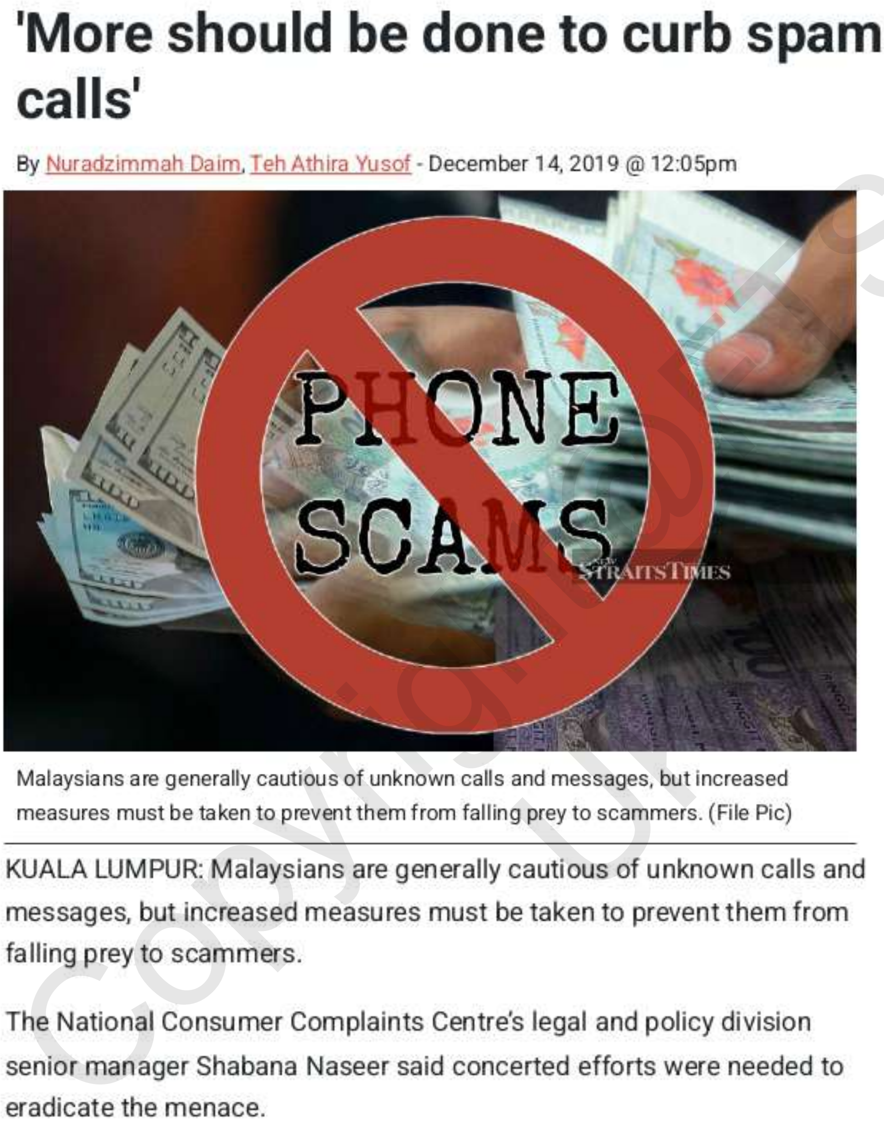
"So far, we have not received any incident report with regards to the attack. We have issued an alert specifically on this incident and we would like to suggest system administrators to refer to our alert and update thru our portal.

"In view of the numerous cyberattacks and various possible online incidents, Internet users must equip themselves with cyber security knowledge. They have to take cyberattacks and online incidents as new challenges in this new digital environment and use technology positively," he added.

Nuradzimmah Daim & Teh Athira Yusof. (2019, Dec 14). More should be done to curb spam calls. *New Straits Times*

Pautan:
https://www.nst.com.my/news/nation/2019/12/547738/more-should-be-done-curb-spam-calls

Tangkapan layar:



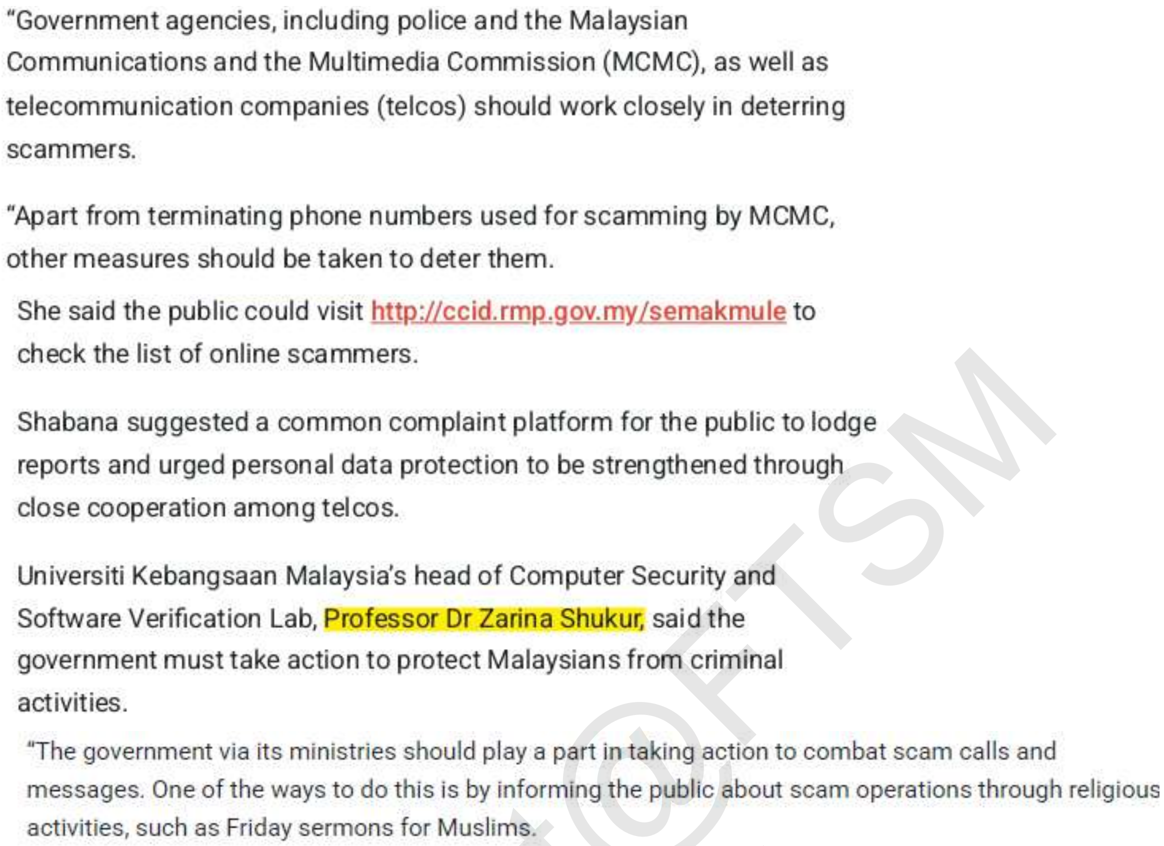
'More should be done to curb spam calls'

By Nuradzimmah Daim, Teh Athira Yusof - December 14, 2019 @ 12:05pm

Malaysians are generally cautious of unknown calls and messages, but increased measures must be taken to prevent them from falling prey to scammers. (File Pic)

KUALA LUMPUR: Malaysians are generally cautious of unknown calls and messages, but increased measures must be taken to prevent them from falling prey to scammers.

The National Consumer Complaints Centre's legal and policy division senior manager Shabana Naseer said concerted efforts were needed to eradicate the menace.



"Government agencies, including police and the Malaysian Communications and the Multimedia Commission (MCMC), as well as telecommunication companies (telcos) should work closely in deterring scammers.

"Apart from terminating phone numbers used for scamming by MCMC, other measures should be taken to deter them.

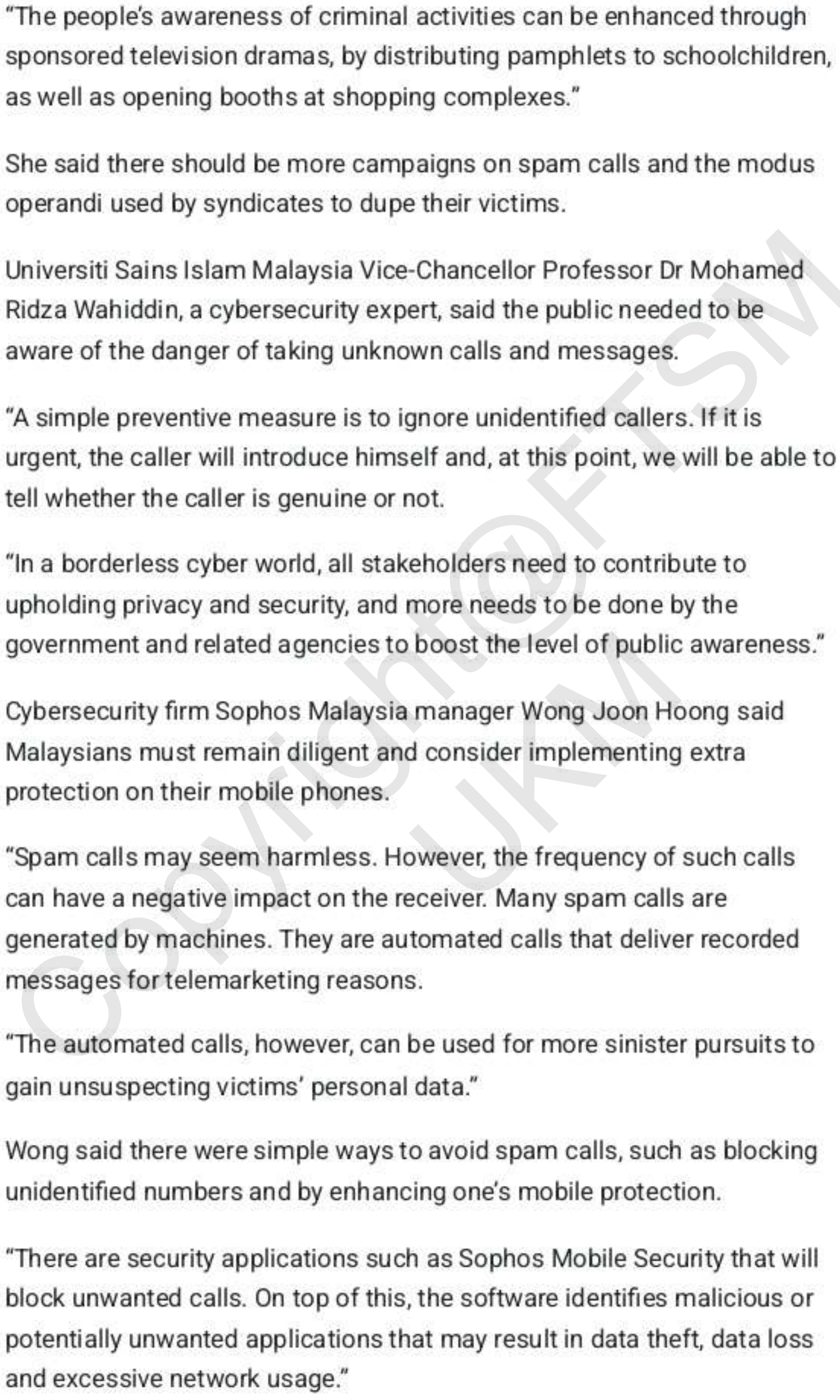
She said the public could visit http://ccid.rmp.gov.my/semakmule to check the list of online scammers.

Shabana suggested a common complaint platform for the public to lodge reports and urged personal data protection to be strengthened through close cooperation among telcos.

Universiti Kebangsaan Malaysia's head of Computer Security and Software Verification Lab, Professor Dr Zarina Shukur, said the government must take action to protect Malaysians from criminal activities.

"The government via its ministries should play a part in taking action to combat scam calls and messages. One of the ways to do this is by informing the public about scam operations through religious activities, such as Friday sermons for Muslims.

Shabana Naseer



“The people's awareness of criminal activities can be enhanced through sponsored television dramas, by distributing pamphlets to schoolchildren, as well as opening booths at shopping complexes.”

She said there should be more campaigns on spam calls and the modus operandi used by syndicates to dupe their victims.

Universiti Sains Islam Malaysia Vice-Chancellor Professor Dr Mohamed Ridza Wahiddin, a cybersecurity expert, said the public needed to be aware of the danger of taking unknown calls and messages.

“A simple preventive measure is to ignore unidentified callers. If it is urgent, the caller will introduce himself and, at this point, we will be able to tell whether the caller is genuine or not.

“In a borderless cyber world, all stakeholders need to contribute to upholding privacy and security, and more needs to be done by the government and related agencies to boost the level of public awareness.”

Cybersecurity firm Sophos Malaysia manager Wong Joon Hoong said Malaysians must remain diligent and consider implementing extra protection on their mobile phones.

“Spam calls may seem harmless. However, the frequency of such calls can have a negative impact on the receiver. Many spam calls are generated by machines. They are automated calls that deliver recorded messages for telemarketing reasons.

“The automated calls, however, can be used for more sinister pursuits to gain unsuspecting victims' personal data.”

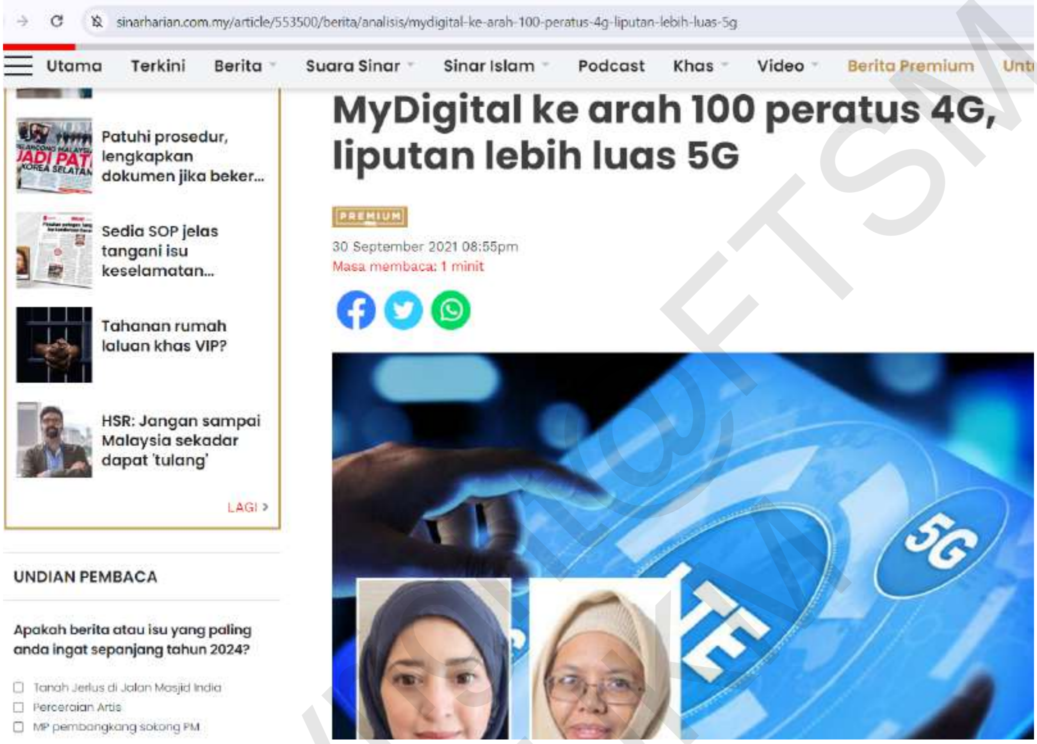
Wong said there were simple ways to avoid spam calls, such as blocking unidentified numbers and by enhancing one's mobile protection.

“There are security applications such as Sophos Mobile Security that will block unwanted calls. On top of this, the software identifies malicious or potentially unwanted applications that may result in data theft, data loss and excessive network usage.”

Nurul Nabila Ahmad Halimy. (2021, Sep 30). MyDigital ke arah 100 peratus 4G, liputan lebih luas 5G. *SinarHarian*

Pautan:
https://www.sinarharian.com.my/article/553500/berita/analisis/mydigital-ke-arah-100-peratus-4g-liputan-lebih-luas-5g#google_vignette

Tangkapan layar:
(Perlu langgan secara premium untuk dapatkan berita penuh)


sinarharian.com.my/article/553500/berita/analisis/mydigital-ke-arah-100-peratus-4g-liputan-lebih-luas-5g
Utama
Terkini
Berita
Suara Sinar
Sinar Islam
Podcast
Khas
Video
Berita Premium
Unt
PREMIUM
5G

Patuhi prosedur, lengkapkan dokumen jika beker...

Sedia SOP jelas tangani isu keselamatan...

Tahanan rumah laluan khas VIP?

HSR: Jangan sampai Malaysia sekadar dapat 'tulang'

LAGI >

UNDIAN PEMBACA

Apakah berita atau isu yang paling anda ingat sepanjang tahun 2024?

☐ Tanah Jerlus di Jalan Masjid India
☐ Perceraian Artis
☐ MP pembangkang sokong PM

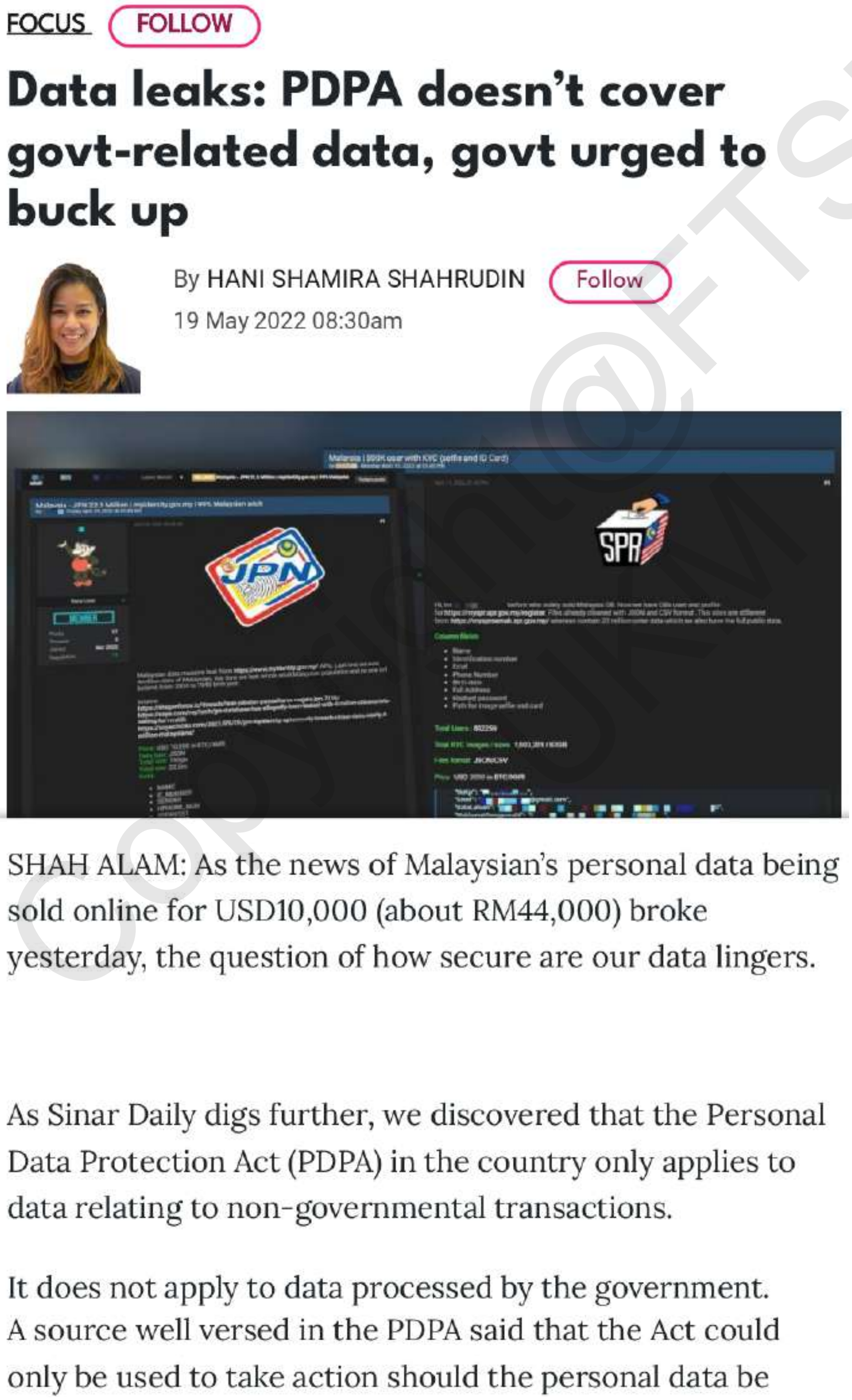
MyDigital ke arah 100 peratus 4G, liputan lebih luas 5G

30 September 2021 08:55pm
Masa membaca: 1 minit

Hani Shamira Shahrudin. (2022, May 19). Data leaks: PDPA doesn’t cover govt-related data, govt urged to buck up. *SinarDaily*

Pautan:
https://www.sinardaily.my/article/174409/focus/national/data-leaks-pdpa-doesnrsquot-cover-govt-related-data-govt-urged-to-buck-up

Tangkapan layar:



Data leaks: PDPA doesn’t cover govt-related data, govt urged to buck up

By HANI SHAMIRA SHAHRUDIN

19 May 2022 08:30am

SHAH ALAM: As the news of Malaysian’s personal data being sold online for USD10,000 (about RM44,000) broke yesterday, the question of how secure are our data lingers.

As Sinar Daily digs further, we discovered that the Personal Data Protection Act (PDPA) in the country only applies to data relating to non-governmental transactions.

It does not apply to data processed by the government.
A source well versed in the PDPA said that the Act could only be used to take action should the personal data be

government servers and systems, could be likened to the government exposing the public to actual harm.
Since PDPA does not include data managed by government entities, she said citizens have no way of demanding accountability for the harms that occurred due to their failure to protect the data.

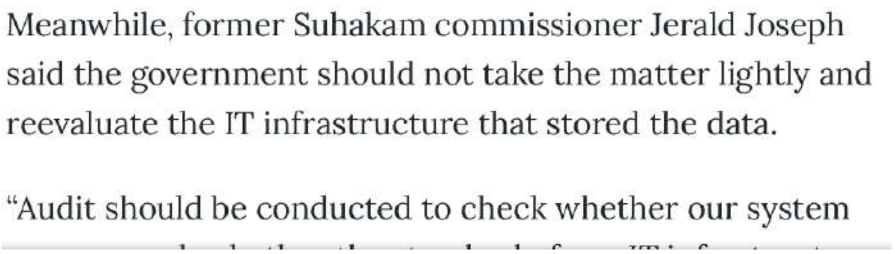
“In the PDPA, we have the right to be notified if there has been a breach of data. But because the law doesn’t apply to government entities, they don’t have an obligation to notify us of the leak.
“The way the government should treat our data should be the same way that they treat us as citizens: protect our general welfare and wellbeing, including our fundamental human right to privacy,” she told Sinar Daily.

When asked how to stop the data breaches, Maryam said technological problems were best solved with technological solutions but the government must first recognise that individuals were the sole owners of their own data

“The ownership of data should not be with any third party, public or private entities.
“Secondly, there should be a way for citizens to transparently protect our data at the click of a button. Provide options because there are currently no technological protection solutions.

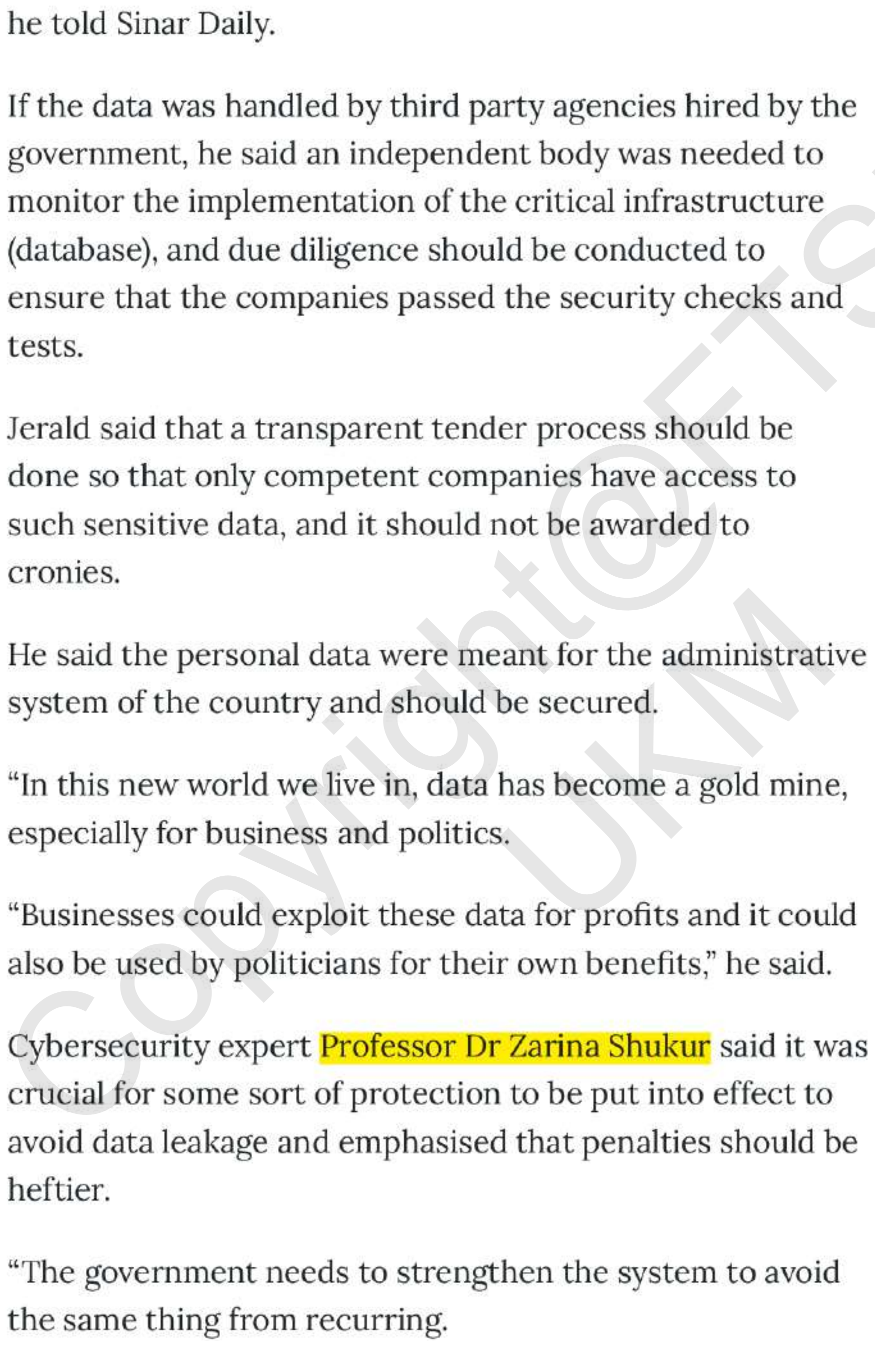
“This would be the long-term solution. Laws and legislation don’t protect us enough in a fast-paced digital world,” she added.

Maryam said there should be a legislation stating that technology solutions providers and administrators must protect users’ privacy by design.



Meanwhile, former Suhakam commissioner Jerald Joseph said the government should not take the matter lightly and reevaluate the IT infrastructure that stored the data.

"Audit should be conducted to check whether our system



he told Sinar Daily.

If the data was handled by third party agencies hired by the government, he said an independent body was needed to monitor the implementation of the critical infrastructure (database), and due diligence should be conducted to ensure that the companies passed the security checks and tests.

Jerald said that a transparent tender process should be done so that only competent companies have access to such sensitive data, and it should not be awarded to cronies.

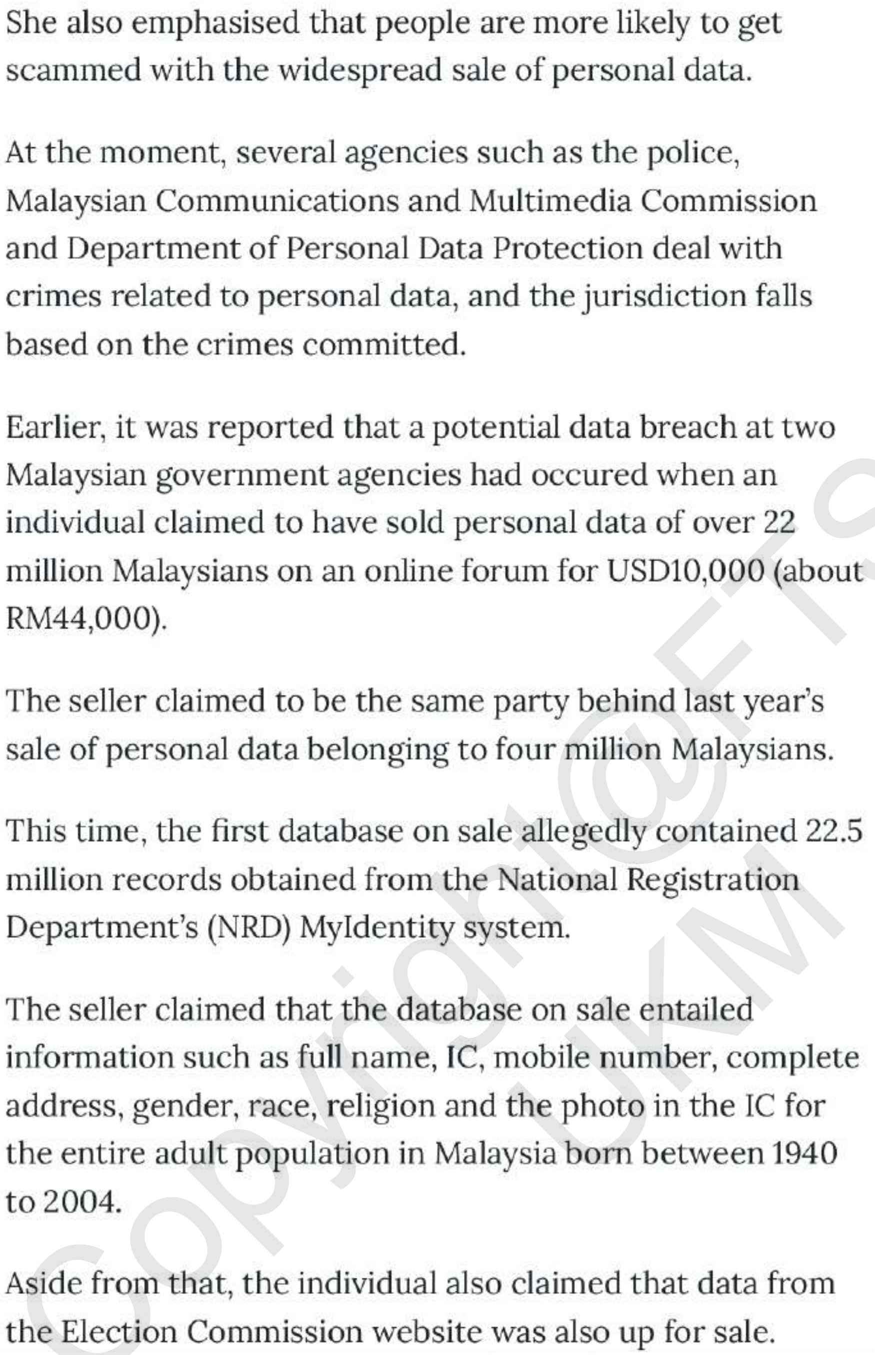
He said the personal data were meant for the administrative system of the country and should be secured.

"In this new world we live in, data has become a gold mine, especially for business and politics.

"Businesses could exploit these data for profits and it could also be used by politicians for their own benefits," he said.

Cybersecurity expert Professor Dr Zarina Shukur said it was crucial for some sort of protection to be put into effect to avoid data leakage and emphasised that penalties should be heftier.

"The government needs to strengthen the system to avoid the same thing from recurring.



She also emphasised that people are more likely to get scammed with the widespread sale of personal data.

At the moment, several agencies such as the police, Malaysian Communications and Multimedia Commission and Department of Personal Data Protection deal with crimes related to personal data, and the jurisdiction falls based on the crimes committed.

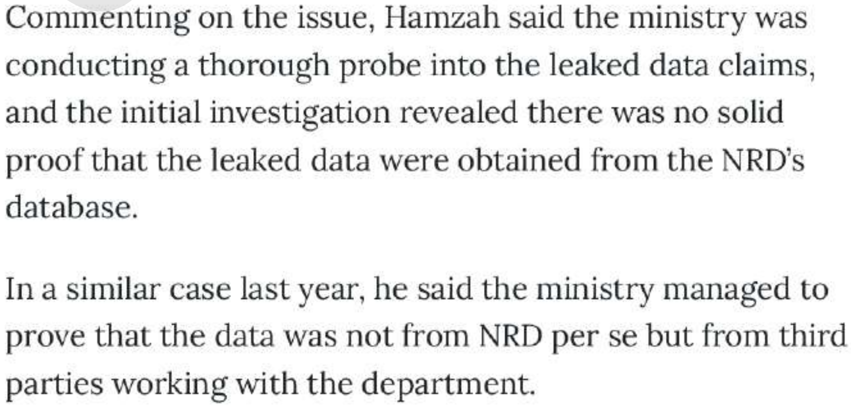
Earlier, it was reported that a potential data breach at two Malaysian government agencies had occured when an individual claimed to have sold personal data of over 22 million Malaysians on an online forum for USD10,000 (about RM44,000).

The seller claimed to be the same party behind last year's sale of personal data belonging to four million Malaysians.

This time, the first database on sale allegedly contained 22.5 million records obtained from the National Registration Department's (NRD) MyIdentity system.

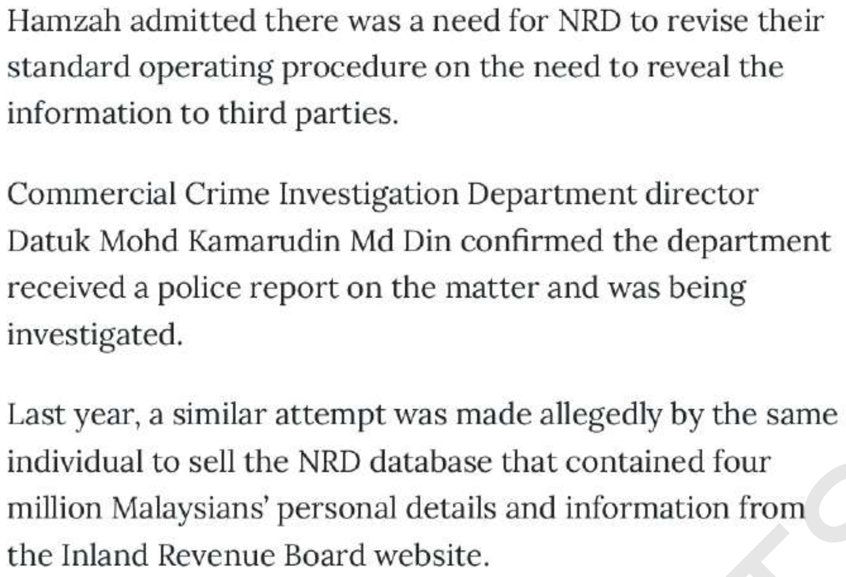
The seller claimed that the database on sale entailed information such as full name, IC, mobile number, complete address, gender, race, religion and the photo in the IC for the entire adult population in Malaysia born between 1940 to 2004.

Aside from that, the individual also claimed that data from the Election Commission website was also up for sale.



Commenting on the issue, Hamzah said the ministry was conducting a thorough probe into the leaked data claims, and the initial investigation revealed there was no solid proof that the leaked data were obtained from the NRD's database.

In a similar case last year, he said the ministry managed to prove that the data was not from NRD per se but from third parties working with the department.



Hamzah admitted there was a need for NRD to revise their standard operating procedure on the need to reveal the information to third parties.

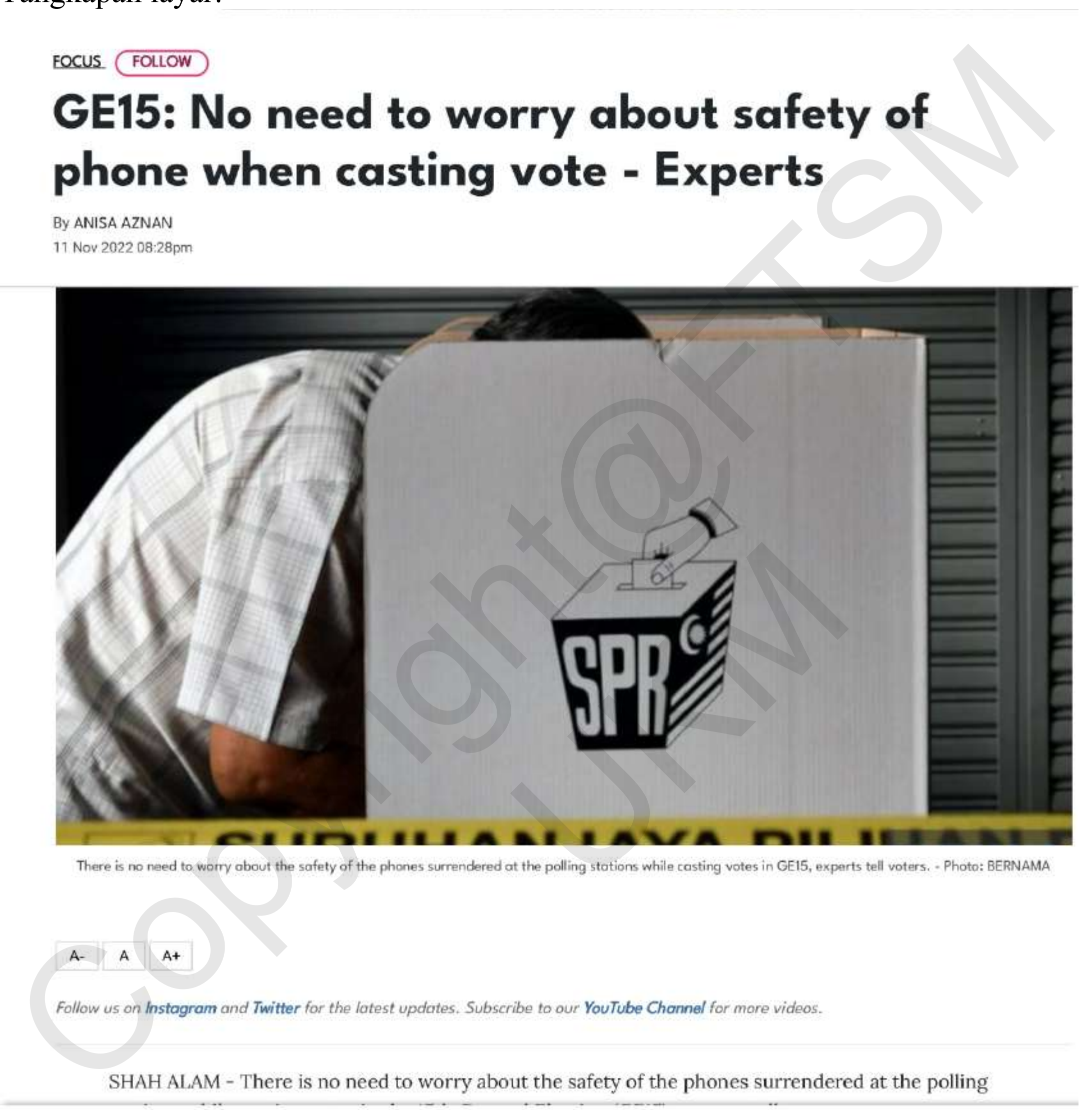
Commercial Crime Investigation Department director Datuk Mohd Kamarudin Md Din confirmed the department received a police report on the matter and was being investigated.

Last year, a similar attempt was made allegedly by the same individual to sell the NRD database that contained four million Malaysians' personal details and information from the Inland Revenue Board website.

Anisa Aznan. (2022 Nov 11). GE15: No need to worry about safety of phone when casting vote – Experts. *SinarDaily*

Pautan:
https://www.sinardaily.my/article/183764/focus/national/ge15-no-need-to-worry-about-safety-of-phone-when-casting-vote---experts

Tangkapan layar:



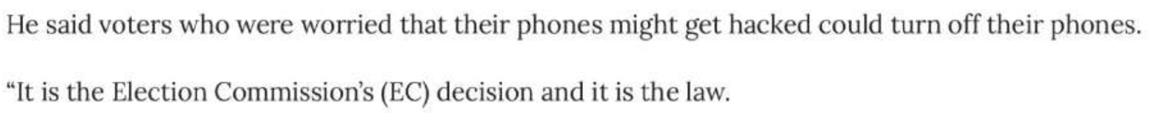
GE15: No need to worry about safety of phone when casting vote - Experts

By ANISA AZNAN
11 Nov 2022 08:28pm

There is no need to worry about the safety of the phones surrendered at the polling stations while casting votes in GE15, experts tell voters. - Photo: BERNAMA

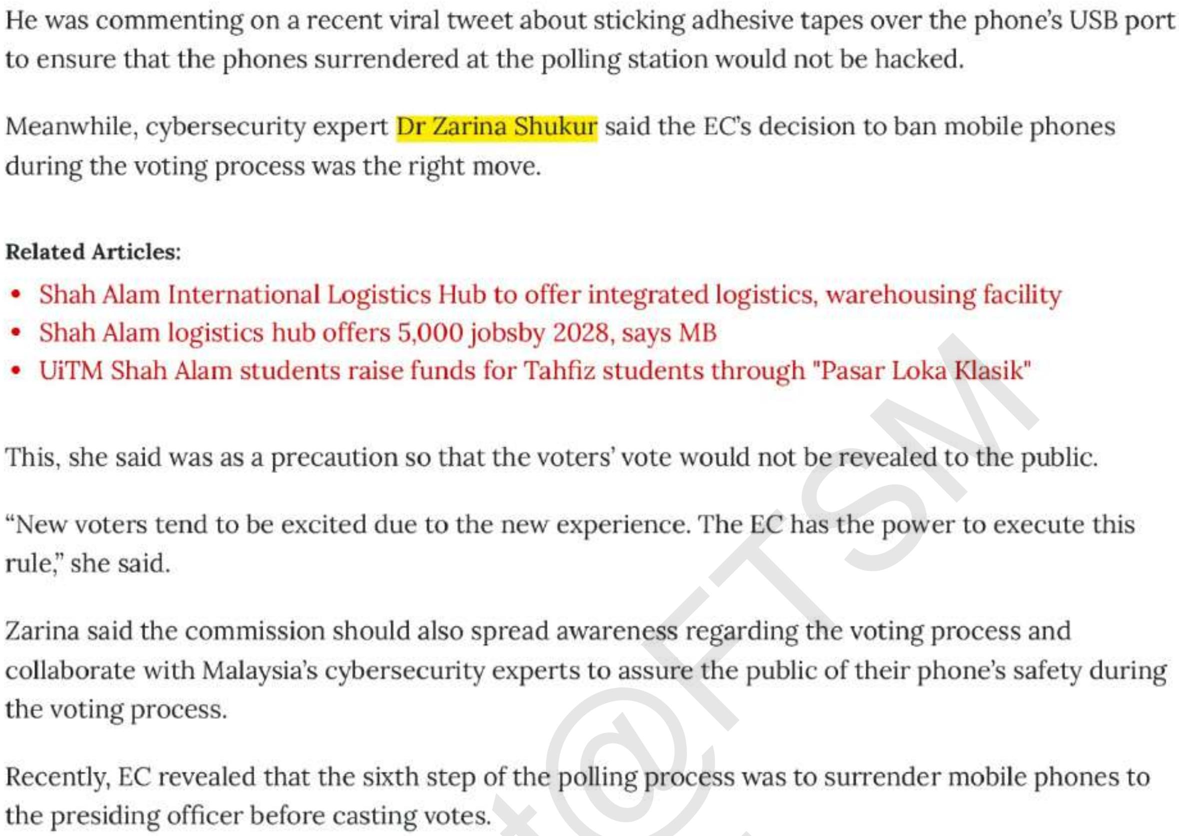
Follow us on Instagram and Twitter for the latest updates. Subscribe to our YouTube Channel for more videos.

SHAH ALAM - There is no need to worry about the safety of the phones surrendered at the polling



He said voters who were worried that their phones might get hacked could turn off their phones.

"It is the Election Commission's (EC) decision and it is the law.



He was commenting on a recent viral tweet about sticking adhesive tapes over the phone's USB port to ensure that the phones surrendered at the polling station would not be hacked.

Meanwhile, cybersecurity expert Dr Zarina Shukur said the EC's decision to ban mobile phones during the voting process was the right move.

Related Articles:

- Shah Alam International Logistics Hub to offer integrated logistics, warehousing facility
- Shah Alam logistics hub offers 5,000 jobsby 2028, says MB
- UiTM Shah Alam students raise funds for Tahfiz students through "Pasar Loka Klasik"

This, she said was as a precaution so that the voters' vote would not be revealed to the public.

"New voters tend to be excited due to the new experience. The EC has the power to execute this rule," she said.

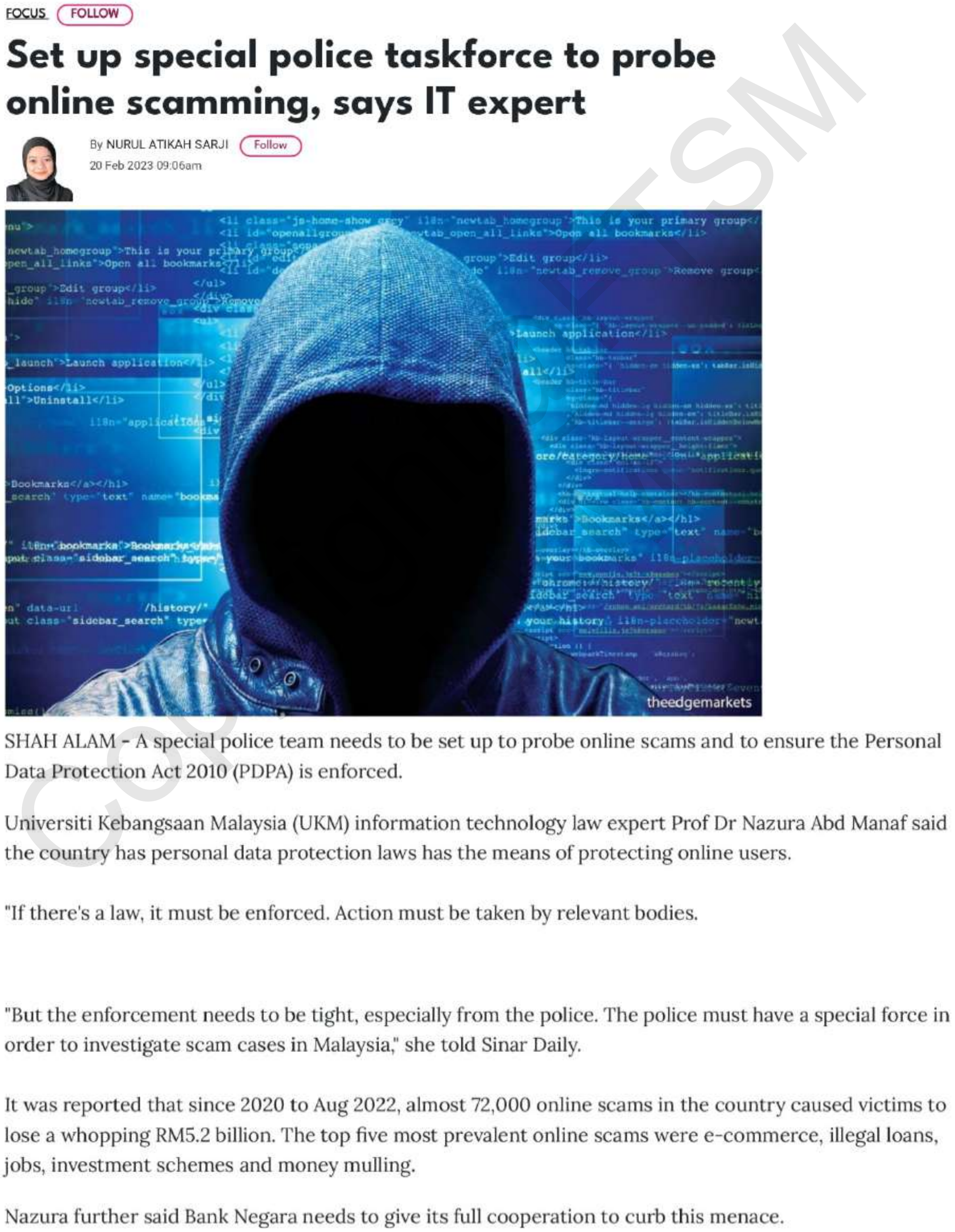
Zarina said the commission should also spread awareness regarding the voting process and collaborate with Malaysia's cybersecurity experts to assure the public of their phone's safety during the voting process.

Recently, EC revealed that the sixth step of the polling process was to surrender mobile phones to the presiding officer before casting votes.

Nurul Atikah Sarji. (2023, Feb 20). Set up special police taskforce to probe online scamming, says IT expert. *SinarDaily*

Pautan:
https://www.sinardaily.my/article/190551/focus/national/set-up-special-police-taskforce-to-probe-online-scamming-says-it-expert

Tangkapan layar:



Set up special police taskforce to probe online scamming, says IT expert

By NURUL ATIKAH SARJI

20 Feb 2023 09:06am

SHAH ALAM - A special police team needs to be set up to probe online scams and to ensure the Personal Data Protection Act 2010 (PDPA) is enforced.

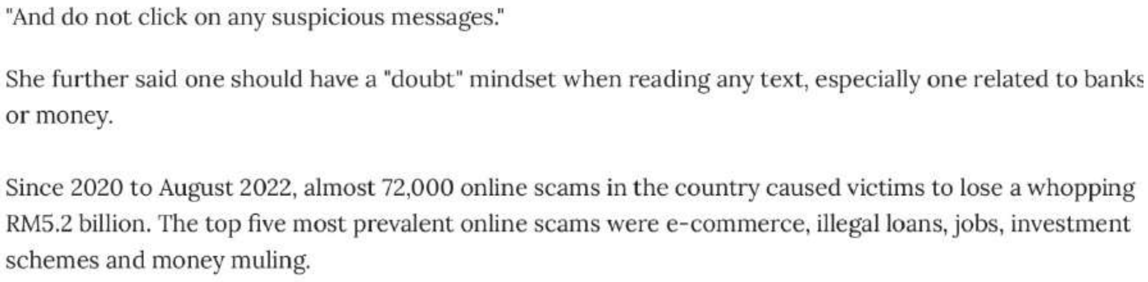
Universiti Kebangsaan Malaysia (UKM) information technology law expert Prof Dr Nazura Abd Manaf said the country has personal data protection laws has the means of protecting online users.

"If there's a law, it must be enforced. Action must be taken by relevant bodies.

"But the enforcement needs to be tight, especially from the police. The police must have a special force in order to investigate scam cases in Malaysia," she told Sinar Daily.

It was reported that since 2020 to Aug 2022, almost 72,000 online scams in the country caused victims to lose a whopping RM5.2 billion. The top five most prevalent online scams were e-commerce, illegal loans, jobs, investment schemes and money mulling.

Nazura further said Bank Negara needs to give its full cooperation to curb this menace.



"And do not click on any suspicious messages."

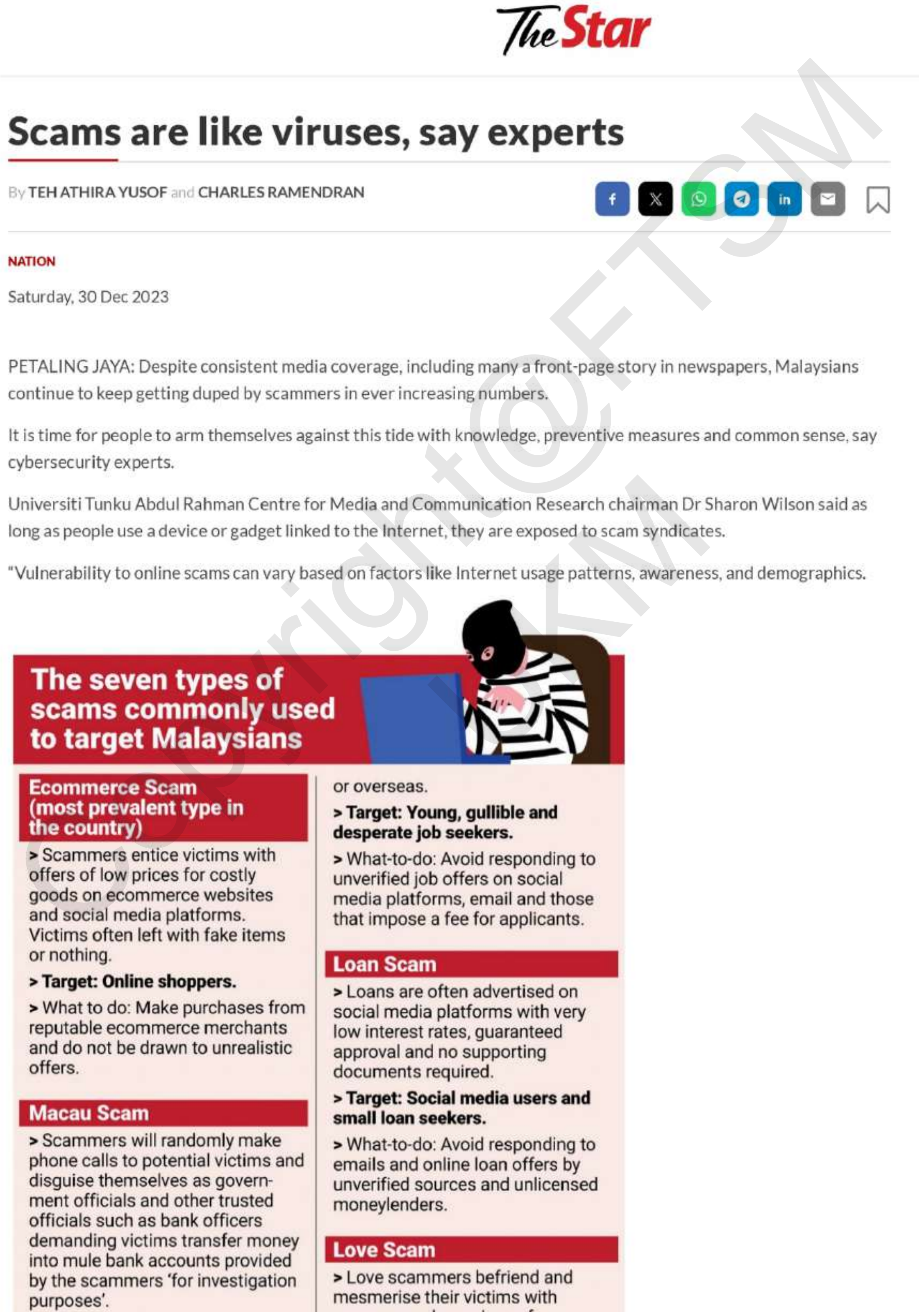
She further said one should have a "doubt" mindset when reading any text, especially one related to banks or money.

Since 2020 to August 2022, almost 72,000 online scams in the country caused victims to lose a whopping RM5.2 billion. The top five most prevalent online scams were e-commerce, illegal loans, jobs, investment schemes and money muling.

Teh Athira Yusof & Charles Ramendran. (2023, Dec 30). Scams are like viruses, say experts. *The Star*

Pautan:
https://www.thestar.com.my/news/nation/2023/12/30/scams-are-like-viruses-say-experts

Tangkapan layar:



The Star

Scams are like viruses, say experts

By TEH ATHIRA YUSOF and CHARLES RAMENDRAN

NATION

Saturday, 30 Dec 2023

PETALING JAYA: Despite consistent media coverage, including many a front-page story in newspapers, Malaysians continue to keep getting duped by scammers in ever increasing numbers.

It is time for people to arm themselves against this tide with knowledge, preventive measures and common sense, say cybersecurity experts.

Universiti Tunku Abdul Rahman Centre for Media and Communication Research chairman Dr Sharon Wilson said as long as people use a device or gadget linked to the Internet, they are exposed to scam syndicates.

"Vulnerability to online scams can vary based on factors like Internet usage patterns, awareness, and demographics.

The seven types of scams commonly used to target Malaysians

Ecommerce Scam (most prevalent type in the country)

> Scammers entice victims with offers of low prices for costly goods on ecommerce websites and social media platforms. Victims often left with fake items or nothing.

> **Target: Online shoppers.**

> What to do: Make purchases from reputable ecommerce merchants and do not be drawn to unrealistic offers.

Macau Scam

> Scammers will randomly make phone calls to potential victims and disguise themselves as government officials and other trusted officials such as bank officers demanding victims transfer money into mule bank accounts provided by the scammers 'for investigation purposes'.

or overseas.

> **Target: Young, gullible and desperate job seekers.**

> What-to-do: Avoid responding to unverified job offers on social media platforms, email and those that impose a fee for applicants.

Loan Scam

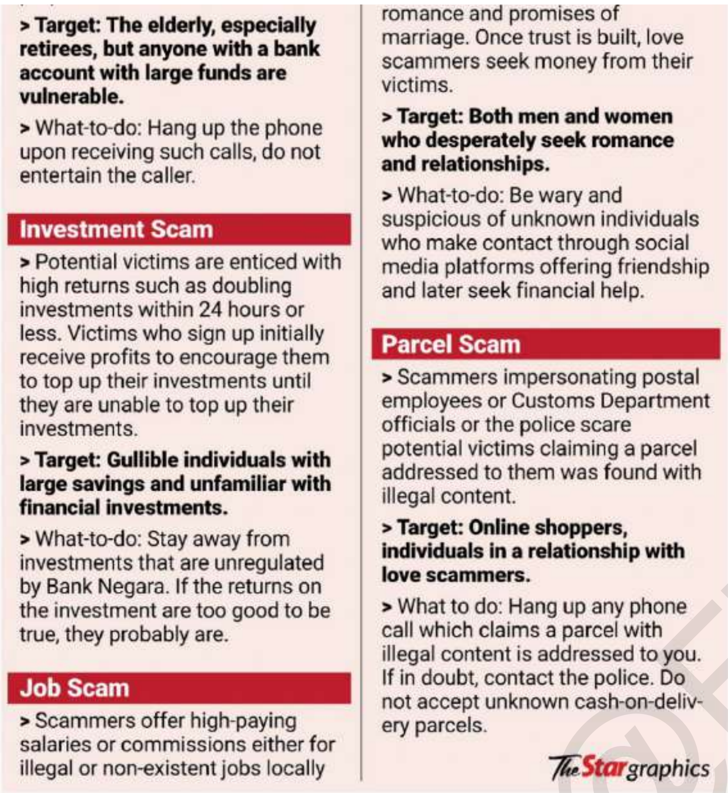
> Loans are often advertised on social media platforms with very low interest rates, guaranteed approval and no supporting documents required.

> **Target: Social media users and small loan seekers.**

> What-to-do: Avoid responding to emails and online loan offers by unverified sources and unlicensed moneylenders.

Love Scam

> Love scammers befriend and mesmerise their victims with



> **Target: The elderly, especially retirees, but anyone with a bank account with large funds are vulnerable.**

> What-to-do: Hang up the phone upon receiving such calls, do not entertain the caller.

Investment Scam

> Potential victims are enticed with high returns such as doubling investments within 24 hours or less. Victims who sign up initially receive profits to encourage them to top up their investments until they are unable to top up their investments.

> **Target: Gullible individuals with large savings and unfamiliar with financial investments.**

> What-to-do: Stay away from investments that are unregulated by Bank Negara. If the returns on the investment are too good to be true, they probably are.

Job Scam

> Scammers offer high-paying salaries or commissions either for illegal or non-existent jobs locally

romance and promises of marriage. Once trust is built, love scammers seek money from their victims.

> **Target: Both men and women who desperately seek romance and relationships.**

> What-to-do: Be wary and suspicious of unknown individuals who make contact through social media platforms offering friendship and later seek financial help.

Parcel Scam

> Scammers impersonating postal employees or Customs Department officials or the police scare potential victims claiming a parcel addressed to them was found with illegal content.

> **Target: Online shoppers, individuals in a relationship with love scammers.**

> What to do: Hang up any phone call which claims a parcel with illegal content is addressed to you. If in doubt, contact the police. Do not accept unknown cash-on-delivery parcels.

TheStargraphics

"Individuals of all ages should stay informed on online security practices to reduce the risk of falling victim to scams," she said.

As of Nov 30, the reported losses via online crime in the country this year had reached more than RM177mil. Of these, 8,213 reports were lodged with the authorities while 529 bank accounts – holding a combined value of nearly RM66mil – were frozen.

According to an Ipsos Malaysia survey, more than 50% of victims in the country did not seek help from the authorities after being scammed.

Wilson said there are several types of scam tactics that can be used to target the different age groups.

"Perhaps Gen Z may be vulnerable to job scams and parcel scams, while senior citizens may be vulnerable to investment scams – but no one is spared," she added.

Universiti Kebangsaan Malaysia's (UKM) Cyber Protection and Governance (CPG) Lab head Prof Dr Zarina Shukur said the people who are most at risk of getting scammed are the ones who often rely on technology for their financial transactions.

"Other people who are vulnerable to fraud are those who remain ignorant of the news and awareness raised by authorities on scam syndicates and their ways," she said.

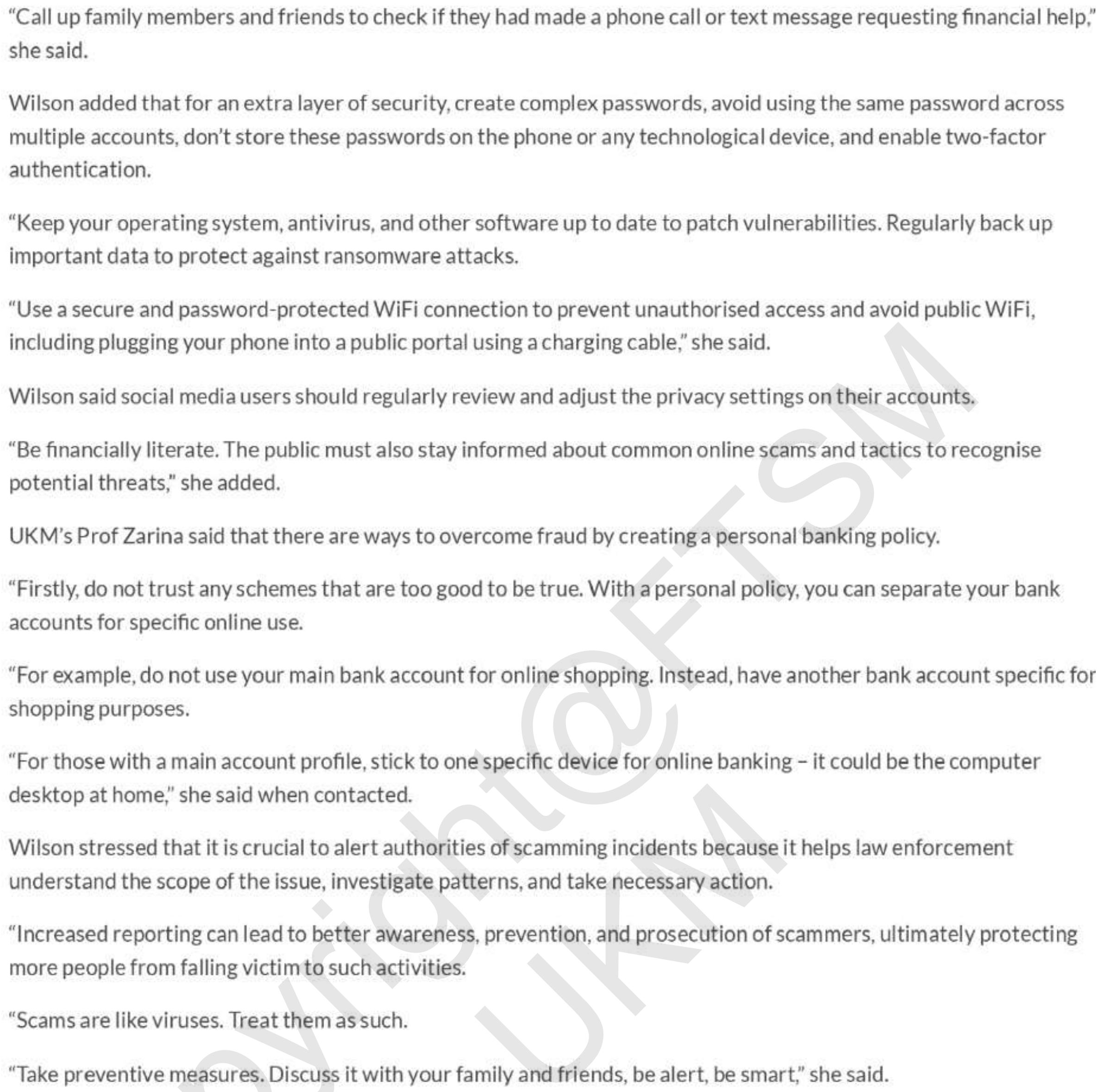
"There are also people in desperate need of financial assistance, causing them to be involved with these activities without much thought on the repercussions."

On ways to prevent getting scammed, Wilson advised users to question and verify any incoming requests for personal information and identify those seeking sensitive information.

Users should check the legitimacy of websites by checking the URL or weblink for spelling errors or unusual domain names, she said.

"Be cautious of emails or messages asking for personal or financial information, especially if they create a sense of urgency. Use trusted platforms and be cautious when making online transactions.

"If shopping online, ensure that the seller does not lure you out of the official shopping platform.



"Call up family members and friends to check if they had made a phone call or text message requesting financial help," she said.

Wilson added that for an extra layer of security, create complex passwords, avoid using the same password across multiple accounts, don't store these passwords on the phone or any technological device, and enable two-factor authentication.

"Keep your operating system, antivirus, and other software up to date to patch vulnerabilities. Regularly back up important data to protect against ransomware attacks.

"Use a secure and password-protected WiFi connection to prevent unauthorised access and avoid public WiFi, including plugging your phone into a public portal using a charging cable," she said.

Wilson said social media users should regularly review and adjust the privacy settings on their accounts.

"Be financially literate. The public must also stay informed about common online scams and tactics to recognise potential threats," she added.

UKM's Prof Zarina said that there are ways to overcome fraud by creating a personal banking policy.

"Firstly, do not trust any schemes that are too good to be true. With a personal policy, you can separate your bank accounts for specific online use.

"For example, do not use your main bank account for online shopping. Instead, have another bank account specific for shopping purposes.

"For those with a main account profile, stick to one specific device for online banking – it could be the computer desktop at home," she said when contacted.

Wilson stressed that it is crucial to alert authorities of scamming incidents because it helps law enforcement understand the scope of the issue, investigate patterns, and take necessary action.

"Increased reporting can lead to better awareness, prevention, and prosecution of scammers, ultimately protecting more people from falling victim to such activities.

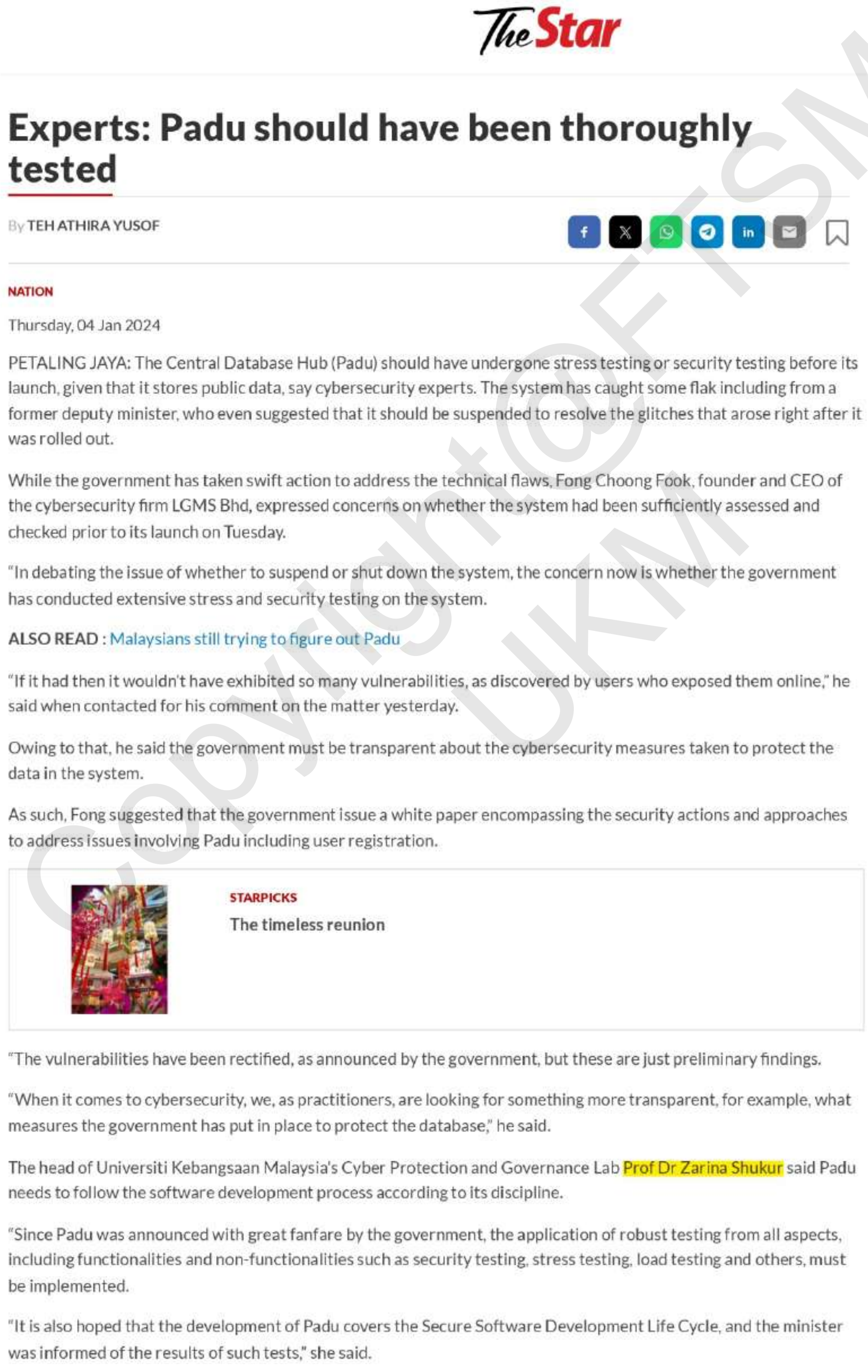
"Scams are like viruses. Treat them as such.

"Take preventive measures. Discuss it with your family and friends, be alert, be smart," she said.

Teh Athira Yusof. (2024, Jan 04). Padu should have been thoroughly tested. *The Star*

Pautan:
https://www.thestar.com.my/news/nation/2024/01/04/experts-padu-should-have-been-thoroughly-tested

Tangkapan layar:



The Star

Experts: Padu should have been thoroughly tested

By TEH ATHIRA YUSOF

NATION

Thursday, 04 Jan 2024

PETALING JAYA: The Central Database Hub (Padu) should have undergone stress testing or security testing before its launch, given that it stores public data, say cybersecurity experts. The system has caught some flak including from a former deputy minister, who even suggested that it should be suspended to resolve the glitches that arose right after it was rolled out.

While the government has taken swift action to address the technical flaws, Fong Choong Fook, founder and CEO of the cybersecurity firm LGMS Bhd, expressed concerns on whether the system had been sufficiently assessed and checked prior to its launch on Tuesday.

"In debating the issue of whether to suspend or shut down the system, the concern now is whether the government has conducted extensive stress and security testing on the system.

ALSO READ : Malaysians still trying to figure out Padu

"If it had then it wouldn't have exhibited so many vulnerabilities, as discovered by users who exposed them online," he said when contacted for his comment on the matter yesterday.

Owing to that, he said the government must be transparent about the cybersecurity measures taken to protect the data in the system.

As such, Fong suggested that the government issue a white paper encompassing the security actions and approaches to address issues involving Padu including user registration.

"The vulnerabilities have been rectified, as announced by the government, but these are just preliminary findings.

"When it comes to cybersecurity, we, as practitioners, are looking for something more transparent, for example, what measures the government has put in place to protect the database," he said.

The head of Universiti Kebangsaan Malaysia's Cyber Protection and Governance Lab Prof Dr Zarina Shukur said Padu needs to follow the software development process according to its discipline.

"Since Padu was announced with great fanfare by the government, the application of robust testing from all aspects, including functionalities and non-functionalities such as security testing, stress testing, load testing and others, must be implemented.

"It is also hoped that the development of Padu covers the Secure Software Development Life Cycle, and the minister was informed of the results of such tests," she said.

Prof Zarina said having a third party consisting of cybersecurity specialists to provide expert opinions during the testing of the system before Padu was launched could have provided better insights into how it would operate.

The launch of Padu, she added, should have been done on a smaller scale through government agencies.

"For example, it could have been done involving government employees according to agencies first before involving all Malaysians.

"From a content point of view, it is stated that the data is combined with other agencies. However, it appears that the data is almost 'empty' without content."

Having said that, Prof Zarina commended the government's efforts in developing Padu.
"Like any other applications, it always goes through the 'upgrading' process," she said.

However, she feels that Padu should be suspended until thorough testing by several parties.

Meanwhile, Fong also raised concerns about how the government is planning to consolidate and protect the database using Padu because "using a centralised database to store data from various sources is kind of old-fashioned".

"The modern way of accessing data from different data points is using an API gateway, like what is being done by the Singapore government," he said, adding that an API gateway allows the government to access various agencies and get data in real time.

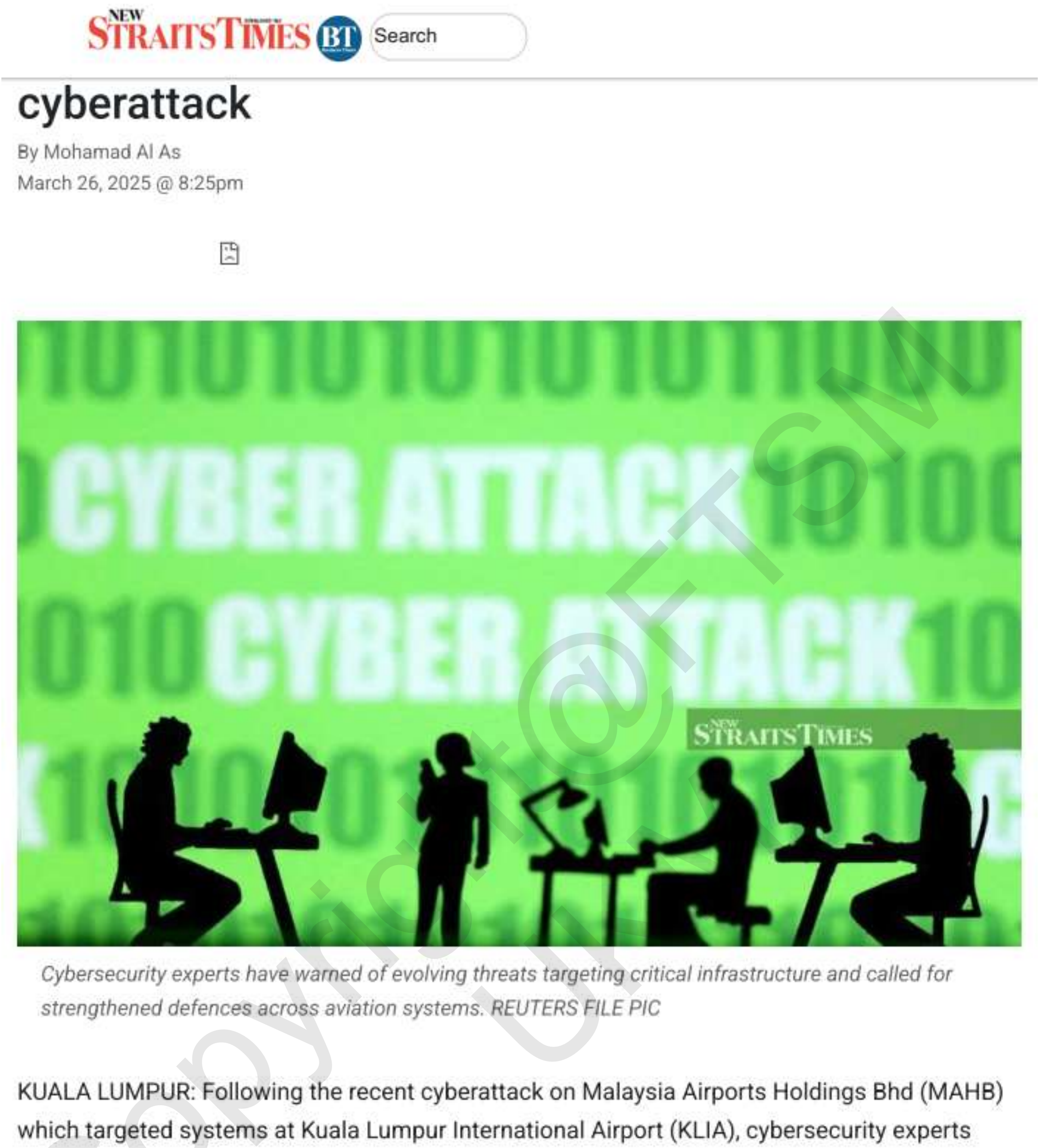
Fong added that if Padu is dependent on a single repository (database), then it's concerning that one single data storage carries all sensitive personal information.

"To be fair, the government has yet to publish anything in-depth about the current infrastructure, so we have no idea whether the government has built up a centralised database that receives data from different agencies, or it could be a hybrid database plus API gateway," he said.

Mohamad Al As. (2025, Mac 26). Experts warn cyber risks following KLIA cyberattack. *New Straits Time.*

Pautan:
https://www.nst.com.my/amp/news/nation/2025/03/1193686/experts-warn-cyber-risks-following-klia-cyberattack

Tangkapan layar:

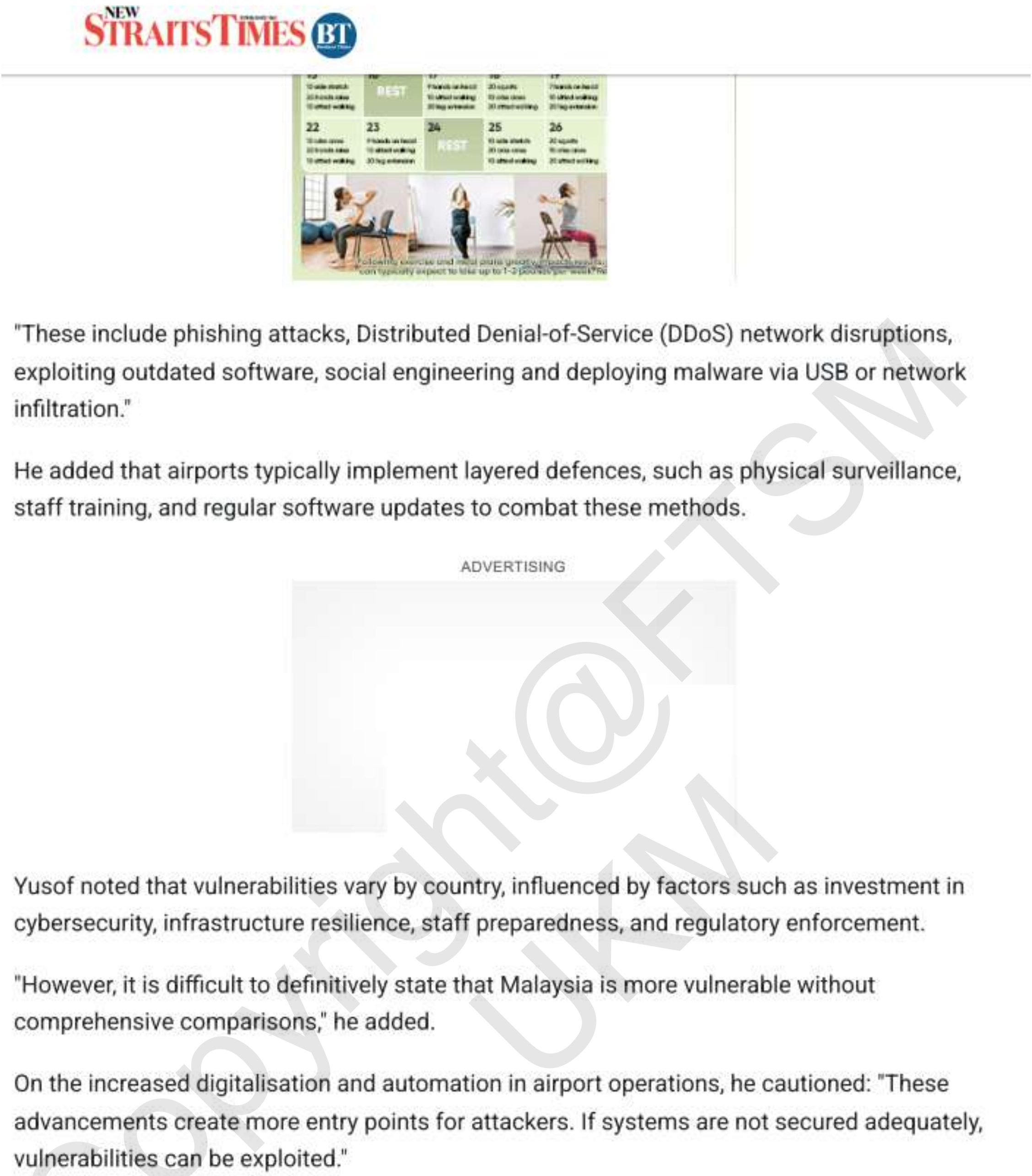


cyberattack

By Mohamad Al As
March 26, 2025 @ 8:25pm

Cybersecurity experts have warned of evolving threats targeting critical infrastructure and called for strengthened defences across aviation systems. REUTERS FILE PIC

KUALA LUMPUR: Following the recent cyberattack on Malaysia Airports Holdings Bhd (MAHB) which targeted systems at Kuala Lumpur International Airport (KLIA), cybersecurity experts



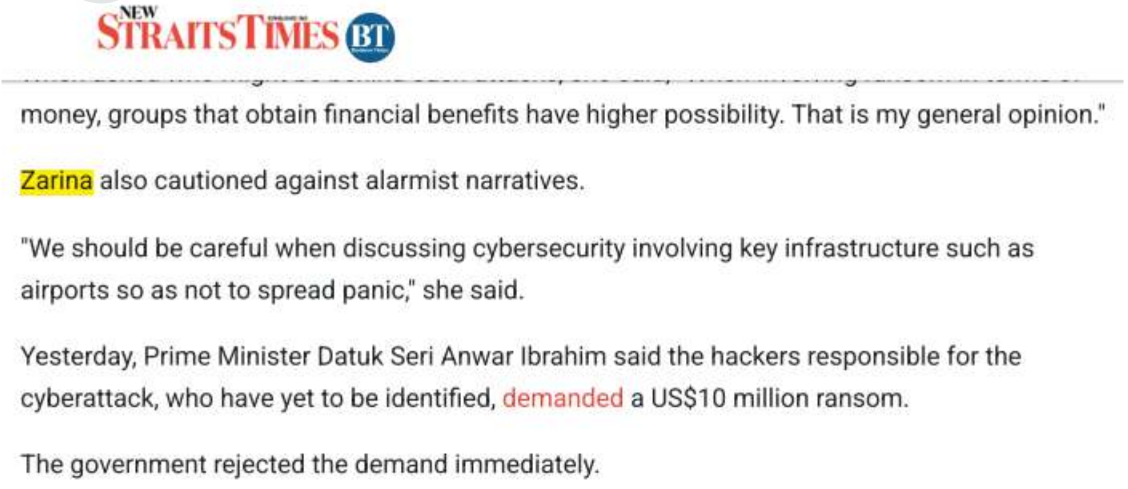
"These include phishing attacks, Distributed Denial-of-Service (DDoS) network disruptions, exploiting outdated software, social engineering and deploying malware via USB or network infiltration."

He added that airports typically implement layered defences, such as physical surveillance, staff training, and regular software updates to combat these methods.

Yusof noted that vulnerabilities vary by country, influenced by factors such as investment in cybersecurity, infrastructure resilience, staff preparedness, and regulatory enforcement.

"However, it is difficult to definitively state that Malaysia is more vulnerable without comprehensive comparisons," he added.

On the increased digitalisation and automation in airport operations, he cautioned: "These advancements create more entry points for attackers. If systems are not secured adequately, vulnerabilities can be exploited."



money, groups that obtain financial benefits have higher possibility. That is my general opinion."

Zarina also cautioned against alarmist narratives.

"We should be careful when discussing cybersecurity involving key infrastructure such as airports so as not to spread panic," she said.

Yesterday, Prime Minister Datuk Seri Anwar Ibrahim said the hackers responsible for the cyberattack, who have yet to be identified, demanded a US$10 million ransom.

The government rejected the demand immediately.