By ANGELIN YEOH
lifestyletech@thestar.com.my

Mind the gap





Butler says research found that while 88% of Malaysian respondents rated their online safety habits as good, only 49% consistently practised strong cyber hygiene. — bolttech



Sharifah Roziah says it's crucial for people to understand that they can remain vulnerable to scams even when they are aware of the risks. — IZZRAFIQ ALIAS/The Star



WHEN it comes to advice on avoiding online scams, you've probably heard it all.

Be wary of that unexpected link, think twice before answering a call from an unknown number and check the website address before handing over your personal details. And, of course, there's the golden rule: if an offer sounds too good to be true, it probably is.

Yet despite these familiar warnings, online fraud cases continue to rise, suggesting that knowing what to do does not always translate into actually doing it.

CyberSecurity Malaysia recorded 4,143 fraud incidents reported by users to the Malaysia Computer Emergency Response Team (MyCert) between January and June this year.

Phishing scams recorded the highest number of incidents with 3,885 cases, followed by Impersonation & Spoofing (120), Bogus Email (59), Fraud Site (50), Business Email Compromise (10), Job Scam (10) and Love/Parcel Scam (9).

"This is concerning because the number of reports of fraud this year is likely to surpass the 5,751 reports that we received last year," says Dr Sharifah Roziah Mohd Kassim, the head of Unit Cyber999 at CyberSecurity Malaysia during an interview with *StarLifestyle* in Cyberjaya.

The majority of reports came from individuals aged 25 to 40, whom she says are mostly working professionals.

In the same period last year, phishing incidents recorded 1,846 cases. MyCert, a cybersecurity incident reporting and response centre operated by CyberSecurity Malaysia, describes phishing as a fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by impersonating a trusted entity. It is commonly carried out through emails or instant messages that direct users to fake websites designed to look like legitimate ones.

"Scammers or attackers are able to exploit trusted names such as banks, government agencies, delivery companies and well-known online platforms to convince victims to click links or provide sensitive information. In most cases, they want to gain access to their Internet banking accounts for the money," she adds.

She explains that MyCert distinguishes the phishing category from bogus email based on the intended purpose of the scam. In phishing cases, the attacker typically attempts to harvest credentials such as usernames, passwords or other account details.

"With a bogus email, on the other hand, it is simply a fake or fraudulent email. It does not necessarily contain a link designed to obtain the recipient's information. Instead, it could be used for other fraudulent purposes, such as impersonating someone and asking the recipient to transfer money," she says.

Based on her experience conducting cybersecurity awareness talks, Sharifah Roziah says people are often surprised by how convincingly scammers can impersonate someone they know or a well-known company.

During these sessions, she shares examples of fraud incidents reported to MyCert without revealing the identities of the victims or companies involved.

"In some cases, scammers impersonate close friends or family members and contact victims to ask for money to be transferred. Some participants say they don't believe they could be fooled by such scams," she says.

The disconnect

Yet this confidence does not necessarily translate into safer online behaviour. Recent findings suggest that being aware of cyber risks does not always mean people consistently practise safer online habits.

In March, insurance technology company bolttech released its Asia-Pacific Cyber Safety Landscape 2026 report involving 3,850 participants in 11 markets, including 350 consumers from Malaysia.

According to Emma Butler, bolttech regional general manager for Australia, Indonesia, Malaysia and Vietnam, the most concerning finding was the disconnect between what Malaysians believe about their online safety and what they actually practise.

"Our research found that while 88% of Malaysian respondents rated their online safety habits as good, only 49% consistently practised strong cyber hygiene," she says in a statement to *StarLifestyle*.

The study uses five cyber safety indexes to assess different dimensions of cyber readiness – experience (measures exposure to cybercrime and threats), habits (everyday cyber hygiene behaviour), response (confidence in responding and recovering from scams) trends (view on the future of cyber safety) and trust (measure of trust on banks, service providers, governments, apps and telcos).

The report indicates that Malaysia is not a market that lacks awareness of cyber risks. In fact, Butler says the country is among the most aware and concerned respondents in the region.

"Nearly seven in 10 (69%) expect someone in their household to fall victim to cybercrime in the coming year, while 95% believe artificial intelligence will make scams more dangerous and harder to detect," she adds.

Compared with other Asia-Pacific markets, Butler says Malaysia performs relatively well on cyber hygiene with the aforementioned 49%.

"While this outperforms the regional average (44%) as well as Singapore (47%), Thailand (43%) and Indonesia (44%), a significant perception gap remains, and almost 70% of respondents in Malaysia still reuse passwords across multiple accounts," she adds.

Why do users continue to reuse passwords despite repeated warnings from cybersecurity experts? For most users, Butler says that everyday convenience continues to undermine cyber resilience.

"It's a simple habit, but one that can significantly increase exposure if a single account is compromised," she adds.

The report also highlighted how most respondents worry that family members, particularly seniors and teenagers, may be vulnerable to increasingly sophisticated scams and may not know how to respond if something goes wrong.

Butler says this has a broader implication for confidence in the digital economy as consumers develop growing concerns over cybercrime.

For the study, Butler explains that cybercrime was considered in the context of consumers' own experiences and those of people they know.

"Incidents covered included scam phone calls, suspicious SMS, suspicious emails requesting info, scams via WhatsApp/Line/Telegram, scams via social media or online ads, unauthorised login attempts, unauthorised bank/e-wallet transactions, and account takeovers.

"This formed part of the study's broader focus on how consumers' habits, experiences, and digital behaviours shape the region's exposure to cyber risks and the need for protection," she adds.

Slow to act

"In some cases involving financial losses where money has been

transferred to a scam account, victims want us to assist them in recovering the funds which we don't directly handle. Instead, we will advise them to immediately inform the bank and contact the National Scam Response Centre (NSRC)'s Hotline 997 to file a report," Sharifah Roziah says.

She adds that the NSRC has the capabilities to stop the fund transaction, however, time is of the essence here.

"Sadly, it's common to hear from the victims that they are not aware of the need to report immediately. It may be too late to prevent losses if the report is only made one or two days later," says Sharifah Roziah.

Details about the amount of financial losses were not immediately available, but she says victims of incidents such as love scams can lose up to RM100,000.

She adds that scammers are increasingly organised, taking the time to research their targets through social media and gather details about their lives. For example, people who publicly announce their retirement plans on social media may attract scammers, who can infer that they are likely to receive a substantial payout from their Employees Provident Fund (EPF) savings.

"This allows them to tailor their approach, build trust and manipulate victims more convincingly through social engineering. One thing we also notice about how attackers exploit is the kindness of Malaysians.

"It's hard for most people to say no when they receive an email or a message from a so-called friend asking for money," she says, adding that there is a need to constantly remind people to be more sceptical when they receive messages requesting for financial help.

Practice makes perfect

Sharifah Roziah also highlighted the growing sophistication of social engineering tactics used by scammers.

"AI is becoming an important enabler, particularly through deepfake images, voice and other synthetic content which make impersonation more convincing and harder to detect for potential victims," she adds.

She says MyCert has also been receiving reports about deepfake content from individuals who are not directly affected by it.

How would you respond to an unexpected call or message? Answer yes or no.

- Do you feel pressured to act immediately when a message says a matter is urgent?
- Would you continue speaking to a caller claiming to be from your bank, telco or another organisation rather than hanging up and calling its official number?
- Would you send money after receiving an time-sensitive request that appeared to be from a friend or family member, without verifying it through another channel?
- Feel more inclined to trust a caller if they knew your name, MyKad number or some other account details?
- Would you move a conversation to another platform, install an app or give someone access to your device because they asked you to?
- Once you have clicked a link or started following instructions, do you find it difficult to stop – even when something feels wrong?

If you answered yes to one or more questions, pause before acting.

Scammers often exploit urgency, familiarity and information obtained from data leaks or social media to make a request appear genuine.

End the call or stop replying, then verify independently through an official number, website or another trusted channel.

Never share your password, PIN, OTP or recovery code.



Pay attention to alerts and warnings. Whether it is a bank notification, a suspicious login alert or a scam warning, taking a moment to verify before clicking can prevent a costly mistake.

This visual is human-created, AI-aided.

Will AI reduce jobs?

By KACHELLE PRATCHER

NEARLY three in four adults under 30 now think AI will take jobs. That number lands in a summer when every company is announcing an AI rollout and none of them are saying what it means for headcount.

Younger workers are using the tools anyway. They just stopped believing the part where it makes their work bigger.

The number comes from a Pew Research Center study that surveyed 3,488 US adults. Among adults under 30, 73% say AI will lead to fewer jobs in the US over the next 20 years, up from 61% two years ago.

For the first time, a majority of that group, 55%, says AI in daily life makes them more concerned than excited.

Two years ago, young adults were the most optimistic working-age group on this question at 61%. Now they sit at 73%, essentially level with people in their 30s and 40s at 74%, and above those 50 to 64 at 72%.

Pew's own line is that the youngest adults are now just as likely as everyone from 30 to 64 to expect loss.

Young adults are calculating

Most adults under 30 say they use chatbots. Pew found they are just as likely to say those tools hurt their own creativity as help it. Also, they are the age group most likely to think AI will be bad for society and bad for them personally.

So, exposure is not the missing ingredient. They have the exposure. They formed the opinion anyway, which means a demo will not move them and neither will a slide at an all-hands.

A 24-year-old hears doing more with less and reads a headcount plan. That is not cynicism. They are reading the same coverage you are, where the economists cannot agree either.

Somebody still runs the machine

Television has already gone through this. I have spent more than a decade in TV newsrooms, and I watched robotic cameras take over much of the manual camera work in control rooms.

The shots got faster and cleaner. Fewer people were needed on a studio floor.

But the cameras did not run themselves. Someone still had to oversee the technology, set the moves, and make the call when the automation got it wrong. The role did not disappear. It moved up a level, from operating the equipment to directing what the equipment does.

That is what a candidate under 30 is trying to find out and cannot ask directly. Not whether you use AI.

But whether the job they are interviewing for is the one that moves up a level or the one that gets absorbed.

Proof beats promises

Not a promise that the job is safe. Nobody hiring can make that promise, and every candidate knows it. Name a role at your company that changed, name the person in it, and say what they do now that they could not do before.

Explain what you are actually implementing and what it is for. Telling a candidate that you are not using AI, when you are, costs more than the honest version ever would.

Then let them watch. Your youngest employees are not reading your AI policy. They are watching what happens to the person sitting next to them, and they are drawing conclusions either way. – Inc./Tribune News Service

"For example, some people report deepfake videos featuring prominent figures such as Prime Minister Datuk Seri Anwar Ibrahim because they are concerned about the potential impact. We will investigate the reports and, where appropriate, notify the relevant service providers to request that the content be taken down," she says, adding that proactive reports are a positive development.

At the end of the day, she says it's crucial for people to understand that they can remain vulnerable to scams even when they are aware of the risks.

"This is because scams exploit psychological and emotional weaknesses rather than simply a lack of knowledge. Strong emotions such as fear, excitement, curiosity and urgency can cause people to react quickly without thinking critically," she adds.

While repeated warnings may increase awareness, Sharifah Roziah says it doesn't guarantee that people will recognise sophisticated scams immediately.

"Vulnerability can also increase when individuals are tired, stressed, distracted or emotionally affected. Most warnings focus on identifying suspicious messages instead of teaching people how to respond when under pressure," she says.

Which is why, she adds that even the smartest of people can make mistakes when a scam is carefully designed to exploit their emotions and decision-making skills. For her, effective scam prevention requires awareness paired with critical thinking, independent verification and the ability to pause before taking action.

"When you receive a call or message from someone claiming to be a friend or a person of authority, ask yourself: is it really them? Take a moment to verify their identity, either by checking with a mutual friend or contacting the person through another trusted channel," she says.

What you can do

Butler says good cyber hygiene does not have to be complicated, with small, consistent habits often making the biggest difference.

"First, use strong, unique passwords for accounts. Reusing passwords remains one of the most common cybersecurity risks and can turn a single breach into multiple compromised accounts," says Butler.

Second, enable two-factor authentication wherever possible. It is one of the simplest and most effective ways to add an extra layer of protection.

Third, Butler says to pay attention to alerts and warnings. Whether it is a bank notification, a suspicious login alert or a scam warning, taking a moment to verify before clicking can prevent a costly mistake.

Another option is to use a password manager, like Apple Passwords or Google Password Manager, which can create strong passwords for you and remember them. Both support passkeys – a two-part cryptographic key designed to replace traditional passwords – that allow logins to websites and apps using a device's fingerprint, face scan, or screen lock PIN.

Essentially, your device creates a pair of digital keys – a public key sent to the website and a private key stored safely on your device. Service providers do not store passwords, only public keys, which are useless without the private keys. This means that even if a service provider's database is breached, attackers cannot obtain user credentials.

Experts also advise combining three random words to create a more difficult to crack password (for example applenemobiro), adding that replacing letters with symbols (like a zero for an 'o') is a trick cyber criminals are also aware of, which renders such passwords less secure while also making them harder to recall.

"Ultimately, it is about building simple, consistent habits while also seeking the protection and support needed to manage cyber risks with confidence," says Butler.