BTS devices exploited for scams

High chance SMS messages containing links are sent by scammers, warn experts

By TEH ATHIRA YUSOF
tehathirayusof@thestar.com.my

PETALING JAYA: The recent foiling of a scam operation involving fake base transceiver station (BTS) devices has highlighted the urgency for the public to be cautious of links received via SMS, even when messages appear to come from trusted numbers.

Cybersecurity specialist Fong Choong Fook said such devices are designed to impersonate legitimate telecommunications towers, causing nearby mobile phones to unknowingly connect to them.

"A BTS is essentially a base station that mimics the operation of a telecommunications company's cell tower, but on a smaller scale. Think of it like a Wi-Fi hotspot," he said.

Fong explained that just as a Wi-Fi router openly broadcasts signals for nearby devices to connect, a fake BTS emits a strong signal while pretending to belong to a legitimate telco.

"Due to weaknesses in mobile phone protocols, phones tend to connect automatically to the strongest signal available. That's why scammers place fake BTS devices in crowded or popular areas to target large groups of people," he said.

Once a phone connects to a fake BTS, scammers can send messages or SMS directly to the device, often launching phishing campaigns aimed at stealing personal or financial information.

"These scams usually come in the form of SMS messages containing a web link. The public should remember that banks and telcos have been instructed not to include clickable URLs in SMS messages.

"As a general rule, if an SMS contains a link, there is a high chance it was sent by scammers. Do not click on it," Fong warned.

He added that common tactics include messages claiming a WhatsApp account will be suspended unless immediate action is taken, or fake alerts supposedly from banks or authorities, all designed to create a sense of urgency.

Fong noted that the use of fake BTS devices is not new and has existed for many years, initially being abused for location-based marketing where promotional messages were blasted to users in the vicinity.

"Today, cybercriminals are using the same technology for scams and fraud," he said.

He added that fake BTS devices can be highly portable, with some small enough to fit into a car boot or be concealed in shop lots or rooftops.

Fong said the recent operation by the Malaysian Communications and Multimedia Commission (MCMC) was part of ongoing enforcement efforts rather than a one-off case.

"MCMC continuously conducts BTS reconnaissance and scanning. Detecting and triangulating the location of a fake BTS is not easy. It requires coordination, technical capability and sustained effort," he said.

Last week, the MCMC successfully shut down the transmission activities of a fake BTS in Genting Highlands, Pahang, following an integrated operation with a telecommunications company.

The commission detected two vehicles believed to have been used to carry out the illegal transmissions, which were used to intercept telecommunications networks and send fraudulent SMS messages, indicating that the activity was carefully planned.

In a related development, fraud examiner specialist Raymon Ram said licensed financial institutions should enforce robust internal SMS policies, employ secure multi-factor authentication, work closely with telecom authorities and proactively raise consumer awareness to stay ahead of evolving SMS-based fraud.

While banks must secure their own SMS infrastructure, he said the root of the problem lies at the telecom and protocol level, where messages can be manipulated before reaching recipients.

Recently, customers of a bank received SMS notifications from an official code containing links that prompted recipients to tap on them, a tactic used to lure victims.

Although the messages were subsequently removed and the bank rectified the issue, Raymon cautioned that SMS should not be relied on for sensitive actions.

He noted that Bank Negara has already mandated the phasing out of SMS-based one-time passwords, advocating instead for more secure authentication methods such as mobile apps or hardware tokens.

"Banks must also implement fraud monitoring mechanisms that trigger rapid investigations when customers report suspicious messages. Cooperation with telcos and regulators, such as the MCMC, is essential," he said.

Experts: SIM card misuse fuelled by weak regulation

PETALING JAYA: Experts have warned that Malaysia's weakly regulated supply chain continues to fuel rampant SIM card misuse.

They said that wider adoption of the government's MyDigital ID could provide a safeguard against identity fraud involving SIM cards.

Universiti Malaya senior lecturer in criminology Dr Haezreena Begum Abdul Hamid said that the core problem of SIM card scams is structural, not user negligence.

"SIM card fraud in Malaysia stems from systemic regulatory weaknesses, poor enforcement and unsecured registration pathways that allow criminals to obtain phone lines anonymously.

"My analysis found that the criminals obtain pre-registered numbers which are already activated using someone else's identity.

"These SIM cards are widely circulated in underground markets where many vendors bypass biometric or MyKad authentication steps, allowing fraudulent registrations to go unnoticed," she said, adding that street-level dealers at night markets, train stations and malls remain a key risk factor.

Digital defense: Experts say MyDigital ID can help stamp out fraudulent purchase of SIM cards. — IZZRAFIQ ALIAS/The Star

"The telco subcontractors often operate with minimal supervision, enabling misuse of registration privileges," she added.

"Dealers also sell pre-registered SIM cards already activated under someone else's name and may operate through subcontractors with little telco oversight.

"SIM card registration should be tied to mandatory biometric verification and only licensed, audited vendors should be permitted to activate SIM cards."

Haezreena also said that as long as personal information is made available, it's easy for criminals to get MyKad information, which is reused to activate SIM cards.

"The current system does not fully track which agent registered each number, making accountability inconsistent.

"These loopholes allow criminals to operate with anonymity, which is the key enabler of scam operations.

"As a result, MyKad holders whose identities are misused may be questioned when scam numbers are traced to them.

"Even if they did nothing wrong, they may still be investigated and asked to explain SIM cards they were unaware of," she said, calling the situation unfair, particularly for vulnerable groups.

Echoing the same view, Malaysian Cyber Consumer Association (MCCA) president Siraj Jalil said the core problem lies with those supplying illegally pre-registered SIM cards, including SIM card agents.

"The moment you hand over your MyKad to someone else (third parties) to register a SIM card for you, the process can be exploited," he said.

Siraj also highlighted the involvement of foreign sellers in the illegal SIM card trade, adding that stronger regulation is needed at the agent and street dealer level.

He urged consumers to adopt MyDigital ID, saying it helps detect unauthorised phone numbers linked to one's MyKad.

"Telcos are also supposed to be aligned with MyDigital ID," he said, adding that regulation should extend to agents and street-level dealers.

Siraj said that registered SIM cards sold online are further complicating enforcement efforts.

He said that the issue should also be viewed from a foreign digital identity systems point, as foreigners are part of the mobile subscriber ecosystem.

Meanwhile, Federation of Malaysian Consumers Associations (Fomca) chief executive officer Dr Saravanan Thambirajah advised consumers to avoid purchasing SIM cards from street vendors or online listings that offer pre-registered or unusually cheap SIM cards.

"These can be linked to illegal registrations and scam activities," he said, adding that public awareness must be strengthened alongside enforcement.