ITSEC™
SECURITY DELIVERED

AUGUST 2025 ITSEC: CYBERSECURITY SUMMIT 2025 EDITION

ITSECBUZZ

CYBERSECURITY MAGAZINE

**CSIRT:
Why Your Organization
Need to Have One?**

**The Bangladesh Bank
Heist that Shook The World**

**IntelliBroń Aman:
Protect Your Phone from
Malicious Threats in
Real Time.**

ITSEC: Cybersecurity Summit 2025

Indonesia Steps Into The Quantum Era of Cyber Defense

WHY PHISHING REALISM MATTERS:

Testing Defenses with Attacks That Look-and Feel-Real

Hi John, it's Michael from IT, can you please confirm your details https://p0rtal.com/deta1ls/iri-isye

In 2025, phishing has evolved far beyond suspicious emails and dubious links. In Southeast Asia—where mobile-first usage, messaging apps, and digital acceleration are booming—cybercriminals are matching their techniques to local habits, languages, and platforms. That makes simulated phishing campaigns harder to get right—and all the more important to get real.

It's time for organizations to stop testing users with outdated or generic email lures and start simulating the actual threats targeting their networks. Because real attackers don't follow templates—and neither should you.

Phishing is Evolving in SE Asia

In markets like Singapore, Indonesia, Thailand, and Malaysia, phishing campaigns are becoming hyper-realistic and platform-diverse. Our customers across Southeast Asia report a high level of activity for social engineering fraud, with messaging-based scams in particular growing rapidly due to high smartphone and mobile payment usage.

Attacks today are not only personalized—they're persistent. Cybercriminals are repurposing real company branding, mimicking internal HR or finance messages, and increasingly using mobile channels like SMS and WhatsApp to bypass traditional email filters.

Recent high-profile trends include the spike in SMS-based scams in Singapore impersonating government agencies and banks and WhatsApp based job scams, particularly in Thailand. These aren't hypothetical risks—they're daily realities for regional businesses and are resulting in losses into the millions.

Beyond Email — Training for Smishing and WhatsApp Threats

The rise of smishing (SMS phishing) and phishing via messaging platforms like WhatsApp has exposed a gap in most organizations' awareness programs: they're still training users to spot threats in inboxes, while attackers are already in their message threads.

Modern awareness programs need to simulate threats across **all relevant channels**—not just email. That means testing employee responses to convincing SMS messages with embedded links, or WhatsApp messages that mimic real conversations from colleagues or vendors.For example, a simulated smishing message might appear to come from your bank's fraud team, urging immediate action. A WhatsApp phishing simulation could replicate a team lead's request to approve a payment "urgently." If your people aren't seeing these simulations during training, how will they respond in real life?

Clone and Repurpose — Real Attacks as Training Material

The best way to simulate a phishing attack? Use one that already worked—or nearly did.

Modern awareness platforms now allow **attack cloning:** the ability to take real phishing emails, sanitize them, and re-use them in simulations tailored to your organization. But Lucy Security goes a step further—we enable **cloning of landing pages too.** That means your simulation doesn't just copy the phishing email—it mimics the malicious website it links to.

Why does this matter? Because attackers are mimicking everything: Microsoft 365 login pages, bank portals, e-signature requests, payment systems. If users can't tell the difference between a real page and a cloned one, your simulations should reflect that challenge.

By using cloned attack components, you can test real scenarios your employees are likely to face—without the guesswork.

What "Realism" Achieves

Realistic phishing training isn't about fear—it's about preparing people for how attackers really operate. Overly simplistic training with fake Amazon receipts or cartoonish Nigerian prince emails may tick a compliance box, but they won't change behavior.

When phishing simulations mirror real-life lures—same style, same tone, same urgency—users engage more critically. That drives higher awareness, better reporting rates, and measurable risk reduction.For regional firms, this realism also means *cultural and linguistic accuracy*. Attack simulations must reflect local norms—like Malay, Thai, or Tagalog messaging patterns, mobile payment requests, or government agency impersonations common in the region.

It's Time to Get Real

Cyber attackers have gone mobile, gone local, and gone sophisticated. If your training programs haven't caught up, your people are walking into attacks unprepared.

By embracing real-world realism—testing WhatsApp and SMS channels, cloning actual attacks, and adapting simulations to your organization's language and threat landscape—you go beyond awareness. You build readiness.

Because in today's threat environment, phishing awareness isn't enough. Phishing realism is what makes the difference.

By **Clifford Ang, Regional Sales Director for Asia at Lucy Security**

LUCY AWARENESS

ITSEC: Cybersecurity Summit 2025 Sponsor

ITSECBUZZ
CYBERSECURITY MAGAZINE

ITSEC™
SECURITY DELIVERED

PT ITSEC Asia Tbk
Noble House, Level 11.
Jakarta 12950, Indonesia

✉ contact@itsec.asia

☎ +62 (21) 29783050

itsec.asia

PT ITSEC Asia Tbk

itsec.asia
itsec.buzz