Trainees taking part in a hands-on session to configure and send malware to hack a burner phone in a controlled setting, to understand the typical tricks scammers use. PHOTO: LIANHE ZAOBAO

New course lets bank staff role-play as malware hackers to spot and thwart scams

Osmond Chia

During an anti-scam training session for UOB front-line personnel, participants were presented with two deepfake videos featuring Communications and Information Minister Josephine Teo speaking in Parliament.

When asked, several of the bank employees quickly noted that the first video – created with the help of a voice actress mimicking Mrs Teo's speech – sounded unnatural.

No one flagged the second video, which was made for the class with artificial intelligence.

Minister of State for Home Affairs Sun Xueling, who joined UOB trainees for the session on March 26, noticed that both videos of Mrs Teo were fake.

"I must say that because I know (Mrs Teo), I am attuned to how her voice sounds," she told the class.

"But if this was shown to any member of the public, they might not naturally be (suspicious of) either video," said Ms Sun, adding that the exercise was an indicator of how convincing deepfake technology has become.

The example was an exercise in a new two-day course, jointly developed by Singtel, UOB and the Singapore Institute of Management (SIM). It offers large enterprises a customised training programme to help their staff spot and manage scams, including malware scams and deepfake scams, which are growing in prominence.

Front-line staff need to be familiar with such scams because of the rise of deepfake technology in particular, which is hard to spot and could be used to trick victims to make transactions on their behalf, Singtel Cyber Security Institute director Wilson Tan told the media during the programme's launch at the institute in Tampines.

"These are things that bank tellers need to verify and not just rely on what they hear," he said.

The Defence Against Cyber Scams programme is part of a shared-revenue partnership between Singtel and SIM. Eligible participants will be subsidised by up to 90 per cent of the $2,880 course fees under the SkillsFuture Singapore scheme, depending on their age.

UOB is the first participant of the course, which is aimed at insurance firms amid a spike in insurance-related scam cases where victims are duped into terminating their insurance schemes prematurely.

Ms Janet Young, UOB's managing director and group head of channels and digitalisation, said the collaboration adds on to the bank's ongoing training programmes for staff and allows the partners to share resources and knowledge in dealing with cyber scams.

Trainees were paired for a hands-on session to configure and send malware to hack a burner phone in a controlled setting to understand the typical tricks scammers use, allowing them to ask the right questions to identify potential scams.

During the training, instructors led participants through a simulation of a malware program that allowed them to choose which phone functions they could potentially access, like camera, microphone, storage or text, in a controlled environment.

Instructors from SIM and Singtel repeatedly reminded trainees not to scan the link using their own phones as this would embed them with a virus.

Once installed, the attacker could see footage covertly streamed from the camera of the hacked device and read private information in the phone's logs.

In an address to participants, Ms Sun said the course can help equip staff with the skills needed to spot and thwart scams, which duped at least 100 victims daily, based on the police's scam statistics for 2023.

"Scammers manipulated the victims into transferring the money and this makes it difficult for the banks because it is, in a way, authorised by the victims...

"This deeper understanding of the technical, psychological and emotional vulnerabilities can better equip all officers with knowledge and skills to identify, report and intervene to prevent scams," she said.

osmondc@sph.com.sg