Cyber Resilience Center

Phishing Simulation Exercise

SBF

新加坡中華總商會
Singapore Chinese Chamber of Commerce & Industry
Since 1906

SGTECH
WHERE TECH MEETS

Overview

- **Complimentary Nationwide Phishing Simulation Exercise**
- **Sept – Nov 2026**
- **Organisations based in SG**
- **300 Organisation (Capped at 30 per Org) – Subjected to increment based on demand**

The exercise aims to help organisations

- Raise employee awareness of phishing threats.
- Assess susceptibility to common phishing techniques.
- Reinforce good cyber hygiene practices.
- Identify opportunities to strengthen cybersecurity awareness programmes.

The exercise is educational in nature and is not intended to penalise participants.

SBF 新加坡中華總商會 Singapore Chinese Chamber of Commerce & Industry Since 1906 SGTECH WHERE TECH MEETS

Exercise Design

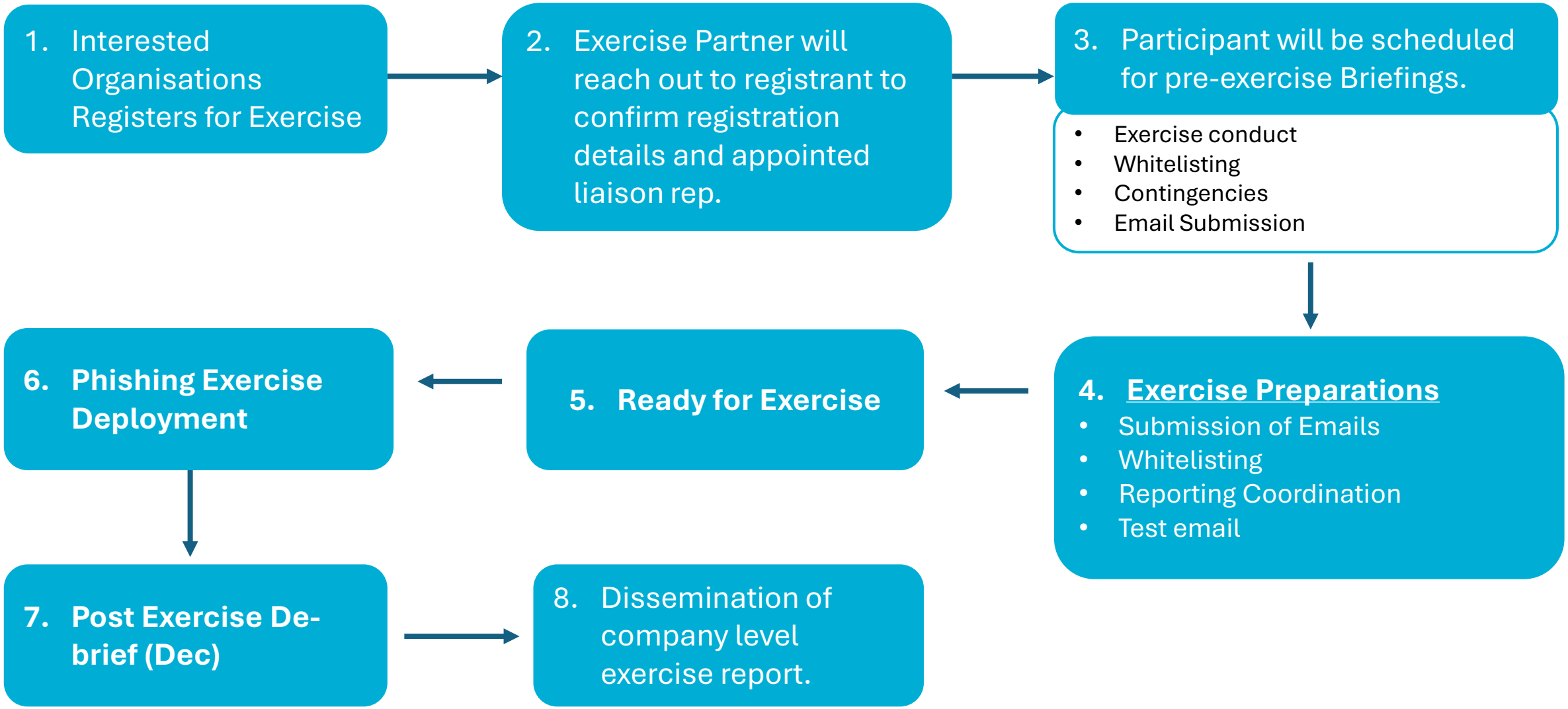
<table>
<tr><td>Theme</td><td>
3rd Party Risk & Social Engineering
• Account & Security Alerts
• 3rd Party Impersonation (e.g. Banking & Finance, Government and Logistic)
• Internal / Corporate Communications (e.g HR@XX.com.sg)
<u>2 Layer Campaign</u>
• Phishing Email with Link (e.g Enter your Password) -> Simulated Credential harvesting (Email/ password/ Mobile)
</td></tr>
<tr><td>Reporting Output</td><td>
• Aggregated exercise result and individual company exercise result of participating Organisations.
<table>
<tr><td>1st Level</td><td>• Opened Rate
• Clicked Rate
• Reporting Rate</td></tr>
<tr><td>2nd Level</td><td>• Industry Breakdown
• Phishing Category Breakdown (Behavioural Insights)
• Average/Median Reporting Time
• Global / Historical Benchmark for above.</td></tr>
</table>
</td></tr>
</table>

Scope and Project Schedule

Outreach and Whitelisting	Aug – 23 Oct 2026 (7 Weeks)
Exercise Period	26 Oct – 20 Nov 2026 (3 Weeks)
Completion and Delivery of Report	07 Dec 2026 (Amended from 6th Dec as it was a Sun)

Months	Aug 2026	Sep 2026	Oct 2026	Nov 2026	Dec 2026
Recruitment	Upon requirement and Scope clearance.				
Whitelisting					
Phishing Deployment					
Post Exercise Briefing & Report Delivery					

Exercise Flow



FAQ

1.	**Is there a Minimum or Maximum no. of participants from each organisation ?** • The minimum number of participants required is one (1) employee. Capacity for each organisation are allocated at 30 participant / email currently, organisations are recommended to utilise the full allocated capacity of 30 participants to facilitate meaningful exercise insights. • That said, organisations are welcome submit more than 30 participants, and the appointed exercise partner will confirm the final number of participant slots allocated during the submission of participating email.
2.	**Do we need to install any software or make any system configuration changes to participate?** • No. Participants are not required to install any software, agents, or applications on their devices. • Participating organisations may be required to whitelist the exercise email domains to ensure simulated phishing emails are delivered successfully. Detailed guidance will be provided during the participant briefing session.
3.	**Is there any cost involved in participating in the exercise?** • No. The phishing simulation exercise is fully complimentary as part of a public good initiative. Participating organisations are not required to pay any fees, purchase software, or subscribe to any services in order to participate.
4.	**Who is eligible to participate?** • The exercise is open to Singapore-based organisations of all sizes and sectors. Participants must have access to a valid email account to take part in the exercise.

5.	**What is required from my organisation to participate?**
	• Participating organisations are encouraged to appoint a Liaison Officer to coordinate exercise activities. While an IT representative is preferred, this is not mandatory.
	• The Liaison Officer will assist with:
	  ○ Participant nomination and submission.
	  ○ Coordination of any required email whitelisting.
	  ○ Communication with the exercise team.
	  ○ Receiving exercise updates and reports.
	• A briefing session will be conducted prior to the exercise to guide organisations through the preparation process and exercise timeline.

FAQ

6.	**Will participants be informed that they are taking part in a phishing simulation exercise?** • The organisation may choose to inform employees that it is participating in the exercise. However, the specific phishing scenarios and timing of simulation emails will not be disclosed in advance to preserve the effectiveness of the exercise.
7.	**Will participants be exposed to any real malware or malicious links?** • No. The exercise is conducted in a controlled and secure environment for cybersecurity awareness and training purposes only. • Simulated phishing emails may direct participants to a secure exercise landing page developed specifically for the exercise. The exercise platform may capture relevant interaction metrics, such as whether a participant opened the email or clicked on a link, to support the generation of exercise insights and reporting. • Any information entered by participants on the exercise landing page will not be captured, stored, or retained by the exercise team or exercise platform. No passwords, personal information, or other user-submitted data will be collected as part of the exercise. • No malware, malicious software, harmful attachments, or unsafe websites will be used during the exercise.
8.	**How will participant information and exercise results be used?** • Information collected during the exercise will be handled in accordance with applicable data protection requirements and used solely for the administration, conduct, analysis, and reporting of the exercise. • Participating organisations will receive exercise reports containing relevant observations and performance metrics to support cybersecurity awareness and resilience-building efforts. The reporting format and level of detail will be communicated prior to the commencement of the exercise. • The exercise is intended as a learning and awareness initiative and is not intended for regulatory, compliance, enforcement, or punitive purposes. Results will be used to help participating organisations better understand potential phishing risks and identify opportunities to strengthen cyber awareness and preparedness.