

20 Aug 2026

CSA Internet Hygiene Portal (IHP) Outreach with ACES

I'm Ting Ying from the Cyber Security Agency of Singapore (CSA), Cyber Security Engineering Centre.

I am reaching out to seek your assistance in introducing the Internet Hygiene Portal (IHP), a key CSA initiative, to your organisation and its members. We believe that given the increasing prevalence of cyber-attacks, IHP can help organisations to strengthen their internet security posture.

About CSA's Internet Hygiene Portal

As part of Singapore's Safer Cyberspace Masterplan, CSA launched the IHP in October 2022. This government initiative helps enterprises strengthen their cybersecurity through awareness, assessment, and adoption of internet security best practices. We invite you to visit our platform at <https://ihp.csa.gov.sg> to perform a quick cybersecurity health check on your website and email domains. This self-service tool provides immediate insights into your current cybersecurity posture of your domains.

Request for Assistance on IHP Outreach

As part of our outreach efforts, we are seeking to connect with more companies and SMEs to raise awareness about IHP. Therefore, we would like to seek your assistance in spreading awareness about IHP among the ACES members. Could you advise if this is something you might be able to support, or perhaps direct us to the most appropriate contact for such collaboration? We are also open to conduct a short sharing on IHP and the cybersecurity landscape in Singapore.

Invitation to CSA's IHP Solutioning Workshop

We would also like to invite the members of ACES to our upcoming IHP Solutioning Workshop. Could we please seek your assistance to send this invitation to the members of ACES?

Greetings from Cyber Security Agency of Singapore (CSA)!

We would like to invite you to participate in a two-day Solutioning Workshop conducted as part of the Cyber Security Agency of Singapore's Internet Hygiene Portal initiative.

This workshop aims to identify key cybersecurity challenges and collaboratively develop practical solutions that help organisations understand risks, prioritise actions, and improve their cybersecurity posture. Participants will be asked to actively contribute their experiences, concerns, and ideas to ensure that the proposed solutions are relevant, understandable, and realistic for SMEs to adopt.

As part of the workshops, we aim to

- Better understand the cybersecurity journey, challenges, and decision-making processes of SMEs
- Identify opportunities to improve how cybersecurity risks and recommended actions are communicated
- Generate and evaluate potential solutions from an SME perspective
- Prioritise solution features based on user needs, business value, and feasibility
- Develop early solution concepts and prototypes for further testing

What participants will be doing

Day 1: Understanding the problem

Participants will explore key challenges, map user experiences, identify opportunity areas, and prioritise the most important issues to address.

Day 2: Developing solutions

Participants will generate and evaluate ideas, develop simple solution concepts and prototypes, gather feedback, and prioritise the strongest solutions.

What we need from participants

Participants will be expected to:

- Share practical experiences and challenges faced by SMEs
- Provide input on how SMEs understand and respond to cybersecurity information
- Highlight concerns relating to cost, time, resources, operational impact, and ease of adoption
- Evaluate whether proposed ideas would be relevant and realistic for SMEs
- Actively participate in group discussions, ideation, prioritisation, and feedback activities

No technical cybersecurity expertise is required. We are particularly interested in participants who can contribute from an SME business, operational, or decision-making perspective.

Details of participation

Dates: 2nd & 3rd September 2026

Venue: CSA, 92 Punggol Way, Tower 92 Punggol Digital District, Level 7

Duration: 9am – 6pm (lunch will be provided)

How to sign up

This workshop is best suited for your company's IT Manager or equivalent. If you are not the right person to attend, we would appreciate it if you could forward this email to the relevant colleague. If you are interested in participating in this workshop, please complete the following questionnaire: <https://form.gov.sg/6a61d2b26def0bdcd6b634b4>.

Your participation will contribute to defining and refining core problem statements, validating key hypotheses, and uncovering real-world pain points and behavioural patterns. These insights will play a critical role in informing the development of more effective and relevant cybersecurity solutions under CSA, ensuring they are grounded in actual user needs and operational realities.

For any additional enquiries, please reach out to: chan_enqi@csa.gov.sg / teo_wei_how@csa.gov.sg.

Thank you and see you!

If you would like more details or clarifications, we would be happy to arrange a call this week. Thank you for your consideration and we look forward to hearing from you soon.

Regards,



**Chai Ting Ying | Cybersecurity Engineering Centre
Cyber Security Agency of Singapore**

92 Punggol Way, #07-163, Singapore 829854

www.csa.gov.sg | Follow us on     

WARNING: This email may contain privileged and confidential information. If you receive this email by mistake, you should immediately notify the sender and delete the email. Unauthorised communication and disclosure of any information in the email is an offence under the Official Secrets Act (Cap 213).