PUBLIC CONSULTATION ISSUED BY THE
INFO-COMMUNICATIONS MEDIA DEVELOPMENT AUTHORITY

ON

PROPOSALS TO STRENGTHEN SAFEGUARDS FOR SMS MESSAGES TO SINGAPORE USERS: IMPLEMENTATION OF ANTI-SCAM FILTER SOLUTION WITHIN MOBILE NETWORKS

15 August 2022

INTRODUCTION

1. A common tactic used by scammers is to deceive victims into clicking malicious links sent via communication channels. By clicking on such links, scammers may then gain access to victims' sensitive data by either (i) infiltrating victims' devices through unauthorised installation of virus or malware; or (ii) leading victims to bogus websites that phishes for information.

2. These tactics, once commonly conducted over emails, have permeated into Short Message Service ("**SMS**") messaging. Given the high mobile penetration rate in Singapore and the availability of SMS as a very common and ubiquitous means of communication available to all consumers with mobile phones, such SMS scams have affected all facets of society and all types of consumers. This has resulted in financial losses to Singapore consumers across all segments of society.

BACKGROUND - ANTI-SCAM FILTER SOLUTION

3. IMDA notes that technology to identify and filter potential scam SMS messages is now commercially available. These solutions can filter out scam SMS messages that are within the Mobile Network Operators' ("**MNOs**") networks, using machine reading technology, before they are delivered to consumers. While such solutions are not fool proof, they will significantly reduce the number of scam SMS messages received by consumers.

4. Driven by the significant uptick in scam SMS messages experienced globally, some MNOs in countries such as Australia and the United Kingdom have already implemented such anti-scam filter solutions in a bid to better combat against scams. This implementation has been reported to have blocked more than 50% of scam SMS messages. To allow all consumers to benefit from this additional level of protection, the MNOs in Australia and the United Kingdom have deployed such solutions at the network level and applied it to all mobile subscribers by default.

5. In essence, the anti-scam filter is designed to work like a security firewall that uses automated machine scanning to review and filter SMS messages based on the following:

    a. SMS messages containing malicious links that may lead consumers to websites asking for sensitive information or trigger installation of malware and viruses; and

    b. Suspicious SMS messages containing patterns indicating that it is a scam message, such as the use of keywords or phrases found commonly in scams.

PROPOSED IMPLEMENTATION OF ANTI-SCAM FILTER

6. To better protect Singapore consumers, IMDA is proposing that the same anti-scam filter solution be implemented by the MNOs in Singapore, which will be done in phases.

Phase 1: Filtering of scam SMS messages through the detection of malicious links

7. This filtering will be conducted through an automated process, via a machine in the mobile network without any human involvement.

    a. Links within SMS messages will be cross-checked and matched against a database of known malicious links. If a match is detected, the SMS message will be filtered out; and

    b. The database of malicious links will be updated continually to stay relevant against new threats.

Phase 2: Further filtering of scam SMS messages that contain suspicious patterns

8. The next tier of filtering capabilities can be introduced in the second phase, given that they will require more time for implementation. Similar to Phase 1, this filtering will be conducted through automated machine scanning without human intervention.

    a. The machine will seek to identify and filter SMS messages based on suspicious patterns within SMS messages. These may include keywords, phrases and message formats that are typically used in scam SMS messages.

    b. Machine learning will be adopted to scan and identify common and new patterns that are characteristic of scammers and scam SMS messages, keeping pace with the evolving tactics of scammers.

9. As part of the machine learning process, there may be some SMS messages that are flagged by the machine as potentially suspicious and further assessment is required to ascertain if these are indeed scam SMS messages. Prior to being routed for further assessment, these flagged suspicious SMS messages will be anonymised by the machine and then channelled to MNO's technical personnel for a second layer of review. Over time, this will allow the machine to develop higher filtering accuracy and efficacy.

10. This review is exclusively for the purposes of improving the machine learning process, and no other purposes are allowed. Further, MNOs continue to bear obligations under the Personal Data Protection Act, including to protect any personal data and not retain the personal data longer than reasonably necessary for facilitating machine learning, or otherwise than authorised by written law.

11. While this further filtering under Phase 2 is not fool proof, it will help to further mitigate risk to consumers.

INVITATION TO COMMENT

12. IMDA would like to seek views and comments on whether the public would welcome the implementation of the anti-scam filter solution and its capabilities, as well as the operational issues that may need to be addressed to make this a more effective solution.

13. Respondents who submit their views or comments regarding the issues identified in this consultation document may organise their submission as follows: (a) cover page (including their personal/company particulars and contact information); (b) summary of major points; (c) statement of interest; (d) comments; and (e) conclusion. Supporting materials may be placed as an annex to the comments raised.

14. All views and comments should be submitted in soft copies (Microsoft Word and PDF Format) and should reach IMDA by 12 noon, 9 September 2022. All views and comments should be addressed to:

Ms Aileen Chia
Director-General (Telecoms and Post)
Deputy CE (Connectivity Development & Regulation)
Infocomm Media Development Authority
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

AND

Please submit your soft copies, with the email header "Public Consultation on the Implementation of Anti-Scam Filter Solution", via email to Consultation@imda.gov.sg.

15. IMDA reserves the right to make public all or parts of any written submission and to disclose the identity of the source. Respondents may request confidential treatment for any part of the submission that the respondent believes to be proprietary, confidential or commercially sensitive, with supporting justification for IMDA's consideration. Any such information should be clearly marked and placed in a separate annex. If IMDA grants confidential treatment, it will consider, but will not publicly disclose, the information. If IMDA rejects the request for confidential treatment, it will return the information to the party that submitted it and will not consider this information as part of its review. As far as possible, parties should limit any request for confidential treatment of information submitted. IMDA will not accept any submission that requests confidential treatment for all, or a substantial part, of the submission.