GUIDELINES ON ONLINE SAFETY

BACKGROUND

The Internet and other digital and information technologies are powerful tools which open up new opportunities for everyone. At the same time, these technologies create challenges for online safety and security. These challenges would include personal data protection and prevention against cyberbullying, cyber threats, identity theft, scams e.g. e-commerce scams and internet love scams, as well as self-radicalisation of individuals.[1] Recognising these threats and risks, Singapore Police Force (SPF) and the Asia Internet Coalition (AIC) have partnered up to form the Online Industry Safety and Security Watch Group (iSSWG).

2 The formation of the Online iSSWG serves to create a safer and secure online community through the following efforts:

a) Promote greater exchange of information to fight crime and counter the threat of terrorism;
b) Enhance public awareness on steps to take to protect oneself against scams and cyber threats;
c) Encourage the sharing of expertise and best practices to strengthen the security of online platforms; and
d) Support the development of guidelines, frameworks or industry standards to create safe online communities.

PRINCIPAL CONSIDERATIONS

3 This set of guidelines, which is based on the combined expertise of the SPF and leading technology companies under the AIC, outlines the below considerations:

a) Explore strategic and practical challenges and risks associated with increased online activities;
b) Develop a framework for empowering users and businesses to detect and act on potential risks in a timely manner;
c) Encourage good cyber hygiene habits and the cultivation of responsible online behaviours; and
d) Promote the concept of Digital Defence which is the sixth pillar of Total Defence. It requires Singaporeans to be alert, secure and responsible online. This includes practising good cybersecurity habits and guarding against fake news and disinformation.

[1] https://www.straitstimes.com/singapore/singaporean-youth-detained-under-isa-for-planning-knife-attack-on-jews-leaving-synagogue

OBJECTIVES

4 This set of guidelines aims to achieve the following objectives:

a) To provide a broad overview on online safety, personal data protection, and our shared responsibility to minimise cyber-crimes and enhance cyber safety;
b) To provide a broad overview on the common types of online harms, crimes, personal data protection, and the available control measures;
c) To provide guidance in enhancing cyber safety for users; and
d) To share best practices undertaken by various online business owners.

CYBER SAFETY STRATEGY

5 The cyber safety strategy integrates industry best practices to help individuals and organisations manage their online risks. The strategy focuses on three broad pillars of (i) safety, (ii) personal data protection, and (iii) shared responsibility to enhance cyber safety as outlined below.

(i) On the first pillar of **Safety**,[2] it focuses on the following key areas, namely

- Help users avoid exposure to illegal or harmful online content;
- Help users avoid being subjected to harmful online interaction with other users;
- Propagate best practices around acceptable online behaviours that minimise the likelihood of, or causes harm; and
- Help users be aware of hidden costs on online portals.

(ii) On the second pillar of **Personal Data Protection,**[3] it aims to inform users on processes in place when an online platform requests for users' personal data such as:

- Users' consent will be required for the collection, use and disclosure of their personal data for the purpose(s) specified and that the users consider as appropriate;
- Online platform owners to put in place reasonable cybersecurity measures to safeguard users' personal data against hacking, unauthorised or illegal access, collection, usage, modification, disposal or similar risks;
- Online platform owners to ensure that protocols and processes are enforced to cease to retain or delete users' personal data when it is no longer needed for any business or legal purposes;

[2] UK Safer Internet Centre
[3] ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN), "ASEAN Framework on Personal Data Protection".

- Users' personal data is protected at a standard comparable to the protection under the PDPA when transferring the personal data to another country/ territory; and
- Implement appropriate data breaches notification processes and protocols for cases where data breach is of significant scale or is likely to result in significant harm.

(iii) On the third pillar of **Shared responsibility** to minimise cyber-crime and enhance cyber safety,[4] it places emphasis on the following:

- Cooperation, collaboration and sharing of information between public and private stakeholders for matters relating to law enforcement, governance and policies affecting the online community ensures that SPF is plugged in on the latest scam trends. It also allows SPF to strengthen our partnership with private stakeholders to conceptualise and execute scam prevention strategies in a more effective and efficient manner through improved public education and the adoption of technology to tackle emerging scam trends. For instance, involving private stakeholders allow SPF to leverage their communication channels to reach out to more members of public, achieving the mulitplier effect for anti-scam message distribution. One example of this is APPACT, where SPF works closely with its members to identify trending scams, formulate and execute impactful joint anti-scam campaigns and strategies;
- Helping users to understand and adopt best practices such as cyber hygiene for online self-protection aims to cultivate personal responsibility of online users to secure the digital space. This is aligned with SPF's belief that a discerning and well-informed public is the best defence against evolving scam tactics and that members of the community play an important role in the fight against scams. A lack of safe cyber hygiene habits may increase our vulnerability and our risk to scams; and
- Tailoring online safety engagement and awareness for specific user groups, which include young children and the elderly. This is aligned with SPF's view that no single anti-scam campaign or strategy is applicable to the entire demography due to their different needs and understanding of technology. By tailoring our engagement efforts, we aim to enhance our public education outreach efforts so that specfic groups can better understand how cyber hygiene is important in their daily lives, making it more relevant and personal to them. One example of this is the SG Cyber Safe Seniors Programme, a joint collaboration by SPF, CSA and IMDA launched in tandem with CSA's "Better Cyber Safe than Sorry" national cyber-security awareness campaign. This programme aims to raise awareness on cybercrime targeted at senior citizens such as social media

[4] David Wall, "Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace", *Police Practice & Research: An International Journal* 8 no.2 (2007)

impersonation scams, and encourages good adoption of good cyber hygiene practices among seniors.

COMMON TYPES OF ONLINE HARMS

6 Further to the three pillars of cyber safety strategy discussed above, the strategy also aims to address the different types of online harms, which comprise of (non-exhaustive and in no order of prioritisation):

- Scams;
- Violent extremist propaganda;
- Dissemination of voyeuristic materials and intimate images;
- Online harassment;
- Doxxing; and
- Online sexual grooming

MEASURES TO ADDRESS ONLINE HARMS

7 With the varying and continued evolution of online harms, the online community as well as online platforms owners and users are encouraged to adopt the following measures:

(i) Transparency and Accountability

- Online platforms owners are strongly encouraged to publish their community guidelines or standards for moderating contents on their websites for transparency on how they moderate content;
- Provide accessible avenues for online platforms users to report any inappropriate contents that appear to violate the standards set out by the platform's community guidelines or prevailing local laws;
- Online platforms owners are encouraged to:
  - Establish a list of blacklist or suspension accounts arising from suspected or user reported accounts used in scams, information theft or fraud related activities;
  - Create verified accounts and trusted sites for official organisations, and reliable accounts that are easily accessible by online platforms users.
- This illustrates the adoption of internal guidelines on the treatment of harmful and sensitive content such as Twitter code of conduct, Facebook community and page standards. Some examples include:

  - Inbuilt automated detection features for objectionable content and reporting channels for users;
  - Verified accounts for publicly significant individuals and organisations;

- Individual blocking capabilities given to users;
- Flagging and gating content unsuitable for the young;
- Explicit measures against solicitation of online personal information;
- Alert mechanisms for suspicious log-ins and activity;
- Dissemination of cyber hygiene and cyber literacy education materials for users;
- Establishing two-factor authentication (2FA) procedures; and
- Giving greater user control over managing third-party applications accessing online platform data.

(ii) User Empowerment Tools, Self-Regulation and Resources

- Empower online platforms users to control how they share their data. For example, through the use of user empowerment tools such as parental control and restricted search filters;
- Provide readily available materials on good cyber hygiene habits, such as safe browsing practices connecting to a secure network and creating strong passwords or passphrases; and
- Creating awareness among users on online threats such as malware infection, publication of private information (doxxing), and financial scams and fraud.

(iii) Knowledge sharing and publications

- Voluntarily and publicly sharing data on the 'prevalence' of content that violates their policies and sharing of initiatives or actions undertaken to address these issues. Please refer to Appendix 1 for more details on initiatives by various AIC member companies.

CONCLUSION

8 This set of guidelines, which shared on best practices put in place by various industry tech players, serves to complement the Government's ongoing review on the levers to tackle online harms. The set of recommended measures was built on existing measures to create awareness among online platforms users on online threats, both crime and security aspects, and to encourage responsible and safe online behaviours for online platforms owners and users.

Appendix: AIC member companies' initiatives to promote online safety

AIC Member Company	Twitter	Facebook	Google	Grab
Initiatives	**"Read before Retweet"** • Introduced in September 2020 where it encourages users to "read the article before retweeting it". This is to prevent misinformation from spreading through retweeting	**"We Think Digital"** • Flagship digital literacy program launched in March 2019 through the partnership with IMDA, the People's Association and TOUCH Cyber Wellness to conduct workshops for senior citizens on a range of safety topics, from account security, privacy awareness and scams. Facebook also have a Safety Centre portal comprising information on safety policies, tools and resources.	**"Be Internet Awesome"** • Aim is to teach kids the fundamentals of digital citizenship and safety so they can explore the online world with confidence. • Programme includes "The Fundamentals: The Internet Code of Awesome": o Be Internet Smart: Share with Care o Be Internet Alert: Don't Fall for Fake o Be Internet Strong: Secure Your Secrets o Be Internet Kind: It's Cool To Be Kind o Be Internet Brave: When in Doubt, Talk It Out	**"Advisory to educate users"** • Regular scam advisories were issued to users to remind them to stay and reiterate the point that Grab does not ask for personal information and OTP in any of their promotional campaigns or advertisements. With that, Grab warned its users that if they come across any campaigns or advertisements asking them for their personal information, it is a scam.

	“Teaching and Learning with Twitter” Handbook • This handbook aims to help educators equip younger generation with media literacy skills, in turn enabling them to ask the right questions and analyse contents (i.e. news and information) they engage online.	**“Google’s Privacy and Security Virtual Exhibition”** • Educates policymakers, businesses and users about the privacy and security practices across various products in an interactive way		