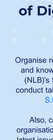
FOSTERING GREATER DIGITAL LITERACY AGAINST TERRORISM

Acts of extremism are often carried out by isolated individuals influenced by online radical content. Businesses can promote and foster a culture of digital literacy in their organisation so that employees are able to discern online content better.



Reinforcing knowledge of Digital Literacy

Share tips with your employees on how to exercise discernment when viewing content online. This can include checking the website's source and cross-verifying information with other trusted websites. You may read our bulletin on combating misinformation and fake news for more information.

Subsequently, you can also conduct assessments to evaluate employees' understanding of digital literacy concepts and discerning abilities.

Fostering a culture of Digital Literacy

Organise regular training for your employees to improve their digital skills and knowledge. You may also reach out to the National Library Board (NLB)'s Source, Understand, Research (S.U.R.E.) team to conduct talks on evolving trends and challenges in online harms such as S.U.R.E. for Work and Generative AI to your workplace.

Also, consider forming a network of Digital Champions within your organisation. They should be knowledgeable about digital literacy and the latest issues on terrorism. By empowering them to be advocates of digital literacy, they can impart relevant knowledge to the rest of your staff and foster a culture of digital literacy.

SPOTLIGHT

> ***Be mindful of what is being circulated and encourage an environment in which the workplace community will know what to watch out for and flag out any potential danger.***
>
> Dr Omer Ali Saifudeen,
> Head (Military Studies Minor)
> and Senior Lecturer of the Public Safety and Security Programme

We had a quick chat with Dr Omer, who presented on current terrorism trends for a SGSecure@Workplaces webinar in May 2023.

Q: Can you share with us more on your research?

A: My research is focused on Countering Violent Extremism and Disinformation. In particular, I have been examining how disinformation tactics are getting more creative and persuasive, and also on the role of AI.

Q: In recent times, we have seen more news on extremist groups utilising digital means to not only conduct attacks, but also propagate extremist narratives. With extremist groups having a greater presence in the digital space, based on your research, how important is digital literacy?

A: The internet and social media are just tools bad actors use to amplify their tactics and persuasive appeal. Ultimately it comes down to one's ability to think critically about any information consumed in order to properly defend against this evolving threat.

HOW we think critically is the more important capacity to nurture. Furthermore, the skills involved in proper critical thinking will need to stay ahead of the tactics by which disinformation and harmful narratives and information flood us.

Digital literacy essentially refers to the ability of someone to safely use any form of electronic communication technology to find, produce and critically analyse and disseminate the digital information they consume. So naturally a big part of this would involve the ability to properly evaluate digital information.

Extremist groups have always been distrustful of who they have in their online communities as they feel they are likely to be infiltrated by spies and law enforcement. This distrust and paranoia might possibly get worse for them too if the whole world is finding it hard to figure out what is real. When this escalates, any social grouping is likely to become more closed up and insular and they are likely to believe only what their group members or leader espouse.

Trust is the new rare commodity to accumulate and not having parochial or polarised worldviews might become harder as the years go by. Hence it is vital to inoculate our youth against these frightening outcomes by nurturing good critical thinking skills early and enhancing these skills to keep up with new technological challenges.

Q: What are some platforms being utilised by extremist groups to conduct attacks and promote extremist narratives that we should be aware of?

A: The first source of disinformation to watch out for are the messages being received over **instant messaging platforms like WhatsApp, Telegram and the whole host of new messaging apps being used these days.** They can be highly disruptive and are the initial means by which any form of divisive hate narratives can gain a foothold in any organisation.

Be mindful of what is being circulated and encourage an environment in which the workplace community will know what to watch out for and flag out any potential dangers. Some of these can be very innocuous, like a humorous video but the slant might be to vilify a particular group or person.

Q: Can you share one tip for workplaces that would like to more effectively promote cyber awareness and digital literacy among their employees?

A: Good cyber awareness and digital literacy among company employees starts in the real world by developing a foundation of trust, good working relationships and encouraging a culture of reporting up any information or narrative (digital or otherwise) that might cause disruptions or promote enmity in the workplace.

There should also be some segment of digital literacy introduced to staff, like in-service training. Such training can inform employees of the latest trends in any form of digital threat, which can range from scams to extremism.

SGSecure@Workplaces Events

SGSecure@Workplaces Webinar: Trends in Terrorism: Navigating our Digital Realms Securely

The SGSecure@Workplaces team held a webinar in May 2023, "Trends in Terrorism: Navigating our Digital Realms Securely", where we had Dr Omer, colleagues from MHA, and Ms Veronica Tan from CSA share on how online spaces are more likely to spread radicalisation, and how businesses can better prepare and protect against the threat of cyber terrorism and cybercrime. Here are some key takeaways:

1. AI chat bots such as ChatGPT are also used by bad actors to craft extremist narratives and for phishing attempts e.g. spear-phishing, which is a targeted and nuanced attempt to steal sensitive information from an individual. You may refer to past SGSecure@Workplaces bulletins on what you can do to be better prepared against various forms of cyber threats such as online scams and electronic data breaches.

2. The speakers also highlighted the risk of data breaches from online activities. For example, around 100,000 ChatGPT accounts and conversations were sold on the Dark Web, raising concerns on its data security.

3. AI chat bot platforms could be prone to Prompt Engineering Attacks. These attacks exploit the behaviour of machine learning models for malicious intent. Thus, businesses should ensure their staff do not key in confidential information into AI chat bots.

Anti-Scam and Harmonious Living event at Cochrane Recreation Centre

From May to July 2023, the SGSecure@Workplaces team partnered with Assurance, Care and Engagement (ACE) Group to engage and sensitise the migrant worker community to the threat of terrorism at various events. More than 1,000 participants participated in activities to learn how to identify fake news and other fraudulent online info at the "Anti-Scam and Harmonious Living" event held at Cochrane Recreation Centre on 18 June 2023.

We hope you have enjoyed reading our refreshed bulletin! From this month onwards, the SGSecure bulletins will feature various SGSecure champions in different fields of expertise, and will be sent out via email once every two months.

Do let us know if you have any feedback by emailing

sgsecure_workplaces@mom.gov.sg

PREPARE YOUR WORKFORCE ✓ PROTECT YOUR WORKPLACE ✓ PARTNER YOUR COMMUNITY

STAY ALERT, STAY UNITED AND STAY STRONG
BE PART OF THE SGSECURE MOVEMENT